UNIVERSITÀ DEGLI STUDI DI CATANIA
DIPARTIMENTO DI GIURISPRUDENZA
DOTTORATO DI RICERCA IN GIURISPRUDENZA
XXXIII CICLO

GIORGIA LO TAURO

VERSO UNA SOVRANITÀ DIGITALE DELL'UNIONE EUROPEA?
L'INCIDENZA DELLA PROTEZIONE DEI DATI PERSONALI SUL PROCESSO DI INTEGRAZIONE EUROPEA

TESI DI DOTTORATO

Tutor: Prof.ssa Adriana Di Stefano
Coordinatrice: Prof.ssa Anna Maria Maugeri

A N N O A C C A D E M I C O 2 0 1 9 / 2 0 2 0

Je n'invente rien, je redécouvre.

Auguste Rodin

INDICE - SOMMARIO

PARTE II

PARTE III

PARTE IV

Introduzione

Il lavoro di ricerca che proponiamo cerca di rispondere alla questione dichiarata sin dal titolo: "Verso una sovranità digitale dell'Unione europea?"

Mantenendo tale interrogativo sullo sfondo, lo sviluppo dell'intera analisi indagherà le dinamiche e gli intenti che dirigono l'andamento dell'Unione europea nella dimensione digitale, da cui deriverà che, se da un alto una tendenza verso la sovranità digitale può dirsi già confermata, dall'altro essa pare ancora incompiuta.

La curiosità rispetto al nuovo tema della "sovranità digitale", sui cui controversi contenuti avremo modo di soffermarci, è sorta, invero, partendo da vecchie (e imperiture) questioni: quelle che implicano la natura dell'Unione europea, le peculiarità del suo ordinamento nel contesto internazionale, le "spinte" che hanno modellato e continuano a plasmare il processo di integrazione europea. Tali vecchie questioni hanno ridestato interesse proprio per le recenti crisi (da quella finanziaria a quella migratoria, sino a quella dei valori fondanti, minacciati in alcuni Stati membri, nonché, da ultimo, quella pandemica) che stanno mettendo ancora una volta in discussione la legittimazione dell'Unione europea. Ebbene, tentando di rintracciare plausibili soluzioni alle ultime crisi di legittimazione (a partire, in particolare, da quella dei valori) siamo arrivati alla dimensione digitale. Tale dimensione, infatti, si è mostrata terreno fertile di indagine, poiché in essa pare che l'Unione europea stia riuscendo ad avere un ruolo di spicco tramite (ancora) l'utilizzo del diritto come "potere" e la tutela dei diritti fondamentali come sigillo del suo operato.

A partire da ciò, quindi, ha preso avvio la seguente domanda di ricerca: se la tendenza verso una sovranità digitale possa costituire per l'Unione europea un valido tentativo di superare almeno alcune delle questioni di legittimazione che le recenti crisi sembrerebbero aver sollevato. Se, cioè, una eventuale compiuta sovranità digitale possa fungere da motivo di (nuova) legittimazione dell'Unione.

Per rispondere a questa domanda, dopo aver definito le peculiarità del sistema sovranazionale, con particolare attenzione ai suoi valori, e dunque rintracciandole, in ultima analisi, in ciò che chiameremo *EU rule of law*, proveremo ad indagarne il nesso con il caso di studio prescelto, ossia il diritto alla protezione dei dati personali (nelle sue varie accezioni). Gli interventi dell'Unione europea rispetto alla protezione dei dati personali appaiono, infatti, e più che in altri settori rilevanti

nella dimensione digitale, particolarmente emblematici delle caratteristiche della *EU rule of law*. Pertanto, cercheremo di rintracciare i momenti di sintesi tra questi due poli, sia esaminandone le prospettazioni teoriche, sia setacciando la copiosa prassi e giurisprudenza dedicata.

Da quei risultati, dovremo essere in grado di valutare se, allo stato attuale, sia possibile riscontrare già alcuni indizi di "sovranità digitale dell'Unione europea" e, in caso affermativo, se essi risultino adeguati a superare alcune critiche alla legittimazione dell'ente. L'analisi rivelerà diverse conferme in tal senso, ma anche non poche carenze e qualche incoerenza nell'operato dell'Unione che parrebbero mantenere aperta la questione e giustificare rinnovate perplessità, che l'attuale crisi pandemica avrebbe palesato. Nondimeno, proprio da questi eventi stanno derivando forti stimoli nella dimensione digitale, risultando sempre più diffusa la consapevolezza sui punti deboli da cui avviare un ripensamento dell'azione dell'Unione.

Il lavoro che segue rappresenta, quindi, il tentativo di offrire un ulteriore contributo alle riflessioni sulle prospettive che si aprono per l'Unione europea nella dimensione digitale, che si rivela già dirimente per gli sviluppi più generali del processo di integrazione europea.

PARTE I

Non la realtà
si deve – dal giurista –
subordinare al concetto,
ma questo a quella.

S. Romano, L'ordinamento giuridico

PARTE I

SOMMARIO: I. Oggetto e obiettivi di ricerca. – 1. Domanda di ricerca, piano dell'opera e metodologia. – 2. Definire la "sovranità digitale". – 3. Alla base della questione: solita vecchia "*legitimacy crisis*"? – II. *La spinta dello spazio sulla forma*. – 1. Spunti di teoria delle relazioni internazionali sul processo di integrazione europea. – 2. *Segue*. Due imprescindibili diramazioni – 2.1. Spunti sulle teorie dell'integrazione europea. – 2.2. Sovranità e diritto internazionale. – III. *La forma* dell'Unione europea: di "sovranità condivisa" e potere da separare. – 1. L'ordinamento giuridico. – 2. Rapporto tra sovranità e potere nell'Unione europea. – IV. Dei valori e delle peculiarità dell'Unione europea: la *EU rule of law*. – 1. Il sistema di valori su cui l'Unione si fonda: perno interno e proiezione esterna. – 2. Farsi un'idea sul concetto di "*EU rule of law*".

CAPITOLO I
OGGETTO E OBIETTIVI DELLA RICERCA

1. Domanda di ricerca, piano dell'opera e metodologia

« *Si l'on s'occupe de ce qui est plein, c'est-à-dire de l'objet comme forme positive, l'espace environnant est réduit à presque rien. Si l'on s'occupe surtout de l'espace qui entoure l'objet, l'objet est réduit à presque rien. Qu'est-ce qui est le plus intéressant ? Ce qui est à l'intérieur ou c'est qui est à l'extérieur de la forme ? Quand on regarde des pommes de Cézanne, on voit qu'il n'a pas vraiment peint des pommes en tant que telles. Ce qu'il a fait, c'est peindre terriblement bien le poids de l'espace sur cette forme ronde. […] C'est la poussée de l'espace sur la forme qui compte* »[1].

Sono i concetti esposti in una didascalia (dal titolo "il vuoto e il pieno"), che accompagnava l'opera di una mostra su *"spazio e vuoto"* di Picasso e Calder, che hanno ispirato questa ricerca, in un marzo parigino.

Proveremo ad utilizzarli per condurre uno studio sul diritto alla protezione dei dati personali come caso privilegiato da cui ricavare prospettive sull'assetto attuale dell'ordine giuridico dell'Unione europea, quale sistema sovranazionale che sempre più fortemente caratterizzato nel contesto internazionale, alla luce di dinamiche che ne modellano la "forma" e ne ridisegnano gli obiettivi.

[1] F. GILOT, C. LAKE, *Vivre avec Picasso*, Paris-Calmann Lévy, 1965.

Ciò al fine di mostrare come, proprio tenendo conto di tali dinamiche, la dimensione digitale, e in particolare il settore della protezione dei dati personali, più di altri campi di intervento, stia offrendo all'Unione europea, corredata dal suo assetto valoriale, l'occasione di affermarsi come attore globale sia nella dimensione interna che, lo si vedrà, nella sua proiezione verso l'esterno. E questo, peraltro, tanto in una prospettiva *de iure condito,* considerando più recenti interventi normativi in materia, quanto in una prospettiva *de iure condendo,* monitorando in particolare l'ingente contributo propulsivo della Corte di giustizia e la recente prassi delle altre istituzioni.

La domanda di ricerca può dunque individuarsi come segue: la dimensione digitale, quale spazio nuovo e da ordinare, potrebbe fornire all'Unione le condizioni per superare alcune criticità che si ripropongono rispetto alla sua legittimazione? Dunque, la tendenza dell'Unione verso una sovranità digitale, caratterizzata dalla fedeltà ai suoi valori ma anche dalla necessità di saper gestire i suoi interessi in quella dimensione, suggerisce una propensione dell'ente in tal senso?

Insomma: ci chiediamo se, alla luce dell'analisi che condurremo, sia possibile ravvisare nella propensione alla sovranità digitale dell'Unione europea una possibile (nuova) fonte di legittimazione, capace di superare almeno alcune delle criticità ultimamente emerse sotto diversi profili, e sino a che punto tale tendenza possa dirsi realizzata ovvero risulti ancora incompiuta.

Ponendo l'accento sul sistema di valori cui l'Unione si fonda, come carattere distintivo dell'ente, ci concentreremo in particolare sull'aspetto che combina quel sistema in uno con principi e peculiarità propri di quell'ordinamento, cercando di decifrarne le diverse declinazioni e implicazioni: ci riferiamo alla nozione di "*EU rule of law*", nella sua centralità assunta in tempi recenti. Ciò assumerà rilievo, tanto nella dimensione interna dell'integrazione europea che nella proiezione esterna dell'azione dell'Unione, rispetto al nesso con il caso di studio preso in considerazione, ossia il diritto alla protezione dei dati personali, che più di altri consente di dimostrare il peculiare atteggiamento dell'Unione nella dimensione digitale.

Pertanto, questa Parte I si occuperà di chiarire gli elementi che compongono tipicamente la *EU rule of law*, a partire dalla particolarissima natura dell'ordinamento giuridico dell'Unione. Quindi, seguirà nella Parte II un indispensabile prospetto del diritto europeo alla protezione dei dati personali.

Le Parti successive cercheranno, così, di mostrare le peculiarità della sintesi tra i due elementi nella dimensione digitale, con un'analisi concentrata prima prevalentemente sui supporti teorici di tale sintesi (Parte III) e, poi, sui possibili riscontri in pratica (Parte IV).

Tutto questo, assumendo a premessa metodologica l'angolo visuale suggerito da Picasso: pensando alla natura morta di Cézanne, egli coglie essenzialmente la capacità dell'artista di rivelare, dipingendo, "il peso dello spazio sulla forma rotonda" delle mele.

È la spinta dello spazio sulla forma che conta.

Questo, dunque il *leitmotiv* dell'analisi (la spinta dello spazio sulla forma) che ne orienterà la trattazione, rivelandone anche ciò che chiameremo "*moto opposto*".

Infatti, se obiettivo della ricerca è tentare di comprendere la direzione che l'Unione sta assumendo e le aspirazioni che la posizioneranno a livello globale nel prossimo futuro (in particolare nella dimensione digitale, e dunque con un *focus* sulla protezione dei dati personali), ci sembra particolarmente utile procedere alla rilettura del suo passato e alla comprensione del modo in cui la "forma" dell'integrazione sovranazionale ha subito sviluppi e mutamenti. Riflessioni del genere suggeriscono una prospettiva di analisi che, pur considerato il carattere "autoreferenziale" dell'ordinamento dell'Unione nel quadro delle dinamiche interne[2], prenda in considerazione (anche) la circostanza che l'Unione, ente *sui generis*, deve parimenti la sua forma (e, va da sé, le perplessità che attualmente la rendono sibillina) alla "spinta dello spazio" esterno su di essa.

Un'analisi concentrata solo sugli interventi nella prospettiva sovranazionale di un ente che agisce tramite e verso gli Stati membri, pur imprescindibili per una comprensione del fenomeno (e che si cercherà di non sottovalutare nel prosieguo della trattazione), potrebbe infatti presentare dei limiti. Prediligere un metodo che guarda alla forma anche come esito delle "spinte dello spazio" significa invece, applicato al caso dell'Unione europea, prendere in considerazione (pur senza pretese di esaustività) anche le principali pulsioni esterne, quelle che nel tempo l'hanno forgiata e quelle che oggi la stimolano a definire la sua presenza sul piano internazionale. La dimensione digitale pare, infatti, particolarmente rivelatrice di queste dinamiche.

Si cercherà, dunque, di proporre *una lettura che parta dall'esterno verso l'interno*, per poi assumere così le ulteriori e spontanee dinamiche *opposte* che dall'interno influenzano l'esterno, e così di nuovo, *viceversa*, svelando la situazione attuale in cui tali dinamiche si combinano nel *moto perpetuo* del processo di integrazione europea.

Questo si traduce, in termini internazionalistici, nell'avviare l'analisi sommaria sull'evoluzione sistemica dell'Unione da riflessioni di teoria delle relazioni internazionali e, in particolare, con

[2] Da alcuni definito dunque "*Autopoietic Law*" come ci ricorda WEILER J.H.H., The Transformation of Europe, in *The Yale Law Journal*, Vol. 100, 1991, pp. 2409-2410. Così anche, non condividendo, MACCORMICK N., The Maastricht-Urteil: Sovereignty now, *European Law Journal*, 1(2), 1995: «*The self-referential, or partially self-referential, character of a legal system has been associated in recent work by Luhmann, Teubner, and others of their school with the idea of 'autopoiesis', the idea of the system as self-generating and regenerating, transforming information received into the system's own terms before absorbing it. This seems somewhat exaggerated, though the idea is suggestive*», p. 262.

riguardo a quegli studi che ne hanno proposto l'applicazione al processo di integrazione europea. Da lì, sarà dovuto il richiamo agli studi sull'integrazione europea che hanno cercato più da vicino di cogliere quell'evoluzione, per giungere così al solco della rimessa a tema del concetto di "sovranità" (statale, ma trasponibile anche a livello unionale?) nel diritto internazionale.

Prima di avviare così l'analisi, tuttavia, si ritiene essenziale anzitutto dare conto dei due elementi che costituiscono il nocciolo duro della questione, fulcro della domanda di ricerca e dunque vero oggetto di indagine: la nozione di "sovranità digitale" dell'Unione europea; la questione di legittimazione che si (ri)propone rispetto all'Unione europea.

Quanto al primo, diremo subito, delle recenti e non del tutto univoche proposte di definizione della formula "sovranità digitale", nonché della sua particolare applicazione all'Unione europea, che è sempre più usata ultimamente in diversi ambiti, ma pare ancora non godere di un preciso contenuto.

Quindi, procederemo ad affrontare il secondo elemento, illustrando per sommi capi e ai fini precipui del nostro lavoro gli aspetti essenziali della dibattuta crisi di legittimazione che connoterebbe (non solo, ma anche e ancora) l'attuale momento del processo di integrazione europea, e che, per la complessità delle cause e la portata delle conseguenze, pare quasi essere divenuta una caratteristica ontologica dello stesso.

2. Definire la "sovranità digitale"

Se è vero che negli ultimi anni i discorsi sulla sovranità, in generale, sono tornati d'interesse[3], in particolare quelli sulla sovranità digitale si sono fatti sempre più numerosi, attribuendo a tale formula significati molto variegati, anche perché utilizzati in diversi ambiti (*lato sensu* giuridico, politico-istituzionale e finanche mediatico). Rinviando al prosieguo della trattazione per la rinnovata attenzione sulla sovranità, in generale, e sul suo rilievo nel diritto internazionale (*infra*, Capitolo II), cercheremo qui di esporre alcune proposte sul significato di "sovranità digitale", come utili premesse che verranno poi riprese e argomentate alla fine dell'intera analisi (*infra*, Capitolo IV, Parte IV).

[3] Discorsi che sono stati ripensati anche rispetto a "nuove forme" di sovranità, di cui quella digitale rappresenterebbe un'espressione, come rilevano R. BIFULCO, A. NATO, The concept of sovereignty in the EU – past, present and the future, in Reconnect – Europe, 2020, in particolare p. 86: «*Thus, in this global perspective, sovereignty cannot be considered as having been abolished. The possible presence of outside threats to the European context, and new forms of sovereignty – think of the so-called digital sovereignty (GUEHAM, 2017) – could even challenge the very existence of individual Member States. This could spark a push toward greater integration and federal-type solutions*».

Anzitutto, segnaliamo tra i primi lavori sulla "sovranità digitale" in generale quello di Bellanger che, da un'analisi della sovranità attualizzata, derivava: «*La souveraineté numérique est la maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques*»[4].

Anche a partire da queste premesse, alcuni anni dopo Gueham poneva l'accento sul fatto che «*The quest for digital sovereignty is therefore a goal shared by companies, public authority stakeholders and, more recently, Internet users, citizens and consumers (…). The balance of power between governments, citizens, companies and consumers is forging a new Internet of sovereignties, a new space whose rules remain to be defined. Several 'circles' of sovereignty are pitted against one another in this environment. The first concerns personal data (…). The second circle concerns the sovereignty of companies and organisations through data (…). The third and final circle concerns the sovereignty of States who, faced with the giants of the web, are only able to influence the debate on data protection within regional entities such as the European Union, whose position and protection mechanisms are being increasingly asserted against American hegemony*»[5]. Dunque, l'ambizione alla sovranità digitale, nell'era della rivoluzione tecnologica, sarebbe ravvisabile non solo nei soggetti "classicamente" sovrani, ossia gli Stati, e la necessità di questi ultimi di fronteggiare le sfide di tale nuova era imporrebbe agli stessi, nel contesto regionale europeo, di agire in modo concertato a livello sovranazionale per riuscire ad avere un effettivo margine di influenza rispetto alle altre "sovranità emergenti". Nondimeno, è proprio in questo "*nuovo spazio in cui le regole restano ancora da definire*" che noi vorremmo collocare l'intervento risolutivo dell'Unione europea, come cercheremo di fare emergere dall'intera analisi proposta in questo lavoro.

Per il momento, questi spunti sono sufficienti per passare a rintracciare i termini della sovranità digitale con specifico riguardo all'Unione europea, sempre a partire da definizioni proposte da altri.

Va intanto ricordato che rispetto all'Unione il termine sarebbe stato coniato per la prima volta con riguardo al programma satellitare Galileo, vent'anni or sono, come ci fa notare la studiosa Hobbs: «All'epoca, il commissario europeo Loyola de Palacio dichiarò che il programma Galileo avrebbe permesso all'Europa di "*mantenere la sua autonomia, la sua sovranità, la sua capacità tecnologica e il controllo delle sue conoscenz*e". Si tratta del primo esempio di un collegamento strategico tra

[4] P. BELLANGER, De la souveraineté en général et de la souveraineté numérique en particulier, in *Les Echos*, 30.08.2011, disponibile qui: http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm .
Per un lavoro più compiuto, si segnala anche ID., *La souveraineté numérique*, Stock, 2014.
[5] F. GUEHAM, Digital Sovereignty – Steps towards a new system of Internet Governance, *Fondation pour l'innovation politique*, January 2017, pp. 9 e 11.

tecnologia e sovranità nella politica dell'UE»[6]. Ciò assume rilievo nell'ottica di intendere il concetto di sovranità digitale, comunque, sempre legato a un mutamento di paradigma spaziale, e quindi a un *luogo nuovo* in cui l'Unione europea può trovare una *propria* sovranità.

Studi dell'*European Council on Foreign Relations* partivano poi dalla sovranità digitale, a cui ambirebbero tutti gli Stati, definendola come la loro "*ability to control the new digital technologies and their societal effects*", per poi passare così a valutazioni, essenzialmente di geopolitica, sul ruolo dell'Unione europea: «*For European policymakers, the idea of digital sovereignty is part of a larger struggle that they face to maintain their capacity to act and to protect their citizens in a world of increased geopolitical competition. On a host of issues (…), it appears that the European Union has never been as sovereign as it thought. A time of fiercer geopolitical competition, and an America more focused on its narrow interests, have exposed the EU's lack of independence in new ways –not least in the digital realm. It is now clear that, if Europeans want to reap the economic benefits of emerging digital technologies, ensure their politics remain free from divisive disinformation, and decide who can know their most personal information, they will have to protect their digital sovereignty and compete with other geopolitical actors in the digital realm*»[7]. In quest'ottica e con questo specifico taglio, l'ECFR proponeva quindi il concetto di "sovranità strategica" che potrebbe agevolare l'Unione nella nuova era di competizione geopolitica[8], cosa su cui si insiste parecchio ultimamente[9].

Dal punto di vista più prettamente accademico, il recentissimo lavoro di Celeste pare molto pertinente alla nostra ricerca, che vuole incardinare questi discorsi nelle peculiarità della *EU rule of law*. L'autore, infatti, partendo dalla sovranità digitale come "*a core value inspiring recent policy in the EU*", ne ricostruiva i passaggi, dall'evoluzione storica del concetto di sovranità alla sua

[6] C. HOBBS, L'Europa alla ricerca di una sovranità digitale: sfide e interessi in gioco, in *Agenda Digitale*, 8 ottobre 2020, enfasi aggiunta.

[7] C. HOBBS (ed.), Europe's Digital Sovereignty: from rulemaker to superpower in the afe of US-China rivalry, in European Council on Foreign Relations – Essay Collection, July 2020, p. 7.

[8] Ibidem, in cui veniva data la seguente definizione di "*strategic sovereignty*": «*Strategic sovereignty implies that the EU and its member states need to preserve for themselves the capacity to act in the world, even as they remain deeply interdependent. Promoting European digital sovereignty is a critical piece of this effort. The purpose of this volume is to aid in that effort by helping readers understand better the challenges and opportunities that digital technologies, and the geopolitical competition over them, poses for Europe and its member states*».

[9] In questo senso può richiamarsi tra tutti, per esempio, quanto riepilogato di recente da G.M. RUOTOLO per spiegare la "sovranità digitale", in considerazione degli orientamenti politici e strategici sovranazionali al riguardo (il riferimento è, per esempio, all'European Political Strategy Centre, Rethinking Strategic Autonomy in the Digital Age, Issue 30, 18 July 2019; ma anche all'EPRS Ideas Paper, Digital Sovereignty for Europe, luglio 2020). L'A. spiega il concetto come la «capacità dell'Unione (e dei suoi Stati membri) di agire in modo indipendente nel mondo digitale con strumenti sia difensivi sia offensivi, per promuovere l'innovazione digitale e proteggersi, al contempo, dall'influenza economica e sociale di imprese tecnologiche extra-UE che, secondo alcuni, starebbero mettendo in pericolo il controllo dei cittadini europei sui loro dati personali, nonché limitando la crescita delle imprese hi-tech europee e addirittura la capacità dei legislatori nazionali e dell'UE di garantire l'enforcement delle proprie normative», in *Scritti di diritto internazionale ed europeo dei dati*, Cacucci editore, 2021, p. 262. Dello stesso tenore, ID., Digital Services Act e Digital Markets Act tra responsabilità dei fornitori e rischi di ne bis in idem, in *SIDIblog*, 29 marzo 2021.

contestualizzazione nell'ecosistema digitale, per addivenire alla seguente risoluzione: «*Digital sovereignty denotes a form of control over digital assets, which can be material and immaterial entities, thus potentially ' located ' in a space that transcends physical boundaries. Moreover, digital sovereignty is not only a prerogative of states, but also of private ' organisations ' that are vested with this power. (...) although the element of ' control ' is still rooted in the concept of digital sovereignty, particular emphasis is placed on the ability to be ' independent ' from external interference*»[10]. Da queste considerazioni, in linea con le altre sopra esposte, l'autore guardava specificamente all'Unione europea, rilevando che le rivendicazioni in termini di sovranità digitale in Europa avrebbero iniziato a prendere piede come reazione alla preponderanza delle compagnie tecnologiche straniere[11], per poi concludere: «*the main rationale behind digital sovereignty claims in the EU lies in the desire to preserve European core values, rights and principles. By invoking control over personal data and digital infrastructures, the EU is seeking to maintain its fundamental values of respect for democracy and human rights unaltered in the face of the challenges of the global digital society*»[12]. Simili valutazioni, come vedremo, tornano spesso nei discorsi sulla sovranità digitale.

Ancora, il recente studio dell'Atlantic Council appare interessante laddove fornisce la misura delle ultime *spinte esterne* e della loro incidenza nella emersione di un'esigenza di sovranità digitale dell'Unione europea, che parrebbe in linea con la metodologia che abbiamo dichiarato di adottare nel condurre il nostro lavoro: «*The current European focus on digital sovereignty has its roots in a much broader discussion about Europe's ability to protect its citizens from an increasingly hostile and challenging world. The financial crisis of 2009–2012, followed by Russian aggression in Ukraine in 2015 and the migration crisis later that same year, led to an awareness of the deterioration in the European Union's external circumstances. The return of geopolitics prompted a review of Europe's strategic position and, at least within EU institutions, gave rise to a belief that Europe should seek greater "strategic autonomy," strengthening its capacity to act externally on its own, especially in the defense realm*»[13]. Questi discorsi, nell'ottica della metodologia che adotteremo e dei risultati dell'analisi teorica e pratica, ci danno sin da ora l'idea dell'ulteriore

[10] E. CELESTE, Digital Sovereignty in the EU: Challenges and Future Perspectives, in F. FABBRINI, E. CELESTE, J. QUINN (Eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford: Hart Publishing, 2020, pp. 217-218.

[11] Ibidem, p. 218: «*the market for digital products and services is dominated by American and Chinese multinational corporations. Multiple risks are identified in the European inability to fully control its data and digital infrastructures. Regaining sovereignty of its portion of the digital ecosystem is seen in the EU as a potential solution to preserve its unique DNA of rights and values*». In tal senso, ciò rievocherebbe le suddette considerazioni esposte anche da G.M. RUOTOLO, *op. cit*., sulla sovranità digitale dell'Unione europea.

[12] E. CELESTE, Digital Sovereignty in the EU, *cit*., p. 220, sottolineato aggiunto.

[13] F. G. BURWELL, K. PROPP, The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?, *Atlantic Council – Issue Brief*, June 2020, p. 3, sottolineato aggiunto.

modellamento (dall'esterno) della "forma" del processo di integrazione e della sua rilevanza nella dimensione digitale.

Quanto al versante più prettamente politico, tralasciando pur valevoli interventi di esponenti statali, segnaliamo intanto che già nel novembre 2019 l'allora Commissario designato al Mercato Interno Thierry Breton durante la sua audizione al Parlamento europeo parlava proprio di "*Industrial and technological sovereignty*"[14], che diventerà centrale nella Strategia della Commissione, di cui diremo, sul *futuro digitale dell'Unione europea*. Divenuto Commissario, Breton fece di tali concetti il suo faro, ribadendoli più volte e sotto diversi profili di intervento, peraltro ricavabili dalle dichiarazioni del settembre 2020: «*Europe has made the historic choice of solidarity to face the crisis and finance recovery and reconstruction. While the pandemic has revealed our dependence on products, critical materials and certain value chains, Europe must now take its strategic interests into its own hands in order to ensure sovereignty, which has become a common necessity. In a world where the balance of power between blocs is hardening, the race for autonomy and power is in full swing. Faced with the "technological war" being waged by the United States and China, Europe must now lay the foundations of its sovereignty for the next 20 years*»[15].

Quindi, anche dal Servizio di Ricerca del Parlamento europeo emergeva in quel periodo l'attenzione verso analoghe questioni: è del luglio 2020 il *EPRS Ideas Paper* dedicato a "*Digital Sovereignty for Europe*" che, prendendo atto delle crescenti preoccupazioni circa la possibile perdita di controllo sui dati e la capacità di innovazione in Europa, incoraggiava l'approccio volto all'autonomia strategica dell'Unione nel settore digitale[16].

Così, ancora, il Consiglio europeo conveniva nelle sue conclusioni dell'ottobre 2020: «*To be digitally sovereign, the EU must build a truly digital single market, reinforce its ability to define its own rules, to make autonomous technological choices, and to develop and deploy strategic digital capacities and infrastructure. At the international level, the EU will leverage its tools and regulatory powers to help shape global rules and standards. The EU will remain open to all*

[14] Hearing of Commissioner-designate Thierry Breton, 14.11.2019, available here: https://www.europarl.europa.eu/news/it/press-room/20191112IPR66319/hearing-of-commissioner-designate-thierry-breton . Il video dell'audizione completa è consultabile qui: https://multimedia.europarl.europa.eu/en/hearing-of-thierry-breton-commissioner-designate-internal-market-opening-statement-by-thierry-breton_I180276-V_v .

[15] European Commission, Europe: Keys to sovereignty, presse release, 11.09.2020, available here: https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en ,in cui continua: «*It is not a question of giving in to the temptation of isolation or withdrawal into oneself, which is contrary to our interests, our values and our culture. It is a question of making choices that will be decisive for the future of our fellow citizens by developing European technologies and alternatives, without which there can be neither autonomy nor sovereignty. Mobilised around major projects developed in partnership, Europe has demonstrated in the past that it has the capacity to play a leading role on the world stage. The time has come to take back the common initiative*».

[16] European Parliamentary Research Service, EPRS Ideas Paper | Towards a more resilient EU, *Digital sovereignty for Europe*, July 2020, pp.1-12.

companies complying with European rules and standards. Digital development must safeguard our values, fundamental rights and security, and be socially balanced. Such a human-centred approach will increase the attractiveness of the European model»[17]. Il cd. *approccio antropocentrico* alla dimensione digitale costituisce l'aspetto fondamentale nella promozione del modello europeo.

Sull'approccio antropocentrico ha insistito infatti, di recente, la Commissione europea nella sua Comunicazione *Bussola per il digitale 2030,* dove si legge: «*la nostra ambizione dichiarata è più che mai pertinente: perseguire politiche per il digitale che conferiscano ai cittadini e alle imprese l'autonomia e la responsabilità necessarie per conseguire un futuro digitale antropocentrico, sostenibile e più prospero (...). Così facendo l'Europa potrà conseguire la sovranità digitale (...)*»[18].

Da quanto brevemente riportato, si potrebbero dunque dedurre due aspetti della propensione verso una "sovranità digitale dell'Unione europea", che Christakis ha utilmente messo in luce e che terremo presenti nel corso della trattazione: quello che enfatizza il *potere normativo/regolatorio* dell'Unione nella dimensione digitale; quello che punta alla sua *autonomia strategica* in quella stessa dimensione[19]. Dagli ultimi interventi delle istituzioni parrebbe, inoltre, che entrambi questi aspetti confluiscano nell'*approccio antropocentrico* che l'Unione vuole adottare per promuovere il modello europeo nella dimensione digitale. Questo, dunque, va considerato sin da ora il nucleo centrale intorno a cui svilupperemo l'intera analisi, sul quale torneremo oltre, solo alla luce dei risultati finali d'indagine (in particolare, *infra*, Capitolo IV, Parte IV).

Riteniamo, così, di avere gli elementi minimi ma sufficienti per una necessaria, quanto generica, introduzione a uno degli elementi oggetto della nostra indagine, che risulterà più chiaro via via che l'analisi sui vari altri aspetti verrà approfondita. Occorre ora, dunque, presentare, sempre nei limiti

[17] European Council, Special meeting – 1 and 2 October 2020, Conclusions, EUCO 13/20, p. 7, available here: https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf .
Queste Conclusioni del Consiglio europeo sembrano contenere i più rilevanti elementi "costitutivi" della sovranità digitale. Uno, tra questi, rievoca la conversazione intrattenuta con il Prof. Hoffman (cfr. meglio, Parte IV) che, a seguito di valutazioni più generali a partire dalla saga Schrems, insisteva sulla caratteristica abilità dell'Unione di consentire (non vietare) gli interessi commerciali esterni nel suo mercato, in uno con la capacità di regolarli, e ciò considerando quegli operatori come attivi sempre nel mercato interno, con le garanzie e le opportunità che quello appresta, ma anche con i suoi limiti.

[18] COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI Bussola per il digitale 2030: il modello europeo per il decennio digitale COM/2021/118 final.

[19] T CHRISTAKIS, 'European Digital Sovereignty': Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy', *Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute*, e-book, December 2020, *Executive Summary – i*: «*sovereignty as regulatory power; and, sovereignty as strategic autonomy and the ability to act in the digital sphere without being restricted to an undesired extent by external dependencies*».

dell'economia del nostro lavoro, l'altro elemento oggetto di indagine, che, insieme con il primo, delimita la domanda di ricerca: quello relativo alle questioni di legittimazione.

2. Alla base della questione: solita vecchia "*legitimacy crisis*"?

Qualsiasi studio che intercetti aspetti sistemici di diritto dell'Unione europea non può non scontrarsi, oggi più che mai, con la questione relativa alla "crisi di legittimazione" dell'ordinamento sovranazionale.

La questione sorge dal riconoscimento (di cui si parlerà più adeguatamente) di un *potere* in capo all'Unione europea che, come tale – nelle sue diverse dimensioni –, deve trovare una legittimazione, e di cui spesso è dibattuta l'origine[20]. Interrogarsi sulla legittimazione dell'Unione europea come ordinamento giuridico ed entità politica significa chiedersi, dunque, "perché l'Unione"[21]. Il periodico riproporsi della questione pare ontologicamente legato ad un "processo di integrazione" – ossia un fenomeno per sua stessa natura *in fieri* – che emerge tutte le volte in cui esso, spinto da fattori esogeni ed endogeni, avanza nella sua evoluzione e così affronta delle crisi (intese nel senso etimologico – dal greco *κρίσις* – di scelta, fase decisiva) che ripropongono le domande sul ruolo e sul futuro dell'Unione[22]. Risulta quindi chiaro che la questione si sia posta per la prima volta in modo eclatante nel periodo che accompagnava la ratifica del Trattato di Maastricht e in quello che lo ha immediatamente seguito[23], ossia in quella fase in cui, caduto il muro Berlino e con esso ingombranti e gravi ostacoli di politica internazionale, l'irenico proposito del costrutto

[20] Sullo specifico pare utile segnalare, *ex multis*, S. DELLAVALLE, Il potere dell'Unione europea, in *Teoria politica. Nuova Serie*, Annali VI, 2016, pp. 193-223, che, a proposito dell'origine della legittimità del potere dell'UE, ci ricorda come punto di partenza: «solo se la matrice da cui nasce la pretesa di esigere da altri un determinato comportamento è individuata come *equa*, l'*autorità* che prescrive tali comportamenti verrà *accettata*» (*cors.agg.*), p. 193.
Molto spesso, come si vedrà, la questione di legittimità si ri(con)duce al suo carattere democratico, e al correlativo deficit che connoterebbe l'Unione. Cfr. B. GUY PETERS, J. PIERRE, Governance Approaches, in A. WIENER, T. DIEZ (Eds), *European Integration Theory – Second edition*, Oxford University Press, 2009, p. 96: «*As any relatively new political entity must, and indeed as well-established political enti· ties must, the European Union must legitimate Itself. The legitimization of any political system may be problematic, but the EU faces more challenges than most in ensuring a position for itself in the governance of its constituent parts. One of the crucial legitimization challenges is the (in)famous democratic deficit (…). That is, while operating in societies that are accustomed to institutionalized forms of democratic governing, the EU is often described as lacking effective democracy*».
[21] La questione è stata affrontata proprio in questi termini da L. KÜHNHARDT, *European Union – The Second Founding. The Changing Rationale of European Integration*, Nomos, 2008.
[22] P. CRAIG a proposito ci ricorda: «*Exogenous shocks external to the EU, which are unforeseen and unforeseeable, can shatter the very best reasoned predictions. Endogenous change from within the EU can, in similar vein, disrupt future visions that would otherwise be plausibly grounded, as attested to by the Catalonia problem in Spain, and electoral change in the Czech Republic, Austria and Italy*», in The EU, democracy and institutional structure: Past, present and future, in W. HEUSEL, J-P REGEADE (Eds), *The Authority of EU Law – Do we still believe in it?*, Springer, 2019, p. 314.
[23] Cfr. G. DE BURCA, The Quest for Legitimacy in the European Union, in *The Modern Law Review*, 59:3, 1996, p. 349 ss.

comunitario pareva trovare piena realizzazione e, così, necessitare di nuove o rivedute giustificazioni per il suo mantenimento e/o la sua ristrutturazione.

Oggi, la questione che si pone riguarda la crisi del progetto europeo in quanto tale – nella sua dimensione economica, ma anche istituzionale e politica[24] – causata dalle sfide "senza precedenti, sia globali che nazionali" che sta affrontando[25]; ciò impone di ripensarne il sistema valoriale e gli obiettivi: «*the crisis of the European project is fundamentally a crisis of values and a crisis of purpose, but also a crisis of results*»[26].

Senza voler scomodare analisi relative ai più ampi interrogativi sulla legittimazione del potere, che hanno assunto particolare rilevanza a partire dagli anni Settanta[27], o sulla loro portata nel diritto internazionale[28], si farà più modestamente riferimento alla questione della crisi che ha interessato l'Unione e che la riguarda nuovamente, utilizzando categorie e argomentazioni che gli studiosi appositamente dedicati al tema hanno definito per la specifica esperienza sovranazionale. Esclusa ogni pretesa di esaustività, il riferimento si ritiene comunque un'interessante premessa per delineare quella che poi chiameremo la "forma" dell'Unione europea e che quindi riprenderà in maniera più ragionata e completerà i concetti che qui funzionalmente si presentano, una volta rintracciatene le spinte esterne soprattutto iniziali. In particolare, una definizione abbastanza lucida del fenomeno ci pare quella effettuata (nel corso di diversi anni, ma visionaria sin dagli esordi) dal professor Weiler, a cui faremo pertanto costante riferimento.

Come si accennava, la questione emerse in particolare nelle more delle Conferenze Intergovernative del 1991 che portarono al Trattato di Maastricht e che discutevano, rispettivamente, dell'Unione economica e monetaria e dell'Unione politica, come decise nei vertici del Consiglio europeo del 1990[29]. Il dibattito, fomentatosi sulla scia della reazione popolare al Trattato, si sarebbe addirittura intensificato negli anni immediatamente successivi[30], ponendosi in termini di "crisi di legittimazione", oggetto di attenzione anche nella successiva Conferenza

[24] Così rileva S. DELLAVALLE, *op. cit*., p. 195, nell'affrontare il discorso sul potere dell'UE, sottolineando anche la crisi etica, dunque che coinvolge i valori dell'UE, di cui si dirà.

[25] Dichiarazione di Roma del 2017, firmata da 27 leaders: https://www.consilium.europa.eu/it/press/press-releases/2017/03/25/rome-declaration/

[26] P. SILVA PEREIRA, The European Union's never-ending search for legitimacy, in W. HEUSEL, J.P. RAGEADE (Eds), *The Authority of EU Law*, Springer, 2019, p. 359.

[27] Vedasi F. LANCHESTER, Legittimità e legittimazione: la prospettiva del costituzionalista, in *Il Politico*, Vol. 6, No. 4, 1998, pp. 547-565. In particolare, l'autore ricorda che il tema della legittimità del potere politico, pur essendo emerso con pensatori del calibro di Schmitt, Weber o Ferrero già negli anni Quaranta, abbia «assunto un peso rilevante nella riflessione politologica e sociologica degli anni Settanta-primi anni Ottanta nell'ambito della discussione sull'ingovernabilità e la crisi di legittimazione degli ordinamenti occidentali», p. 549.

[28] Si veda al riguardo per tutti T. FRANCK, The Power of Legitimacy and the Legitimacy of Power: International Law in an Age of Power Disequilibrium, in *The American Journal of International Law*, Vol. 100, No. 1, 2006, pp. 88-106.

[29] Si vedano, su tutti, le Conclusioni della Presidenza del Consiglio europeo, Roma, 14 e 15 dicembre 1990, disponibili al seguente link: https://www.consilium.europa.eu/media/20535/1990_dicembre_-_roma_it_part_i.pdf .

[30] Cfr. C. CARTER, A. SCOTT, Legitimacy and Governance beyond the European nation State: conceptualising governance in th European Union, in *European Law Journal*, Vol. 4, No.4, December 1998, pp. 429-445.

intergovernativa del 1996[31], che portò al Trattato di Amsterdam. Quest'ultima, infatti, ricercava ancor più una sorta di legittimazione popolare. Ciò perché, è stato al riguardo notato, «le clausole di Maastricht configuravano certamente importanti cessioni di sovranità a fronte delle quali però non erano previsti meccanismi compensativi sul piano dell'occupazione e degli ammortizzatori sociali. Le regole della stabilità economica e monetaria erano state poste in primo piano per il futuro dell'integrazione economica e della moneta unica, senza prevedere tuttavia interventi nell'ambito politico e sociale capaci di creare le premesse per tale stabilità»[32]. Così, quelle incoerenze vennero trattate nel 1996.

A quel punto parecchi studiosi e osservatori notavano come i progressi realizzati sino ad allora fossero stati relativamente incontestati, si parlava al riguardo di "*permissive consensus*" o "*popular consent*"[33], mentre da qualche anno iniziavano ad emergere serie contestazioni, che portarono dunque a considerare il 1992 come una data centrale per le implicazioni rivoluzionarie che rappresentava[34]. Al riguardo, Weiler notava da un lato come la portata imponente dei mutamenti identificati nel 1992 fosse prevedibile, considerando quella data come "una mutazione sismica, esplosiva e visibile, ma comunque *nella natura di un'eruzione*", come inevitabile conseguenza di profondi cambiamenti che l'avevano preceduta, ciò avvenendo in tre fasi distinte, ciascuna delle quali trasformava ogni volta una caratteristica fondamentale dei rapporti tra livello sovranazionale e domestico[35]. Nondimeno, dall'altro lato, lo stesso autore riconosceva quel momento come «*the first major change in the architecture of the Community polity in relation to which general public legitimacy could be claimed*»[36]. Vale la pena dunque tentare di comprendere meglio le ragioni dell'emersione delle perplessità che questionavano la legittimità del costrutto europeo, nonostante la pretesa di maggiore trasparenza che quei mutamenti cercavano di realizzare.

Intanto, da una prospettiva che guarda agli avvenimenti esterni e al loro impatto sul costrutto europeo, una prima ragione – si è già detto – può rintracciarsi nella caduta del muro di Berlino (va da sé, di ovvia portata internazionale e non meramente europea) e dunque nella fine della Guerra fredda e della divisione del mondo in due blocchi nettamente distinti, che comportava la necessità di

[31] Alla quale ultima, infatti, si riferisce spesso la De Burca nel suo scritto che ci viene qui in ausilio, cfr., *op. cit*., p. 349. In generale, cfr. G. EDWARDS AND A. PIJPERS (Eds), The Politics of European Treaty Reform: The 1996 Intergovernmental Conference and Beyond, London: Pinter, 1997.

[32] P. GRAGLIA, *L'Unione europea – perché stare ancora insieme*, Il Mulino, 2019, p. 30.

[33] Così notano sia G. DE BURCA, *op. cit*., p. 350, che C. CARTER, A. SCOTT, *op. cit*., p. 430.

[34] Ancora G. DE BURCA, *op. cit*., p. 350 s., che C. CARTER, A. SCOTT, *op. cit*., p. 430 ss. Si veda anche P. GRAGLIA, *L'Unione europea, cit.*, pp. 27-29.

[35] J.H.H. WEILER, The Transformation of Europe, *cit.*, p. 2408, in cui precisa: «*only the combination of all three can be said to have transformed the Community's "operating system" as a non-unitary polity*». Per le tre fasi della trasformazione, sulle quali non ci si può qui soffermare, si rinvia al medesimo scritto, p. 2408 ss. Su questo concetto di "eruzione" l'autore ritorna di nuovo in J.H.H. WEILER, U. R. HALTERN, The autonomy of the community legal order-through the looking glass, in *Harvard International Law Journal*, 37(2), 1996, p. 443.

[36] J.H.H. WEILER, After Maastricht: Community legitimacy in Post-1992 Europe, in W.J. ADAMS (Ed.), *Singular Europe: Economy and Polity of the European Community After 1992*, The University of Michigan Press, 1995, p. 12.

ripensare gli obiettivi e le finalità comuni da perseguire. Appare abbastanza evidente, infatti, che «sia Maastricht sia il successivo Trattato di Amsterdam sono figli delle speranze e dei rivolgimenti che le trasformazioni nell'Est europeo hanno prodotto»[37]. Inoltre, da una prospettiva interna, lo stesso Weiler individuava una prima ragione nei cambiamenti strutturali già preconizzati dall'Atto Unico Europeo (del 1986) e assunti nel 1992, che imponevano di ripensare alcune caratteristiche centrali della costruzione europea. In questa prospettiva l'autore rintracciava poi anche la diffusa e perpetrata *confusione* nell'identificare del tutto la questione della legittimazione con il tema del deficit democratico che, per quanto ne ne rappresenti un aspetto preponderante, non è l'unico. Da ciò però derivava il presupposto – ritenuto dall'autore erroneo – che se il deficit democratico fosse stato affrontato non vi sarebbero più stati problemi di legittimità: «*My view is that certain very real issues of legitimacy go well beyond the question of any democracy deficit*»[38]. Valutazione comprensibile, oggi, riconoscendo i passi avanti fatti su tale fronte, da ultimo con Lisbona[39] – per quanto, in realtà, non effettivamente tali da escludere completamente il problema, che si mantiene nella misura in cui persiste lo scarto tra l'aumento dei poteri del Parlamento europeo e l'effettiva influenza degli elettori rispetto agli orientamenti politici dell'UE[40] – e, cionondimeno, la riproposta crisi di legittimazione. L'esposizione che segue dovrebbe spiegare perché non possa ravvisarsi una coincidenza totale.

Per comprendere i termini della crisi, già nel primo periodo alcuni suggerivano di riflettere, più che semplicemente sull'evoluzione dell'architettura costituzionale dell'Unione, sulle *modalità* attraverso cui alcuni mutamenti venivano trasposti dal livello domestico a quello sovranazionale[41]. Per tratti essenziali, la legittimità in senso lato sarebbe intesa come la *giustificazione*, l'accettazione dell'autorità e dell'esercizio del potere[42]; un'accettazione/accettabilità che si spiegherebbe sia in virtù della adesione alle regole da parte del governo e delle istituzioni, sia come impegno degli

[37] P. GRAGLIA, *op. cit.*, p. 30.
[38] Ibidem. Da notare anche la precisazione: «*To suggest that the legitimacy of the polity, or of same of its features, may be called into questions is not to say that the polity is about to become illegitimate, either in the strict legal sense or in the court of public opinion. But it does mean that one may expect dislocations and destabilisation problems that are novel in relation to the past of the Community*». In questo senso, più approfonditamente, anche J.H.H. WEILER, U. HALTERN, F. MAYER, European democracy and its critique – Five uneasy pieces, in *The Jean Monnet Centre for International and Regional Economic Law&Justice*, September 1995, p. 2 ss.
[39] Sugli avanzamenti avutisi nei sessant'anni da Roma a Lisbona in termini di maggiore democraticità – tuttavia in modo funzionale da evidenziarne le attuali permanenti criticità, si veda P. SILVA RIVEIRA, *op. cit*., p. 360.
[40] Problema che infatti persiste proprio perché in realtà il Trattato di Lisbona non è intervenuto così a fondo rispetto alla possibilità per gli elettori di far sentire effettivamente la loro voce. Cfr. P. CRAIG, *op. cit*.: *« The legal and political reality, as reflected in the Lisbon Treaty, was an institutional decision- making process in which State interests still predominated, and in which, notwithstanding the increase in the EP's power, the voters could not directly affect a change of policy direction in the EU by removing the incumbents and replacing them with those espousing different policies*», p. 315.
[41] Così C. CARTER, A. SCOTT, *op. cit.*, p. 429.
[42] G. DE BURCA, *op. cit*., p. 349.

stessi a soddisfare valori e aspirazioni sottostanti della società[43]. Ciò evoca la distinzione spesso proposta, e delineata anche da Weiler, delle cui analisi ci agevoleremo per adombrare il discorso sull'attuale "*legitimacy crisis*" del processo di integrazione europea, ritenendole esaurienti ai nostri fini, pur nella consapevolezza della vastità del dibattito, che include autori di grande spessore finanche delle scienze sociali e politiche e che qui non verranno menzionati, conducendo un'esposizione molto più modesta ma, si spera, bastante.

Utile punto di partenza si ritiene il cenno alla macro-distinzione sulla derivazione del potere pubblico (e dunque alle sue fonti di legittimazione), come applicata specificamente all'Unione europea da un'esauriente analisi di Dellavalle. L'autore ha prospettato intanto la classica dicotomia tra potere "ascendente" e "discendente": mentre il primo, derivando "dal basso", si giustificherebbe sulla base della volontà di coloro che decidono di sottomettervisi; il secondo, derivante "dall'alto" (ossia da un'autorità naturale o divina), discenderebbe poi dai governanti ai governati. Quindi, l'autore ha esposto l'applicazione di entrambe le concezioni al caso dell'Unione europea: "la visione «discendente» del potere pubblico (…) ha trovato nel contesto europeo un accogliente e fertile terreno di coltura. Il fatto che l'Europa unita sia stato il palcoscenico su cui ha ripreso vigore una *visione elitaria del potere* non significa, tuttavia, che questa sia l'unica possibilità di interpretarne la realtà e i possibili sviluppi. Al contrario, anche il potere pubblico unionale è stato visto come almeno potenzialmente legittimabile «dal basso», così da mantenere i più elevati standard democratici anche al livello delle istituzioni dell'UE"[44].

Riconoscendo la visione "ascendente" del potere dell'Unione nella sostenuta quanto problematica legittimazione democratica, e la visione "discendente" nella complessa c.d. legittimazione tecnocratica, l'autore espone diverse correnti di pensiero che riconduce rispettivamente a ciascuna visione. Ne riferiamo qui (pur senza soffermarci e rinviando per alcuni aspetti di interesse al prosieguo) solo al fine di chiarire che l'autore, seguendo tale dicotomia, mentre ha trattato la questione del *deficit* democratico nell'ambito della visione "ascendente" del potere dell'Unione, ha invece proposto alcune delle distinzioni prospettate da Weiler, di cui a seguire, riconducendole alla concezione tecnocratica della legittimazione del potere UE (dunque discendente)[45].

Andando dunque all'analisi di Weiler, questi ripropone la prima macro-distinzione (di genere) tra legittimazione formale (o normativa) e legittimazione sociale (o empirica)[46]. La legittimazione

[43] Ancora C. CARTER, A. SCOTT, *op. cit.*, p. 431.
[44] S. DELLAVALLE, *op. cit*., pp. 201-202, corsivo aggiunto.
[45] *Ibidem*, p. 202 ss. e p. 210 ss.
[46] Così J.H.H. WEILER, The Transformation of Europe, cit., p. 2468 ss.; ma poi ancora, tra gli altri, in: ID., After Maastricht: Community legitimacy in Post-1992 Europe, *cit*., p. 19 ss.; ID., In the Face of Crisis: Input Legitimacy, Output Legitimacy and the Political Messianism of European Integration, in *Journal of European Integration*, 34:7,

formale implicherebbe che tutti i *requisiti di legge* siano rispettati nella creazione delle istituzioni e del sistema. Ciò di fatto, nei Paesi occidentali, si traduce essenzialmente nelle basi democratiche delle strutture e dei processi di potere. Questa concezione, hanno notato altri, sarebbe assolta a livello sovranazionale dalla caratteristica "doppia fonte di legittimazione" (di un Parlamento europeo eletto direttamente e di un Consiglio legittimato a livello domestico) nel funzionamento del costrutto istituzionale europeo[47]. Pertanto, Weiler rilevava che, poiché i Trattati istitutivi attribuivano un ruolo limitato al Parlamento europeo in quanto comunque approvati dai Parlamenti degli Stati membri, «*Proposals to give more power to the European Parliament have failed, for a variety of reasons, to survive the democratic processes in the Member States*»[48]. Questo è noto e variamente ribadito nei discorsi che guardano alla struttura istituzionale originaria per affrontare le questioni che si pongono ai giorni nostri e per l'avvenire: «*The reality was that the original disposition of power in the Rome Treaty saw little role for direct democratic input*»[49]. Dunque, avendo precisato la distinzione rispetto alla mera "legalità"[50], Weiler confermava sulla legittimazione "formale" che la struttura e il processo esistenti poggerebbero su un'approvazione formale da parte dei Parlamenti democraticamente eletti a livello domestico[51].

Quanto, poi, alla legittimazione *sociale*, essa sarebbe una componente sostanziale aggiuntiva e riguarderebbe piuttosto quella *accettazione* del potere/governo da parte della società empiricamente determinata di un dato sistema, indicando dunque la rilevanza riconosciuta nel processo di governo ai valori propri della cultura politica generale di quel sistema[52].

Sul rapporto tra questi due modi di intendere la legittimazione, l'autore a più riprese ha sottolineato che, mentre qualsiasi sistema deve godere di legittimazione formale per poter godere di legittimazione sociale (così, almeno, nella maggior parte dei casi, ossia quelli delle democrazie

---

2012, p. 826 ss.; ID., Europe in crisis – on 'political messianism', 'legitimacy' and the 'rule of law', in *Singapore Journal of Legal Studies*, December 2012, pp. 248-250. L'autore viene ripreso in questa distinzione anche da DELLAVALLE, *op. cit*., p. 212.

[47] P. SILVA RIVEIRA, *op. cit*., p. 361.

[48] J.H.H. WEILER, The Transformation of Europe, *cit.*, p. 2468. Nello stesso senso anche in Id., After Maastricht: Community legitimacy in Post-1992 Europe, *cit*., pp. 19-20.

[49] P. CRAIG, *op. cit*., p. 313, in cui continua: «*The Assembly was accorded limited power, and its only role in the legislative process was a right to be consulted where a particular Treaty article so specified*».

[50] Così anche in J.H.H. WEILER, In the face of crisis: Input Legitimacy, Output Legitimacy and the Political Messianism of European Integration, *cit.*, p. 827; nonché in Id., Europe in crisis – on 'political messianism', 'legitimacy' and the 'rule of law', *cit*., p. 249.

[51] Cfr. J-L. SAURON, L'UE: quelle légitimité ? Quel avenir ?, in The Authority of European law: do we still believe in it?, IN W. HEUSEL, J-P REGEADE (Eds), *The Authority of EU Law – Do we still believe in it?*, Springer, 2019, p.372, laddove parla di « *Un problème de légitimité ascendante : le révélateur européen de la crise nationale de la démocratie* ».

[52] J.H.H. WEILER, The Transformation of Europe, *cit.*, p. 2469.

occidentali, in cui lo Stato di diritto è parte integrante – come noto – della filosofia politica), non è necessariamente vero il contrario[53].

Ebbene, il problema della crisi di legittimazione attraversata a livello sovranazionale, già dopo il 1992 ma a più riprese dopo il 2008 e nuovamente adesso, starebbe proprio in questo: sin dal 1991 l'autore evidenziava come, escluse perplessità sulla legittimazione formale, fosse la "*social legitimacy*" a rappresentare l'aspetto cruciale per il successo del processo di integrazione europea[54]. In tal senso la De Burca, seguendo la Conferenza Intergovernativa del 1996, rilevava l'opinione di molti commentatori dell'epoca sulla sfida per la legittimazione dell'Unione costituita dalla mancanza di sostegno popolare (nonché la difficoltà di rintracciarne in modo chiaro le cause). Nondimeno, l'autrice riteneva che, nonostante l'enfasi posta dopo Maastricht sulla necessità di rinvigorire il sostegno popolare per l'Unione, a suo dire le questioni di base della legittimazione normativa/formale non erano state prese sufficientemente sul serio, mentre su di esse avrebbero dovuto rintracciarsi le ragioni sostanziali della disaffezione[55]. Simili perplessità evocano il rapporto tra legittimazione e popolarità esplorato da Weiler: prospettandone la differenza, questi precisava come spesso più profonde sono le risorse di legittimazione di un regime, più esso pare in grado di adottare misure impopolari in tempo di crisi[56]. Guardando all'integrazione europea, lo stesso scriveva nel 2012: «*The problem is European, but Europe as such is finding it difficult to craft the remedies. I would like to argue that in the present circumstance, the legitimacy resources of the European Union – referring here mostly to social legitimacy – are depleted, and that is why the Union has had to turn to the member states for salvation. Solutions will still have to be Europe-wide, but they (…) will require the legitimacy resources of the member states – in many countries close to depletion too – in order to gain valid acceptance in Europe*»[57]. Queste considerazioni ci consentono di procedere all'ulteriore distinzione tra tre diversi "tipi" di legittimazione rispetto all'esperienza sovranazionale, che porterebbe l'autore a riproporre sotto altre prospettive le medesime perplessità e relative proposte.

I tre diversi "tipi" di legittimazione, ritenuti centrali dallo stesso autore nell'evoluzione dell'integrazione europea, parrebbero vagamente richiamare la distinzione tra i tre tipi ideali di potere di weberiana memoria[58]. Accanto alle due "classiche" tipologie di *input* (o *process*) e *output*

[53] Cfr. *Ibidem*, nonché Id. In the face of crisis, *cit*., pp. 826-827, e allo stesso modo Id., Europe in crisis, *cit*., p. 249, in cui l'autore riporta alcuni esempi storici al riguardo.
[54] Ancora ID., The Transformation of Europe, *cit*., p. 2472, nonchè ID. After Maastricht, *cit*., p. 22. Sulla coerenza della legittimità formale, si veda la ricostruzione dedicata da N. ROJAS-HUTINEL, *La séparation du pouvior dans l'Union européenne*, mare&martin, 2017, pp. 267-305.
[55] G. DE BURCA, *op. cit*., pp. 351-352, nonché l'analisi immediatamente successiva sulla natura del dibattito.
[56] J.H.H. WEILER, In the face of crisis, *cit*., p. 827.
[57] J.H.H. WEILER, In the face of crisis, *cit*., p. 827; nonché, Id., Europe in crisis, *cit*., p. 249.
[58] Il riferiento è al famoso M. WEBER, Economia e società, 1922 (prima pubbl.).

(o *result*) *legitimacy* lungamente utilizzate dalle scienze politiche e sociali[59], Weiler propone infatti la *telos legitimacy* o, da lui così individuata, di "*political messianism*" [60].

La *input legitimacy* altro non è che quella concezione che guarda alle cause, alle fondamenta, al processo di formazione, per individuare la legittimazione di un dato governo o centro di potere. Dunque, semplificando, l'autore facilmente identifica questa tipologia con la caratteristica democrazia negli Stati membri: un centro di potere, un organo di governo, è legittimo se poggia il suo fondamento su basi democratiche.

La *output legitimacy*, invece, guarderebbe all'opposto, ossia ai risultati, alla realizzazione di obiettivi prefissati da un centro di potere per considerarsi legittimo – ciò che l'autore identifica con *panem et circenses*. Questo tipo di legittimazione deriverebbe da una commistione di fattori che guarderebbe al successo dell'ente nel perseguimento dei risultati e sarebbe, dall'analisi dell'autore, ciò che guida di fatto l'operato della Commissione ("non c'è modo migliore per legittimare una guerra che vincerla").

La terza tipologia, quella di *political messianism*, concepirebbe la legittimazione come qualcosa che viene acquisita non dal processo di formazione né dai risultati ottenuti da un dato centro di potere, bensì dalla aspettativa di un fine ultimo più grande, una "terra promessa", un ideale o una missione.

Precipuamente nel 2012, ma per sommi capi già anche prima, Weiler dimostrava con la sua analisi perché tutte e tre le tipologie di legittimazione, pur in diversi momenti e modi, non riuscissero ad avere successo nelle varie fasi dell'integrazione europea e pertanto, costantemente, riproponessero questioni di legittimazione, sino a quella di cui si parla oggi (affrontata dallo stesso, tra gli altri, in uno scritto recente a cui faremo riferimento).

Cercando di riproporre in termini semplicistici il ragionamento logico sviluppato da Weiler, il primo tipo di legittimazione (*input*) imporrebbe di considerare ciò che rappresenta una caratteristica connaturata al costrutto europeo, ossia il deficit democratico (che pertanto, come si è detto, rappresenterebbe solo una parte della questione). Le manifestazioni di questo deficit si mostrano persistenti e non sono state (né, nella prospettiva di Weiler, verranno) debellate da interventi sul Parlamento europeo. Il punto, sviluppato dall'autore, è che se è vero che l'Unione non è uno Stato, e dunque come tale non potrebbe (e non dovrebbe?)[61] replicare categorie e strutture propriamente

[59] In particolare il riferimento è a F.W. SCHARPF, *Governing in Europe: Effective and democratic?*, Oxford University Press, 1999.Tra gli altri, si veda anche L. KÜHNHARDT, European Union – The Second Founding, *cit*.

[60] J.H.H. WEILER, In the Face of Crisis: Input Legitimacy, Output Legitimacy and the Political Messianism of European Integration, *cit.*, p. 828 ss.; Id., Europe in crisis – on 'political messianism', 'legitimacy' and the 'rule of law', *cit.*, p. 250 ss.; ID., The Authority of European law: do we still believe in it?, in W. HEUSEL, J-P REGEADE (Eds), *The Authority of EU Law – Do we still believe in it?*, Springer, 2019, p. 16 ss.

[61] È noto il grande sostenitore delle opportunità di avanzamenti nel senso della possibilità di concepire uno "Stato Europa" (una forma di federalismo, dunque; per questa e altre correnti nelle teorie dell'integrazione si veda *infra*), il

domestiche a livello sovranazionale (in termini, per esempio, di controllo e responsabilità tra intervento parlamentare e azione governativa), è altresì vero però che nel settore della governance essa ha occupato vaste aree (alcune anche critiche) in precedenza proprie degli Stati membri. E ciò coinvolge direttamente la questione del deficit democratico, perché, dice dell'autore: «*Democracy is not about States. Democracy is about the exercise of public power – and the Union exercises a huge amount of public power*»[62]. Questo il motivo per cui la questione del deficit democratico è stata, ed è tuttora, così fortemente legata alla questione della legittimazione. La De Burca, infatti, era tra coloro che, già dopo Maastricht, ritenevano questo aspetto cruciale nel dibattito sulla legittimazione: «*The Union exercises a great deal of power and there are few clear boundaries to its sphere of competence, yet these powers cannot be justified by reference to the typical processes and structures of the democratic state. Herein lies the crux of the legitimacy debate on the European Union. It is not a state in its political structure or mode of governance, yet it possesses many of the powers of a state, and has many characteristics which distinguish it clearly from a typical intergovernmental organisation of independent states. Not only does it have very wide and loosely defined legislative and regulatory powers, but much of its law has a direct impact, unmediated by the Member States, on actors throughout the Union*»[63]. Dunque, conclude Weiler, se persistiamo nella convinzione che qualsiasi esercizio del potere pubblico debba essere legittimato democraticamente, allora si capisce come la prima tipologia di *input legitimacy*, la legittimazione del processo, non possa funzionare a livello europeo. E ciò, spiega l'autore, essenzialmente per la strutturale mancanza di quelli che sono due principi basilari di ogni democrazia: quello di responsabilità e quello di rappresentazione[64]. Senza poterne approfondire i termini, basti dire che ciò parrebbe strutturalmente ineliminabile nella peculiare sembianza dell'Unione europea quale "*governance without government*", ossia – per sommi capi – una governance non progettata per la responsabilità politica, mancante di un effettivo governo che possa essere eventualmente "eliminato" in caso di insoddisfazione per il suo operato, con il perdurante varco (cui si è già fatto cenno) tra ciò che esprimono gli elettori e la loro effettiva capacità di influire per eventuali

giudice Mancini, con cui Weiler si è trovato in prima persona a discutere (e, in particolare, a spiegare il suo scetticismo), a seguito di apposite sollecitazioni del primo: G.F. MANCINI, Europe: The case for Statehood, *in European Law Journal*, vol. 4, no. 1, 1998, pp. 29-42; J.H.H. WEILER, Europe: The Case Against the Case for Statehood, in *European Law Journal*, vol. 4, no. 1, 1998, pp. 43-62.

[62] J.H.H. WEILER, In the Face of Crisis, *cit.*, p. 829; Id., Europe in crisis, *cit.*, p. 251; Id., The Authority of European law: do we still believe in it?, in W. HEUSEL, J-P REGEADE (Eds), *The Authority of EU Law – Do we still believe in it?*, Springer, 2019, p. 14.

[63] G. DE BURCA, *op. cit.*, p. 352. i

[64] L'autore si sofferma sulle caratteristiche di questi due principi e, nel farlo, richiama importante letteratura al riguardo, cfr. J.H.H. WEILER, In the Face of Crisis, *cit.*, p. 829-830; ID., Europe in crisis, *cit.*, p. 251-253; Id., The Authority of European law, *cit*., pp. 14-15.

Su questo, tra i numerosissimi contributi, si veda in particolare: H. LINDAHL, Sovereignty and Representation in the European Union, in N. WALKER (ed.), *Sovereignty in transition*, Hart Pulishing, 2003, pp. 115-144.

mutamenti di scelte politiche[65]. Nondimeno, di recente non è mancato chi ha posto l'accento della crisi di democraticità europea sulla più generale crisi di democraticità all'interno dei singoli Stati membri[66]. Ad ogni modo, le considerazioni sul deficit democratico richiederebbero enormi approfondimenti – specie su interessanti proposte risolutive, quale quella di Habermas (cui si farà solo un cenno nel prosieguo)[67] –; qui basti dire che esse sono pure state sottoposte a diverse critiche, a partire dalle quali anche Weiler ha esposto il secondo tipo di legittimazione, quella dei risultati, la *output legitimacy*.

Le critiche si sostanzierebbero nel ritenere errati i criteri applicati all'Unione nell'analisi del fenomeno, considerate appunto le sue peculiarità e dunque l'irriducibilità a categorie prettamente statali, nonché – questa è la seconda critica, che conduce alla legittimazione dei risultati – nella necessità, in virtù di quelle peculiarità, di rintracciarne la legittimazione *altrove*. Richiamando diversi studiosi di scienza politica, Weiler dimostrava come effettivamente la legittimazione dell'Unione (e, nello specifico, dell'operato della Commissione) potrebbe forse riposare spesso nei risultati raggiunti, così evocando le concezioni funzionaliste del processo di integrazione (sia classiche che più avanzate), di cui si dirà meglio nel prosieguo. Invero, questa prospettiva era abbastanza diffusa tra gli studiosi, specie all'indomani della fallita Costituzione europea nonché dopo Lisbona[68]. Pur abbastanza scettico sull'effettiva rilevanza di tale tipologia di legittimazione rispetto alla "forza mobilitante" del costrutto europeo, l'autore le riconosce nondimeno una qualche incidenza, specialmente in situazioni critiche, quantomeno nella considerazione del processo di integrazione. Nella misura in cui, infatti, emergevano i problemi economici dalla crisi dell'euro, essi venivano attribuiti, più o meno erroneamente, alla costruzione europea, con inevitabili ostilità all'interno degli Stati membri: «*The worst way to legitimate a war is to lose it, and Europe is suddenly seen not as an icon of success but as an emblem of austerity, thus in terms of its promise of prosperity, failure. If success breeds legitimacy, failure, even if wrongly allocated, leads to the opposite*»[69].

---

[65] *Ibidem*. Sul concetto di "*governance without government*", tra tutti (poiché lo si riprenderà nel prosieguo, *infra* par. 3) M.A. POLLACK, Theorizing the European Union: International Organization, Domestic Polity, or Experiment in New Governance?, in *Annual Review of Political Science*, 2005, da p. 380 ss. Inoltre, insiste sul "perdurante varco" – e sulla responsabilità degli Stati membri rispetto allo *status quo*, P. Craig, *op. cit.*, p. 313 e anche da 330 ss. Su questi aspetti, tuttavia, si veda meglio *infra*, sulle teorie integrazione europea e sulla "forma" dell'Unione.

[66] Così J-L. SAURON, *L'UE: quelle légitimité ? Quel avenir ?*, cit., p.372.

[67] J. HABERMAS, Democracy in Europe: Why the Development of the EU into a Transnational Democracy Is Necessary and How It Is Possible, *European Law Journal*, Vol. 21, No. 4, July 2015, pp. 554-555.

[68] Non si ha qui modo e spazio di parlare dell'intricata questione di una Costituzione per l'Europa, per la quale si consideri su tutti il celeberrimo botta e risposta avvento in tempi più risalenti tra Grimm e Habermas: D. GRIMM, Does Europe need a Constitution?, in *European Law Journal*, 1 (1995), 282-302; J. HABERMAS, Remarks on Dieter Grimm's 'Does Europe need a Constitution?', in *European Law Journal*, 1 (1995), pp. 303-307.

[69] J.H.H. WEILER, In the Face of Crisis, *cit.*, p. 831; Id., Europe in crisis, *cit.*, p. 255; Id., The Authority of European law, *cit.*, p. 16.

Nondimeno, se la *input legitimacy* risiederebbe essenzialmente nella democraticità del processo di formazione, che intesa nel senso domestico non apparterrebbe strutturalmente al costrutto europeo, e la *output legitimacy* fallirebbe nel mancato raggiungimento dei risultati, la cui fallacia difatti sarebbe emersa la prima volta in cui si pose la questione con la crisi dell'euro, come mai una "crisi" di legittimazione non è sorta prima di Maastricht, quando il processo, avanzando indisturbato, pareva tendenzialmente considerato legittimo?[70]

Qui entra in gioco il terzo tipo di legittimazione, che secondo l'autore ha più degli altri guidato l'integrazione per diverso tempo e sin dagli albori. Il "*political messianism*" di cui parla Weiler consentirebbe di legittimare l'integrazione a partire dalla nobiltà del suo fine ultimo, del suo ideale, della "promessa" di un futuro migliore: «*in messianic visions the end always trumps the means*»[71]. L'autore ci ricorda, rifacendosi ad altri studiosi, come ciò – pur avendo in questo caso connotati più liberali e nobili – non sia una novità ma, al contrario, una caratteristica precipua del modo di procedere di monarchi e imperatori europei, come anche dei totalitarismi che occuparono il continente nel primo dopoguerra. Ebbene, secondo Weiler "l'impresa" comunitaria dopo la Seconda Guerra mondiale costituiva per gli Stati europei di allora il progetto messianico per eccellenza. A suo dire, in ciò starebbe la vera forza trainante del costrutto europeo, che ne spiegherebbe anche le basilari scelte strutturali e istituzionali, e che forse sarebbe stata troppo spesso sottovalutata.

Egli ripropone, sin dalla Dichiarazione di Schuman, una lettura in chiave messianica dell'intero processo, riconoscendovi tale caratteristica sia nella retorica che nella sostanza. Proprio questo modello, questa ambizione che permeava l'intero costrutto, spiegherebbe dunque l'assenza di un qualsivoglia riferimento – sia scritto (nei Trattati ma finanche nella Dichiarazione di Schuman) che prospettato tra i chiari obiettivi dell'integrazione – ai concetti/valori di democrazia e tutela dei diritti umani, che pure si pretendeva venissero garantiti e condivisi da tutti gli Stati membri (di essi si avrà traccia nel diritto primario solo con Lisbona).

Ma se ciò è vero, dove risiederebbe allora il fallimento anche di questo tipo di legittimazione? In cosa esso non avrebbe funzionato o funzionerebbe, al punto da riportare a questioni che impongono un ripensamento del costrutto europeo? L'autore ci dà una risposta che sembrerebbe quasi un paradosso, tanto essa pare ontologicamente connessa al *political messianism*. In parole povere, se è chiaro che (come per l'*output legitimacy*) questa concezione non funziona nella misura in cui fallisce, ossia non realizza la promessa, non soddisfa l'aspettativa, è invece peculiare che questa concezione di legittimazione non funzioni soprattutto quando essa riesce, quando realizza l'ideale

[70] L'autore ribadisce questo aspetto, ampiamente trattato nello scritto già citato del 1991, anche poco dopo in occasione della pronuncia tedesca sul Trattato di Maastricht, cfr. J.H.H. WEILER, Does Europe Need a Constitution? Demos, Telos and the German Maastricht Decision, in *European Law Journal*, vol. 1, no. 2, 1995, p. 237.
[71] J.H.H. WEILER, In the Face of Crisis, *cit.*, p. 832; ID., Europe in crisis, *cit.*, p. 256.

prospettato, la rivoluzione promessa: «*Europe is a victim of its own success*»[72]. Ciò è evidente nel caso comunitario e soprattutto spiega perché la prima questione si sia posta col Trattato di Maastricht.

È quanto si diceva già sopra: se la forza motrice che mobilitava gli Stati europei ad unire le forze e perseguire i medesimi interessi economici, per rendere una eventuale guerra non solo impensabile ma "materialmente impossibile", era il fine idilliaco di una pace che pareva allora una chimera, l'effettiva realizzazione di quella pace con la caduta del muro e poi ancora il perdurare di una situazione fuori da belligeranze per decenni hanno fatto non solo sparire l'ideale per cui aveva un "senso" muoversi insieme, ma anche la portata dell'effettivo significato di quell'ideale. E ciò sarebbe ancor più comprensibile considerando i profondi mutamenti che il sostrato sociale europeo ha subito dalla Dichiarazione di Schuman: si tratta di generazioni che non conoscono altra realtà che la pace, che dunque, lungi dal costituire un'ambizione, rappresenta "solo" il contesto di *default*.

Inoltre, l'autore sottolinea come pure l'emersione della cultura dei diritti individuali (ma sono cose spesso dette), pur rappresentando una conquista indiscussa, avrebbe nondimeno contribuito ad una perdita generalizzata di sensibilità verso questioni che presentino profili di collettività, per cui: «*The result is that if political messianism is not rapidly anchored in the legitimation that comes from popular ownership, it rapidly becomes alienating*»[73]. Questa alienazione derivante dal distacco dalla "proprietà popolare" sarebbe stata secondo l'autore prevedibile nella misura in cui: il carattere democratico era sin dalle origini escluso dal "DNA" del processo di integrazione[74], e come tale, in qualche modo, è rimasto, semplicemente in virtù delle scelte in tal senso costantemente assunte dagli Stati membri nel tempo[75]; il messianismo politico non funziona per i motivi che si sono detti; i risultati immediati, di una visione peraltro concepita dall'autore come materialista[76], non sono stati raggiunti, venendo, così, meno anche la prospettiva più pragmatica. Constatando l'inadeguatezza di tutte le possibilità legittimanti prospettate, l'autore suggeriva nel 2012 che, pur nella necessità di rintracciare una soluzione a livello europeo – essendo i problemi essenzialmente europei –, la risposta dovrebbe essere "percepita come legittima" all'interno degli Stati membri e che dunque, non potendo fare affidamento sul processo decisionale sovranazionale, il ripensamento verso una più stretta integrazione potrebbe avvenire solo a partire dalle strutture politiche, giurisdizionali e

[72] J.H.H. WEILER, In the Face of Crisis, *cit.*, p. 836; ID., Europe in crisis, *cit.*, p. 268.
[73] J.H.H. WEILER, In the Face of Crisis, *cit.*, p. 837; ID., Europe in crisis, *cit.*, p. 268.
[74] Ibidem, cfr. anche p. 835.
[75] Così fa notare, come è emerso già in parte *supra*, P. CRAIG, *op.cit.*: «*Insofar as there is a democratic deficit (…), it flows from choices made expressly and repeatedly by the Member States over time as to the institutional structure for decision-making which they are willing to accept. These choices could have been different. There is no a priori block in this respect. There is, to the contrary, no especial difficulty in devising an EU decision-making regime that would meet the democratic shortcomings (…). The EU itself is not blameless with respect to the mode of decision-making*», p. 312.
[76] J.H.H. WEILER, da ultimo (ma già nel 1995 e poi nel 1998) in The authority of European law: do we still believe in it?, *cit.*, p. 8 ss.

decisionali degli Stati membri. È quanto in realtà diceva già con riguardo al "genere" di legittimazione sociale. Le *comunità nazionali*, secondo questa comprensibile visione, sarebbero la più profonda fonte di legittimazione del processo di integrazione europea, ed è ad esse, dunque, che bisogna guardare per trovare nuova linfa[77].

Questo ordine di idee, che meglio preciseremo nei paragrafi seguenti, può comunque sin da ora verificarsi rispetto all'attuale *legitimacy crisis*, se si considera il recente monito dello stesso autore circa la necessità di non sottovalutare alcuni bisogni "ancestrali" che le comunità nazionali presenterebbero inevitabilmente e che, invece, parrebbero (essere stati?) negati nell'evoluzione del processo di integrazione. E ciò, come spiega l'autore, sarebbe dipeso dalla necessità di creare una *cesura* quanto più netta con le esperienze negative (essenzialmente di totalitarismo) che avevano preceduto il progetto comunitario e che parevano intrise di quei bisogni. Weiler spiega bene questo concetto, che tanto potrebbe sembrare bizzarro quanto invece non dovrebbe essere sottovalutato, distinguendo tra "Trinità santa" e "Trinità empia" nella retorica e nell'etica del processo di integrazione. Senza soffermarci sul precipuo significato dei singoli valori che ciascuna di queste "Trinità" contiene, pare qui degna di nota la distinzione da lui proposta.

Alla "Trinità santa" farebbero capo i valori di governance democratica, *rule of law* e tutela dei diritti umani, ribaditi più volte come – l'autore sottolinea – quelli che definiscono il sistema valoriale su cui si regge il costrutto europeo. Alla ironicamente definita "Trinità empia" farebbero invece capo il patriottismo[78], la celebrazione della unicità individuale e collettiva, il senso di dovere e responsabilità. L'autore, soffermandosi sul significato di ciascuno di essi, li considera parte di una seconda categoria di valori che sarebbe stata lungamente repressa a livello sovranazionale al punto da essere considerata quasi illegittima, pur essendo invece, a suo dire, molto cara al cuore dei cittadini europei.

Ebbene, l'errore drammatico dell'Unione europea, protratto per lungo tempo e giustificabile con la considerazione della necessità di staccarsi in maniera eclatante dai regimi totalitari che fomentavano quei valori, sarebbe stato quello di negarli e, una volta ignorati, considerarli quasi contrari all'assetto di valori propriamente sovranazionale. La recente emersione di populismi tra diversi Stati membri non sarebbe altro che la testimonianza di tale errore, mentre una considerazione delle comunità nazionali come fonte principale di legittimazione del processo di integrazione non dovrebbe prescindere dalla necessità di ritenerli ancora, epurati dai fanatismi che pervertivano gli aspetti più genuini, come rilevanti per l'avanzamento dell'integrazione tra i popoli

[77] ID., In the Face of Crisis: Input Legitimacy, Output Legitimacy and the Political Messianism of European Integration, in *Journal of European Integration*, 34:7, 2012.
[78] Per questo in particolare si veda L. KÜHNHARDT, *op. cit.*, p. 483 ss. (capitolo XII. *Toward European Patriotism?*).

europei[79]. E questo ultimo aspetto, però, ci riporta inevitabilmente alla necessità di meditare sulla legittimazione democratica (considerati anche i limiti di quella tecnocratica; cfr. *infra*). Una questione che ha assunto nel tempo variegate declinazioni, mutando con l'evoluzione del processo europeo, sulla quale possiamo qui solo accennare lo stimolante dibattito tra il giudice Mancini e Weiler, nel lontano 1998, circa l'opportunità di un (ormai accantonato) possibile "Stato europeo" (introducendo concetti che verranno chiariti *infra*).

A fronte della opportunità (di procedere verso una forma di organizzazione del governo sovranazionale come statale) prospettata dal primo e ritenuta sconveniente dal secondo (paventando il rischio che l'Unione andasse a incappare negli stessi limiti per il superamento dei quali gli Stati avevano deciso di cooperare a livello sopra-nazionale), entrambi sicuramente concordavano sulla paradossale quanto impressionante constatazione *di un diritto che ha forza di imporsi con autorità* (principi del primato e degli effetti diretti) *su ordinamenti e soggetti, pur non essendo totalmente legittimato da quei soggetti*. Oggi, con le revisioni ai Trattati parecchie cose sono cambiate, da più parti si ribadisce la necessità di rintracciare un effettivo "demos" legittimante il potere sovranazionale[80]. E se questa esigenza pare abbastanza (pur considerati i recenti richiami nazionalisti) condivisa, ciò che risulta ancora faticoso è cosa si intenda effettivamente per demos: «*the absence of a common understanding of demos would still rob it of the moral authority for a claim to obedience to the Rule of Law*»[81].

Qui comprendiamo la correlazione tra i concetti di potere (prima ancora, di sovranità?), sua legittimazione, democraticità, stato di diritto e tutela dei diritti come valori comuni agli Stati ma soprattutto propri dell'Unione, e dunque il loro confluire nella definizione dell'autorità del suo diritto (nella duplice dimensione interna ed esterna).

Riteniamo dunque di poter muovere verso un'analisi che ci consenta di cogliere, in qualche modo, le peculiarità di quel diritto, per poi valutare l'eventuale portata della sua autorità (analizzando le interazioni tra quelle e il fecondo settore prescelto della protezione dei dati personali).

L'avvio di questa analisi, come detto, dall'esterno ci invita a procedere con l'esposizione di studi di teoria delle relazioni internazionali che hanno dedicato qualche attenzione all'integrazione europea.

---

[79] J.H.H. WEILER, The authority of European law, cit.

[80] Il riferimento, in senso negativo, è ai sostenitori della c.d. *no demos thesis.*

[81] J.H.H. WEILER, Epilogue: Living in a glass house – Europe, Democracy and the Rule of Law, in C. CLOSA, D. KOCHENOV (Eds), *Reinforcing Rule of Law Oversight in the European Union*, Cambridge University Press, 2018, p. 325.

CAPITOLO II

LA *SPINTA DELLO SPAZIO SULLA FORMA*

1. Spunti di teoria delle relazioni internazionali sul processo di integrazione europea

Le considerazioni proposte, pur mantenendo aperti diversi interrogativi e suggerendo ulteriori approfondimenti, impongono un riferimento preliminare alla *teoria delle relazioni internazionali*, o meglio all'utilizzo che di essa si è fatto per analizzare gli sviluppi del processo di integrazione europea. Tale riferimento non solo appare utile per comprendere le dinamiche che saranno esaminate oltre, rispetto al caso di studio prescelto, ma pare anche il più fedele adattamento della concettualizzazione della "spinta dello spazi sulla forma" che abbiamo assunto come approccio metodologico.

Un cenno a spunti tratti dalle teorie sulle relazioni internazionali consentirà infatti di ricavare elementi utili all'analisi dell'influenza dello spazio esterno *sul* fenomeno che oggi chiamiamo Unione europea (e, dunque, da lì, consentirà anche viceversa, di muovere *verso* l'esterno). Se le posizioni principali che brevemente qui richiameremo hanno caratterizzato la teoria delle relazioni internazionali da ben prima che l'Unione europea emergesse nel contesto internazionale[82], la loro applicazione al processo d'integrazione è utile a comprendere come effettivamente un "modellamento" dall'esterno abbia accompagnato l'ente sovranazionale sin dalla sua formazione e stia, inevitabilmente, continuando a plasmarlo secondo dinamiche per molti versi consolidate. Partiremo da qui, dunque, per poter poi meglio trattare le teorie dell'integrazione europea *tout court*, ossia quelle che, analizzando precipuamente l'avanzamento del processo di integrazione, toccano la questione (in parte anticipata sopra) della legittimazione del potere dell'Unione e dell'autorità del suo diritto, dunque delle prospettive per il suo futuro.

---

[82] J.-J. ROCHE ci ricorda al riguardo: « *Le besoin d'étudier les relations internationales avec des instruments spécifiques, distincts de l'histoire et du droit, est apparu au lendemain de la Première Guerre mondiale. La première chaire spécialisée fut ainsi créée en 1919 à l'Université du Pays de Galles, avant d'être copiée par les universités américaines. Les relations internationales se constituèrent donc en un domaine autonome de recherche sous l'effet de trois facteurs (…)*» rintracciando – in sintesi – questi tre fattori in: necessità di riflessioni sulle cause della guerra e sulle condizioni di una pace durevole, specie una volta infranto il mito della "missione civilizzatrice" dell'Occidente a seguito della Prima Guerra Mondiale; la necessità, stimolata dalle trasformazioni dei meccanismi di equilibrio dell'Europa del XIX secolo, di andare oltre l'analisi delle sole cause storiche della guerra per studiare l'influenza delle "forze profonde" sul comportamento degli attori; la necessità di una riflessione più generale sul ruolo del potere e sull'azione diplomatica, specie a seguito del rifiuto USA di assumere il ruolo che gli spettava dopo il decisivo intervento nel 1917; così in
Théories des relations internationales, 4e édition, Montchrestien, 2001, p. 20.

A tal proposito, è senz'altro da segnalare l'analisi di Pollack che ha mostrato come l'evoluzione del processo di integrazione europea abbia interessato tre diversi principali approcci teorici.

Il primo sarebbe quello che, appunto, ha proposto le più ampie riflessioni di teoria delle relazioni internazionali anche per spiegare il processo di integrazione europea. Il secondo avrebbe invece rigettato quella teoria in favore di approcci comparativi che analizzano il costrutto europeo partendo da paradigmi domestici. Il terzo guarderebbe l'Unione come un sistema emergente di *governance* multilivello[83]. Gli ultimi due approcci verranno solo brevemente accennati, concentrando invece l'attenzione sul primo di essi.

Il dibattito sulle prospettive future dell'Unione europea nell'ambito della teoria delle relazioni internazionali ha coinvolto, com'è noto, i tre modelli principali: realismo, liberalismo e costruttivismo[84]. Nel ripercorrere le caratteristiche principali di ciascuno di essi, si trarrà spunto anche da recenti riflessioni di Maher, ritenute particolarmente interessanti per il tentativo di superare la dicotomia pessimismo/ottimismo di approcci al processo di integrazione europea, che ricondurrebbe tradizionalmente i realisti alla prima e i liberalisti e costruttivisti alla seconda categoria. Egli ha infatti dimostrato che possono ravvisarsi elementi sia di pessimismo che di ottimismo in ciascuna delle tre correnti tradizionali (dunque, che vi sono realisti che guardano con ottimismo alle prospettive future dell'Unione e costruttivisti che invece hanno un approccio più scettico) pur mantenendo, ciascuna corrente, le peculiarità che la caratterizzano[85]. Sono queste ultime che ci interessano particolarmente per agevolare la comprensione di ciascun orientamento e, quindi, l'apporto teorico rispetto alle analisi sul processo di integrazione europea.

Realismo

Partendo dal *realismo*, scuola di pensiero classica della teoria delle relazioni internazionali – intesa addirittura come «*matrice disciplinaire*»[86] –, al suo interno si rinvengono diverse correnti, tutte però accomunate dalle stesse premesse basilari: una visione stato-centrica delle politiche mondiali, e una attenzione particolare alla rilevanza degli interessi statali nella politica

[83] POLLACK M.A., Theorizing the European Union: International Organization, Domestic Polity, or Experiment in New Governance?, in Annual Review of Political Science, 2005, pp. 357-398. Sul terzo aspetto, si veda anche, e*x multis*, L. HOOGHE, G. MARKS, *Multi-level Governance and European Integration*, Rowman & Littlefield Publishers, Inc., 2001.

[84] Per un'analisi esaustiva delle teorie delle relazioni internazionali si rinvia per tutti a J.-J. ROCHE, *Théories des relations internationales*, *cit.*, che in realtà presenta le molteplici e variegate correnti, distinguendo essenzialmente tra l'egemone realista (in cui individua anche un realismo liberale), gli approcci stato-centrici (all'interno dei quali colloca anche alcune teorie dell'integrazione europea, di cui si dirà), gli approcci non stato-centrici (in cui inserisce anche, oltre al transnazionalismo, le teorie critiche, di cui si dirà molto brevemente nel prosieguo).

[85] R. MAHER, International Relations Theory and the Future of European Integration, in *International Studies Review*, 2019, 0, pp. 1-26.

[86] Così J.-J. ROCHE, *op. cit*, p. 22.

internazionale[87]. Maher ci aiuta ad individuare tre aspetti fondamentali: la natura degli attori, la natura delle preferenze statali e il modo di intendere la struttura del sistema internazionale.

Quanto al primo aspetto, gli attori – che per i realisti sono prevalentemente statali, riconoscendo agli altri esistenti nel contesto internazionale (individui, organizzazioni, gruppi, società) un impatto limitato – sono entità politiche razionali e unitarie, che cercano di massimizzare i loro interessi. Le loro preferenze sono fissate, mantenendosi per tutti in due perenni preoccupazioni: sopravvivenza dello Stato e sicurezza nazionale. Quanto al sistema internazionale, la sua struttura è *anarchica* e dunque senza un governo centrale oltre gli Stati, cosa che costringe questi ultimi a competere continuamente tra loro e così ne influenza inevitabilmente i comportamenti. Le teorie realiste avrebbero un'ontologia materialista che guarda principalmente agli interessi materiali e alle considerazioni sul potere, piuttosto che a norme e idee, ritenendo quindi i comportamenti statali essenzialmente condotti dalla distribuzione delle capacità materiali. Quanto, poi, alla considerazione delle istituzioni internazionali, i realisti non ne riconoscono un ruolo autonomo e indipendente, ma le considerano meri strumenti statali, né le ritengono capaci di aiutare gli Stati a superare il rischio di conflitti inevitabilmente derivante dall'anarchia del sistema internazionale. Le istituzioni internazionali rifletterebbero dunque la distribuzione del potere ma, soprattutto a causa dell'incertezza sulle intenzioni e capacità degli altri Stati, non sarebbero in grado di vincolare i comportamenti statali: non possono dunque sostenere un'effettiva cooperazione senza potere coercitivo[88].

Come si riflettono queste premesse sul processo di integrazione europea?

Erdem fa notare che i realisti sostennero fortemente la concezione per cui la principale causa della fondazione della Comunità europea del Carbone e dell'Acciaio (CECA, 1950) e della Comunità economica europea (CEE, 1957) fu il contesto bipolare della Guerra fredda e la necessità per gli americani di sostenere l'Europa (attraverso la NATO e il Piano Marshall) per mantenere la sicurezza del continente rispetto alla minaccia sovietica. Dunque, l'integrazione europea avrebbe essenzialmente assecondato gli interessi strategici degli Stati Uniti. In quest'ottica, alcuni realisti hanno sostenuto che la fine della Guerra Fredda avrebbe fatto venir meno la ragion d'essere del costrutto europeo (qualcuno preconizzandone quindi la fine). Ciò è in linea con la recente analisi di Maher sull'individuazione di studiosi pessimisti e ottimisti rispetto alle prospettive future sul processo di integrazione europea.

[87] E. I. ERDEM, European Integration and International Relations Theory, in *Florida International University – Working Paper*, December 2006, p. 12 ss.
[88] R. MAHER, *op. cit.*, pp. 4-5; E.I. ERDEM, *op. cit.*, pp. 12-13. Sulle istituzioni, Maher riporta che i realisti le considerano "*epiphenomenal*".

L'autore infatti espone le tre principali ragioni dei realisti pessimisti sul futuro dell'Unione: l'assenza di una minaccia alla sicurezza esterna tale da costringere gli Stati membri a compiere i difficili passi verso una maggiore integrazione; le crescenti politiche di rinazionalizzazione in Europa; una Germania egemone sempre più riluttante a sostenere costi e oneri dell'Unione. Il primo di questi aspetti pone proprio l'accento sul fatto che sin dagli esordi l'integrazione europea ebbe un *imperativo geopolitico*, essendo essenzialmente pensata come risposta alla minaccia sovietica. Una volta venuta meno quest'ultima, l'imperativo strategico per gli Stati europei di integrare le loro economie, società e sistemi politici sarebbe svanito di conseguenza. L'assenza di una minaccia esterna (che, secondo i realisti pessimisti rappresenterebbe la principale ragione di unione) sarebbe poi ulteriormente aggravata dalla riduzione della presenza di truppe statunitensi in Europa dalla fine della Guerra Fredda. Dunque, verrebbero a mancare gli elementi che rendevano di fatto impossibile una guerra tra Stati europei, ossia la minaccia sovietica e la presenza consistente di truppe USA in territorio europeo, mentre aumenterebbero le instabili multipolarità interne[89].

Dall'analisi di Maher emergono nondimeno le visioni di realisti che guardano con ottimismo alle prospettive future dell'integrazione europea, almeno su tre profili: quello per cui una maggiore integrazione sarebbe indispensabile per rendere l'Europa una potenza maggiore, al fianco di USA, Cina e Russia; quello della perdurante necessità di vincolare la Germania all'interno deldenso quadro istituzionale; quello relativo al dilemma della sicurezza tra Stati membri e Unione, che secondo questi studiosi sarebbe in realtà benigno, perché consentirebbe soluzioni comuni a problemi comuni e anche perché molti dei fattori di conflitto in passato sono oggi minori o assenti.

Quanto al primo punto, in particolare, i realisti ottimisti auspicano una maggiore cooperazione su sicurezza e difesa che consentirebbe all'Unione di mettere in comune risorse e tecnologie derivanti dagli Stati membri: «*absent deeper cooperation and even integration in foreign policy and defense, the EU would remain strategically dependent on the United States, and Europe's interests would be permanently subordinated to American strategic concerns and priorities*»[90]. Oltre a questi aspetti, dalla concezione realista delle istituzioni internazionali inoltre deriverebbe la considerazione del processo di integrazione europea quale prodotto del potere degli Stati membri realizzato per soddisfarne gli interessi, che però non sarebbe, viceversa, capace a sua volta di incidere sui suoi membri in modo significativo[91], specie data la suddetta assenza di potere coercitivo (si tornerà su questo aspetto come elemento distintivo della sovranità statale e invece assente nell'Unione).

Liberalismo

[89] Ibidem.
[90] R. MAHER, *op. cit.*
[91] E.I. ERDEM, *op. cit.*, pp. 13-14.

Passando al *liberalismo,* scuola di pensiero che coinvolge pur essa diverse correnti, anche qui è possibile ravvisare un nucleo comune. Riprendendo i tre aspetti fondamentali già richiamati per i realisti, sostanzialmente i teorici del liberalismo si caratterizzano per il riconoscimento: di un primato degli individui e di gruppi privati tra gli attori del contesto internazionale; di *anarchia* come caratteristica del sistema internazionale ma anche *interdipendenza* tra gli attori operanti in esso; di un ruolo centrale delle istituzioni internazionali nella gestione delle interazioni tra Stati. La centralità riconosciuta all'interdipendenza tra gli Stati consentirebbe infatti di mitigare l'anarchia tipica del contesto internazionale e di influenzare il comportamento degli attori statali, incentivandoli a trovare soluzioni comuni a problemi comuni e a realizzare guadagni congiunti. In questo processo, si capisce la rilevanza delle istituzioni internazionali nel promuovere e facilitare tale interdipendenza e reciprocità tra Stati[92] (sull'interdipendenza come elemento di ridimensionamento del concetto classico di sovranità e come caratteristica dell'attuale contesto anche europeo, *infra,* par. 2.2).

Quanto al processo di integrazione europea, poiché le politiche interne hanno per il liberalismo un peso rilevante nella politica internazionale (come anche le relazioni tra società civile e istituzioni statali, gli interessi commerciali e l'opinione pubblica), esso offrirebbe interessanti spunti per spiegarne lo sviluppo istituzionale. Erdem fa notare in particolare che i liberalisti rintracciano le cause primarie della fondazione del costrutto europeo nella comunanza di bisogni tra Stati europei, nel garantire pace e welfare che erano stati per troppo tempo assenti a causa delle perpetrate belligeranze. In ciò, i liberalisti sarebbero spesso accostati ai funzionalisti, tra i teorici dell'integrazione europea (vedi *infra,* par. 2.1.), ma a differenza di questi ultimi accetterebbero (come si è detto) la rilevanza degli interessi domestici e del nazionalismo. Inoltre, poiché le istituzioni internazionali assumono un ruolo centrale nell'incentivare la cooperazione tra Stati, i liberalisti considerano le istituzioni europee non semplici strumenti del potere statale (come per i razionalisti), ma capaci di incidere effettivamente sugli interessi e sui comportamenti degli Stati membri. Tali studiosi avrebbero perciò considerato l'evoluzione del processo di integrazione europea come emblematica della cooperazione tra Stati membri e dunque ancora più promettente dopo la fine della Guerra Fredda (in contrapposizione alla visione realista), così contribuendo meglio a spiegare sia il ruolo crescente che ha avuto negli anni la Corte di giustizia nel far avanzare il processo di integrazione e nel rapportarsi con gli Stati membri, che l'allargamento di tale processo ad altri Stati europei. Nondimeno, l'autore ravvisa qualche debolezza della posizione liberalista nel riconoscimento della centralità delle entità statali e nella considerazione del processo di

[92] R. MAHER, *op. cit.,* p. 4. L'autore, peraltro, richiama tra gli altri anche Moravcsik, come principale esponente di questa scuola di pensiero, precisando che lo stesso sottolinea un particolare aspetto, ossia che gli Stati rappresentano i sottogruppi della società, i cui interessi cercano di avanzare.

integrazione come fenomeno essenzialmente internazionale. Questo porterebbe i liberalisti a sottovalutare l'importanza delle dinamiche transnazionali non statali e degli attori diversi da questi nell'influenzare le istituzioni europee. Inoltre, anche le teorie liberaliste sarebbero razionaliste, cosa che escluderebbe la rilevanza di norme, idee e tutti gli altri aspetti che coinvolgono la vita sociale e fuoriescono da calcoli razionali.

Riprendendo poi l'analisi di Maher che distingue tra pessimisti e ottimisti all'interno della stessa scuola di pensiero, l'autore individua tre ragioni principali che secondo gli ottimisti sosterrebbero una resilienza dell'Unione: l'elevato livello di interdipendenza economica tra gli Stati; la fitta rete di istituzioni; l'impegno condiviso di principi democratici tra gli stessi membri. Questi tre elementi sarebbero correlati e si rafforzerebbero a vicenda, rendendo una eventuale divisione non solo costosa ma anche difficile da realizzare. Non mancano però i pessimisti, che prevedono al contrario una disintegrazione del costrutto europeo nel prossimo futuro, basata su: le esternalità negative dell'integrazione economica; l'eccessiva complessità istituzionale (che porta a rischi sistemici e reciproche vulnerabilità); le perplessità derivanti dalle dinamiche politiche – interne agli Stati membri e proprie dell'Unione – che ribadirebbero il deficit democratico e la crisi di legittimazione dell'Unione[93].

Costruttivismo

Quanto poi al *costruttivismo*, anche qui si tratta di una scuola di pensiero policentrica, i cui fautori sarebbero accomunati da un nucleo principale di assunti teorici, che arriva agli studi sull'integrazione europea relativamente tardi, concentrandosi particolarmente sugli effetti della stessa sui popoli e sui governi europei[94].

Maher ricorda che sono due gli aspetti fondamentali che distinguono i costruttivisti dalle altre due scuole di pensiero: il contesto in cui agiscono gli Stati e gli altri attori è sia materiale che sociale; i contesti sociali possono costituire gli Stati e gli altri attori. Dunque, un approccio che va oltre la prospettiva materialista delle altre due scuole di pensiero, sottolineando come le strutture materiali assumano il loro significato attraverso il contesto sociale e soprattutto che gli interessi e le identità non siano realtà date, ma *costruite socialmente*. Ciò consente di comprendere che tali interessi, le stesse identità, possono cambiare, anche tramite l'interazione con altri attori. In questo contesto, le istituzioni internazionali possono fornire direttive per incentivare comportamenti socialmente appropriati per gli Stati e gli altri attori e così stimolare processi di socializzazione[95].

[93] R. MAHER, *op. cit.*, p. 5.
[94] E.I. ERDEM, *op. cit.*, p. 19.
[95] R. MAHER, *op. cit.*, p. 5 ss.

Ciò secondo alcuni costruttivisti porterebbe anche all'emersione di una "identità condivisa" tra i vari attori del contesto internazionale, stimolando una maggiore cooperazione.

Erdem sottolinea la differenza rispetto alla concezione razionalista – propria sia del realismo che del liberalismo – degli attori del contesto internazionale, che tenderebbero a perseguire ed aumentare i loro interessi. I costruttivisti, invece, accantonerebbero questa logica utilitaristica, sostituendo "la logica delle conseguenze alla logica dell'adeguatezza"[96] quanto ai comportamenti statali. Dunque, i costruttivisti insistono sulla rilevanza di idee, norme, culture e identità nelle politiche internazionali. Ciò si traduce anche nella considerazione del processo di integrazione europea: molti studiosi costruttivisti hanno sostenuto che le istituzioni europee modellano non solo le preferenze ma anche l'atteggiamento e le identità dei governi e degli individui degli Stati membri[97]. Erdem elogia l'apporto costruttivista all'analisi sul costrutto europeo, che sarebbe parziale se limitata agli aspetti razional-utilitaristi propri delle altre due scuole di pensiero, ritenendo dirimente la considerazione della costruzione sociale del comportamento degli Stati, delle loro preferenze e delle scelte dei leader a livello domestico, sovranazionale e internazionale di governance[98]. Per meglio comprenderne le caratteristiche, anche qui va inserito un cenno all'analisi di Maher, che rintraccia tra i costruttivisti tanto pessimisti quanto ottimisti. Gli ottimisti riterrebbero esistenti buoni motivi per l'unità dell'Unione, rintracciabili nell'emersione di una identità transnazionale europea e nella socializzazione di Stati e individui nell'ambito di strutture e istituzioni europee. Dunque, un'identità europea possibile, che completerebbe le identità nazionali senza sostituirsi ad esse. I pessimisti, invece, sosterrebbero il fallimento dell'emersione di un'effettiva identità europea, dopo sessant'anni di integrazione, nonché l'assenza di effettiva socializzazione e europeizzazione.

Altre correnti

Erdem aggiunge infine un riferimento alle ulteriori correnti delle *teorie critiche* delle relazioni internazionali e al *Marxismo*, quanto all'analisi su origini e sviluppo del processo di integrazione europea, puntando su due argomenti in particolare: essi vedono tale processo come posto al servizio

[96] E.I. ERDEM, *op. cit*., p. 19: « Instead of 'logic of consequences', constructivism follows 'logic of appropriateness' for state behavior». Così anche M. A. POLLACK, *op. cit*., p. 365, che fa riferimento all'edizione speciale del *Journal of European Public Policy* del 1999 come punto di svolta in tal senso.

[97] M.A. POLLACK, ibidem, che, riportando testualmente l'estratto di un articolo di quell'edizione speciale, ribadisce che l'integrazione europea veniva riconosciuta da quegli autori come avente un "*trasformative impact*" sugli Stati europei.

[98] E.I. ERDEM, *op. cit*., p. 25: «*Rationalist theories including realist and liberal theories of IR generally follow utilitarian logics of social behavior while constructivists deal with inter-subjective and normative dimensions of human action. This also applies into state behavior and national interests. The social world involves both logics of consequences (rationalists follow) and logics of appropriateness (constructivists argue)*».

delle classi capitaliste e degli interessi commerciali europei, dunque, come fenomeno eminentemente economico.

L'autore critica l'approccio marxista perché lo considera esclusivamente deterministico e dunque, data la sua ontologia materialista, tale da ignorare tutte le altre dinamiche non materiali, come appunto idee, norme, culture e identità, che invece giocherebbero un ruolo rilevante. Nondimeno, riconosce a queste teorie il merito di sottolineare la questione del *deficit democratico* nel processo di integrazione, che – come si è già accennato – merita una qualche attenzione[99].

L'esposizione in pillole dell'apporto di queste teorie all'analisi del processo di integrazione europea dimostra la capacità degli Stati di cooperare per obiettivi comuni, e inoltre il ruolo sempre più preponderante delle istituzioni europee sollecita uno studio che vada oltre la prospettiva domestica nell'osservazione del fenomeno[100]. Pollack ha notato al riguardo che la discussione tra razionalisti e costruttivisti – forte negli anni Novanta – rifletteva il più ampio dibattito di quelle scuole di pensiero nella teoria delle relazioni internazionali sul processo di integrazione europea, proprio perché «*the EU serves as a laboratory for broader processes such as globalization, institutionalization, and socialization*»[101]. Lo stesso autore, tuttavia, dava conto del fatto che nel corso del tempo, come si è accennato, diversi studiosi si sono approcciati al processo di integrazione europea non solo attraverso le lenti della teoria delle relazioni internazionali, ma anche considerandolo come sistema (politico) simile a quelli domestici. Si tratta di analisi comparative, che considererebbero l'UE come un sistema politico in cui le regole formali modellano il comportamento degli attori governativi e non, nonché come una variante di sistemi politici esistenti.

Pur non essendo oggetto delle nostre riflessioni, ad esse si farà cenno nel prosieguo nella misura in cui analizzano l'UE guardandola dalla prospettiva della separazione dei poteri, sia in senso orizzontale che verticale[102]. Nondimeno, è bene dare atto che esse si sono aggiunte alle analisi sul processo di integrazione, coesistendo con il primo approccio della teoria delle reazioni internazionali e, successivamente, con un terzo, ulteriore, approccio, come riportato da Pollack: «*the traditional international relations and comparative politics approaches to the EU now coexist with yet a third approach, typically labeled the governance approach, which draws from both international relations and comparative politics and which considers the EU not as a traditional*

[99] E.I. ERDEM, *op. cit.* p. 21.
Per un'analisi più ampia sulle teorie critiche si veda J.-J. ROCHE, *op. cit*., p. 189 ss.
[100] Ancora E.I ERDEM, *op. cit*., pp. 27-28.
[101] M.A. POLLACK, *op. cit*., p. 368.
[102] M.A. POLLACK, *op. cit*., pp. 368-379, ma anche p. 380. Delle analisi comparatistiche dà brevemente conto anche E.I. ERDAM, op. cit., pp. 25 e 27-28.

international organization or as a domestic political system, but rather as a new and emerging system of "governance without government"»[103].

Pare utile, a questo punto, soffermarsi un momento sul "*governance approach*", perché consente di fare luce su alcuni profili che riprendono i concetti in parte già esposti su legittimità e deficit democratico.

Pollack riferisce che questo approccio considera la *governance* UE come non gerarchica, caratterizzata da networks di attori pubblici e privati impegnati per la risoluzione di problemi comuni attraverso norme informali e istituzioni formali. Gli studiosi di questo approccio sottolineano inoltre la necessità di un nuovo vocabolario per cogliere le caratteristiche proprie del costrutto europeo, scartando la concezione comparativista che lo vedrebbe invece come variante di sistemi esistenti. Essi pongono inoltre l'accento sulla capacità dell'Unione di favorire deliberazione e persuasione nell'elaborazione delle politiche, consentendo agli attori di essere aperti a cambiare le proprie preferenze.

Ancora, gli studiosi del *governance approach*, come i comparativisti, sottolineano il problema – soprattutto dal punto di vista normativo – del deficit democratico, concentrandosi però particolarmente sulla promessa dell'Unione come democrazia deliberativa «*in which collective problem solving offers a normatively superior alternative to majoritarian rule in a multinational union*»[104]. L'autore analizza poi la letteratura sulla governance soffermandosi su quattro aspetti chiave: il concetto di "governance" come derivato sia dalla letteratura comparativa che da quella delle relazioni internazionali; le prime applicazioni di tale concetto all'Unione europea, nelle letterature sulla "governance multilivello" e sulle reti politiche; la letteratura sulle capacità di governance degli Stati membri e delle istituzioni dell'Unione nonché sui problemi di legittimità relativi a queste ultime; nuove considerazioni sull'Unione quale processo di sovranazionalismo deliberativo capace di risolvere dilemmi normativi. Non potendo ripercorrere l'intera analisi svolta da Pollack, riporteremo solo gli aspetti funzionali al percorso argomentativo che vogliamo tracciare.

In particolare, quanto al concetto di "governance", riferendosi a diversi studiosi, l'autore in sostanza lo definisce come *quell'insieme di interrelazioni tra attori pubblici e privati per l'allocazione di risorse e la fornitura di servizi.* Benché questa considerazione non sia nuova, l'autore nota che l'adozione di politiche liberiste/neoliberali in Europa e negli Stati Uniti avrebbe stimolato un'apertura in tal senso, portando a ridurre le dimensioni del settore pubblico e a deporre maggiori responsabilità sulla fornitura dei servizi in capo ai settori privato e volontario. Sarebbe

[103] M.A. POLLACK, *op. cit.*, p. 380.
[104] Ibidem.

questo passaggio "dal governo alla governance" – intendendo il secondo fenomeno *più comprensivo* del primo – a caratterizzare il processo di integrazione europea: l'approccio governance sottolineerebbe infatti la rilevanza di reti non gerarchiche e di interazioni pubblico-privato, riconoscendo nel costrutto europeo ciò che è stato chiamato "*governance without government*" (cui si è fatto cenno *supra*), con le perplessità che ne conseguono (soprattutto in termini di democraticità).

La crescente interdipendenza tra governi e fattori non governativi che si trovano a livelli territoriali diversi, è stata indicata come "governance multilivello" e Pollack riporta qualche autore che – nell'analizzare il fenomeno in senso verticale – ha parlato in tal senso di un notevole "passaggio di autorità" dai governi nazionali all'arena europea e ai governi subnazionali e nazionali, come fenomeno abbastanza diffuso in diversi Stati membri, mentre altri avrebbero rilevato più gli aspetti orizzontali di interrelazione con attori privati.

L'autore riferisce poi di una parte di studiosi che, a partire dagli anni Settanta ma con un incremento negli anni Novanta, ha esaminato il fenomeno della "europeizzazione", ossia quel processo tramite cui istituzioni e politiche europee influenzerebbero quelle degli Stati membri[105].

L'autore dà infine conto – e questo è l'aspetto che più ci interessa – di quella corrente del *governance approach* che ha sottolineato la critica normativa all'Unione europea. In questa prospettiva, l'Unione avrebbe minato la governance a livello domestico – erodendo diversi ambiti di intervento a livello nazionale – senza riuscire a garantire una capacità di governance sostanziale e democraticamente legittimata a livello sovranazionale. Da ciò anche deriverebbe, dunque, il discorso sul deficit democratico: in questo scritto del 2005, l'autore dava conto delle molte posizioni pessimistiche in tal senso e riportava anche la posizione di Weiler relativa alla mancanza – a prescindere da interventi di carattere istituzionale – di un "senso di comunità", di un "*we-feeling*" quale base costituente di una democrazia sovranazionale. Queste ed altre considerazioni portavano i teorici della governance a ravvisare la profonda crisi di legittimazione che stava interessando l'Unione in quel periodo, insistendo sulla necessità di aumentare le capacità di governance dell'Unione e la responsabilità democratica. All'indomani del nuovo millennio questi studiosi ravvisavano dunque, come riferisce l'autore, un minore affidamento al concetto di *output legitimacy*, rispetto al passato, e le sempre maggiori richieste di aumentare la *input legitimacy*, in termini di maggiore responsabilità democratica delle istituzioni europee, riconducibili a tre principali proposte: parlamentarizzazione, costituzionalizzazione e deliberazione. Tutto ciò pare perfettamente in linea con quanto si è già detto sui tipi di legittimazione e, in particolare, sulle

[105] POLLACK, *op. cit*., p. 384, laddove parla di "Europeanization". Qualcosa di simile, quantomeno nell'analisi del funzionamento del meccanismo comunitario rispetto agli apparati statali, viene proposta da E. CANNIZZARO, *Diritto internazionale*, Quinta edizione, Giappichelli, 2020, p. 330 (cfr. *infra*).

conseguenze che poi dopo, specie con la crisi economica, hanno posto ulteriori perplessità quanto all'opportunità di considerare l'*output legitimacy*.

Prime considerazioni conclusive e prosecuzioni

Questo quadro così brevemente delineato ci aiuta a fare luce sulle principali correnti che "da uno sguardo esterno" hanno analizzato il processo di integrazione europea nella sua evoluzione e sino ai giorni nostri, cercando di rintracciarne prospettive future. In questo senso, il contributo di Maher, di cui si è già detto, pare particolarmente interessante per un'attendibile comprensione, nella sua capacità di rintracciare presso ciascuna scuola di pensiero studiosi sia ottimisti che pessimisti rispetto al futuro dell'integrazione europea, tutti con posizioni razionalmente argomentate: «*The differences within the three perspectives are in some ways more interesting than the differences across them. Economic integration, for example, can generate positive externalities that support European integration but can also produce negative externalities that threaten the EU's cohesion. The structure of the international system generates compelling reasons for the EU to stick together to enhance its strategic autonomy and influence but also creates expectations for why it will struggle to stay united in the absence of an external threat. Social environments can lead to a convergence of interests and identities among states and other agents, but they can also reinforce perceptions of mistrust, rivalry, and hostility*»[106].

Con queste consapevolezze è possibile dunque mettere meglio a fuoco il fenomeno dell'integrazione europea, analizzando due percorsi che in qualche modo derivano dai discorsi sulla teoria delle relazioni internazionali, o comunque ad essi si legano, guardando da un lato alle dinamiche di cooperazione tra gli Stati membri (le teorie dell'integrazione europea) e dall'altro alla loro individualità e a quella dell'Unione come soggetti di diritto internazionale (la sovranità).

2. *Segue*. Due imprescindibili diramazioni

Delineato molto brevemente lo "spazio" che circonda l'oggetto principale del nostro studio, ossia il contesto internazionale e le caratteristiche principali delle relazioni tra i soggetti che in esso si muovono ed interagiscono, inevitabilmente contaminandosi, abbiamo visto come i diversi approcci teorici richiamati abbiano anche cercato, partendo dalle medesime premesse, di spiegare le dinamiche tra Stati nel contesto sovranazionale europeo. I due profili di analisi che seguono sono intesi come diramazioni di questo preliminare discorso. Da un lato, un focus sul processo di

[106] MAHER, *op. cit.*, p. 18.

integrazione e sulle teorie dell'integrazione europea. Dall'altro, un discorso sulle dinamiche interazioni tra attori-soggetti della comunità internazionale (qui, in particolare "solo" tra Stati e, eventualmente, tra questi e l'Unione europea), inevitabilmente riferito al concetto di sovranità. Procederemo, quindi, nell'ordine prospettato.

2.1. *Spunti sulle teorie dell'integrazione europea*

La necessità un riferimento alle teorie dell'integrazione europea si impone nel quadro di un'analisi volta ad indagare ciò che l'Unione europea è ed appare ad oggi, il suo modo di governare e gestire le criticità attuali (e quasi ormai croniche) e, soprattutto, le sue prospettive venture[107]: invero, per "*European integration theory*" può intendersi ampiamente «*the field of systematic reflection on the process of intensifying political cooperation in Europe and the development of common political institutions, as well as on its outcome*»[108].

Prendendo le mosse dalle teorie delle relazioni internazionali, è qui utile una veloce rassegna sull'integrazione sovranazionale e sulle teorie ad essa specificamente dedicate. A seguire, il percorso di analisi approderà ad alcune considerazioni di fondo sul tema della sovranità.

Senza pretese di esaustività, e ai limitati fini del presente lavoro, ci pare necessario offrire nuovi spunti per comprendere le attuali sfide e i nodi che mettono in crisi il processo di sviluppo dell'Unione europea: ciò che verificheremo a partire dal modo in cui il caso della protezione dei dati personali ha a che fare, in termini di incidenza e risolvibilità, con questo stato di cose (come verrà meglio affrontato nei paragrafi 5, 6 e 7 di questo capitolo, nonché poi soprattutto nei capitoli III e IV). Pertanto, tenteremo qui di delineare un quadro generale delle teorie sull'integrazione europea come le premesse a tali discorsi; nella parte finale, utili prospettive saranno ricavate dal riferimento all'interessante esperimento proposto da Hooghe e Marks, con l'analisi di tre orientamenti sulle questioni problematiche che coinvolgono l'Unione, come la crisi dell'Eurozona, la crisi migratoria, la Brexit e non da ultimo le sfide illiberali. Con riferimento a tale ultima questione, ne riproporremo i risultati.

---

[107] Tra i molteplici studi, ma anche letture innovative e finanche timide possibili soluzioni: D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *Theory and reform in the European Union*, Manchester University press, 2003, p.7; anche se il riferimento è soprattutto a M. FICHERA, *The foundations of EU as a polity*, Elgar, 2018, in particolare a p. 21 ss., in cui comincia ad esporre la propria lettura del processo di integrazione all'interno della "meta-logica" della sicurezza del processo liberale europeo e, nel farlo, propone di riprendere degli elementi dalle teorie del processo di integrazione europea. Si riprenderà spesso questo concetto fondamentale, nel prosieguo.

[108] A. WIENER, T. DIEZ, Introducing the Mosaic of Integration Theory, in A. WIENER, T. DIEZ, *European Integration Theory* (second edition), Oxford University Press, 2009, p. 4. *Ibidem*, pp. 2-6, per un'esplicazione dei due termini costitutivi "teoria" e "integrazione", nonché per l'importanza di simili teorie nello studio dell'integrazione europea.

Nel riferire di tali diverse correnti, le premesse di teoria delle relazioni internazionali saranno d'ausilio.

Come si sa, le prime scuole di pensiero si preoccupavano essenzialmente di concepire dei metodi per evitare ulteriori conflitti. Il riferimento è dunque, inevitabilmente, alle principali correnti del *federalismo* e del *funzionalismo*, ma anche al meno diffuso *transazionalismo*.

Federalismo

Il *federalismo* è stato un potente ideale[109], che avrebbe trovato il suo caposaldo nel celeberrimo Manifesto di Ventotene di Altiero Spinelli ed Ernesto Rossi del 1941 (ispirato al famoso intervento di Cousdenhove-Kalergi tra le due guerre mondiali, *Pan-europa*) e si caratterizza appunto per l'approccio federale al processo di integrazione europea[110]. Di ispirazione idealista, il federalismo considera il conflitto non endemico alla comunità internazionale, ma evitabile attraverso la creazione di apposite organizzazioni internazionali, ritenendo che il nazionalismo sia invece la causa principale delle conflittualità e proponendo, pertanto, di indebolire lo Stato-nazione sia dall'alto, con un trasferimento di competenze a livello superiore, che dal basso, riattribuendone delle altre alle entità regionali e locali[111]. L'idea di fondo dell'approccio federalista è quella, dunque, di creare, tramite accordo, diversi livelli di autorità che consentano di conciliare le diverse comunità politiche ma al tempo stesso mantenerne le relative peculiarità.

Gli aspetti salienti: «*the dialectics of power-sharing in a compound political setting; its emphasis on in-built democratic arrangements linking different levels of governmental authority; its often flexible interpretation of the sovereignty principle; its focus on constitutional issues touching upon sensitive areas of individual and collective liberties, legislative representation and the allocation of competences; and its deeper concern about how to organise in a mutually reinforcing way the concurrent demands for 'unity in diversity'*»[112]. I federalisti hanno infatti posto particolare enfasi sulla ricerca del costante equilibrio tra unità e diversità[113], ritenendo gli Stati-nazione anacronistici e, specie dopo le guerre mondiali, viziati da una profonda crisi strutturale che può essere sanata solo a un livello superiore, attraverso accordi democratici. L'accento sul processo democratico è infatti una caratteristica fondamentale dell'approccio federalista, che ravvisa nella rappresentatività delle

[109] POLLACK, *op. cit.*, p. 371.
[110] R. SCHWOK, *Théories de l'intégration européenne – Approches, concepts et débats*, Editions Montchrestien, 2005, p. 23.
[111] Ibidem, pp. 28-29.
[112] D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *Theory and reform in the European Union*, cit., p. 10.
[113] R. SCHWOK, *Théories de l'intégration européenne – Approches, concepts et débats*, cit., pp. 29-30 : « *Le fédéralisme doit être compris comme un difficile compromis entre, d'une part, une pression unitaire, c'est-à-dire où les différentes unités sont soumises aux pressions homogénéisantes du «centre», et, d'autre part, la souveraineté respective des différents États, peuples, nations et communautés* ».

istituzioni centrali il mezzo per spronare i popoli europei[114]: *«Une des vertus incontournables de l'approche fédéraliste est de rappeler que l'Union européenne ne peut pas faire éternellement abstraction d'un débat démocratique sur sa forme politique finale»*[115]. In tal senso, infatti, il federalismo nasceva col proposito di incoraggiare la diversità democratica istituendo un sistema di sfere di autorità coordinate ma indipendenti basate su una divisione del potere tra agenti statali e federali; emerse presto, tuttavia, il limite di questo progetto nella resistenza dei governi nazionali a rinunciare alla sovranità statale in favore di un governo federale (per cui, secondo Spinelli, la soluzione avrebbe potuto rintracciarsi nel c.d. metodo costituente)[116].

È stato infatti notato che, per quanto l'Unione potrebbe già intendersi come un sistema federale con separazione costituzionalmente garantita dei poteri tra livelli sovranazionale e nazionale nonché doppio sistema di rappresentanza tramite Parlamento europeo e Consiglio, comunque la questione più difficile resta proprio la distribuzione dei poteri tra i livelli di governo[117]: «*as most federalists have acknowledged, however, the difficulty of the task lay not so much in convincing the European peoples of the need for a federation, but in convincing them that they, rather than their national governments, must create it*»[118]. Ulteriori perplessità derivano inoltre dall'ambiguità concettuale, che vedrebbe il federalismo non solo come metodo d'analisi, ma anche come strumento di contrasto politico e, in quest'ultimo senso, dalla possibile – per quanto paradossale – deriva verso una sorta di "nazionalismo europeo" nella misura in cui la prospettiva sarebbe quella di uno Stato federale come stadio finale[119] (un po' quello che si è detto rispetto alla posizione di Mancini e alla reazione di Weiler al riguardo). Aldilà dei limiti e delle perplessità che, come diremo subito, portarono alla consolidazione dell'alternativa corrente funzionalista, va comunque dato atto di quello che è stato riconosciuto come il più grande contributo del federalismo alla causa dell'unità europea: «*in the 'inclusive' political community, power and responsibility should be seen as being mutually*

[114] D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *Theory and reform*, cit., p. 13.
[115] R. SCHWOK, *op. cit*., p. 37.
[116] D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *Theory and reform*, cit., pp. 13-14, in cui si precisa: «*The justification of Spinelli's 'constituent method' lay in the belief that such an assembly was the only acceptable body to transform the possibility of popular participation in the affairs of the federation into political reality. The constitution was to be based on a declaration of fundamental rights, democratic institutions and the separation of powers: it was believed that a balanced structure of national and federal competences based on the principle of dual federalism would preserve national identity and diversity in a way compatible with the democratic ethos. Thus it was agreed that the federation should have limited but real powers, with the remaining spheres of competence resting on state jurisdiction*».
[117] M.A. POLLACK, *op. cit*., p. 372.
[118] D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *Theory and reform*, cit., p. 14.
[119]R. SCHWOK, *op. cit*., pp. 33-34.

supportive, rather than as a competitive tussle for political authority between the collectivity and the segments»[120].

Funzionalismo

Anche se nell'immediato dopoguerra la riorganizzazione dell'Europa non seguì la via del federalismo[121], la carica idealista di quest'ultimo influenzò il differente *funzionalismo*. Infatti, tra la situazione postbellica e l'inizio della Guerra fredda divenne abbastanza chiara la necessità per gli Stati europei di collaborare e di creare istituzioni comuni, e in tal senso ebbero il favore degli Stati Uniti (il Piano Marshall, per esempio, aveva il chiaro intento politico di sostenere la stabilità del sistema europeo ed evitare tensioni che avrebbero potuto agevolare l'espansionismo sovietico). Il Congresso dell'Europea a L'Aja del 1948 palesò l'idea diffusa di un'Europa unita e fece emergere il confronto tra la tendenza federalista e quella funzionalista[122]. In quest'ultima direzione si sviluppò l'integrazione negli anni seguenti, per merito dell'idea di Monnet – incisa nella lapidaria Dichiarazione di Schuman – che verrà meglio qualificata come *federalismo funzionale*, così intesa per essere "funzionalista nella concezione ma federalista nella prospettiva"[123].

La teoria funzionalista fu invero sviluppata tra gli anni Trenta e Cinquanta principalmente da Mitrany che riteneva che gli affari internazionali potessero essere meglio gestiti da agenzie specializzate amministrate da esperti piuttosto che dai rappresentanti dei governi, ciò facendo tramite delle forme che dovevano corrispondere alle *funzioni* da esercitare[124].

Il *funzionalismo*, riconducibile alla più ampia categoria dei primi *approcci liberali* della teoria delle relazioni internazionali (v. *supra*, par. 1) partiva dalla centralità degli Stati e della loro sovranità in un mondo incline ai conflitti[125], vedendo nella costruzione di comunità internazionali il rimedio alla frammentazione della comunità mondiale in gruppi rivali (prodotta dal nazionalismo e dall'anarchia internazionale); il suo concetto fondamentale stava nella previsione di comuni interessi tra gli attori coinvolti nel processo di integrazione e quindi di mezzi non coercitivi di

[120] D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *op. cit.*, p. 13. Qui si insiste peraltro sul l'impegno dei federalisti verso il processo democratico e l'opposizione a concezioni utilitaristiche di convergenza di interessi come condizione preliminare per trasferimenti di "substantive public loyalty", cfr. p. 15.
[121] P. GRAGLIA, *op. cit.*, p. 14.
[122] Ibidem, pp. 15-17. Qui in realtà l'autore indica, accanto a federalisti e funzionalisti, anche la corrente unionista, che vedeva l'Europa come un insieme di Stati sovrani che sarebbero dovuti rimanere tali.
[123] D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *op. cit.*, p. 14. Nello stesso senso anche R. SCHWOK, *op. cit.*, p. 40 : «*même Jean Monnet, le fonctionnaliste, était inspiré par un courant de pensée de type fédéraliste. Il ne partageait certes pas la méthode préconisée par les fédéralistes classiques comme Altiero Spinelli, mais il poursuivait le même objectif final. Les sentiments et les idées fédéralistes ont influencé l'évolution de l'UE et ont aidé à définir à la fois ses problèmes et ses réponses*».
[124] R. SCHWOK, *op. cit.*
[125] Così, infatti, lo spiegano A. WIENER, T. DIEZ, Introducing, *cit.*, p. 7.

risoluzione dei problemi[126]. Di qui la costruzione, a livello europeo, di istituzioni comuni che avrebbero consentito il perseguimento di obiettivi condivisi e la realizzazione del benessere generale, nonché la riduzione dei conflitti. Ma nel ritenere ciò, Mitrany era inteso come sostenitore di un "*technocratisme non dogmatique*", guardando non tanto a una forma ideale di società internazionale quanto alle sue funzioni essenziali[127]. Questo aspetto è dirimente per segnare la differenza con l'approccio federalista: proprio in quanto limitata alle aree tecniche ed economiche, l'integrazione funzionale non richiede né persegue la creazione di un nuovo potere sovrano a livello superiore e quindi non presenta alcuna sfida alla sovranità degli Stati: «*the 'functional imperative' (...) rejected the inevitability of constitutional requirements and fixed divisions of political authority, instead focusing on problems which, although they cannot really be ignored, cannot be solved separately by each government acting alone. This has been termed as the 'unitary trap'*»[128]. In questa direzione, lo sviluppo dell'integrazione veniva pensato sempre attraverso il riconoscimento e perseguimento di interessi comuni, con la inevitabile tendenza ad estendere la cooperazione, a poco a poco, ad altre sfere di azione rilevanti. In questo senso risultò particolare l'idea prospettata da Monnet, che era orientato ad evitare i confronti diretti sulle questioni più controverse (specie implicanti la sovranità nazionale) ritenendo che delle solidarietà "di fatto" si sarebbero sviluppate a mano a mano che i successi funzionali avrebbero mostrato i loro frutti[129].

Il funzionalismo è stato criticato per essere eccessivamente tecnocratico e, privilegiando una gestione tramite dei funzionari non eletti democraticamente, eccessivamente staccato dalle realtà politiche – di cui invece, in qualche modo, il federalismo si faceva portavoce. Tra i meriti, invece, senz'altro esso ha posto le basi per il neo-funzionalismo e il relativo concetto di "*spillover funzionale*" (di cui si dirà a breve) ed ha consentito l'incremento di agenzie specializzate in seno all'Unione[130]. L'aspetto fondamentale da ribadire sul funzionalismo, su cui si vuole puntare l'attenzione per comprendere com'è avvenuta la costruzione europea e dunque spiegare meglio il discorso che seguirà, è proprio quello che, rigettando aspetti politici, fa affidamento su *strumenti giuridici* per avanzare l'integrazione nei settori economici: «*la méthode fonctionnaliste confirme cette idée en ce qu'elle est pétrie par la conviction que les Etats doivent être unis par des liens*

[126] D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *op. cit.*, pp. 8-9.
[127] R. SCHWOK, *op. cit.*, p. 42.
[128] D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *op. cit.*, p. 9. Gli stessi autori, poi, precisano su Mitrany: «*Functionalism in the Mitranian tradition is above all a theory of international society based on the principle of technical self-determination, reliance upon non-coercive means of international community-building, and an inherent mistrust of constitutional prescriptions of power-sharing. Mitrany's main concern was how to replace territorially defined structures of decision-making with international functional agencies, leading towards a 'working international system'*».
[129] R. SCHWOK, *op. cit.*, p. 37. Celeberrima è la frase emblematica del c.d. federalismo funzionale di Monnet: "federate i loro portafogli, federerete i loro cuori".
[130] R. SCHWOK, *op. cit.*, pp. 43-44.

juridiques plutôt que politiques, ces derniers étant perçus comme autant de risques de voir ressurgir des rapports d'affrontement et de confirmation»[131]. Questo approccio settoriale è proprio all'origine della *preponderanza del diritto* in seno alle Comunità europee, inteso quale strumento per orientare e riunire gli Stati membri verso obiettivi comuni[132]; infatti, nonostante successivi mutamenti, integrazioni e adattamenti, rimarrà latente sullo sfondo ad avanzare il processo di integrazione e a definire l'azione dell'Unione.

Transazionalismo

Prima di passare alle teorie successive, che trovano fondamento su quelle appena esposte e che caratterizzeranno in maniera preminente la formazione e l'effettivo sviluppo del processo di integrazione[133], un brevissimo cenno al *transazionalismo,* che pure si faceva strada in quel periodo. Tale approccio avrebbe spostato l'enfasi dagli sforzi teorici dei precedenti a un'analisi più empirica[134]. Concepito da Karl Deutsch, il transazionalismo guardava con favore a qualsiasi forma di integrazione e si caratterizzava essenzialmente per la convinzione che l'aumento di transazioni e comunicazioni tra diverse società potesse meglio consentire lo sviluppo dell'integrazione regionale e dunque la creazione di "comunità di sicurezza". Per aver posto l'accento sulla relazione tra integrazione internazionale e comunicazione sociale, esso è stato visto anche come precursore delle teorie sociologiche sulla comunicazione, nonché ripreso in parte dai costruttivisti[135].

Nuove teorie dell'integrazione europea

Come si accennava, l'avvio del processo di integrazione portò con sé l'elaborazione di nuove teorie che lo accompagnarono negli sviluppi. Gli studiosi fanno infatti approssimativamente risalire la "prima fase" effettiva delle teorie dell'integrazione al periodo che va dai Trattati di Roma agli inizi degli anni Ottanta[136]. In particolare, mentre nel primo periodo sino agli anni Sessanta esso sembrava procedere in maniera spedita, così condotto e spiegato dall'approccio allora preminente, il *neofunzionalismo*, dagli anni Sessanta ai primi anni Ottanta, specie sotto l'egida dell'intervento gaullista, esso trovò diversi limiti e vide infatti la predominanza dell'*intergovernamentalismo*.

---

[131] N. ROJAS-HUTINEL*, La séparation du pouvoir dans l'Union européenne*, *cit*., p.38.

[132] Così, *ibidem*, p. 41 e p. 116, nonché, in particolare, sulla proceduralizzazione del potere a livello sovranazionale come risultato del metodo funzionalista p. 188 ss. (di ciò si dirà meglio *infra*, par. 5).

[133] A. WIENER, T. DIEZ, Introducing the Mosaic, *cit*., precisano infatti che il funzionalismo (come anche la prima parte di federalismo, che si è esposta, rappresentavano un periodo di "proto-integrazione normativa" che precedette l'integrazione *politica* vera e propria: "*The normative proto-integration period predates the actual development of political integration in Europe, It is an important precursor of the three phases of integration theory building*"; p. 7.

[134] CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *op. cit.*, p. 19. Si veda anche B. ROSAMOND, *Theories of European Integration*, MacMillan, 2000, nonché ERDEM, op. cit., p. 7.

[135] R. SCHWOK, *op. cit*. pp. 46-47 e 50, ma anche sino a p. 51. Si veda inoltre B. ROSAMOND, *op. cit*., pp. 42-47, e D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *op. cit.*, pp. 19-21.

[136] A. WIENER, T. DIEZ, *European Integration Theory*, cit., pp. 7-8.

Pollack spiega bene questa dicotomia e il suo superamento, dagli anni Novanta, che avrebbe aperto nuovi divari tra ulteriori e rinnovate teorie: «*From the beginnings of the integration process through the early 1990s, the dominant theoretical traditions in EU studies were neofunctionalism, which saw European integration as a self-sustaining process driven by sectoral spillovers toward an ever-closer union, and intergovernmentalism, which emphasized the gate keeping role of EU member governments and their resistance to any whole sale transfer of sovereignty from the member states to a new center in Brussels. By the 1990s, however, this debate had largely faded, replaced by a new divide between rationalist approaches, such as liberal intergovernmentalism and rational choice institutionalism, and constructivist approaches, which emphasized the potentially transformative potential of the EU*»[137]. Procediamo dunque a delineare le caratteristiche essenziali delle due *grand theories* che si contesero la scena sino a Maastricht, soprattutto perché (come vedremo) consentiranno di spiegare anche le attuali perplessità.

- *Neofunzionalismo*

Il *neofunzionalismo* trova in Ernst Haas il primo e principale esponente. Questi parrebbe proprio essersi ispirato all'approccio pragmatico che Monnet era riuscito a introdurre attraverso la CECA e che trovava compimento nei Trattati di Roma: la prima opera in cui Haas esponeva la nuova teoria (*The Uniting of Europe*) apparve infatti proprio l'indomani, nel 1958[138]. Nondimeno, va precisato che il suddetto "*federalismo funzionale*" di Monnet, qualificandosi per l'approccio graduale all'integrazione, presentava senz'altro punti comuni a funzionalismo e neofunzionalismo, ma non si identificava completamente con nessuno dei due[139].

Derivante da pluralismo e funzionalismo[140], il neofunzionalismo poneva l'accento sulle dinamiche interne al costrutto europeo e considerava l'importanza della *collaborazione* tra i vari attori (non solo statali, ma anche non statali e gruppi d'interesse), che avrebbe realizzato un rafforzamento reciproco tramite l'indispensabile *effetto spillover*: nell'integrazione per tappe successive, il passaggio dall'una all'altra avrebbe inevitabilmente comportato un travalicamento verso tappe ulteriori, i progressi avrebbero chiamato altri progressi. Questo, invero, era il principio già alla base della teoria di Mitrany, che introduceva il concetto di "*spillover funzionale*", poi da Haas affinato e precisato: la cooperazione in un dato settore indurrebbe degli effetti tecnici a catena

[137] M.A. POLLACK, *op. cit.*, p. 359. Qui l'autore riferisce anche che la prima letteratura sulle Comunità europee elaborava teorie dell'integrazione europea partendo dalla teoria delle relazioni internazionali.
[138] R. SCHWOK, *op. cit*, p. 55-56.
[139] D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *op. cit.*, p. 22.
[140]HOOGHE L.-MARKS G., Grand Theories of European integration in the twenty-first century, (2019), Journal of European Public Policy, 26:8, p.1114. si veda in tal senso anche D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *op. cit.*, che citano Haas laddove affermava "l'integrazione funzionale richiede il pluralismo".

nei settori correlati conducendo così al trasferimento di funzioni e competenze supplementari[141]. Haas insiste su questo concetto, ritenendo che l'estensione dell'integrazione da un certo settore ad altri condurrebbe quindi a uno *spillover politico*, con una sempre maggiore pressione a livello sovranazionale, coinvolgendo attori sia a quel livello, come la Commissione europea, sia a livello subnazionale, come gruppi di interesse, producendo ancora pressioni per un'ulteriore integrazione che dovrebbe quindi diventare autosufficiente sino a creare una nuova entità politica con centro a Bruxelles[142]. In ciò, dunque, lo scarto con il funzionalismo, di cui pure riprende le premesse di fondo.

Un altro fondamentale contributo del neofunzionalismo sta nella previsione del c.d. *metodo comunitario* (che si opporrà a quello intergovernativo) per operare nel sistema integrato: «*Such a 'method' consisted, inter alia, of high levels of elite socialisation, joint lobbying activities of organised interests, the Commission's right of legislative initiative, the involvement of national governments in complex negotiations at the European level, and a certain culture on the part of the Commission for upgrading the Community interest. It was not accidental, therefore, that in the early stages of the Community's development, neofunctionalism acquired the status of an ideology in Brussels*»[143].

Se pur queste erano le previsioni, che invero guidarono per un poco il processo di integrazione, la riaffermazione delle prerogative di sovranità degli Stati con il c.d. compromesso lussemburghese generata da De Gaulle nella metà degli anni Sessanta, nonché la crisi economica degli anni Settanta (peraltro, guardando alle vicende giurisdizionali, si ricorda *en passant* che sono quelli gli anni in cui iniziano ad emergere i primi "*controlimiti*" nazionali, da un lato, e le più nette definizioni delle prerogative essenziali del costrutto europeo da parte della Corte di giustizia, dall'altro), posero ostacoli che condussero ad abbandonare questo approccio verso interventi intergovernativi. Lo stesso Haas, infatti, ne riconobbe la debolezza e, ben presto, l'obsolescenza[144], mentre in generale le critiche vertevano: sull'assenza di dati empirici che confermassero di fatto il realizzarsi della teoria; alcuni hanno insistito sul fatto che l'interdipendenza funzionale avesse impiegato tempo per emergere e che non ci sarebbe stato effettivamente un effetto *spillover* automatico; sull'errata considerazione di un ruolo attivo della Commissione, a cui i funzionalisti avrebbero dato troppa enfasi nella previsione dell'avanzamento dell'integrazione, e di un ruolo invece ridimensionato della Corte di giustizia e dei suoi interventi; sulla concezione semplificata del

[141] N. ROJAS-HUTINEL, *op. cit*., p. 189 che, per questa esplicazione di spillover funzionale cita infatti Mitrany, pur essendo essa, come si è detto, meglio elaborata ed affinata da Haas.
[142] R. SCHWOK, *op. cit*, pp. 60-61.
[143] D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *op. cit.*, p. 22.
[144] L'autore pubblicò infatti un'opera al riguardo: E. B. HAAS, *The Obsolescence of Regional Integration Theory*, Institute of International Studies, University of California, 1975.

ruolo degli Stati nella costruzione europea; nonché, in particolare (ai nostri fini), sull'omessa considerazione dell'importanza della dimensione internazionale e dei fattori esogeni che invece avevano condizionato fortemente l'atteggiarsi dell'evoluzione del processo di integrazione (omissione ritenuta ancor più impressionante per la pretesa universalista che invece il neofunzionalismo aveva sullo sfondo)[145]. Inoltre, se è vero che la caratteristica peculiare di questa teoria era proprio l'interesse verso la *direzione* che l'integrazione regionale doveva intraprendere piuttosto che verso il *risultato finale*, questo però portava a maggior ragione delle perplessità: proprio l'incompletezza del progetto creava la necessità di nuovi accordi, ma anche l'impossibilità di individuare uno stadio finale dell'integrazione e quindi di precisare la forma istituzionale che la stessa avrebbe dovuto avere[146].

Nonostante queste critiche e i limiti riscontrati nel corso degli anni – che portarono all'affermazione dell'*intergovernamentalismo* – la teoria neofunzionalista è stata tra le preponderanti e, come si vedrà, continua in qualche modo ad abitare i discorsi sul processo di integrazione. Ad, essa, tra gli altri, va il merito di aver riconosciuto il ruolo giocato dalla Commissione e di aver ispirato, in qualche modo, le due successive teorie di istituzionalismo e governance multilivello[147].

- *Intergovernamentalismo*

L'*intergovernamentalismo*, sorto in reazione a tutte le teorie sin qui esposte, emergeva dagli sviluppi che caratterizzarono il processo di integrazione dalla metà degli anni Sessanta, ossia l'ostruzionismo di De Gaulle e, poi, l'adesione di nuovi Stati membri (Regno Unito, Irlanda e Danimarca, nel 1973). Il principale esponente di questa teoria, Hoffmann, nella sua famosa opera del 1966, derivava da quegli interventi la resilienza e "l'ostinatezza" degli Stati-nazione[148], che non erano affatto superati come il federalismo e il neofunzionalismo volevano intendere, ma anzi al contrario assumevano e rivendicavano un ruolo centrale nella costruzione europea.

Riprendendo la teoria delle relazioni internazionali, l'intergovernamentalismo affonda le proprie radici nel realismo, di cui assume le premesse, in termini di anarchia del sistema internazionale, nonché centralità degli Stati e delle loro preferenze (si veda meglio *supra*, par. 1), e dunque

[145] Ciascuna di queste critiche, assieme ad altre complementari (per esempio, laddove specifica «*l'intégration a tendu à connaître plus de succès dans des domaines où les gouvernements procédaient à des libéralisations comme le marché commun, mais moins dans des domaines dans lesquels l'intervention étatique était marquée, comme la production d'énergie nucléaire (EURATOM)* », p. 63), viene più dettagliatamente descritta da R. SCHWOK, *op. cit.*, pp. 62-69.
[146] Ibidem.
[147] R. SCHWOK, *op. cit.*, p. 70.
[148] Il riferimento è a S. HOFFMANN, *«Obstinate or Obsolete? The Fate of the Nation-State and the Case of Western Europe»*, Daedalus 95(3), 1966.

riconosce il ruolo crescente di diversi tipi di attori (come multinazionali, istituzioni o gruppi di interesse) nella sfera internazionale ed europea nonché la possibilità che gli Stati cedano parti di sovranità, purché, però non intacchino il nocciolo (come le corti nazionali ribadivano in quegli anni, appunto), dunque solo in aree minori ("*low politics*") e al fine della cooperazione[149]. Secondo questo approccio, quindi, paradossalmente, il processo di integrazione rifletterebbe proprio la continua primazia degli Stati e dei loro interessi.

Questo orientamento venne rielaborato, poco più tardi (anni Novanta), da un allievo di Hoffmann che propose il c.d. *intergovernamentalismo liberale*: assumendo alcuni spunti sia liberali che realisti, Moravcsik ribadiva la centralità degli interessi statali nei vari passaggi del processo di integrazione europea, leggendo l'interdipendenza e gli impegni istituzionali come mossi dal vantaggio economico nazionale, e quindi il ruolo decisivo svolto dagli Stati anche nel rilancio del costrutto europeo (specie con l'Atto Unico Europeo del 1986)[150]. Chiarito che lo Stato è l'attore principale del processo di integrazione, Moravcsik proponeva poi lo sviluppo del processo decisionale in tre tappe: nella prima, i governi definiscono i loro interessi a livello nazionale; nella seconda, essi portano le loro preferenze a livello sovranazionale per trattative che riflettono il potere di ciascuno Stato, mentre istituzioni come la Commissione non esercitano particolare influenza o intermediazione (come invece avrebbero inteso i neofunzionalisti); nella terza, i risultati delle contrattazioni riflettono sempre i diversi interessi degli Stati che, nell'aver creato istituzioni a livello sovranazionale, a favore delle quali avrebbero condiviso parte di sovranità con il fine di aumentare il proprio compromesso (cosa, per Moravcsik, confermata empiricamente dai Trattati di Roma come da quello di Maastricht)[151].

Nondimeno, Moravcsik ammetteva che sulle questioni di "*haute politique*", come la cooperazione in materia di politica estera, sicurezza e difesa, gli Stati non sarebbero altrettanto propensi a delle cessioni di sovranità[152]. Aspetto da sottolineare è che la formazione delle preferenze statali (non fissate definitivamente) è il frutto di un processo politico complesso che si realizza all'interno degli Stati stessi – per cui la politica interna assume particolare rilievo – e da ciò deriverebbe anche l'idea del c.d. *two level games* di Putnam, in termini di relazioni tra politica interna e relazioni internazionali (per cui, i governi si confronterebbero con dilemmi strategici al livello interno quanto internazionale e quindi le loro azioni assunte ad un livello interagirebbero con quelle prese nell'altro)[153]. Questa teoria fu fondamentale negli anni Novanta per spiegare diversi

[149] R. SCHWOK, *op. cit.*, pp. 83-84.
[150] Fondamentale in tal senso, tra le altre, la seguente opera: A. MORAVCSIK, *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht*, Cornell University Press, 1998.
[151] M.A. POLLACK, *op. cit.*, 2005, pp. 360-361.
[152] R. SCHWOK, *op. cit.*, p. 87.
[153] D.H. CHRYSSOCHOOU, M. J. TSINISIZELIS, S. STAVRIDIS, K. IFANTIS, *op. cit.*, p. 46.

aspetti del processo di integrazione (finanche apprezzati da alcuni neofunzionalisti) e nondimeno prestò il fianco a diverse critiche, specie di studiosi di relazioni internazionali riconducibili alle correnti riconducibili a neo-istituzionalismo e costruttivismo.

- *Neo-istituzionalismo*

Mentre il neofunzionalismo e l'intergovernamentalismo sono considerate "*grand theories*" poiché emerse appositamente per spiegare il processo di integrazione europea, il *neo-istituzionalismo* non nasce come teoria dell'integrazione ma propone – nelle scienze politiche – una generale riconsiderazione del ruolo delle istituzioni in diverse teorie che le avevano sottovalutate[154] (cfr. *infra*, par. 1, Capitolo III, per un riferimento ai maggior esponenti dell'istituzionalismo nella teoria generale del diritto). Così, rispetto all'integrazione europea, si presta a spiegare il fenomeno ponendo essenzialmente l'accento sul ruolo delle istituzioni sovranazionali e sulla loro capacità di causare conseguenze non intenzionali[155]. All'interno di questa ampia categoria rientrano invero diverse correnti di cui qui si indicheranno le tre principali che, sviluppatesi tra gli anni Ottanta e Novanta, interessarono gli studi sull'integrazione europea: il neo-istituzionalismo razionale (*rational choice*), quello storico, quello sociologico.

Il neo-istituzionalismo razionale, emerso tra gli studiosi americani per comprendere le dinamiche delle istituzioni del Congresso USA (tra i principali esponenti si veda Shepsle), si concentrava sul modo in cui gli attori razionali concepiscono le istituzioni per ottenere reciproci vantaggi e su come poi queste ultime incidono nei processi decisionali di politica interna e internazionale.

Il neo-istituzionalismo storico poneva l'attenzione sugli effetti delle istituzioni nel tempo e sull'incidenza delle scelte iniziali nella struttura del loro successivo sviluppo (per cui si è parlato di "*path-dependence*", concetto che però sta di recente subendo un superamento)[156].

Il neo-istituzionalismo sociologico, infine, guarda essenzialmente al modo in cui le istituzioni sono capaci di influenzare il comportamento degli attori[157]. In realtà, quest'ultima corrente viene sempre presentata assieme al costruttivisimo, piuttosto che alle due precedenti correnti del neo-istituzionalismo, e Pollack ci spiega bene perché: «*despite their differences on substantive issues, liberal intergovernmentalism, rational choice institutionalism and most historical institutionalism arguably constitute a single rationalist research program: a community of scholars operating from similar basic assumptions and seeking to test hypotheses about the most important determinants of*

[154] M.A POLLACK, *Institutionalism and European Integration*, Preliminary draft of a paper to be published in A. WIENER, T. BÖRZEL, T. RISSE, *European Integration Theory* (3rd edition), 11 July 2018, p. 2, in cui l'autore si riferisce a "such as behaviourism, pluralism, Marxism, and neorealism".
[155] A. WIENER, T. DIEZ, European Integration Theory, cit., pp. 7-8.
[156] M.A. POLLACK, *op. cit.*, pp. 15-16 e pp. 26-27.
[157] SCHWOCK, cit., p. 96.

European integration. By contrast, constructivist and sociological institutionalist approaches argue that the most profound effects of EU institutions are precisely in the potential remaking of national preferences and identities in the crucible of EU institutions»[158].

Prima, quindi, di fare un cenno al costruttivismo, si può concludere che gli approcci istituzionalisti sia razionale che storico hanno avuto un peso preponderante negli ultimi decenni degli studi sull'integrazione europea per spiegarne le dinamiche nonché le battute di arresto: l'interesse comune di entrambi gli approcci è il focus sul modo in cui le istituzioni vengono scelte e su come, poi, influenzano le scelte degli attori (guardandole dall'interno come fisse, nel primo caso, e valutandone gli sviluppi nel tempo, nel secondo caso). Pollack pone l'accento sul fatto che tali approcci condividono degli assunti di base, non solo tra loro, ma anche con teorie razionaliste di politica europea, comparative e di politica internazionale e che pertanto dovrebbero essere intese come un completamento di ogni altro approccio teorico, continuando a svilupparsi (sia a livello generale, che con specifico riguardo all'UE) e a fornire nuove considerazioni sull'evoluzione e i cambiamenti dell'Unione europea, utili anche per spiegarne le recenti crisi[159]. Le critiche agli approcci istituzionalisti rappresentano, in qualche modo, l'altra faccia della medaglia: la categoria raggrupperebbe orientamenti anche molto divergenti tra loro (si è visto, anche in termini di definizione del concetto di "istituzioni") che spesso hanno come denominatore comune il solo riferimento all'importanza del ruolo delle istituzioni[160].

- *Costruttivismo sociale*

Si è già analizzato il *costruttivismo*, trattando degli approcci di teoria delle relazioni internazionali. Risse ci ricorda, infatti, che il "*social constructivism*" ha raggiunto gli studi sull'integrazione europea alla fine degli anni Novanta, principalmente come "spillover" dagli studi sulle relazioni internazionali e come per superare il ristretto dibattito tra neofunzionalisti e intergovernamentalisti liberali, sfidando questi due approcci[161]. Assumendo le premesse già esposte, con specifico riguardo all'applicazione agli studi sull'Unione europea (la corrente costruttivista che si è più sofferma su questi studi è infatti quella dell'istituzionalismo sociale)[162] basti ribadire

[158] M.A. POLLACK, *op. cit*, 2005, p. 364 ma si veda anche p. 363.
[159] M.A. POLLACK, op. cit., 2018 p. 27. In questo contributo, infatti, l'autore si concentra sulla spiegazione istituzionalista della crisi finanziaria dell'Eurozona, ma suggerisce la possibilità di utilizzare tale approccio anche per valutare altri fenomeni, come la crisi migratoria o la Brexit.
[160] SCHOWCK, p. 97 e pp. 104 ss.
[161] T. RISSE, Social Constructivism and European Integration, in A. WIENER, T. DIEZ (Eds), *European Integration Theory* (second edition), Oxford University Press, 2009, p. 144.
[162]: R. SHWOCK : « *Le courant constructiviste qui s'est le plus penché sur l'Union européenne s'intitule l'institutionnalisme sociologique. Il s'agit donc d'une forme d'institutionnalisme (...). Elle se différencie cependant de l'institutionnaliste du choix rationnel, qu'elle considère comme étant trop rationaliste. L'institutionnalisme*

l'insistenza di tale approccio sull'influenza delle istituzioni europee, che modellerebbero non solo i comportamenti degli Stati membri ma anche le preferenze e le identità degli individui e dei loro governi, e dunque dell'impatto trasformativo del costrutto europeo sui sistemi statali[163].

Le critiche generalmente sollevate ai costruttivisti riguardano la difficoltà di un'effettiva comprensione empirica dell'integrazione europea, mancando di verificare le ipotesi formulate[164]. Nondimeno, tra i fondamentali contributi si riconosce l'importanza di aver sottolineato gli effetti costitutivi del diritto e delle politiche europei per studiare come l'integrazione europea modelli le identità sociali e gli interessi degli attori, in questo senso affermandosi come "epistemologia essenziale" nello studio dell'Unione europea[165].

- *Approcci di governance applicati all'Unione europea*

È stato notato che la "fase" delle teorie dell'integrazione europea corrispondente al periodo tra gli anni Ottanta e Novanta sarebbe stata marcata (oltre che, agli inizi, da un'apertura verso studi comparati – per cui infatti le teorie istituzionaliste e gli approcci governance vengono talvolta ricondotti alle "*comparative politics*"[166]) da un qualche ritorno alla teoria delle relazioni internazionali – allora caratterizzata dall'emersione di approcci critici e costruttivisti – e dal superamento della dicotomia tra funzionalisti/intergovernamentalisti in favore di quella tra realisti/costruttivisti[167], come parrebbe invero confermato dalle correnti appena esposte. Accanto e tra queste, infatti, negli anni Novanta il sempre più crescente dibattito sulla legittimità della *governance* europea proponeva questioni che videro lo sviluppo degli *approcci di governance* anche rispetto agli studi sull'integrazione, mentre il suddetto costruttivismo sociale attingeva da essi e al contempo ne agevolava la comprensione[168]. Presupponendo le premesse già esposte rispetto alla teoria delle relazioni internazionali, che in quel periodo vedeva emergere anche correnti che consideravano il costrutto europeo come "*governance without government*"[169], si aggiungeranno qui alcuni aspetti specificamente legati all'applicazione degli approcci di governance all'Unione europea.

---

sociologique insiste sur les capacités de chaque acteur à socialiser les autres acteurs et ainsi à influencer leurs intérêts, leurs politiques et leurs identités. »

[163] M.A. POLLACK, *op.cit.*, 2005, p. 365.

[164] M.A. POLLACK, *op.cit.*, 2005, p. 366; nello stesso senso R. SHWOCK, p. 110 e pp. 120-121.

[165] Così R. SHWOCK, cit., p. 121 e RISSE, *op. cit.*, p. 151. Quest'ultimo, in particolare, applica queste astratte considerazioni alla questione dell'identità europea, di particolare rilievo per la costruzione dell'UE sia in termini politici che analitici, pp. 152-156.

[166] ERDEM, op. cit., p. 9 ss.

[167] Così M.A. POLLACK, *op. cit.*, 2005, p. 368, nonché A. WIENER-T. DIEZ, op. cit, pp. 9-10.

[168] Wiener , Diez, pp. 10-11.

[169] Cfr. M.A. POLLACK, Theorizing the European Union, 2005, cit., p. 380 ss.

Il successo di tali approcci negli studi sull'Unione deriverebbe dalle peculiarità del sistema, in cui le decisioni sono prese e le politiche pubbliche sono applicate attraverso un meccanismo che vede un governo non eletto e responsabile[170]; vi è inoltre chi ha notato che la creazione di capacità di governance per le istituzioni dell'Unione sarebbe addirittura parte dell'obiettivo del processo di integrazione[171]. La governance europea si caratterizza senz'altro per il fatto che gran parte delle attività di elaborazione e attuazione delle politiche riguarda diversi livelli di intervento: si è già visto che si parla spesso di *governance multilivello* rispetto all'Unione (tra i principali si ricordi Marks già a metà degli anni Novanta), che riconosce accanto al livello sovranazionale l'importanza non solo degli organi nazionali, ma anche di quelli regionali/subnazionali e delle negoziazioni tra questi, e dunque riguarda non solo gli aspetti tecnici dell'attuazione di interventi europei ma anche le varie conseguenze politiche, per cui si è parlato di "*policy networks*" tra i diversi attori: queste sarebbero agevolate proprio dalla natura segmentata del processo decisionale europeo[172].

L'importanza dell'approccio di *governance multilivello* al processo di integrazione si giustifica non solo con il generale affermarsi, dagli anni Novanta (periodo a partire dal quale si inizierà a parlare anche, a livello più squisitamente giuspubblicistico, del noto *costituzionalismo multilivello*)[173], della globalizzazione internazionale (con riduzione del dominio degli Stati e ampliamento delle interazioni tra individui e gruppi, tramite nuove tecnologie ed economia transnazionale) ma anche con gli ingenti mutamenti che la costruzione europea subiva in quel periodo (mercato interno, moneta unica, sviluppo nuove politiche e conseguente proliferazione di meccanismi decisionali) e della centralità in tal senso del ruolo della Commissione[174]. Peraltro, in ciò si evince l'influenza che ha avuto su tale approccio il neofunzionalismo, quanto all'importanza riconosciuta al ruolo della Commissione e ai gruppi di pressione (quali gruppi di interesse, lobbies, multinazionali)[175].

Tra le molteplici e interessanti riflessioni sulla governance dell'Unione, che non possono qui neppure accennarsi, va fatto richiamo – perché legato con quanto già detto e dunque funzionale alla nostra analisi – a quelle analisi che rilevano la centralità della governance ai fini dei discorsi sulle

---

[170] Così R. SHWOCK, cit.

[171] Così B.G. PETERS, J. PIERRE, Governance Approaches, cit., p. 91, in cui precisano: «*European integration is to some extent an end in itself, but it may also be the means for attaining the capacity to govern a large territory with complex economic and social structures*».

[172] R. SHWOCK, *op. cit*., p. 124 nonché p. 128, europea. Nonché B. GUY PETERS, J. PIERRE, *op. cit*., pp. 95-98.

[173] Il cui principale esponente è, come si sa, I. PERNICE che introdusse il concetto con la sua prima opera alla fine degli anni Novanta e continua ancora a riproporlo seguendo l'evoluzione del processo di integrazione. Cfr. Multilevel Constitutionalism and the Treaty of Amsterdam. Constitution-making revisited?, in *Common Market Law Review*, 36, 1999, pp. 703-750; Multilevel constitutionalism in the European Union, in *European Law Review*, 2002; The Treaty of Lisbon: Multilevel Constitutionalism in Action, *Columbia Journal of European Law*, Vol. 15, No. 3/2009, p. 349-407; Multilevel Constitutionalism and the Crisis of Democracy in Europe, in *European Constitutional Law Review*, 11, 2015, pp. 541-562.

[174] R. SCHWOK, op. cit., p.125, che insiste sulla funzionalità politica della nozione di "governance" per la Commissione

[175] Ibidem. p. 70.

sfide di legittimazione che l'Unione si trova ad affrontare (per cui è stato rilevato che "*Governance is Crucial for Output legitimization*"). Oltre alle perplessità – legate anche a quanto in parte già notato – sul persistente deficit democratico che, nonostante gli aggiustamenti, rende il sistema di governance ancora carente di democraticità effettiva, e sul carattere spiccatamente burocratico di quest'ultimo, tali riflessioni pongono anche l'accento sul fatto che l'Unione affronterebbe solo tangenzialmente alcuni settori politici che sono invece cruciali a livello nazionale per legittimare i governi[176].

L'aspetto che però, tra le analisi sulla governance dell'Unione, si ritiene meriti più di tutti attenzione ai fini delle nostre riflessioni è quello che pone l'accento sulle *trasformazioni della governance europea*: «*it is changing not only how it performs its governance functions, but also what it does*». Sarebbero due, dunque, le dimensioni trasformative rilevanti, che spesso vengono confuse perché inevitabilmente intrecciate: quella sul *modo* e quella sull'*oggetto* della trasformazione.

La prima dimensione appare di interesse perché richiama quanto esposto da Majone (soprattutto con il suo "*Regulating Europe*" del 1996) sullo stile di governance "normativo dominante", concentrandosi sulle forme di regolamentazione a livello sovranazionale e rilevando che in gran parte degli interventi per guidare le economie e le società degli Stati membri l'Unione abbia usato il *diritto* quale strumento fondamentale (su questo concetto si tornerà) per ottenere i risultati (peraltro, criticato per certi aspetti perché inteso come eccessivamente interventista e travalicanti i limiti di competenze e poteri attribuiti all'Unione).

L'altro aspetto trasformativo riguarderebbe invece l'*oggetto*, e in particolare l'ampliamento delle aree politiche di intervento in cui la governance europea viene coinvolta direttamente e che in precedenza erano esclusivo appannaggio degli Stati. Basti fare cenno a questi spunti di riflessione, senza possibilità di approfondirli in questa sede ma con la consapevolezza di mantenerli sullo sfondo per le riflessioni che seguiranno, per l'importanza che essi assumono nel rilevare lo stretto legame tra le capacità di governance dell'Unione e l'avanzamento del processo di integrazione[177].

---

[176] GUY PETERS, J. PIERRE, op. cit., pp. 96-98. Con riferimento alle politiche sociali.

[177] Ibidem, pp. 99-103. Di particolare importanza il passaggio: «*As the tasks of the Union continue to expand, the style of governing will have to adapt. The changing tasks and the changing instruments being utilized in European governance reflect the need to use more democratic means to make and implement policy. Thus the democratization of the EU may not come through the usual means of mass politics and ministerial responsibility but rather through more indirect means on the output side of the governing process. These may not correspond to the usual understandings of political democracy, but they do increase public involvement in EU governance and may in fact open the governance system to a greater extent than a model of democratization based more on conventional parliamentary democracy. The increased availability of democratic mechanisms for governance within the EU does not eliminate the need for effective governance. EU governance may become more democratic and that will be certainly be a positive development, but in the end output legitimization appears to remain the more crucial aspect of the activities of the EU. Several of the changes in the style of European governance may be designed to improve the implementation of programmes, but these reforms also run the risk of further disaggregating a governance system already beset by excessive fragmentation. The*

- *Post-funzionalismo*

Avendo delineato per sommi capi le principali correnti che hanno cercato di spiegare la costruzione del processo di integrazione da prima del suo avvio sino a tempi recenti, pare opportuno un riferimento ai caratteri essenziali del c.d. *post-funzionalismo*, una teoria dell'integrazione europea proposta da Hooghe e Marks[178] per fornire ulteriori spiegazioni ai mutamenti recenti, presentando la loro analisi sull'impatto delle tre attualmente maggiori teorie rispetto alle correnti sfide illiberali che coinvolgono l'Unione.

Il *post-funzionalismo*, sviluppatosi in tempi recenti (fine anni Duemila) e dunque conscio di tutti gli approcci precedenti, focalizza la sua attenzione sul potenziale di *scontro* tra pressioni funzionali e identità esclusiva, valutando cause ed effetti della politicizzazione. Hooghe e Marks ce lo spiegano in tre fasi: la prima vede la discrepanza tra lo *status quo* istituzionale e le pressioni funzionali derivanti dall'*interdipendenza* propria della governance multilivello; la seconda si concentra sulla "arena" in cui si attua il processo decisionale; la terza analizza come il processo di integrazione modella la struttura del conflitto politico.

Seguendo questi passaggi, anzitutto, l'integrazione sarebbe vista come un fenomeno più ampio, come la riconfigurazione degli Stati per ottenere il beneficio di fornire beni pubblici su più larga scala, dal livello locale a quello nazionale a quello internazionale.

Quindi, viene prestata particolare attenzione all'arena in cui si discute il problema (più o meno isolata, e considerate sia la posta in gioco che la capacità di contendere degli attori) poiché essa influenzerebbe la natura del conflitto.

Infine, l'ultimo aspetto riguarda gli atteggiamenti dei partiti, le loro interazioni, la competizione e la scelta degli elettori e l'influenza che su tutto ciò può giocare l'integrazione europea nella misura in cui attivi questioni di identità (specie rispetto alla riconfigurazione dello Stato). Dunque, seguendo queste premesse, a differenza delle altre correnti, e soprattutto delle *grand theories*, che guardano all'integrazione come un processo cooperativo tra gruppi di interesse e governi, i *postfunzionalisti* lo vedrebbero come un processo conflittuale che emerge da sistemi di convinzioni incompatibili; come una forma di "*jurisdictional restructuring*", uno sviluppo dello Stato nazionale

above discussion should indicate that governance therefore is intimately related to the possibilities of further European integration, or to the maintenance of such integration as has been achieved», p. 103.

[178] L. HOOGHE, G. MARKS, A Postfunctionalist Theory of European Integration: From Permissive Consensus to Constraining Dissensus', in *British Journal of Political Science*, published online by Cambridge University Press, January 2009, pp.1-23.

che avrebbe prodotto profondi divari culturali e che quindi, tra i possibili esiti, non esclude anche la disintegrazione[179].

Ciò detto, l'interessante analisi condotta da Hooghe e Marks sull'atteggiarsi delle tre "scuole di pensiero" di neofunzionalismo, intergovernamentalismo e postfunzionalismo rispetto alle crisi che stanno coinvolgendo l'Unione europea merita qui un richiamo quanto alla posizione di quegli orientamenti rispetto alle sole sfide illiberali.

Gli autori, in particolare, si sono interrogati su come la genesi, il corso e i risultati di quattro fondamentali episodi che in qualche modo caratterizzano ciò che essi individuano quale attuale "disintegrazione" europea avviatasi dal 2008 e ancora in atto: la crisi dell'Eurozona; la crisi migratoria; la Brexit; l'emersione di forti pressioni illiberali. Rinviando al sapiente contributo degli autori per un approfondimento sui primi tre, l'analisi del quarto ambito ha qualche interesse ai nostri fini per capire la funzionalità di queste teorie rispetto all'analisi di come l'Unione sta affrontando quelle sfide che pongono sotto attacco il sistema di valori dell'Unione.

La recente sfida illiberale proveniente da alcuni Paesi del gruppo Visegrad, com'è noto, mette in dubbio alcuni capisaldi di *rule of law* che dovrebbero considerarsi fondativi dell'Unione e (in quanto) comuni a tutti i suoi membri, generalmente improntati a una forma di governo che garantisca l'indipendenza della magistratura, la separazione dei poteri e la protezione dei diritti e delle libertà fondamentali[180].

La messa in discussione di questi caratteri distintivi indispensabili per identificare una comunanza valoriale tra gli Stati membri sta minacciando in maniera preponderante la legittimazione dell'Unione europea. Il punto centrale, che gli autori hanno ben evidenziato, è proprio che si tratta di criticità che non intaccano l'interdipendenza economica, ma che minano le radici valoriali dell'Unione: «*events in Hungary and Poland undermine the core values of the European Union, but they do not pose an economic threat. Governments of both countries have been careful to comply with the rules of the single market while backsliding on liberal democracy*»[181].

Quanto alle posizioni delle tre teorie rispetto al modo in cui l'Unione sta affrontando questa sfida, gli autori rilevano che: l'intergovernmentalismo si concentra sulla spiegazione della difficoltà

[179] Così, precisamente, HOOGHE L., MARKS G., *Grand theories, cit.*, pp. 1116-1117, ove peraltro spiegano la derivazione della denominazione "postfunzionalismo": "*The study of mass politics has its roots in political psychology and is distinct from the rationalist-economic logic that underpins neofunctionalism and intergovernmentalism. Public opinion scholars regard economic preferences as just one possible motivation of human behavior, and one that is often less powerful than religion, ethnicity, or communal identity. Hence the label postfunctionalist, which is a term that stresses agnosticism about whether decision making or its outcome will be characterized by functionality*".

[180] Si veda il recente report della Commissione europea al riguardo, *2020 Rule of Law Report*, del 30 settembre 2020, disponibile qui: https://ec.europa.eu/info/publications/2020-rule-law-report-communication-and-country-chapters_en .

[181] HOOGHE L., MARKS G., *op. cit*., p. 1125.

di imporre il meccanismo sanzionatorio di cui all'articolo 7 TUE – quanto soprattutto all'imprescindibile coinvolgimento degli attori statali; il neofunzionalismo focalizza l'attenzione sugli interventi (non di attori statali, ma) della Commissione e della Corte di giustizia; il post-funzionalismo si concentrerebbe più sulle cause e misure interne di illiberalismo, suggerendo così le potenzialità degli attori transnazionali quando hanno la collaborazione dell'opposizione domestica. Gli autori precisano che le varie intuizioni non si escludono a vicenda e anzi, possono servire insieme a dare una visione più nitida dell'intera situazione[182].

Tutto ciò posto, è possibile ora passare finalmente ad un concetto ombreggiato durante tutta la trattazione sin qui svolta e che ha ora tutte i presupposti per essere trattato.

2.2. *Sovranità e diritto internazionale*

Motivi di interesse

Eccoci finalmente arrivati al punto di partenza: la sovranità.

Il punto di partenza del presente studio e dell'ipotesi di ricerca, ma anche delle dottrine e teorie che ne stanno a fondamento.

Anzitutto, è il punto di partenza del presente studio, cuore della domanda di ricerca che indaga la tendenza dell'Unione verso una "sovranità digitale". Ciò implica la necessità di trattare (almeno in pillole) le peculiarità di ciascuno dei due termini che definirebbero l'oggetto della tendenza che vorremmo attribuire all'Unione. Mentre delle implicazioni legate all'aggettivo "digitale" diremo a partire dalla Parte II, è il caso di affrontare da subito gli aspetti principali che il concetto di "sovranità", nella sua problematicità e continua evoluzione, porta con sé. Del resto, gli argomenti trattati sino ad ora hanno più volte ad esso fatto richiamo, mentre quelli che seguono ne richiedono un chiarimento.

Inoltre, a buon giudizio, il concetto di "sovranità" va inteso come punto di partenza delle discipline di riferimento di questo studio, ossia il diritto dell'Unione europea e, ancor prima, il diritto internazionale (assumendosi il primo giuridicamente fondato sul secondo)[183]. Come si ricorderà a breve, infatti, è sul concetto di sovranità statale che è si è generata la comunità internazionale e, dunque, la regolazione delle relazioni intercorrenti tra gli Stati quali soggetti della

[182] Ibidem, p.1128.

[183] Su questo aspetto si veda, su tutti, A. PELLET, Les fondements juridiques internationaux du droit communautaire, *Academy of European Law (ed.) – Collected Courses of the Academy of European Law*, Volume V, Book 2, Kluwer Law International, 1997, pp. 193-271.

stessa: «*What counts as sovereignty depends on the nature and structure of the international legal order and vice-versa*»[184].

Posto che – si decida o meno di affrontarlo e quale che ne sia l'approfondimento – il concetto di "sovranità" è archetipo di qualsiasi discorso sul diritto internazionale, l'intero studio qui proposto tenta di rispondere alla domanda: si può parlare davvero (e, se sì, cosa si intende) di "sovranità digitale dell'Unione europea"? La questione verrà trattata compiutamente nella Parte IV, dopo le necessarie analisi teoriche e pratiche relative all'incidenza della protezione dei dati personali sul processo di integrazione europea; per farlo è imprescindibile qui inquadrare il contesto di riferimento, a partire dai discorsi sulla definizione della "forma" dell'UE.

Anzitutto, occorre chiarire brevemente i seguenti punti: cosa si intende (o si è inteso) tendenzialmente con il concetto di "sovranità" in relazione al diritto internazionale; in che termini il concetto di "sovranità" può considerarsi una qualità dello Stato; è possibile (*rectius*, in che termini), oggi, riferire questo concetto in continua trasformazione ad un soggetto di diritto internazionale *diverso* dallo Stato, in particolare a un'organizzazione internazionale *sui generis* quale l'Unione europea.

Sulla nozione di sovranità: origini ed evoluzione

In primo luogo, per individuare una generica definizione di "sovranità" che consenta di porre le basi all'analisi successiva, prenderemo in prestito quella elaborata nel rinomato saggio di Walker nell'ambito di una raccolta dedicata al fenomeno della "sovranità in transizione": «*the discursive form in which a claim concerning the existence and character of a supreme ordering power for a particular polity is expressed, which supreme ordering power purports to establish and sustain the identity and status of the particular polity* ***qua*** *polity and to provide a continuing source and vehicle of ultimate authority for the juridical order of that polity*»[185]. Così intesa, la sovranità riecheggia quella concezione "classica" di *summa potestas* statale concepita – beninteso – nella duplice dimensione interna ed esterna: infatti essa, nella nozione tradizionale, «si presenta al tempo stesso come *criterio* (cioè come mezzo per riconoscere l'esistenza di un potere "decisivo" in ultima istanza e per affermarne le prerogative, distinguendole da quelle dei poteri subordinati in quanto da essa derivati) e come *strumento* di monopolizzazione della produzione del diritto e dell'uso della forza

[184] S. BESSON, *Sovereignty*, in Max Planck Encyclopedias of International Law, Oxford Public International Law, latest updated April 2011, par. 1.
[185] N. WALKER, *Late Sovereignty in the European Union*, in N. WELKER (ed.), *Sovereignty in transition – essays in European law*, Hart Publishing, 2003, p. 6.

(strumento cui si attribuisce storicamente la fondazione della concezione giuspositivistica dello Stato e dello stesso paradigma del diritto internazionale moderno)»[186].

Ancora, Kelsen intendeva che «*the problem of the sovereignty of the state is the problem of the sovereignty of the national legal order in its relation to the international legal order*», facendo da qui derivare la questione della sovranità come questione della relazione tra l'ordine nazionale e l'ordine internazionale ed esponendo le teorie rappresentative di tale relazione, ossia quella monistica e quella dualistica[187]. Le due posizioni sono ben note (come nota è l'adesione dell'autore alla prima); aldilà del merito di ciascuna (che si assuma, dunque, il primato del diritto internazionale ovvero di quello domestico), quanto precede basta a rendere evidente l'inestricabile e vicendevole legame tra sovranità e diritto internazionale, e dunque intendere la connaturale *eguaglianza sovrana* tra Stati come principio cardine dell'ordinamento internazionale.

Prima di trattare questo rapporto, si consenta di precisare che si partirà dalla considerazione della "sovranità moderna", ossia dal moderno senso del concetto, consapevoli ovviamente delle sue lontane radici storiche: «ogni riflessione sulla sovranità non può invece prescindere dalla sua dimensione propriamente storica, giacché la nozione di sovranità costituisce il punto cruciale di una tradizione dottrinale nella quale si consuma il dramma della distruzione e della ricostruzione di una paradigma giuridico del potere, che è all'origine della civiltà dell'Occidente moderno così come oggi la vediamo ancora in quello che da alcuni si vorrebbe il suo lento tramonto. In questo senso la sovranità è un concetto "classico" (…)»[188].

Oltre che come categoria storica, accogliamo altresì la caratterizzazione "funzionalista" della sovranità, intesa «come legittimazione sul piano giuridico di una effettività che fonda se stessa (…). In questo senso il concetto di sovranità è inteso appunto come un potentissimo strumento teorico per l'affermazione dello Stato moderno (…). Tale strumentalità, beninteso, vale tanto per il normativismo alla Kelsen quanto per il decisionismo alla Schmitt, giacché in entrambi i casi e in modi opposti si "utilizza" la sovranità per isolare la potenza politica nel suo rapporto con l'ordinamento (…)»[189].

Orbene, com'è noto la concettualizzazione della sovranità moderna si colloca nel XVI secolo, con la pioneristica opera di Bodin "*Les Six Livres de la République*" del 1576, in cui l'autore insisteva sull'impellente necessità dell'unificazione del potere in capo allo Stato, per poi cedere il passo all'apoteosi della comprensione assoluta della sovranità con il Leviatano di Hobbes. Tuttavia,

[186] D. QUAGLIONI, *La sovranità*, Laterza, 2004, pp. 7-8.
[187] H. KELSEN, Sovereignty and International Law, *Georgetown Law Journal*, vol. 48, no. 4, 1960, p. 628 per citazione. L'analisi delle opposte teorie della relazione procede da p. 629 ss. Al riguardo si veda anche, ovviamente, Id., *Lineamenti di dottrina pura del diritto*, 1934, Einaudi (1952), p. 156 ss.
[188] D. QUAGLIONI, *op. cit.*, p. 14.
[189] *Ibidem*, pp. 4-5.

fuor di teorizzazioni, si suole convenzionalmente indicare la fine della Guerra dei Trent'anni (1618-1648) e quindi la pace di Westfalia come *dies a quo* per un concreto riscontro di quella concettualizzazione, delineando la moderna comunità internazionale composta di Stati tutti ugualmente sovrani.

"*In the 1648 the principle of sovereignty brought peace*"[190].

Questa affermazione pare magistralmente cogliere l'essenza del rapporto tra sovranità e diritto internazionale, perlomeno come comunemente inteso. Infatti, per quanto vi fossero già prima di quella data modelli di governo di territori[191] come anche relazioni tra sovrani che si consideravano già reciprocamente su un piano paritetico[192], è solo con la pace di Westfalia che si sancisce la "soggettivazione dello Stato"[193], l'emancipazione dal predominio del potere religioso (stabilendo soprattutto regole per la tolleranza religiosa in Germania)[194] e dunque "la dissoluzione delle pretese universalistiche tipiche dell'età degli imperi"[195]. Quell'evento formalizza quindi il riconoscimento di diritti (sovrani) in capo agli Stati in quanto soggetti della comunità internazionale, definendo così quest'ultima come una realtà priva di un'autorità al di sopra di tutti e ufficializzando l'*eguaglianza sovrana* tra Stati come suo principio cardine.

Ciò traspone in capo agli Stati quelle pretese di libertà e uguaglianza che un secolo dopo saranno prerogative rivendicate dagli individui proprio nei confronti degli Stati. È questa l'idea che traspare dalla citata affermazione, tanto essenziale nel legame tra il principio di sovranità e una data – pur non del tutto pacifica[196] – ormai divenuta convenzionale nel sancire la "attuale frammentazione

---

[190] J. DE WILDE, *Saved from oblivion: interdependence theory in the first half of the 20th Century – A study on the causality between war and complex interdependence*, Dartmouth, 1991, p. 194.

[191] M FIORAVANTI, Stato e costituzione, in M. FIORAVANTI (a cura di), *Lo Stato moderno in Europa – Istituzioni e diritto*, Laterza, 2011, p. 6. Cfr. anche M. LOUGHLIN, Ten Tenets of Sovereignty, in N. WALKER (ed.), *Sovereignty in Transition*, Hart Publishing, 2003, pp. 56-59.

[192] S. MANNONI, Relazioni internazionali, in M. FIORAVANTI (a cura di), *Lo Stato moderno in Europa – Istituzioni e diritto*, Laterza, 2011, p.206 ss., che addirittura riporta il riferimento ad un trattato di non aggressione ed alleanza tra egiziani e ittiti del 1280 a.C.

[193] R. SAPIENZA, *Diritto Internazionale – Quattro pezzi facili*, Giappichelli, 2013, da p. 7 ss. Peraltro, di rilievo il breve quanto chiarificatore riferimento alla distinzione (di kelseniana memoria, cfr. *supra*) tra monismo e dualismo sul concetto di sovranità statale e sul suo ruolo nei rapporti tra ordinamenti: «per il monismo, la sovranità è una situazione di libertà riconosciuta se non addirittura concessa dal diritto internazionale agli Stati, mentre per il dualismo, la sovranità degli Stati è un dato fondamentale dal quale parte tutto il ragionamento. Ed essa è per il diritto internazionale una situazione di fatto che esso protegge proprio perché, così facendo, protegge le sue stesse fondamenta. Ma non può circoscriverla se non con il consenso degli Stati», p. 8.

[194] Così S.D. KRASNER, Sovereignty, *Foreign Policies*, No. 122, 2001, p. 22. Nel ridimensionare il riferimento convenzionale alla Pace di Westfalia, chiarendo che essa non ha creato *d'emblée* il sistema moderno degli Stati autonomi, l'autore precisa: «*Westphalia - which ended the Thirty Years' War against the hegemonic power of the Holy Roman Empire - delegitimized the already waning transnational role of the Catholic Church and val idated the idea that international relations should be driven by balance-of-power considerations rather than the ideals of Christendom. But Westphalia was first and foremost a new constitution for the Holy Roman Empire*», cfr. S.D. KRASNER, Sovereignty, *Foreign Policies*, No. 122, 2001, p. 21. Si veda anche R. SAPIENZA, *Diritto Internazionale – Quattro pezzi facili*, cit., pp. 6-7, sul "reale significato della pace di Westfalia", che consentirebbe di intendere che quella circostanza mettesse fine non solo alla supremazia della Chiesa cattolica ma anche all'Impero germanico.

[195] E. CANNIZZARO, *Diritto Internazionale*, Quinta edizione, Giappichelli, 2020, p. 3.

[196] *Ex multis*: S. MANNONI, Relazioni internazionali, *cit.*, pp. 201-211; S.D. KRASNER, *Sovereignty*, *cit.*, pp. 20-29.

dell'Europa"[197], quanto significativa nel palesare il paradosso che il principio di sovranità nel diritto internazionale porta con sé: emerso come strumento per stabilire la pacifica coesistenza tra Stati sul piano internazionale, parrebbe oggi quasi un ostacolo al migliore funzionamento dell'interdipendenza tipica della realtà internazionale globalizzata e forse, pur con le precisazioni che si diranno, in costante tensione con le pretese di libertà e uguaglianza proprie degli individui[198].

Consideriamo questo aspetto cruciale per la comprensione del rapporto tra sovranità e comunità internazionale ai fini che qui interessano. Infatti, se, come ricordato, il processo di integrazione europea è stato eminentemente condotto dall'orientamento funzionalista (nelle diverse sembianze che esso ha assunto nel tempo, dalle origini sino all'attuale post-funzionalismo teorizzato da alcuni), allora un'analisi – come la presente – che cerchi di indagarne l'attuale forma e comprenderne la direzione proponendone una visione "dall'esterno" non può misconoscere la posizione di coloro che si son fatti portavoce di quell'orientamento quanto proprio al rapporto tra sovranità e comunità internazionale. In breve, guardiamo a questo rapporto condividendo la prospettiva di Mitrany, come riproposta da De Wilde.

Quest'ultimo, infatti, riferendosi alla pacificazione di Westfalia come chiaro riconoscimento del pluralismo in Europa, poneva l'accento sull'*interdipendenza* e quindi celebrava l'osservazione di Mitrany nel ritenere quest'ultima la causa dei due contrastanti sviluppi che avanzavano a partire da quel periodo: la sempre maggiore unificazione "materiale" (i.e. essenzialmente economica), da un lato; l'incrementale disintegrazione/frammentazione politica, dall'altro. Pertanto, De Wilde tracciava un legame tra quelle premesse e gli aspetti più recenti: «*On the basis of this observation it can be hypothesized that the development from medieval cosmopolitism to the late-twentieth century individualist age, with its emphasis on human rights (individual sovereignty), is inextricably tied to the development from medieval local isolationism and parochial autarchy to the late-twentieth century world politics and world economy. This would mean that the development from cosmopolitism via state sovereignty and national sovereignty to human rights closely relates to the development towards global interdependence*»[199]. Così, il principio di sovranità avrebbe consentito all'Europa di sganciarsi dal "cosmopolitismo medievale" e però poi, paradossalmente, proprio in

[197] Così, spiegando la posizione di Mitrany al riguardo, J. DE WILDE, *op. cit*., p. 192 e anche: «*In 1648 in Europe, the artificial cosmopolitan unity was replaced by the universal recognition of actual fragmentation: the principle of state sovereignty*», p. 193.

[198] Mentre, come si è detto, l'eguaglianza sovrana rappresenterebbe proprio l'equivalente, in capo agli Stati, di quelle pretese riconosciute agli individui: «*The idea of sovereignty – or, more precisely, of sovereign equality – is the international equivalent of the principle that men are born and remain free and equal in rights*», V. LOWE, *International Law: A Very Short Introduction*, Oxford University Press, 2015, p. 6.
Per una considerazione critica (quasi dissacrante) di questi comuni convincimenti si rinvia a S.D. KRASNER, *Sovereignty*, cit., di cui si dirà meglio a breve.

[199] J. DE WILDE, *op. cit.*, pp. 193-194.

virtù della sempre maggiore interdipendenza così stimolata, avrebbe portato ad un "universalismo funzionale" che metterebbe ora quello stesso principio in discussione[200].

Invero, è bene puntualizzare che tale interdipendenza rappresenta uno sviluppo recente e ben lontano dalle premesse. Infatti, in diritto internazionale la sovranità, precipua caratteristica dello Stato, convergerebbe nella sua *indipendenza*, quale requisito della soggettività internazionale ad esso riconosciuta[201]. Così, infatti, la prassi internazionale l'ha tradizionalmente identificata: si suole abitualmente richiamare, al riguardo, la definizione datane dall'arbitro Huber nella sentenza della Corte permanente d'arbitrato sul *caso dell'Isola di Palmas* (1928), come anche l'opinione individuale del giudice Anzilotti rispetto al parere della Corte permanente di giustizia internazionale sul caso *Régime douanier entre l'Allemagne et l'Autriche* (1931), nonché la precedente celeberrima sentenza sul caso del *vapore Wimbledon* della medesima Corte (1923) – considerato ormai «*the locus classicus of the modern international law doctrine of sovereignty*»[202]– che riteneva compatibile con questa caratteristica, e dunque con la riconosciuta sovranità, un trattato che limitasse la libertà di azione di uno Stato[203].

È ciò che si intende per *sovranità esterna* (distinta, ancorché connessa, dalla *sovranità interna*), che coglie quindi la caratteristica indipendenza degli Stati al di fuori dei propri confini territoriali e dunque la parità nelle loro reciproche relazioni. Cannizzaro ci ricorda, infatti, che «La sovranità ha necessariamente due dimensioni L'affermazione della sovranità interna, concepita come il potere originario e assoluto di regolamentare i comportamenti della comunità territoriale, implica necessariamente anche la piena autonomia dello Stato nei rapporti esterni»[204].

Su ciò, invero, si pose maggiormente l'accento a partire dal XIX secolo (mentre prima l'attenzione era focalizzata, appunto, sulla sovranità *interna*, intesa come estrema autorità in un dato territorio e su una data popolazione) e dunque con lo sviluppo del diritto internazionale classico (in

---

[200] Ibidem, infatti: «*During the nineteenth century, Europe had developed itself into an "intimite organic unity", mainly because of economic developments. That created the fascinating historical paradox which has been discussed before: thanks to the principle of sovereignty, Europe escaped from the artificial cosmopolitism of the Middle Ages, but, because of the continued growth of interdependence, pressures from below forced a functional universalism that confronted the principle of sovereignty straightforwardly*», p. 196.

[201] *Ex multis*: R. SAPIENZA, *Elementi di diritto internazionale*, Giappichelli, 2002, p. 28 e p. 36; B. CONFORTI, *Diritto Internazionale*, pp. 17-18.

[202] B. DE WITTE, Sovereignty and European Integration. The Weight of Legal Tradition, *Maastricht Journal*, 2, 1995, p. 146.

[203] Tra gli innumerevoli: E. CANNIZZARO, *Diritto Internazionale*, Quinta edizione, Giappichelli, 2020, pp. 281-282; B. DE WITTE, Sovereignty and European Integration: The Weight of Legal Tradition, *Maastricht Journal*, 2, 1995, pp. 145 ss.; S. BESSON, op. cit., parr. 37 ss. e par. 56 ss.; R. SAPIENZA, Verso la deterritorializzazione del diritto internazionale della transizione infinita. Una premessa schmittiana ad un programma di ricerca, *Fogli di lavoro per il Diritto internazionale*, n. 2.2, 2009, p. 7.; B. CORTESE, Riflessioni sull'autonomia come limite: l'equilibrio tra libertà e condizionamento nel diritto dell'Unione europea, tra Unione, Stati membri ed individui, in *Liber Amicorum Antonio Tizzano – De la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, Giappichelli, 2018, p. 230.

[204] E. CANNIZZARO, *La sovranità oltre lo Stato*, Il Mulino, 2020, p. 27.

particolare dal Congresso di Vienna del 1815) e della possibilità di riconoscere dei limiti allo Stato che derivassero dalla volontà collettiva di tutti gli Stati: «*Quickly, external and internal sovereignty became two necessary sides of the same coin (…). If States were to remain ultimate authorities on the inside, they needed to be independent on the outside* (…). *It rapidly became clear that public international law and sovereignty implied each other. To be fully in charge of its relations with other States in a society of equally sovereign States and to be externally sovereign, and hence in turn to be able to protect its internal sovereignty, a State needed to be submitted to public international law. However, for public international law to arise, it needed independent sovereign States to freely consent to mutual rights and obligations and to their regulation. As a result, since sovereignty implies the existence of public international law, it became self-evident that sovereignty is inherently limited*»[205].

Una pacifica coesistenza, dunque, tra Stati indipendenti e sovrani, resa possibile dal diritto internazionale che ne regolava le relazioni e ne risolveva le controversie, tramite principi quali *par in parem non habet iurisdictionem* o non intervento negli affari interni (tale, perlomeno, ne era l'ambizione, come testimoniato dai diversi "progetti per la pace perpetua" dopo Westfalia[206]), nonché, a mano a mano (con l'avvio del c.d. diritto internazionale moderno), tramite tipi di cooperazione tra Stati che prendevano la forma di organizzazioni internazionali. Peraltro, come si sa, nel tempo quelle considerazioni sulla sovranità (esterna), oltre ad essere emerse nella prassi, furono anche codificate, come testimoniato – su tutti – dall'art. 2 della Carta ONU.

Ebbene, proseguendo con queste considerazioni, pare opportuno un riferimento a Walker a proposito del moderno uso del linguaggio della sovranità, distinguendo una prima "fase Westfaliana" e una seconda "fase post-Westfaliana".

Durante la prima, l'ordine internazionale sarebbe stato sostenuto da due ordini giuridici complementari: il diritto costituzionale, a governare l'ordine interno degli Stati, e il diritto internazionale, a governare le relazioni tra Stati sovrani, pur precisandone la configurazione "uni-dimensionale" dell'autorità giuridica.

La seconda fase, che sarebbe quella contemporanea (o quella a cui essa tende), invece caratterizzata dalle pressioni della globalizzazione (economica, ma non solo) e dal *pluralismo costituzionale*[207]. Su quest'ultimo concetto si tornerà, ma per il momento ciò basta a fornire alcuni elementi chiave per connotare quell'*interdipendenza* cui si è fatto spesso riferimento (nel *liberalismo* delle relazioni internazionali come nel *neofunzionalismo* dell'integrazione europea, sino

[205] S. BESSON, *op. cit.*, parr. 29-31 ; v. par. 109, sottolineato aggiunto.
Così pure B. DE WITTE, *op. cit.*: «*'External' and 'internal' sovereignty may be distinguished for the sake of clarity, but they are two dimensions of one and the same concept*», p. 147.
[206] Al riguardo, per tutti, si veda R. SAPIENZA, *Elementi di diritto internazionale*, *cit.*, pp. 11-14.
[207] Cfr. N. WELKER *Late Sovereignty in the European Union*, cit.

alle più ampie considerazioni di *governance multilivello*), che metterebbe in discussione la concezione di sovranità sin qui delucidata, in termini di precipua caratteristica dello Stato come sua originarietà e indipendenza nel contesto internazionale.

Ciò ci porta ad affrontare il secondo dei tre punti di perplessità sopra prospettati – che indaga l'oggetto della questione come attributo dello Stato –, riprendendo brevemente l'osservazione sul concetto di sovranità sviluppata durante il XX secolo nella teoria politica e nella teoria del diritto. Nel fare ciò, ci viene d'ausilio la breve ma esaustiva ricognizione di Besson, sulla "formalizzazione" del concetto di sovranità e sulla sua enfatizzazione come attributo dello Stato tramite il confronto dei principali pensatori del tempo al riguardo, ossia Kelsen e Schmitt.

«*In the first part of the 20 century, the concept of sovereignty entered into a formalization phase which progressively emptied it from any evaluative content and consequently of the normative constraints which were inherent to it since Locke. Sovereignty remains a function or property of the State or the legal order, but it is no longer limited by external values, and this is reminiscent of Bodin's and Hobbes' early modern approach to sovereignty. One finds this formal concept of sovereignty at work in Kelsen's, but most vigorously in Schmitt's writings. According to Kelsen's legal theory, sovereignty remains a normative concept, but it is a legally normative concept and not a moral or political one. State sovereignty implies that its legitimacy and authority can be established exclusively by reference to the legal system itself. It requires no reference to principles outside that very legal order. According to Schmitt, by contrast, the concept of sovereignty is not even normative in a legal sense anymore. It is a legal concept, but a purely empirical one in that it refers to a factual situation; the sovereign is that entity which is vested with the ultimate power of solving extreme situations. For Schmitt, the mixture of legal and moral elements in earlier conceptions of sovereignty actually constituted the fundamental problem of sovereignty throughout its history*»[208].

Orbene, a partire dal secondo dopoguerra, come si sa, tutte queste considerazioni trovano un ridimensionamento nella nuova comprensione del diritto internazionale quale diritto della cooperazione tra Stati, pur ancora sovrani, che si traduce nella suddetta *interdipendenza*. E l'emersione di organizzazioni internazionali, nuovi soggetti di diritto internazionale, ne è la più emblematica (ancorché non unica) conferma. Ciò appare "cruciale" perché introduce nel contesto internazionale la soggettività di un altro ente che però non ha sovranità territoriale, quindi vede quest'ultimo attributo sgretolarsi, in una sempre maggiore "*deterritorializzazione del diritto internazionale*": «L'indagine dedicata alla evoluzione che conduce all'affermarsi delle organizzazioni internazionali quali nuovi soggetti del diritto internazionale intende mostrare come

[208] S. BESSON, *op. cit*., parr. 40-41.

questo processo muova da una iniziale trasposizione verso l'alto (ossia oltre, al di sopra degli Stati) di moduli ricavati dalla esperienza statale di governo del reale, postulando prima e creando poi dei meccanismi in grado di "governare" le relazioni fra gli Stati prima e poi l'intero universo delle relazioni umane anche, se del caso, bypassando lo Stato»[209].

Ciò non significa che la considerazione dello Stato sovrano – e dell'eguaglianza sovrana tra Stati – sia tramontata, ma semplicemente che abbia cominciato a subire un inevitabile ripensamento, forzato dalla sempre più pressante interdipendenza: «*more recently, sovereignty has come to be associated with the idea of control over transborder movements. When contemporary observers assert that the sovereign state is just about dead, they do not mean that constitutional structures are about to disappear. Instead, they mean that technological change has made it very difficult, or perhaps impossible, for states to control movements across their borders of all kinds of material things (from coffee to cocaine) and not-so-material things (from Hollywood movies to capital flows*»[210]. Ebbene, è proprio in questo contesto di radicale trasformazione e ripensamento del concetto di "sovranità" che l'integrazione europea iniziava ad avverarsi[211].

Besson ci aiutava ancora a comprendere che questi svolgimenti non rappresentassero – come pure paventato – la fine della sovranità, ma solo il suo naturale adattamento a nuove circostanze, che avrebbe quindi realizzato una "internazionalizzazione della sovranità moderna" derivante, a dire dell'autrice, da due sviluppi chiave: *l'internazionalizzazione della sovranità popolare*; lo *sviluppo della sovranità oltre lo Stato*[212].

L'internazionalizzazione della sovranità moderna

Com'è noto, a partire dalla fine del XVIII secolo i discorsi sulla sovranità popolare e sulla democrazia – a partire dalle distintive vicende in America e in Francia – cominciarono ad affollare i discorsi sulla sovranità. Invero, ciò derivava, *ça va sans dire*, dal già accennato ridimensionamento della concezione assoluta di sovranità e quindi dalla possibilità di comprenderla come "limitata", come avvenne dalla fine del secolo precedente proprio a partire dalle arcinote teorie del contratto

[209] R. SAPIENZA, Verso la deterritorializzazione del diritto internazionale della transizione infinita. Una premessa schmittiana ad un programma di ricerca, *Fogli di lavoro per il Diritto internazionale*, n. 2.2, 2009, p. 10. Sul punto si veda anche E. MILANO, The Deterritorialization of International Law: Setting the Context, in A DI STEFANO (a cura di), *Un diritto senza terra? Funzioni e limiti del principio di territorialità nel diritto internazionale e dell'Unione europea - A Lackland Law? Territory, Effectiveness and Jurisdiction in International and EU Law*, Giappichelli, 2015, pp. 53-70. Le parole virgolettate in precedenza sono tratte dal medesimo contributo.

[210] S. D. KRASNER, *op. cit*., p. 21.

[211] A. TOKÁR, Something Happened. Sovereignty and European Integration, in *Extraordinary Times – IWM Junior Visiting Fellows Conferences*, Vol. 11, Vienna 2001, p. 2, sottolineato aggiunto.

[212] S. BESSON, op. cit., parr. 46-47. Per rendere l'idea : «*In short, modern international sovereignty is as important for the self-determination of democratic States in international law as ever, but to serve the same purpose its modalities have changed*», par. 46.
Sui mutamenti della nozione di sovranità in questo periodo storico si vada anche D. QUAGLIONI, *op. cit*., nel capitolo dedicato a "*La sovranità nella crisi del moderno*", p. 108 ss.

sociale, particolarmente con Locke, Bentham e soprattutto Rousseau, che concettualizzava la sovranità popolare come limite al potere del sovrano[213]: «*sovereignty and democracy were clearly bound from then on*»[214]. Pertanto, occorre spiegare brevemente i due sviluppi chiave che hanno accompagnato la trasformazione del concetto di sovranità dal secondo dopoguerra, partendo dal primo che risolve in parte una questione accennata incidentalmente all'inizio (ossia la probabile tensione tra sovranità e diritti individuali).

Quanto all'*internazionalizzazione della sovranità popolare*, essa può chiaramente comprendersi con il fatto che mentre la "sovranità classica" si identificava con la (sola) sovranità dello *Stato*, il soggetto della "sovranità moderna" sarebbe il *popolo*[215]. Ciò è ad uno causa e conseguenza della democratizzazione degli Stati e dello sviluppo della protezione (costituzionale) dei diritti umani all'interno degli Stati a seguito dei tragici abomini che avevano dilaniato l'Europa e il mondo intero, segnando la svolta nella comprensione dello stesso diritto internazionale (da allora, come si è detto, caratterizzato dalla cooperazione): «*domestic sovereignty had gradually become more and more limited and found its source in a democratically legitimate legal order. Post-1945, international law was seen by modern democracies as a new way to secure their democratic development and, given the relationship between human rights and democracy, to entrench human rights protection from the outside through minimal international standards*»[216].

Questa considerazione della "sovranità limitata" ha giocato un ruolo preponderante nell'emersione della cultura dei diritti umani e della democrazia: «il concetto di autolimitazione è perciò pensabile solo in una democrazia, nella quale i soggetti e il sovrano non sono che gli stessi uomini considerati sotto diversi rapporti (…). L'interdipendenza fra interesse comune e autodeterminazione dei singoli fonda una nuova legittimazione del potere sovrano, poiché è tale interdipendenza a costituire "la sola garanzia che il cittadino ha di non obbedire ad altre norme che a quelle che egli stesso ha contribuito ad emanare"»[217].

Queste osservazioni non devono far cadere nell'errore di considerare il concetto di sovranità (statale) come completamente contrapposto a quello di diritti umani. È un aspetto delicato che merita di essere chiarito e sul quale si ritornerà: se senz'altro la tutela dei diritti individuali sorge (tra gli altri aspetti dello Stato di diritto, nell'accezione lata) come necessario limite all'opprimente

[213] Al riguardo si fa riferimento ai concisi quanto chiari riferimenti di S. Besson, *op. cit.*, parr. 21-24 e N. ROJAS-HUTINEL, *op. cit.*, pp. 27-29.
[214] S. BESSON, *op. cit.*, par. 25.
[215] Ibidem, par. 153.
[216] *Ibidem*, par. 48.
Si vedano inoltre i parr. 130-140 dedicati proprio al rapporto tra sovranità e diritti umani, nonché quelli 141-149 su sovranità e democrazia.
[217] D. QUAGLIONI, *op. cit.*, pp. 85-86, laddove cita V. Mura, *J-J Rousseau. La teoria dell'obbligo politico.*

potere statale – dunque, in qualche modo, al concetto assoluto di sovranità – è comunque vero che la tutela degli stessi non potrebbe concepirsi *senza* sovranità.

Spiega Besson al riguardo: «*sovereignty, and sovereign equality, in particular, protects democratic autonomy in a State's external affairs and remains justified for this separately from international human rights. This development explains, for instance, why it is wrong to oppose sovereignty to human rights in the second part of the 20 century; without sovereignty, many human rights-related developments, such as decolonization, would not have taken place and without the role human rights played in their creation, many of today's sovereign States would not exist. Of course, this is not to say that sovereignty cannot be in tension with human rights. However, when it is, the tensions are reminiscent of those between popular sovereignty and human rights in the domestic context and ought actually to be resolved in the domestic context (…). Of course, the internationalization of modern sovereignty goes hand in hand with the democratization of international law itself*»[218]. Dunque, sicuramente può dirsi che i concetti di sovranità e diritti umani (universali) mantengano una costante tensione, ma deve anche dirsi che (perlomeno assumendo la nuova accezione della prima) essi si implicano a vicenda, per cui sarebbe errato ritenere la proliferazione dei secondi come una sfida o minaccia della prima[219].

Senza dilungarci su questo aspetto che si avrà modo di riprendere, appare parecchio interessante l'altro elemento chiave che avrebbe contribuito a stimolare la suddetta "internazionalizzazione della sovranità moderna", ovvero lo *sviluppo della sovranità oltre lo Stato*. Questo ci porta sia ad affrontare il terzo punto di perplessità prospettato nel corrente paragrafo (e relativo, cioè, alla possibilità di intendere il concetto di sovranità come categoria attribuibile ad enti diversi dagli Stati) sia, soprattutto, ad introdurre il paragrafo che segue e che (pur in pillole) sarà dedicato proprio ai suoi svolgimenti.

La trattazione potrebbe trovare un idoneo incipit nell'analisi di MacCormick dedicata alla questione: *Beyond the Sovereign State*[220]. Ritenendo distorcente la prospettiva stato-centrica della

[218] S. BESSON, *op. cit*., parr. 49-50 e 52

[219] Così, *ex multis*, S.D. KRASNER, op. cit., p. 22, ci ricorda al riguardo: «*The struggle to establish international rules that compel leaders to treat their subjects in a certain way has been going on for a long time. Over the centuries the emphasis has shifted from religious toleration, to minority rights (often focusing on specific ethnic groups in specific countries), to human rights (emphasizing rights enjoyed by all or broad classes of individuals). In a few instances states have voluntarily embraced international supervision, but generally the weak have acceded to the preferences of the strong*». Sul punto pare anche interessante D. Quaglioni, *op. cit.*, p. 118: «Piaccia o no, il paradigma hobbesiano, sul quale tanta parte del pensiero del nostro tempo ha costruito l'immagine dell'ordine politico, segna l'eclissi del diritto naturale e con essa l'avvento del paradosso della modernità, per il quale bisogna essere sottomessi a un unico e onnipotente *dominium* per potere avere dei diritti, poiché solo lo Stato conferisce il diritto di avere diritti. In tal senso il diritto può concepirsi come totalmente disancorato da presupposti di ordine morale-religioso, perché tra diritto e morale non c'è più alcun rapporto necessario, e si può giungere a parlare, nelle forme più sottilmente aberranti della riflessione giuspolitica del nostro tempo, di una "tirannia dei valori"».

[220] N. MACCORMICK, Beyond the Sovereign State, in *Modern Law Review*, vol. 56, no. 1, 1993, p. 1-18.
Potrebbe anche farsi un richiamo, tra gli innumerevoli, al dibattito tra Mancini e Weiler.

concezione dei sistemi giuridici, l'autore sosteneva, quasi trent'anni or sono, che non potessero più considerarsi esistenti "Stati sovrani" (nel senso assoluto del termine) e che però ciò non implicasse l'automatica acquisizione di sovranità da parte di altri enti a scapito degli Stati, proponendo piuttosto la questione: «*how does the European Community affect our own sovereignty? How does it affect the analysis of law in terms of sovereign commands or in terms of some rival analytical apparatus?*»[221].

Queste valutazioni, oggetto di profonde analisi e critiche, vengono oggi rivedute e in qualche modo superate da considerazioni che si interrogano sulla plausibilità che adesso ci si stia muovendo (o meglio, si sia già) "*beyond the Post-Sovereign State*"[222]. Di ciò si dirà meglio trattando specificamente dell'Unione, mentre qui basti dire che, riprendendo il discorso introduttivo, si condivide la prospettiva proposta da Walker di una "*late sovereignty*", abbastanza efficace nel delineare l'atteggiarsi del concetto di sovranità nel nuovo ordine "multi-dimensionale", che, seguendo l'autore, si connoterebbe per quattro caratteristiche fondamentali: continuità; carattere distintivo; irreversibilità; potenziale trasformativo[223].

Rinviando al prosieguo l'approfondimento funzionale di alcuni aspetti richiamati, ciò che preme sottolineare sin da ora è il riferimento fatto dall'autore ai "nuovi" confini della sovranità nell'era post-Westfaliana, che – come peraltro può evincersi da quanto già detto – non sono più territoriali ma essenzialmente *funzionali* (aspetto che, dei quattro succitati, esprimerebbe il carattere distintivo): «*The key to sovereignty is the double-claim to ultimate authority over where the boundary between the inside and the outside lies and to ultimate authority, to final power of decision which defeats any claim of 'external' encroachment, within that self-defined boundary. The key difference in the claim made in the multi-dimensional post-Westphalian order is that the boundaries are no longer merely* territorial*, but, if in an increasingly permissive sense, also* functional*. To be sure, states in the age of late sovereignty still make claims to territorial authority* tout court*, but non-state polities typically make claims to authority bounded by territory and by function. In other word, the political societies which non-state polities claim to constitute are no longer just territorial communities but also functional communities (...). In the new post-Westphalian order (...) with the emergence of functionally-limited polities which do not claim*

[221] *Ibidem*, p. 2. È noto, peraltro, il paragone fantasioso proposto dall'autore circa l'eventuale "perdita" di sovranità e di verginità: cfr. p. 16 e più ampiamente, sul punto, pp. 1, 15-16.
[222] M. WILKINSON, Beyond the Post-Sovereign State? The Past, Present and Future of Constitutional Pluralism, in *Cambridge Yearbook of European Legal Studies*, 21, (2019), pp. 6-23. Nell'analisi critica della posizione di MacCormick, l'autore precisa: «*The argument in brief is that MacCormick erred in his diagnosis, basing it on a reductive view of sovereignty in line with his legal positivism. But he was wrong in a revealing way. A 'post-sovereign ideal-type' did emerge out of postwar reconstruction, paradigmatically in West Germany. Sovereignty, however, was not transcended as the label might suggest; it was folded in, or repressed*», p. 7.
[223] N. WALKER, *op. cit.*, p. 19 ss.

comprehensive jurisdiction over a particular territory it becomes possible to conceive of autonomy without territorial exclusivity – to imagine ultimate authority, or sovereignty, in non-exclusive terms»[224]. Si tratterebbe, insomma, di una delegazione di competenze e funzioni dagli Stati ad organizzazioni internazionali per ottenere una migliore cooperazione a livello transnazionale, internazionale e sovranazionale[225].

Ciò ci riconduce a quanto detto dall'inizio, confermando dunque che – ben lungi dalle sue premesse – qualsiasi valutazione sulla sovranità nel diritto internazionale non può oggi prescindere dalla caratteristica *interdipendenza* tra i soggetti ai quali la si vorrebbe (ancora e/o *ex novo*) attribuire. E ciò, però, ci conduce anche inevitabilmente a considerare la "soggettività funzionale" riconosciuta alle organizzazioni internazionali, "attribuita loro per le finalità che esse perseguono"[226] e tale, peraltro – seguendo la medesima logica di MacCormick – da non inficiare affatto la soggettività degli Stati. Tuttavia, banalmente, la realtà attuale spinge a domandarsi «se questo schema tradizionale sia ancor oggi valido in riferimento al nuovo fenomeno degli enti sovranazionali. Con tale formula si indicano generalmente gli enti ai quali sono stati trasferiti poteri di sovranità tipicamente esercitati dagli Stati e che quindi appaiono maggiormente simili ad uno Stato che ad una classica organizzazione internazionale. Difatti, per indicare tali enti si è diffusa la formula *state-like entities*»[227].

Più precisamente, appare molto utile e condivisibile al riguardo l'esposizione che fa Cannizzaro sulla "trasformazione" della sovranità: «In questa sua permanente trasformazione, la sovranità è apparentemente riuscita a rimanere, paradossalmente, eguale a sé stessa. La sovranità è stata evocata, per secoli e ancora oggi, al fine di indicare la fonte suprema del potere politico e del suo ordinamento giuridico, e tale rimane ancora oggi. Sol che, attraverso un graduale processo di rarefazione, essa è stata confinata ai margini dell'ordinamento, se non addirittura al di fuori di esso (…). Se la sovranità non è più utile per concettualizzare le dinamiche politiche e giuridiche all'interno dello Stato, essa ben potrebbe esserlo per concettualizzare quelle dinamiche che si svolgono al di là dello Stato. Proprio la progressiva rarefazione della sovranità nel corso della storia, e il suo utilizzo come mezzo di difesa rispetto alla sfera esterna all'ordinamento costituito, indicano che quello possa essere l'ambiente giuridico e politico nel quale la sovranità abbia ancora un ruolo: l'ambiente esterno allo Stato dove le comunità possono ancora crearsi, confliggere,

[224] Ibidem, pp. 22-23. Cfr. Anche E. CANNIZZARO, *op. cit.*, p. 284, secondo il quale, «in situazioni di questo tipo, il tentativo di determinare un ente assolutamente sovrano sembra privo di senso scientifico». In realtà, non sono state presentate da subito perplessità al concetto, derivante da quello espresso nell'estratto, di "sovranità funzionalmente limitata", cfr. G. DE BURCA, Sovereignty and the Supremacy Doctrine, in in N. WALKER (ed.) *Sovereignty in Transition*, Hart Publishing, 2003, pp. 458-459.
[225] Cfr. S. BESSON, *op. cit.*, par. 54.
[226] Così E. CANNIZZARO, *Diritto Internazionale*, *cit.*, p. 323.
[227] Ibidem.

integrarsi o distruggersi; nel quale gli Stati pretendono ancora di esercitare un potere assoluto, solo in parte arginato dai flebili limiti dell'ordinamento internazionale»[228].

Da queste considerazioni, segue dunque, spontaneamente, il terzo punto di ambiguità, ossia la questione relativa alla possibilità e all'opportunità di trasporre il "nuovo" concetto di sovranità in capo all'Unione europea, o per lo meno cercare di comprendere come esso si pone nei suoi riguardi. Cercheremo di rispondere a questo nel paragrafo che segue. Più oltre, ciò interroga sul fondamento e sull'obiettivo, sul funzionamento e sulla missione di quell'ente (e dunque, di nuovo, porta a questioni di legittimazione), per indagare le sembianze che tale Unione europea assumerebbe, delle sue precipue caratteristiche (che la renderebbero *altro* da un ente statale come anche da un'organizzazione internazionale *tout court*) e della sua considerabilità nel contesto internazionale. Il metodo di analisi "dall'esterno" avrebbe, dunque, l'ambizione di consentire, alla fine, una comprensione che consente di realizzare in maniera più consapevole il "moto opposto" (cfr. *infra*, Capitolo I, Parte III), ossia centrifugo, nell'osservazione dell'atteggiarsi dell'Unione, con specifico riguardo alla protezione dei dati personali nella dimensione digitale, come attore (e non semplice soggetto) nello scacchiere internazionale.

[228] E. CANNIZZARO, *La sovranità oltre lo Stato*, cit., pp. 65-66.

CAPITOLO III
LA *FORMA* DELL'UNIONE EUROPEA: DI "SOVRANITÀ CONDIVISA" E POTERE DA SEPARARE

1. L'ordinamento giuridico

«*Un ordinamento giuridico di nuovo genere nel campo del diritto internazionale a favore del quale gli Stati membri hanno rinunziato, se pure in settori limitati, ai loro poteri sovrani ed al quale sono soggetti non soltanto gli Stati membri, ma pure i loro cittadini*»[229].

La celeberrima formula, che ridonda negli anni, sentenziava il riconoscimento del "nuovo" ente come qualcosa di inedito, richiamando quasi provocatoriamente un concetto tanto ovvio quanto arcano: *l'ordinamento giuridico*.

Cercheremo di esporre nell'ordine, per brevi cenni, gli aspetti essenziali dei passaggi che ci consentiranno di sviluppare poi il ragionamento (intrecciandolo al caso di studio sulla protezione dei dati personali) nelle Parti III e IV. Per farlo, un utile spunto ci è dato da questa introduzione:

«*The value of European integration, serves as a fundamental ideal of the legal order of the European Union, inviting reconsideration of the conceptual features of law*»[230].

Partiamo, dunque, proprio dall'*ordinamento giuridico*, in generale, delle organizzazioni internazionali e poi, nello specifico, dell'Unione europea.

Delle organizzazioni internazionali, in generale

Che le organizzazioni internazionali siano dei soggetti di diritto internazionale, e dunque titolari di diritti e doveri internazionali, è ormai pacifico, come pure confermato dalla prassi internazionale (così, per tutti, nel parere reso l'11 aprile 1949 dalla Corte Internazionale di Giustizia sul caso relativo alla *Riparazione dei danni subiti al servizio delle Nazioni Unite;* o ancora nel successivo parere del 1980 *sull'accordo tra l'OMS e l'Egitto*)[231]. Dalla stessa prassi emerge che le organizzazioni internazionali sono dotate di un proprio ordinamento giuridico, ciò che può leggersi e ricondursi ugualmente agli approcci teorici di riferimento: *normativismo* e *istituzionalismo.* Ci riferiamo rispettivamente alle posizioni di Kelsen e Hart e a quelle di Hariou e Romano, in

[229] Corte di giustizia, 26/62, *Van Gend & Loos c. Administratie der Belastingen*, sentenza del 5 febbraio 1963, p. 23.
[230] T. MOORHEAD, *The Legal Order of the European Union – The Institutional Role of the Court of Justic*e, Routledge, 2014, p. 1.
[231] CIG, parere del 20.11.1980 sull'Accordo tra l'OMS e l'Egitto.

particolare[232]. Semplificando estremamente, può dirsi che il normativismo considera il diritto come norma, mentre l'istituzionalismo lo considera come istituzione.

Pertanto, si avrà che secondo Kelsen «il diritto come ordinamento, o l'ordinamento giuridico, è un sistema di norme giuridiche (…). Una pluralità di norme forma un'unità, un sistema, un ordinamento quando la sua validità può essere ricondotta a un'unica norma come fondamento ultimo di questa validità. Questa norma fondamentale (*Grundnorm*), come fonte comune, costituisce l'unità nella pluralità di tutte le norme che formano un ordinamento (…). La dottrina pura del diritto si vale di questa norma fondamentale come di un fondamento ipotetico. Se si parte dal presupposto che tale norma sia valida, è valido anche l'ordinamento giuridico che si fonda su di essa»[233]. Di qui l'identificazione del diritto con la norma giuridica, che ne costituisce la base, e l'articolazione delle norme dell'ordinamento come conseguenza (in virtù di una dipendenza formale) della norma fondamentale.

Quanto alla specifica posizione di Hart, il suo principale contributo ai nostri fini è la considerazione dell'ordinamento giuridico come insieme di norme primarie e secondarie, considerando le prime precettive e le seconde alle prime funzionali, la cui esistenza sarebbe ciò che permette effettivamente i mutamenti dell'ordinamento.

Considerando invece l'*istituzionalismo* (da intendere anche come base delle teorie del costruttivismo – nelle relazioni internazionali – e del neo-istituzionalismo – quanto all'integrazione europea; cfr. *supra* Capitolo II), Santi Romano assumeva una posizione diametralmente opposta nel descrivere l'ordinamento giuridico: «è un'entità che si muove in parte secondo le norme, ma, soprattutto, muove, quasi come pedine in uno scacchiere, le norme medesime, che così rappresentano piuttosto l'oggetto e anche il mezzo della sua attività, che non un elemento della sua struttura»[234]. Così, l'autore arrivava poi a spiegare la considerazione dell'ordinamento giuridico come *istituzione*: «il diritto, prima di essere norma, prima di concernere un semplice rapporto o una serie di rapporti sociali, è organizzazione, struttura, posizione della stessa società in cui si svolge e che esso costituisce come unità, come ente per sé stante (…). Se così è, il concetto che ci sembra

[232] Si considerino, rispettivamente, le celeberrime opere: M. HAURIOU, *Théorie de l'institution et de la fondation*, 1925; H. KELSEN, *Lineamenti di dottrina pura del diritto*, 1934; S. ROMANO, *L'ordinamento giuridico*, 1946 (2°ed.); H.L.A. HART, *The concept of Law*, 1961.

[233] H. KELSEN, *op. cit.*, p. 95 e p. 98. Peraltro, come si è accennato, da qui deriva notoriamente la prospettiva *monista* del diritto e dunque dei rapporti tra diritto internazionale e diritto domestico, di cui l'autore è il principale esponente.

[234] S. ROMANO, *L'ordinamento giuridico*, Quodlibet, 2018, pp. 29-30. È interessante anche riferire come continua l'autore: «Sotto certi punti di vista, si può anzi dire che ai tratti essenziali di un ordinamento giuridico le norme conferiscono quasi per riflesso: esse, almeno alcune, possono anche variare senza che quei tratti si mutino, e, molto spesso, la sostituzione di certe norme con altre è piuttosto l'effetto che la causa di una modificazione sostanziale dell'ordinamento».

necessario e sufficiente per rendere in termini esatti quello di diritto, come ordinamento giuridico considerato complessivamente e unitariamente, è il concetto di istituzione»[235].

A questa concezione che parte dall'ordinamento e che vede il diritto "soprattutto come organizzazione" aderiva peraltro anche Schmitt, che proprio grazie a Romano avrebbe avuto la sua "svolta istituzionalista"[236]. Peraltro, Romano si rifaceva proprio alla posizione di Hauriou, aiutandoci così nella comprensione di quest'ultimo: «Secondo questo scrittore, l'istituzione è un'organizzazione sociale (…). Si dovrebbero invero distinguere due specie d'istituzioni: quelle che appartengono alla categoria delle cose inerti (…) e quelle che invece formano dei corpi sociali, cioè le istituzioni corporative. (…) ma nel sistema giuridico sono da prendersi in considerazione come figura a sé stante soltanto le istituzioni corporative, poiché ad esse, a differenza delle altre, compete un'autonomia. Ciò implica che ogni istituzione di questo genere è una vera realtà sociale, un ente chiuso (…). Esso quindi si può considerare sotto due aspetti: dal punto di vista della sua vita di relazione, e allora viene in rilievo la sua individualità subbiettiva, la sua personalità giuridica; e dal punto di vista della sua vita interiore, e allora assume la figura di un'individualità obbiettiva. Quest'ultimo suo aspetto, che si traduce nella sua autonomia, importa che l'istituzione corporativa è fonte originaria del diritto, in quanto che genera spontaneamente le tre forme del diritto: quello disciplinare, quello consuetudinario e quello statutario o legale. Questo è il nucleo fondamentale della dottrina dell'Hauriou»[237].

Si consenta, inoltre, di precisare che – com'è ampiamente noto – la fama di Romano è dovuta altresì alla sua tesi sulla *pluralità degli ordinamenti giuridici*, che rappresenterebbe «un logico corollario dell'istituzionalismo che, facendo propria la formula *ubi societas ibi ius*, riconosce la presenza del diritto non solo nell'ordinamento statale, ma in ogni corpo sociale che esibisca esistenza unitaria, organizzata ed oggettiva»[238].

Questa minuta (e dimessa) digressione su temi di teoria generale del diritto non pare inopportuna né superflua, se si considera, come è stato acutamente rilevato, che proprio il *sincretismo* tra le differenti posizioni esposte consente di rendersi conto che ogni organizzazione internazionale è dotata di un proprio ordine giuridico, con proprie norme, un proprio fondamento, nonché una

[235] Ibidem, p. 38, in cui precisa: «Ogni ordinamento giuridico è un'istituzione, e viceversa ogni istituzione è un ordinamento giuridico: l'equazione fra i due concetti è necessaria e assoluta».
[236] S. PIETROPAOLI, Ordinamento giuridico e *Konkrete Ordnung* – Per un confronto tra le teorie istituzionalistiche di Santi Romano e Carl Schmitt, in *Jura Gentium*, n. 2/2012, pp. 1-22.
[237] Ibidem, pp. 41-42. Con un'importante precisazione, però, che distingue i due istituzionalisti: «Hauriou non vuole definire il diritto: ciò che gli interessa è mostrare che un ordinamento giuridico nasce da un fatto sociale e non da una volontà. Romano e Schmitt non hanno invece alcun interesse a scendere sul piano sociologico: l'istituzione non è pre-giuridica. Quando un giurista come Romano parla di diritto come istituzione, ciò non vuol dire che esso si risolva in qualsiasi raggruppamento sociale, ma in quel tipo di società in cui le attività dei membri sono ordinate attraverso una rete di norme che organizzano la società», così S. Pietropaoli, op. cit., p. 22.
[238] Così F. DE VANNA, L'*ordinamento giuridico* di Santi Romano e il pluralismo oltre l'orizzonte dello Stato: alcuni percorsi interpretativi, in *Jura Gentium*, XV (2018), 2, p. 42.

missione e degli obiettivi; e ciò consente così di "decriptarne" il potere normativo espresso proprio da quell'ordine giuridico[239].

Tutto ciò vale per ogni organizzazione internazionale (si faceva notare che, per esempio, il succitato parere della Corte Internazionale di Giustizia nell'elaborare la nota *teoria dei poteri impliciti* seguitasse la posizione dell'Hauriou – per cui tutte le organizzazioni sono dotate di personalità giuridica)[240], ma vale ancor più, ai nostri fini, per l'Unione europea, parecchio emblematica di quel sincretismo.

Dell'Unione europea, in particolare

Ciò pare evidente, da un lato, nella distinzione tra diritto primario e derivato – che richiama hartiane considerazioni – nonché nei molteplici interventi in cui Corte di giustizia insiste sulla valenza dei Trattati come norma fondamentale nonché, come si dirà meglio, sulla "forza" segnante del *diritto come potere normativo*[241], con chiare influenze del normativismo kelseniano (nonché nell'afflato spesso monista – portavoce proprio dell'autore praghese – quanto alla trattazione dei rapporti con gli ordinamenti degli Stati membri, pur non in assenza di interventi antitetici).

Ma ancora di più, dall'altro, ciò pare evidente ad uno sguardo sistematico dell'assetto in cui l'Unione si pone, che la riconduce alle considerazioni dell'Hauriou rassomigliandola al concetto di istituzione come ente chiuso e dotato di autonomia (come si dimostrerà a breve) e palesa inoltre l'attualità del pluralismo giuridico di Romano. È stato notato a quest'ultimo riguardo, infatti, che «una parte estremamente significativa degli studi sul *legal pluralism* e sul 'diritto transnazionale' abbia identificato nelle tesi di Romano un prezioso e tuttora attuale supporto teorico, e dunque un solco d'indagine conducente per la sistematizzazione dei fenomeni inediti riguardanti il diritto contemporaneo. L'accento posto sulla intrinseca pluralità del giuridico, e il contestuale declassamento della nozione di unità, rappresentano oggi una premessa epistemica appropriata per aggiornare le nostre griglie teoriche e comprendere la 'frammentazione' che, in modo inesorabile, caratterizza il destino della regolazione giuridica. Si pensi, ad esempio, all'emersione di *global regulators* che, nella maggior parte dei casi corrispondono a *non-State actors* – regimi, dunque,

[239] Queste riflessioni sono infatti stimolate da una lezione sull'ordinamento giuridico delle organizzazioni internazionali tenuta dal Prof. F. LATTY durante il suo corso *Droit des organisations internationales*, nel pomeriggio del 12 marzo 2019 presso l'*Université Paris Nanterre*.

[240] Nel parere consultivo n. 1/49, la CIG elaborava la teoria dei poteri impliciti secondo cui, anche se non è esplicitamente definita da un trattato, l'attribuzione del potere di concludere accordi in capo all'ONU risponde al suo fine di garantire la pace nel mondo e dunque per realizzare la sua missione implicitamente questo potere deve necessariamente ritenersi sussistente. Di essa si sono poi avute tracce nell'ordinamento comunitario, a partire da due pareri della CGCE su accordi internazionali n. 1/76 e 1/91.

[241] Cfr. N. ROJAS-HUTINEL, *op. cit.*: «*La construction européenne a ceci de particulier qu'elle crée un système juridique qui subordonne clairement le monopole juridique des Etats à une norme européenne*» p. 29. Ciò si approfondirà meglio nel corso della trattazione.

autonomi – che esprimono un nuovo potere normativo, in aree generali o specializzate dell'attività umana, tagliando trasversalmente ordinamenti e barriere. Dal momento che sono spesso indicati come *self-contained legal regimes*, il concetto di 'istituzione', rinviando ad una dimensione materiale, è ciò che meglio ne coglie l'essenza, effettiva e organizzata – più di quanto possa fare la prospettiva normativistica di matrice kelseniana (ma anche hartiana)»[242]. Queste considerazioni non solo confermano quanto già detto sull'interdipendenza come elemento di ridimensionamento della concezione della sovranità (statale), ma addirittura agevolano la comprensione del *pluralismo costituzionale* come consona teoria regolatoria dell'Unione europea[243]. Prima di toccare questo punto (che peraltro, richiamando osservazioni sull'ordine eterarchico, evoca, come si dirà, le teorie di Luhmann), , occorre chiarire altri aspetti.

Tutto quanto detto sin ora ci consente di confermare che l'Unione europea sia un *ordinamento giuridico*. Nondimeno, l'esegesi del celeberrimo estratto di *Van Gend en Loos* che abbiamo preso a fondamento, nonché la logica del discorso che vogliamo condurre, impongono ulteriori precisazioni.

Come si anticipava riprendendo gli istituzionalisti, riconoscere l'UE come un ordinamento giuridico "*nel campo del diritto internazionale*" ne implica la sua *autonomia,* concetto tanto caro alla Corte di giustizia che, com'è noto, non ha mancato (e continua ancora) di precisarne le caratteristiche, rispetto al diritto degli Stati membri nonché al diritto internazionale (specie nelle relazioni esterne, con riguardo a progetti di accordi internazionali). Molto di recente, infatti, pronunciandosi sul CETA la Corte ha ribadito: «*Quest'autonomia, che esiste nei confronti sia del diritto degli Stati membri, sia del diritto internazionale, deriva dalle caratteristiche essenziali dell'Unione e del suo diritto. Quest'ultimo si caratterizza, infatti, per la circostanza di essere il prodotto di una fonte autonoma, costituita dai Trattati, per il suo primato sui diritti degli Stati membri nonché per l'efficacia diretta di tutta una serie di disposizioni applicabili ai loro cittadini e agli stessi Stati membri. Tali caratteristiche hanno dato origine a una rete strutturata di principi, di norme e di rapporti giuridici mutualmente interdipendenti, che vincolano reciprocamente l'Unione*

[242] F. DE VANNA, *op. cit.*, p. 55, sott. aggiunto. L'autore conclude: «La globalizzazione e l'estrema accelerazione degli scambi e delle comunicazioni, in particolare, hanno consentito la riemersione del carattere spontaneo del fenomeno giuridico essenzialmente sotto tre profili: a) quello dell'autonomia rispetto alla catena di comando statuale; b) quello della trasversalità rispetto ai confini statuali; c) e, non da ultimo, sotto il profilo della rottura dell'identificazione tra *ius* e *iussum*, tra diritto e 'comando' espressivo di una volontà. Questi profili, sottaciuti da una buona parte della giuspubblicistica preoccupata di difendere e ricostruire l'usbergo della sovranità statuale, erano chiaramente intuiti da Romano nell'ambito di una riflessione aperta ai cambiamenti della società e libera dalle astrattezze del concettualismo dogmatico: sta qui, ancora oggi, l'elemento più rilevante della sua eredità intellettuale.», pp. 55-56.

[243] Cfr. *Ex multis* gli interessanti contributi in M. AVBELJ, J. KOMÀREK (Eds), *Constitutional pluralism in the European Union and beyond*, Hart Publishing, 2012.

stessa e i suoi Stati membri, nonché questi ultimi tra di loro. *Detta autonomia consiste pertanto nella circostanza che l'Unione è dotata di un quadro costituzionale che le è proprio»*[244].

Ebbene, per un verso tornano alla memoria le risalenti considerazioni di Pellet che, nel riconoscere detta autonomia, avvertiva della relatività della stessa, sol che si cambiasse punto di osservazione – dunque, assumendone uno interno o internazionale – rispetto alla prospettiva prettamente comunitaria[245]. In tal senso, il riferimento, costantemente ribadito dalla stessa Corte, ai Trattati parrebbe riconoscere il carattere che potremmo dire "non originario" di quell'ordinamento (come per ogni organizzazione internazionale ed in contrapposizione, per esempio, agli ordinamenti statali)[246], definendolo dunque "creato" e come tale fondato sul diritto internazionale[247].

Queste, pur astrattamente condivisibili, considerazioni necessitano però di essere rimodulate proprio alla luce delle peculiarità ribadite stessa Corte e ripetute, si è visto, finanche nel parere CETA. La chiave di tale rimodulazione va proprio trovata letteralmente tra le righe di *Van Gend en Loos*, dove la Corte definisce per la prima volta quell'ordinamento giuridico "*di nuovo genere*".

Infatti, come ci ricorda Cannizzaro, quella sentenza ha proprio «inaugurato un orientamento giurisprudenziale coerentemente mantenuto fino ad oggi, tendente ad affrancare l'ordinamento giuridico dell'Unione da quello degli Stati membri proclamandone l'*autonomia* e l'*originarietà*. Storicamente, l'ordinamento dell'Unione si fonda bensì su un atto di volontà degli Stati membri, i quali hanno trasferito ad essa determinati poteri, istituendo, al contempo, un apparato istituzionale per il loro esercizio. Giuridicamente, però, l'ordinamento dell'Unione si sarebbe distaccato dall'originario atto di volontà degli Stati membri, *imponendosi per forza propria*, come un nuovo ordinamento giuridico autonomo, *completamente autodeterminato e privo di vincoli di dipendenza sia nei confronti degli ordinamenti statali che di quello internazionale*»[248]. Ciò non significa,

---

[244] Corte di giustizia, parere n. 1/17, 30 aprile 2019, punti 109-110. Dello stesso identico tenore (tra tutti) i punti 166-167(8) del parere 2/13 del 18 dicembre 2014. *il diritto dell'Unione si caratterizza per il fatto di derivare da una fonte autonoma, costituita dai Trattati, per il suo primato sul diritto dei singoli Stati membri* (…), *nonché per l'effetto diretto di tutta una serie di disposizioni applicabili ai cittadini di detti Stati membri nonché agli Stati stessi* (…)

[245] A. PELLET, *op. cit*., p. 246: «*L'autonomie, indiscutable, de l'ordre juridique communautaire n'a donc pas forcément les conséquences radicales qu'en tirent les auteurs communautaristes si l'on se place dans une perspective «internationaliste» ou «interniste»*.». E ancora :« *Parce qu'il constitue un véritable ordre juridique, le droit communautaire est autonome par rapport au droit international. Toutefois, cette autonomie est relative, pour au moins deux raisons : d'une part, l'ordre juridique communautaire est une création du droit international ; d'autre part, il entretient avec celui-ci des rapports de systèmes qui s'apparentent d'ailleurs, de manière frappante, à ceux qu'entretiennent le droit interne et le droit international* », p. 247.

[246] R. SAPIENZA, per esempio, ci ricorda la "originarietà dello Stato, espressione che vuole sottolineare appunto che lo Stato è il frutto di un avvenimento politico libero, non voluto da altri Stati", cfr. Quattro pezzi facili, cit., p. 10.

[247] A. PELLET, *op. cit.* : «*l'ordre juridique communautaire n'est pas, à la différence de l'ordre juridique étatique, une donnée factuelle; c'est un ordre créé; et il l'est par une série de traités. Il s'agit donc d'une création du droit international* », p.206.

[248] E. CANNIZZARO, *Il diritto dell'integrazione europea – L'ordinamento dell'Unione*, Terza edizione, Giappichelli, 2020, p. 9 (enfasi aggiunta). Su questo aspetto, appare utile qui approfondire cosa specifica l'autore poco dopo: «La difficoltà logica di concepire un trattato come fondamento giuridico di un nuovo ente autonomo e originario può indurre a ritenere che il processo di trasformazione di un trattato, da fonte del diritto internazionale a fonte costituzionale di un

beninteso, negare le radici internazionalistiche dell'ente, cosa che peraltro la stessa Corte non ha mai espressamente fatto (la saga *Kadi*, per esempio, ne è testimonianza)[249].

Ebbene, a rendere questo ordinamento "*sui generis*" sono proprio le sue caratteristiche essenziali, tra le quali – procedendo con l'estratto principale succitato – risalta soprattutto che ad esso siano "*soggetti non soltanto gli Stati membri, ma pure i loro cittadini*".

Questo passaggio è distintivo nella definizione del carattere innovativo dell'ordinamento dell'Unione rispetto ad una "semplice" organizzazione internazionale, poiché introduce la rivoluzionaria conseguenza per cui proprio in virtù di tale «base soggettiva complessa, che include non solo gli Stati, ma anche i cittadini, le norme del Trattato possono avere *effetti diretti*»[250]. Così, com'è noto, quella sentenza poneva il primo fondamentale pilastro di ciò che verrà poi considerato il "*triangle magique*" su cui l'intero costrutto si fonda: principio degli *effetti diretti*, principio del *primato del diritto dell'Unione* su quello degli Stati membri, meccanismo del *rinvio pregiudiziale*[251]. La portata dirompente di ciascuno di essi è ben nota, così com'è nota la loro inestricabile correlazione, ognuno trovando ragione e compimento nell'altro ai fini dell'effettivo funzionamento dell'architettura su di essi fondata.

L'ultimo punto del succitato estratto di *Van Gend en Loos* è quello il cui chiarimento ci consentirà di "chiudere il cerchio", di legare insieme i discorsi sull'ordinamento giuridico sviluppati in questo paragrafo con quelli sulla sovranità, proposti nel paragrafo precedente (nonché sulla *legitimacy crisis* introdotta nell'incipit), e dunque con le intere valutazioni che hanno condotto la trattazione delle teorie sull'integrazione europea, ponendoci dinanzi alla questione in maniera più nitida e consentendo così di completare le premesse indispensabili per la costruzione del ragionamento sulla sovranità digitale dell'Unione europea. Il riferimento è alla peculiarità per cui

---

nuovo ordinamento, sia un fenomeno di mero fatto, non disciplinato dal diritto. I Trattati istitutivi dell'Unione, di conseguenza, presentano questa singolare dissociazione logica. Essi costituiscono una fonte di diritti ed obblighi per gli Stati membri, regolati dal diritto internazionale. D'altra parte, essi si sarebbero affermati in via di fatto come il fattore costitutivo di un nuovo ordinamento giuridico. Secondo quanto affermato dalla Corte di giustizia nel caso *Van Gend en Loos*, si tratterebbe di un ordinamento complesso, sia nella sua dimensione strutturale che in quella soggettiva. Strutturalmente, esso avrebbe incorporato gli ordinamenti degli Stati membri in un complessivo ordine giuridico, dettando altresì le regole di conflitto applicabili al suo interno. Dal punto di vista soggettivo, si tratterebbe di un ordinamento "di nuovo genere", il quale "riconosce come soggetti, non soltanto gli Stati membri, ma anche i loro cittadini". È in questo ordinamento di nuovo genere, quindi, che, finalmente, il problema della determinazione degli effetti delle norme dell'Unione trova soluzione», ivi p. 115.

[249] Così ci ricorda infatti M. FICHERA, *The foundations of the EU as a polity*, cit., 2018, p. 7: «the CJEU has often on the one hand reiterated its classic formula of 'EU as autonomous legal order having a 'constitutional charter based on the rule of law', and on the other hand never explicitly denied EU law's international legal roots».

[250] E. CANNIZZARO, *Il diritto dell'integrazione europea*, cit., enfasi aggiunta, p. 113.

[251] U. VILLANI, Una rilettura della sentenza *Van Gend&Loos* dopo cinquant'anni, *Studi sull'integrazione europea*, n. 2/2013, in cui l'autore rileva: «nella sentenza *Van Gend&Loos* c'è già, per molti versi in forma compiuta, per altri in maniera embrionale, la "sistemazione" del diritto comunitario, nel senso, precisamente, di ricomposizione dello stesso in un sistema, il quale (...) si fonda su un "*triangle magique*" costituito dall'effetto diretto, dal primato e dal rinvio pregiudiziale. Riconsiderare, a cinquant'anni di distanza, la sentenza *Van Gend&Loos* rappresenta, dunque, non un omaggio rituale, ma il riconoscimento della sua "paternità" dei caratteri essenziali e distintivi dell'ordinamento comunitario», p. 236.

nell'ordinamento comunitario "*gli Stati membri hanno rinunziato, se pure in settori limitati, ai loro poteri sovrani*".

Il riferimento ai "*poteri sovrani*" consente finalmente di palesare un aspetto sin ora sottaciuto ma abbastanza evidente: la concatenazione tra sovranità e potere, nel senso di ritenere che è sovrano chi detiene il potere e, viceversa, che l'esercizio legittimo del potere esprime la sovranità.

Orbene, se così è, da questa asserzione derivano due fondamentali interrogativi:

- Come si combina questo rapporto tra sovranità e potere in una realtà in cui i poteri e le competenze – pur in alcuni settori – vengono ceduti e dunque la sovranità è per un verso "limitata" e per altro "condivisa"?
- La constatazione di questa "rinuncia" degli Stati "a favore" dell'Unione realizza delle attribuzioni, in capo quest'ultima, tali da consentire di parlare di una (limitata o condivisa quanto si voglia) "sovranità europea"? E se sì, in che termini e con quali sembianze? Da qui, sarà molto utile richiamare gli illuminanti studi condotti sulla *natura* del potere dell'Unione europea, sulle sue peculiarità e dunque inevitabili ripercussioni sulla sua organizzazione[252].

La risposta, nell'ordine, a entrambi gli interrogativi ci condurrà, da un lato, (di nuovo) alla questione della crisi di legittimazione dell'Unione – con problemi di come conciliare ciò che è stata definita come "*ipergiuridicità"* dell'organizzazione unionale con gli appelli a una maggiore; dall'altro, al quadro costituzionale dell'UE quale carattere essenziale e peculiare della stessa e, così, questi due aspetti si troveranno a confluire nel discorso che ci consentirà di introdurre il (peculiare) sistema di valori dell'Unione.

Invero, simili interrogativi sono stati affrontati, *mutatis mutandis*, nell'interessante saggio della De Burca sviluppato a partire dall'analisi del *principio del primato* emerso con *Costa c. ENEL*, che si proponeva di analizzare se i termini "supremazia del diritto dell'Unione" e "sovranità dell'Unione" potessero riferirsi allo stesso concetto[253]. La sua analisi ci tornerà utile per trovare le nostre risposte. Intanto, va precisato (aspetto invero non affrontato ma che, chiaramente, è nelle cose) che il concetto di sovranità può avere valenza sia politica che giuridica, le due spesso intersecandosi e sussumendosi a vicenda, ma che talvolta presentano profili di dissomiglianza[254].

---

[252] Cfr. N. ROJAS-HUTINEL, *op. cit.*, e S. DELLAVALLE, *op. cit.*, nonché H. LINDHAL, Sovereignty and Representation in the European Union, cit., p. 89 ss.

[253] G. DE BURCA, Sovereignty and the Supremacy Doctrine of the European Court of Justice, in *N. Walker (ed.) Sovereignty in Transition*, Hart Publishing, 2003, pp. 449-460.

[254] Per esempio, può aiutare S. QUAGLIONI, *op. cit.*, nel descrivere la sovranità come "nozione tradizionale": «la sovranità si presenta, appunto come nozione di tradizione giuspolitica, come lo specchio di una realtà soggiacente a ogni ordinamento, sia pure con diverse accentuazioni nella giuspubblicistica e nella politologia del nostro tempo, dove lo schema trova la sua più naturale collocazione, presentandosi con tutti i connotati di una conformazione giuridica (in senso positivistico) del potere, talvolta con un significato totalizzante», p. 9.

Orbene, il riferimento al *trasferimento di poteri sovrani* dagli Stati membri all'Unione (peraltro acutamente rilevato da De Witte nel suo utilizzo semantico tramite un'analisi comparata con alcune costituzioni interne)[255] richiama anzitutto il concetto di sovranità "limitata" che Besson ci aiuta a comprendere.

2. Rapporto tra sovranità e potere nell'Unione europea

Quanto al primo interrogativo, ovviamente abbandonata ogni considerazione assolutistica della sovranità propria della sua accezione classica (bodiniana – hobbesiana), si è detto che l'interdipendenza tipica della realtà post-wesfaliana ha inevitabilmente comportato un ridimensionamento del concetto, con un sempre più frequente trasferimento e divisione di competenze, di cui il processo di integrazione europea (da qualunque teoria dell'integrazione lo si consideri, seguendone l'evoluzione) è estremamente emblematico.

Ma cosa comporta di preciso tale constatazione? Besson ci torna molto utile nel chiarire i termini della c.d. "sovranità limitata", intesa non semplicemente come autolimitazione dello Stato sovrano propria del diritto internazionale classico, ma come conseguenza di limitazioni che derivano dall'interdipendenza esterna: «*these inherent limitations to external sovereignty have also become constitutive limitations to internal sovereignty in modern international law. Besides domestic constitutional limitations and transnational human rights guarantees, more and more constitutional orders have become so intertwined that much of their laws and decision-making competences overlap and their internal sovereignty has been affected, as is the case in the EU in particular*»[256]. Il problema, in questa concezione di sovranità limitata e frammentata, è individuare la "*soglia*" oltre la quale i limiti di sovranità o il trasferimento di poteri sovrani possano arrivare a svuotare la posizione di chi li deteneva.

Perplessità dello stesso tenore si pongono per quella variante molto simile del concetto, intesa come sovranità "condivisa" o "disaggregata". Essa deriverebbe proprio dall'affermarsi, a partire dal secondo dopoguerra, della sovranità popolare, per cui – ci ricorda Besson – "*i popoli sono diventati*

[255] B. DE WITTE, Sovereignty and European Integration, *cit*., p., qui l'autore rileva la distinzione tra *trasferimento di poteri sovrani*, a cui fa chiaro riferimento *Van Gend en Loos*, come anche alcune Costituzioni statali, e *limitazione di sovranità*, che pure compare in altre Costituzioni di Stati membri, e fa quindi derivare che, sebbene potrebbero esserci trattati internazionali che comportano limitazioni di sovranità (come la giurisprudenza Wimbledon conferma) senza per questo trasferire poteri alle relative istituzioni, nello specifico caso comunitario "le due operazioni sono inseparabili" e ciò sarebbe infatti palesato sin dalla seminale sentenza *Costa c. ENEL, per concludere dunque che nell'Europa del* secondo dopoguerra sarebbe emerso un "compromesso dottrinale", comune ai vari stati, tra il concetto tradizionale di sovranità statale e le nuove esigenze della cooperazione internazionale e dell'integrazione europea. Egli enuncia così questa dottrina:«s*overeignty continues to reside in the people and is to be exercised primarily by the institutions of the state*».

[256] BESSON, *op. cit*., par.76.

i soggetti della moderna sovranità popolare": «*those peoples organize and constrain their sovereignty through the international and the domestic legal orders at once*»[257]. In realtà, però, questo concetto di sovranità condivisa ha destato perplessità per la sua vaghezza, per la difficoltà di determinare chiaramente gli spazi e i confini di questa condivisione (e dunque di una "sovranità funzionalmente limitata")[258], perché ciò contrasterebbe con la stessa considerazione di sovranità quale ultima autorità, per cui "se la sovranità è ovunque, allora pare che da nessuna parte sia particolarmente importante"[259].

Ancora, tra punti deboli e note di merito, Cannizzaro rilevava al riguardo: «la dottrina della sovranità ripartita, pur logicamente aberrante, ha avuto un merito, (…) ha contribuito a far emergere la nuova sfida portata alla sovranità da sistemi complessi, quali gli Stati federali (…) E tuttavia, la sfida portata alla sovranità dal sistema delle competenze (…) è riemersa prepotentemente nel diverso contesto della devoluzione di competenze a favore di enti sovranazionali»[260].

Difatti, se le perplessità sul concetto di "sovranità condivisa" paiono condivisibili, specie considerando l'evoluzione del processo di integrazione, per cui empiricamente «*it can reasonebly be argued that ther is no sphere of national policy which is fully autonomous and which is not capable of being significatly circumscribed by a rule or principle of EU law*»[261] (constatazione che, a distanza di anni, ridimensiona parecchio l'inciso della *Van Gend en Loos* sul trasferimento "in settori limitati"), dall'altro lato ciò non implica automaticamente una "dissoluzione" del concetto di sovranità, derivante dalla difficoltà di "collocare" o "ripartire" tale ultima autorità.

In tal senso, si condividono le risalenti ma ancora attuali riflessioni di De Witte, in commento al turbolento periodo che accompagnò l'ingresso di Maastricht e il famoso intervento del Tribunale tedesco al riguardo. In sostanza, l'autore affermava che «*if sovereignty is divided, it loses its distinguishing trait*» e però riferiva, rispetto alla necessità di superare questa difficoltà, la posizione di parecchi autori che, piuttosto che formulare una concezione della sovranità alternativa e "adatta all'Europa", suggerivano di abbandonare il concetto, ormai obsoleto. Notava dunque l'autore: «*one would like to be convinced by the arguments offered, but the conclusion, that sovereignty is neither here nor there but dissolved in thin air, is rather troublesome. How should one order the complex*

---

[257] Ibidem, par. 83.

[258] Così G. DE BURCA, op. cit., p. 456.
In questo ordine di considerazioni, pare non inopportuno iscrivere, per esempio, un riferimento, alle interessanti ed esaustive riflessioni di Arena sulla nozione di "situazioni puramente interne", rispetto alla quale l'A. conclude: «Tale nozione, al contrario, costituisce la cifra del carattere *sui generis* dell'integrazione perseguita dall'Unione europea: un'integrazione *più intensa* di quella generalmente promossa dalle organizzazioni internazionali, ma *meno profonda* di quella che normalmente caratterizza gli Stati federali, in quanto per realizzarsi pienamente *all'interno* degli Stati membri necessita, ancora oggi, della collaborazione degli organi statali », in A. ARENA *Le «situazioni puramente interne» nel diritto dell'Unione Europea*, Editoriale Scientifica, 2019, p. 267.

[259] Così N. WALKER nel descrivere questo approccio e i suoi limiti; Late sovereignty in the European Union, cit., p. 15

[260] E. CANNIZZARO, *La sovranità oltre lo Stato*, cit., p. 38 e 40.

[261] G. DE BURCA, *ibidem.*

web of legal relationships in Europe today without the help of the principle of sovereignty determining where final authority, in the case of conflict, lies? (….) Could it be that sovereignty lies with the peoples of the European Union taken together, rather than with each of those peoples separately? That might be a heretical statement for the German Constitutional Court, but the Russian Constitution of 1993 shows that it can make constitutional sense to attribute sovereignty to a multinational people»[262]. Ciò ci riconduce al tema della sovranità popolare e dunque alla (accennata) proposta di Habermas di una sovranità condivisa intesa come "doppio sovrano": «*double sovereign of European citizens and peoples*»[263], alludendo ai discorsi già introdotti su cause ed effetti della *legitimacy crisis* e sulla possibilità o meno di individuare un "popolo" come "potere costituente"[264].

Ma ancor più, ciò consente adesso di comprendere la necessità delle teorie sopra esposte che cercano di spiegare il processo di integrazione.

Infatti, è proprio tra queste parole della *Van Gend en Loos* che l'analisi delle teorie delle relazioni internazionali e di quelle sull'integrazione europea trova più opportuna collocazione: ossia, laddove emerge la difficoltà di definire l'effettiva portata del trasferimento di poteri (e autorità?) all'Unione (dunque, in sostanza l'imperitura questione dei rapporti tra ordinamento dell'Unione e domestici – che non vogliamo qui approfondire).

Così, basti solo notare che con evidenza la teoria realista delle relazioni internazionali, così come l'intergovernamentalismo tra le teorie dell'integrazione (ma anche, per certi aspetti, il funzionalismo) continuano a ritenere, nonostante i contrapposti interventi della Corte di giustizia, che la sovranità degli Stati non sia effettivamente colpita. Mentre, dall'altro lato rinnovati richiami federalisti (non senza reminiscenze neo-funzionaliste) sono stati proposti – con qualche successo – proprio per spiegare il progressivo trasferimento di poteri sovrani dagli Stati all'Unione[265].

Tuttavia, non sono mancati punti deboli a queste considerazioni, per cui per esempio: «*the attempt of federalism to* secure *an authoritative foundation for the EU system (…) either by*

[262] B. DE WITTE, *op. cit.*, p. 172-173.
[263] J. HABERMAS, Democracy in Europe: Why the Development of the EU into a Transnational Democracy Is Necessary and How It Is Possible, *European Law Journal*, Vol. 21, No. 4, July 2015, pp. 554-555.
[264] Cfr. FICHERA, op. cit., p. 15.
[265] Così ci fa notare anche M. FICHERA, *op. cit.*, pp. 5-9, che espone le perplessità sul primo approccio: «*some definitions employed in the field of international relations (…), while pinpointing some important features of the EUs production on the global scene, do not provide a comprehensive picture of the legal and political implications of the creation of the machinery that at the same time challenges traditional Westphalian categories and relies on their factual support both for its existence and justification*». Quanto, invece, al secondo, precisa: «*this mind-frame has been expressed by its proponents in ever subtler and more refined ways. Thus, while recognising the awkwardness of applying to the EU all the standards of a federal State, it has been increasingly argued over the years that, by relinquishing the ideas of absolute and undivided sovereignty and united constituent power, we should be able to identify a combination between international law and national law elements, and, as a result, define the EU as a sort of 'federation of States'. The EU would stand out as a coherent legal and political order, in which dual sovereignty is already operative (…). No priority is conferred on either source of authority*», pp. 8-9.

proposing a federal State of a federation of States as a finalité, leads to invoking a final source of legal authority (…), which threatens the project itself by circumscribing its democratic credentials. The sources of legitimacy for transnational integration seems to be identified ultimately through a top-bottom rather than bottom-top, perspective»[266].

Muovendo da qui, un diverso approccio sembrerebbe più adeguato a spiegare la realtà dei "rapporti di sovranità" tra Stati e Unione, tentando di rispondere a interrogativi come "*what are the ultimate foundations – if any – of the EU as a polity? In what sense and to what extent, should we ascribe as a 'compound or association of States' coming together formally by way of an International Treaty the 'normative power' of a constitutional community?*" [267]. Si tratta dell'approccio che – come si accennava – considera *l'ordine eterarchico*[268] e che può essere ravvisato, nelle varie sfaccettature del *pluralismo costituzionale*.

Diversi sono i sostenitori, pur con posizioni non identiche, di questa concezione (*species* del più generale pluralismo giuridico, di romaniana memoria), intesa come la più fedele a fotografare l'attuale assetto dei rapporti nell'ambito dell'ordinamento dell'Unione. Esso concepirebbe la sovranità come una "pluralità di unità" e di possibili relazioni al suo interno[269].

Così Walker, in uno dei suoi primi contributi sul tema, chiariva: «*Constitutional monism merely grants a label to the defining assumption of constitutionalism in the Westphalian age which we discussed earlier, namely the idea that the sole centres or units of constitutional authorities are states Constitutional pluralism, by contrast, recognizes that the European order inaugurated by the Treaty of Rome has developed beyond the traditional confines of international law and now makes its own independent constitutional claims, and that these claims exist alongside the continuing claims of states. The relationship between the orders, that is to say, is now horizontal rather than vertical - heterarchical rather than hierachical*»[270]. Senza poterci addentrare, ma giusto per rendere il concetto più chiaro, Maduro lo spiegava – almeno nella sua valenza empirica – come «*what best describes the current legal reality of competing constitutional claims of final authority among different legal orders (belonging to the same legal system) and the judicial attempts at*

[266] Ibidem, pp. 11-12.
[267] M. FICHERA, op.cit.
[268] Invero, il concetto di *ordine eterarchico* (in contrapposizione a *gerarchico*) emerge nelle scienze sociali grazie a Luhmann ed effettivamente, *rebus sic stantibus*, pare essere abbastanza congeniale per comprendere l'attuale meccanismo europeo, come faceva rilevare il Prof. A. Andronico, durante un seminario per dottorandi tenuto nel dicembre 2019 all'Università di Catania, Dipartimento di Giurisprudenza. Cfr. N. LUHMANN, *Teoria della società*. 1992.
[269] N. WALKER, *Late sovereignty*, *cit*., p. 18.
[270] N. WALKER, The Idea of Constitutional Pluralism, in *EUI Working Paper LAW*, No 2002/1, pp. 26-27.
Si veda per una recente riconsiderazione Id., Constitutional Pluralism Revisited, *European Law Journal*, vol. 23, no. 3, 2016, pp. 333-355.

accommodating them»[271]. Senz'altro l'argomento andrebbe approfondito poiché ricco di spunti variegati, come pure andrebbero trattate le non poche critiche ad esso mosse che ne individuano limiti e debolezze[272], ma ciò per il momento è sufficiente per trarre le fila del nostro discorso. Si aggiunga solo una notazione, che consente di legare quanto detto al secondo interrogativo che abbiamo formulato a partire dalle parole della seminale sentenza. La notazione, fatta presente da Maduro, per cui il pluralismo costituzionale è stato considerato non semplicemente come un rimedio al rischio di conflitti costituzionali di autorità, ma ancor più come "la migliore rappresentazione degli ideali di costituzionalismo per l'attuale contesto di accresciuto pluralismo e *deterritorializzazione del potere*"[273].

Proprio quest'ultimo aspetto ci dà il *la* per tentare una risposta al secondo interrogativo, quello che dall'assunto per cui gli Stati hanno "*trasferito poteri sovrani*" si domanda se ciò possa implicare – oltre quanto detto rispetto alla posizione degli Stati, dunque guardando dalla prospettiva opposta – una qualche affermazione di *sovranità dell'Unione* (pur in un senso "adattato" o "rimodulato" del concetto di sovranità). La questione riprende, in qualche modo, il simpatico e ormai celebre parallelismo proposto da MacCormick tra i concetti di sovranità e verginità, tale per cui la "cessione" da parte di chi la detiene non ne implica l'acquisizione a chi la riceve[274]. In realtà, per quanto attraente, l'argomento nel caso di specie non è così scontato[275].

La cessione di poteri sovrani dagli Stati membri all'Unione europea

Affrontare questo aspetto, nel modo più congeniale e chiaro, impone un richiamo alla nota sentenza che viene generalmente associata a quella in analisi e ne costituisce un imprescindibile corollario: *Costa c. ENEL* e l'elaborazione del principio del *primato del diritto comunitario* su quelli degli Stati membri.

In uno dei passaggi fondamentali, essa così recita: «*a differenza dei comuni trattati internazionali, il Trattato C.E.E. ha istituito un proprio ordinamento giuridico, integrato nell'ordinamento giuridico degli Stati membri all'atto dell'entrata in vigore del Trattato e che i giudici nazionali sono tenuti ad osservare (…). Tale integrazione nel diritto di ciascuno Stato*

[271] M. POIARES MADURO, *Three claims of Constitutional Pluralism*, in M. AVBELJ -J. KOMÁREK (Eds), Constitutional Pluralism in Europe and beyond, 2012, pp. IV-5.
[272] M. FICHERA, op. cit.; WILKINSON, cit.
[273] M. POIARES MADURO, Ibidem.
[274] N. MAC CORMICK, *op. cit*., p. 16: «*Let us think of it rather more as of virginity, which can in at least some circumstances be lost to the general satisfaction without anybody else gaining it*».
[275] *Ex multis*, per esempio, CANNIZZARO riconosce la mancanza di potere coercitivo (solitamente distintivo per identificare la sovranità di uno Stato) in capo all'Unione, alla quale sono stati trasferiti "solo" poteri normativi, e ammette però che "appare difficile che l'esercizio di tali poteri ad opera dell'Unione non abbia causato una contrazione della titolarità di poteri e prerogative internazionali degli Stati membri". Cfr. E. CANNIZZARO, *Diritto internazionale*, cit., p. 330.

membro di norme che promanano da fonti comunitarie, e più in generale, lo spirito e i termini del Trattato, hanno per corollario l'impossibilità per gli Stati di far prevalere, contro un ordinamento giuridico da essi accettato a condizione di reciprocità, un provvedimento unilaterale ulteriore, il quale pertanto non potrà essere opponibile all'ordine comune»[276].

Oltre a ribadire le peculiarità del "proprio" ordinamento giuridico, la Corte introduceva un principio cardine per dare effettività a quello pronunciato poco prima in *Van Gend en Loos*: gli *effetti diretti* di quel diritto verrebbero svuotati se si consentisse alle autorità nazionali di applicarlo a piacimento, facendo prevalere disposizioni interne.

Orbene, se in ciò può a ragione già ravvisarsi un intervento fortemente performativo del diritto comunitario rispetto ai diritti domestici, la Corte non si sbilanciava a parlare espressamente di sovranità. Né, invero, lo ha fatto successivamente, come ha notato De Witte[277]. Questo proprio perché, rileva acutamente l'autore, la Corte non ha cercato – e non cerca ancora, si direbbe – di creare una sorta di espressa "*dottrina alternativa della sovranità*", specie considerati i cadenzati ritorni di molte Corti nazionali (e che non si arrestano: si pensi alla pronuncia del Tribunale federale tedesco del 5 maggio 2020)[278] che, utilizzando termini più o meno ammorbiditi, in sostanza ribadiscono proprie prerogative sovrane.

Al contrario, evitando un "attacco frontale" sul punto, a partire proprio dai principi elaborati in quelle sentenze la Corte realizzerà la compiuta affermazione del diritto comunitario *semplicemente* esortando gli Stati affinché le loro prerogative sovrane non siano tali da ostacolare quei principi[279]. Nel "botta e risposta" che, come si è accennato, non cessa di perpetrarsi, la Corte non parla mai direttamente di sovranità come attributo proprio dell'Unione, ma continua (e il parere CETA ne è un importante esempio) a definire le caratteristiche che rendono quell'ordinamento peculiare. E nel fare ciò, però, può ravvisarsi implicitamente una sorta di "sovranità autoproclamata"?

Riteniamo di concondare con la De Burca che ha ritenuto al riguardo, commentando i principi derivanti da *Van Gend en Loos* e *Costa*, che «*while the doctrines of supremacy and direct effect articulated by the European Court of Justice do not in themselves entail or include a prior judicial assertion of the independence, original nature and autonomy of the EC legal order, these legal doctrines nonetheless follow as consequences from that assertation. In other words, they follow*

[276] Corte di giustizia, 6/64, 15 luglio 1964, p. 1144.
[277] B. DE WITTE, op.cit., pp. 154-155.
[278] Per un autorevole commento a caldo cfr. M. POIARES MADURO, *Some Preliminary Remarks on the PSPP Decision of the German Constitutional Court*, in Verfassunblog, 6 maggio 2020, disponibile qui: https://verfassungsblog.de/some-preliminary-remarks-on-the-pspp-decision-of-the-german-constitutional-court/
[279] B. DE WITTE, *op. cit*., p. 155: «*the recognition of the direct effect and primacy of Community law within the domestic legal order of the Member States. Yet (…) sovereignty inevitably casts its shadow on this matter of the reception of Community law*».

from the ultimate self-defending authority of that legal order. Supremacy of EC law is thus a consequence of the sovereignty of the EC rather than vice versa»[280].

Più in generale, questa tendenza, riscontrabile negli interventi della Corte di giustizia, parrebbe palesare l'andamento dell'intero processo di integrazione europea, secondo quella che è stato definito "il modello dell'integrazione senza sovranità": «l'integrazione europea (…) si è tenuta lontana dai simboli della sovranità, ma ha teso, piuttosto, a svuotarla del proprio contenuto»[281].

Dunque, saremmo tentati di riconoscere sommessamente una qualche "sovranità" in capo all'Unione, pur nel senso improprio del termine, pur molto distante da quello classico e non facilmente conciliabile con quello più moderno.

Sicuramente, per esempio, va escluso – nonostante il principio del primato – quel profilo della sovranità che la considera come "*ultimate authority*" proprio in considerazione dell'eterarchia che, si è detto, caratterizzerebbe il costrutto europeo: *«in the EU such authority is typically conferred upon the States. EU as transnational law thus consists not only of shared sovereignty and interactive executive, legislative and judicial powers, but also of complex networks, agencies, heterarchical sources of authority and source legislations. True, the transnational dimension does not rule out, but instead, enhances the possibility of conflict between different sources of authority. Yet, the principle of primacy of EU law does not imply that, in case of conflict with national law, the latter is invalidated: the national rule is rather disapplied. In other words, conflicts concern the applicability, not the validity of norms*»[282]. Non potrebbe spiegarsi, altrimenti, ciò che – nella diversa ottica di un sistema giuridico tradizionalmente gerarchico – verrebbe considerato il "paradosso giuridico" dell'Unione, che comporterebbe il riconoscimento della "primazia" del diritto dell'Unione rispetto a quello degli Stati membri «ma non la superiorità gerarchica complessiva nel sistema delle fonti»[283].

Invero, se consideriamo i quattro interrelati interrogativi che Lindhal propone come legati al concetto di sovranità (come problema filosofico), allora dobbiamo considerare anche altri fattori. Le

[280] G. DE BURCA, *Sovereignty and the supremacy doctrine, cit*., p. 454.

[281] E. CANNIZZARO, *Sovranità oltre lo Stato*, cit., p. 89, laddove continua: «Da questo punto di vista, l'esperienza europea costituisce la sfida forse più grande mai portata alla sovranità dello Stato». Invece,l'autore parla di "modello di integrazione senza sovranità" a p. 90, chiarendo: «A differenza del disegno delle Nazioni Unite, quindi, l'integrazione avrebbe dovuto progredire senza turbare la sovranità degli Stati, ma, nel contempo, erodendone progressivamente il contenuto e preparare il terreno per altre, e ben più impegnative, forme di integrazione», cfr. *infra*, par. 2, Capitolo I, Parte IV.

[282] M. FICHERA, *The foundations, cit.*

[283] Così S. DELLAVALLE, *op. cit*., p. 207, in cui, appunto, precisa che il "paradosso" è tale se si assume la tradizionale considerazione di un sistema gerarchico e, esponendo la soluzione proposta da Habermas, ravvisata nella suddetta "sovranità condivisa". Quindi poi conclude l'autore: «Ne risulta che, in un sistema giuridico non strettamente e generalmente gerarchico, ma pluristratificato e poliarchico, i conflitti tra norme giuridiche non potranno essere risolti facendo appello a una piramide delle fonti che qui non esiste, bensì solo ricorrendo al dialogo tra istituzioni, in generale, e tra corti in particolare», p. 208.

sue domande sono: «*(1) under what conditions does a political community constitute and maintain itself as a* unity*? (2) In what way do these conditions reveal that political unity is* contingent*? (3) What structure of* power *manifests itself in the process of constituting and maintaining a contingent political unity? (4) Finally, in what way does the structure of power, by constituting and maintaining a contingent political unity, shed light on the concept of* sovereignty*?»*[284]. Ebbene, senza poter approfondire la fine analisi dell'autore, vediamo già da queste semplici domande che un aspetto fondamentale è dato dal nesso con la struttura (e dunque, anche, l'esercizio) del potere. Qui vengono d'ausilio i preziosi studi sulla *natura* del potere dell'Unione, che riferiamo solo brevemente e riprenderemo all'occorrenza.

La natura del potere dell'Unione europea

Valutazioni sul potere dell'Unione assumono rilievo sia rispetto all'organizzazione dello stesso, per meglio comprendere il funzionamento dell'ente, sia perché impongono di interrogarsi sulla legittimazione di quel potere, e così riconducono alla questione di partenza. Su questo aspetto, dunque, si è visto che Dellavalle[285] ha analizzato l'origine del potere pubblico per giustificarne un esercizio legittimo, distinguendo tra potere "ascendente" e "discendente" e – dopo averne esposte le caratteristiche – applicando questi paradigmi all'Unione europea.

Alla prima categoria si riferirebbe la legittimazione democratica, con tutte le implicazioni relative al perenne *deficit* riscontrato nell'Unione, come anche alle posizioni che sostengono la *no demos thesis* (o *democracy without demos*) battendo sulla mancanza di un vero "popolo" europeo.

All'altra categoria, invece, si rifarebbe la legittimazione tecnocratica, da basare sulla "fiducia diffusa nella superiore competenza degli organi unionali", ma della quale l'autore mostrava i fallimenti, per proporre una rinnovata legittimazione dal basso esortando, a tal fine, una riforma istituzionale[286].

Un altro aspetto, estremamente interessante, sulla natura del potere dell'Unione è quello che deriva dalle riflessioni di Rojas-Hutinel e che ci condurrà a chiudere questa Prima Parte introducendo gli ultimi tasselli indispensabili per lo sviluppo del ragionamento sulla sovranità digitale, a partire dalla Parte III. L'autrice infatti ha notato che, se non mancano lavori sulla separazione dei poteri nell'Unione[287], poche sono state le riflessioni sulla *natura* di tale potere, che lei invece si proponeva di indagare. È proprio tenendo conto delle specificità dell'Unione che

[284] H. LINDHAL, Sovereignty and Representation in the European Union, in N. WALKER (ed), *Sovereignty in Transition*, Hart Publishing, 2003, p. 89.
[285] Ibidem, pp. 193-202, in cui l'autore sostiene che «esiste uno specifico potere pubblico dell'UE, nato originariamente dal trasferimento di competenze da parte degli stati membri, ma fin dall'inizio non pienamente riconducibile all'esercizio delle loro libere sovranità».
[286] Ibidem, pp. 203-220.
[287] Si segnala interessante ad esempio STRAUSS e K. LEANERTS.

l'autrice preferiva parlare di "potere" piuttosto che di "poteri" e, così, spiegava perché uno dei principi cardine dell'odierno Stato di diritto, ossia la montesquieuiana separazione dei poteri, non potrebbe trovare luogo *telle quelle* nell'Unione.

Molto brevemente, l'autrice mette in rilievo che il principio della separazione dei poteri ben può concepirsi all'interno di uno Stato, essendo la sua finalità quella di evitare la concentrazione del potere nelle mani di un solo organo che comporterebbe il rischio di dispotismo, in virtù della natura del potere statale essenzialmente politica.

Al contrario, nota l'autrice, un simile problema non si porrebbe a livello dell'Unione, essendo il suo potere essenzialmente di *natura giuridica*. Questa considerazione del potere giuridico risalirebbe proprio all'origine del progetto europeo: «*construire une paix durable entre les Etats européens en créant, par des mécanismes juridiques, les conditions de leur interdépendance de telle manière qu'ils ne soient plus en mesure de se faire la guerre (…). Dit autrement, l'Union de droit a été conçue comme préalable au projet politique européen ; or, par nature, un pouvoir juridique ne peut devenir arbitraire puisqu'il est tout entier pensé comme encadré* »[288].

Dunque, se il pericolo di abusi di potere è sventato, non ha senso parlare di separazione di poteri, da un lato; dall'altro, nondimeno, una concentrazione di potere può sempre aversi, producendo in tal caso – non abusi, ma – "*ipergiuridicità*".

È questo, secondo l'autrice, il principale problema che si pone per il potere dell'Unione, spiegandone le caratteristiche, proponendone una "moderazione" e paventando il connesso problema di "depoliticizzazione" che condurrebbe, in definitiva (e come confermato dalle ultime crisi), alla questione di legittimazione dell'Unione[289].

Nel condividere questa tesi, la si apprezza soprattutto per il merito di aver messo in risalto – se pur evidenziandone anche le criticità e i risvolti negativi – un aspetto forse scontato ma fondamentale, che nel diritto alla protezione dei dati personali, e nella sua portata (extra)territoriale, troverà particolare conferma: che il potere dell'Unione sta nel suo *diritto*.

In realtà, nella considerazione strumentale del diritto rispetto ad obiettivi ulteriori (di carattere economico ma con tendenza ad un fine politico) non si fa altro che riprendere la teoria funzionalista che, come detto più volte, ha permeato e in certa misura – nelle sue piccole varianti – continua ad accompagnare il processo di integrazione europea. Ma l'autrice sottolinea che proprio nel passaggio da "sistema giuridico" a "ordinamento giuridico", in cui i differenti Stati membri si uniscono verso un obiettivo comune, «*un fonction d'encadrement par le droit s'est dégagée progressivement*» e tale funzione viene definita come «*l'activité tendant à favoriser la cohérence entre les ordres*

[288] Così A. LEVADE, Préface, in N. ROJAS-HUTINEL, *La séparation du pouvoir*, cit., p. 20.
[289] N. ROJAS-HUTINEL, *La séparation du pouvoir*, *cit.*, pp.1-441. Sui concetti di ipergiuridicità, depoliticizzazione e moderazione si vedano in particolare le pp. 18-197, 203, 207, 224-227, 255-259,389-397.

juridiques nationaux et la production normative générée par l'Union européenne elle-meme au moyen du droit».[290]

In ciò sta il cuore del nostro discorso, che, come diremo (*infra*, Capitolo III, Parte III e Capitolo III, Parte IV), insiste anche sull'importanza del principio di coerenza nell'azione dell'Unione e nella complessiva architettura sovranazionale, per risaltare la centralità del diritto come caratteristica fondamentale che rende quell'ordinamento *sui generis*. In questo senso, è possibile rintracciare quindi qualche sembianza di sovranità: «Delle varie dimensioni dello Stato sovrano, l'Unione ne possiede essenzialmente una: la *dimensione normativa* (…). L'intero imponente edificio dell'integrazione europea si fonda sulle norme prodotte dall'Unione e sulla loro effettività»[291].

Come la Corte, peraltro, ci ricorda, è peculiare di tale edificio il fatto di essere dotato di un "quadro costituzionale proprio" e che «*rientrano in tale quadro i valori fondatori enunciati nell'articolo 2 TUE*»[292].

Passiamo dunque ad illustrarne gli aspetti essenziali, che ci consentiranno di chiudere questa parte di premesse basilari e sviluppare il ragionamento su queste fondamenta.

[290] Ibidem, pp. 115-116.
[291] E. CANNIZZARO, *La sovranità oltre lo Stato*, cit., p. 92, enfasi aggiunta.
[292] Corte di giustizia, Parere 1/17 del 30 aprile 2019 (CETA), punto 110.

CAPITOLO IV
DEI VALORI E DELLE PECULIARITÀ DELL'UNIONE EUROPEA: LA *EU RULE OF LAW*

1. Il sistema di valori su cui l'Unione si fonda: perno interno e proiezione esterna

«*(...) Una siffatta costruzione giuridica poggia sulla premessa fondamentale secondo cui ciascuno Stato membro condivide con tutti gli altri Stati membri, e riconosce che questi condividono con esso, una serie di valori comuni sui quali l'Unione si fonda, così come precisato all'articolo 2 TUE»*[293].

È curioso notare quanta enfasi venga posta sul carattere fondante del sistema di valori dell'Unione, intendendo quel sistema come qualcosa che sta alla base, all'origine dell'intero costrutto, al punto da ritenerne a ragione l'attuale crisi come qualcosa di destabilizzante e quasi irreversibilmente traumatico, ma poi accorgersi che la prima ufficiale previsione di diritto primario risale al Trattato di Lisbona[294]. Quasi che il riconoscimento pacificamente condiviso di quel sistema sia avvenuto all'alba della sua crisi. Ma, com'è noto, questo, oltre ad essere il perfezionamento del progetto funzionalista di integrazione europea, che vedeva il progressivo raggiungimento di un'Unione politica, è stato essenzialmente il risultato di una risalente e solida giurisprudenza della Corte di giustizia.

Ai nostri fini, basti qui premettere che l'articolo 2 TUE sancisce oggi che l'Unione si fonda su dei valori, che elenca, e che guidano tanto la sua azione interna (art. 3 par. 3 TUE) quanto quella esterna (art. 3 par. 4 TUE), dunque che sono propri della (e riferibili a) Unione ma anche "comuni" agli Stati membri, che a loro volta su quelli devono fondarsi, così da definire «un patrimonio costituzionale comune idoneo a definire l'essenza stessa dell'identità europea, pur nel rispetto (…) della diversità (…) dei popoli d'Europa»[295].

Se indiscussa è la portata ideale e politica di questo enunciato, è bene nondimeno chiarire la violazione dei valori "*produce conseguenze giuridiche",* sia per le istituzioni dell'Unione che per gli Stati membri, ma anche, come chiaramente deriva dalla necessità di proiettare all'esterno quei

[293] Corte di giustizia, parere 2/13, 18 dicembre 2014.
[294] Invero, Adam e Tizzano ci fanno notare che dei richiami ai valori iniziarono ad aversi a partire dall'Atto Unico Europeo, ma non in maniera sistematica come con l'attuale articolo 2 TUE, cfr. R. ADAM, A. TIZZANO, *Lineamenti di Diritto dell'Unione europea*, Giappichelli, 2016, p. 290.
[295] Ibidem, p. 291.

valori tramite l'azione esterna (art. 3 par. 3 e art. 21 TUE), nelle relazioni con Stati terzi[296]. In tale ultimo caso il riferimento è alla condizionalità, che non solo conduce la definizione degli accordi conclusi dall'Unione, ma governa anche le politiche di allargamento, definendo i criteri di adesione per Paesi terzi eventualmente candidati (art. 49 TUE). Tra gli strumenti a salvaguardia dell'articolo 2 TUE, è noto il (faticoso) meccanismo dell'articolo 7 TUE e le relazioni con la procedura di infrazione.

Orbene, i valori di cui all'enunciazione "sommaria" dell'articolo 2 TUE devono inevitabilmente considerarsi "a contenuto variabile" e dunque «poiché queste nozioni possono variare nel tempo, ciò che è importante determinare non è il loro contenuto astratto, ma piuttosto la *metodologia per individuare tale contenuto* in relazione a circostanze concrete e in un momento storico determinato»[297].

Ciò è vero quando questi valori vengono in risalto nella considerazione dei rapporti con singoli Stati membri, terzi o organizzazioni internazionali – dunque rispetto a contesti ordinamentali diversi dall'Unione – ma lo è ancor più nell'ambito stesso del contesto dell'Unione. Così, quanto al primo aspetto, Cannizzaro fa notare, per esempio, rispetto ai valori che si riferirebbero più alla forma di governo degli Stati membri, ossia stato di diritto e democrazia, che «È difficile, in proposito, ritenere che il medesimo *standard* valevole nell'ordinamento dell'Unione possa essere trasposto *tel quel* agli ordinamenti degli Stati membri. (…) proprio a causa dello stretto legame che c'è fra il contenuto di questi principi e la società che essi sono tesi a governare, sarebbe illusorio pensare di poter trasporre meccanicamente di modelli di democrazia e di stato di diritto da un ordinamento ad un altro»[298].

A maggior ragione ciò si impone nell'esercizio dell'azione esterna dell'Unione, laddove cioè essa è chiamata a "mostrarsi" verso l'esterno con una precisa identità. In questo senso, l'Unione è addirittura chiamata (art. 3 TUE) a promuovere suoi valori verso l'esterno (oltre che salvaguardarli dall'esterno). Questo aspetto verrà particolarmente trattato nella Parte IV, che cercherà di dimostrare come ciò effettivamente avvenga nello specifico settore della protezione dei dati personali, consentendo così all'Unione di definire il suo profilo nel contesto internazionale.

---

[296] Ibidem, pp. 291-292.

[297] E. CANNIZZARO, Il ruolo della Corte di giustizia nella tutela dei valori dell'Unione europea, in *Liber Amicorum Antonio Tizzano – De la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, Giappichelli, 2018, p. 162, corsivo aggiunto.

[298] Ibidem, pp. 162-163, laddove continua: "al suo interno alcuna Corte costituzionale. Ne consegue che la valutazione delle norme o delle condotte che violano i principi dello stato di diritto e di democrazia non potrà essere compiuta in astratto, sulla base di indici astratti di misurazione della loro osservanza. Non è, in altre parole, la congruenza normativa fra un ordinamento e dei parametri predeterminati, a fornirci tale valutazione, quanto piuttosto l'effetto concreto prodotto dalle norme costituzionali sulla società che esse governano".

Nell'azione esterna, in particolare, la Corte di giustizia ha sempre più spesso ribadito le peculiarità del sistema e la necessità di salvaguardarle, e i pareri sopra riportati (sull'adesione alla CEDU e sul CETA) ne sono un grande esempio. La dimensione esterna, infatti, è quella in cui meglio pare palesarsi la tendenza dell'Unione europea, e della Corte in particolare, alla sovranità come elemento di (auto)legittimazione. A tal fine, pare perfettamente in linea quanto notato da Mastroianni al riguardo: «Invero, però, il rigore della Corte nell'ammettere l'ipotetica possibilità di un controllo esterno, anche in casi in cui (come per l'adesione alla CEDU) la partecipazione ad un sistema istituzionale distinto sembra richiesto dai Trattati, ha ingenerato il dubbio che, nelle reali intenzioni della Corte, *il vero bene fine non sia rappresentato dalla salvaguardia dei valori europei quanto, piuttosto, dalla "sovranità" della Corte stessa, al punto di arrivare a preservare dall'incidenza "esterna" anche sfere di giurisdizione a lei al momento precluse, come nel caso della PESC*»[299], laddove la "sovranità della Corte stessa" si traduce inevitabilmente nella auspicata sovranità dell'Unione. Dunque, si tratterebbe di un'insistenza sui valori mossa dalla necessità di definire la propria identità, soprattutto all'esterno, attraverso la quale tentare una pretesa, ancorché implicita, sovranità, che potrebbe valere come risposta plausibile alla crisi di legittimazione dell'Unione laddove sussistano le condizioni per il suo realizzarsi.

Così, da un lato, si capisce perché la "crisi" interna di quei valori riproponga questioni di legittimazione, per cui torna tutto quanto abbiamo esposto sin ora; dall'altro, si spiega il nostro tentativo di proporre la dimensione digitale come quella nella quale parrebbero presentarsi le condizioni per il suo realizzarsi.

In particolare, riteniamo che la riprova di questa ipotesi di ricerca possa rintracciarsi nel *nesso*, che cercheremo di riscontrare in teoria e in pratica, tra ciò che chiameremo *EU rule of law*, come insieme peculiare di principi e obiettivi che caratterizzano l'Unione europea nella sua specificità, e protezione dei dati personali, come settore privilegiato in cui la prima troverebbe espressione nella dimensione digitale.

La seconda parte del lavoro si occuperà, dunque, di fornire le basilari conoscenze sul diritto alla protezione dei dati personali, mentre le parti terza e quarta si occuperanno di dimostrare in teoria e in pratica se tale nesso sussiste e funziona, per sfociare quindi in considerazioni sulla tendenza verso una sovranità digitale dell'Unione europea come tentativo di superamento della crisi di legittimazione dell'Unione. Per affrontare tutto questo, sarà quindi necessario, a seguire, un preliminare chiarimento su cosa intendiamo, e come utilizzeremo nell'intero lavoro, con il concetto di "*EU rule of law*".

[299] R. MASTROIANNI, Le garanzie dei valori nell'azione esterna e il ruolo della Corte di giustizia, in SCISO, R. BARATTA, C. MORVIDUCCI (a cura di), *I valori dell'Unione europea e l'azione esterna*, Giappichelli, 2016, p. 223, enfasi aggiunta.

2. Farsi un'idea sul concetto di "*EU rule of law*"

Con *EU rule of law* esprimiamo ben più del riferimento a uno dei valori fondanti elencati nell'articolo 2 TUE e comuni agli Stati membri. La "*EU rule of law*" si compone anche di quello, ma è molto di più: essa esprime le caratteristiche peculiari di ciò che identifica la *Unione di diritto*.

Nel novero di questi discorsi, è molto frequente esordire con il celebre discorso del presidente della Commissione Walter Hallstein all'Università di Padova nel lontano 1962, titolato proprio "La Comunità economica europea come una Comunità di diritto": «*[the] Community was not created by military power or political pressure, but owes its existence to a constitutive legal act. It also lives in accordance with fixed rules of law and its institutions are subject to judicial review. In place of power and its manipulation, the balance of powers, the striving for hegemony and the play of alliances we have for the first time the rule of law. The European Economic Community is a community of law […] because it serves to realize the idea of law*»[300].

Si sa bene che, poi, è stato a partire da *Les Verts* negli anni Ottanta che la Corte di giustizia ha espressamente dichiarato che «*la Comunità economica europea è una comunità di diritto nel senso che né gli Stati che ne fanno parte, né le sue istituzioni sono sottratti al controllo della conformità dei loro atti alla carta costituzionale di base costituita dal trattato*»[301], continuando da allora ribadire, con le parole e con la prassi, l'essenza di questo concetto.

L'essenza di questo concetto, riprendendo tutto quanto detto sin ora, starebbe proprio nell'idea dell'Unione come *ordinamento giuridico* autonomo e dotato di specifiche peculiarità: «*the idea of a legal order, in its existence and operation*»[302].

Il concetto di *EU rule of law* non si identifica, dunque, totalmente con quello di Stato di diritto o di *rule of law* classicamente inteso, di cui pure condivide l'aspetto essenziale: quello, cioè, della *necessità di limitazione del potere*; per il resto, quanto a sembianze e modalità, esso si caratterizza per le peculiarità proprie dell'Unione come comunità di diritto.

---

[300] Così riporta T. VON DANWITZ, The Rule of Law in the Recent Jurisprudence of the ECJ, in *Fordham International Law Journal*, Vol. 37, 5, 2014, pp. 1312-1313.
Si trova un riferimento anche nel Briefing del Parlamento europeo, *The EU as a community of law – Overview of the role of law in the Union*, March 2017, p. 2, disponibile qui: https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599364/EPRS_BRI(2017)599364_EN.pdf

[301] Corte di giustizia, 294/83, *Les Verts c. Parlamento europeo*, sentenza del 23 aprile 1986, p. 23.

[302] G. PALOMBELLA, Beyond Legality – Before Democracy. Rule of Law Caveats in the EU Two-Level System, in C. CLOSA, D. KOCHENOV (Eds), *Reinforcing Rule of Law Oversight in the European Union*, Cambridge University Press, 2016, p. 36.

L'utilizzo della formulazione in inglese, infatti, renderà meglio l'idea delle peculiarità dell'Unione, rievocando "l'impostazione di Dicey" di «un *complesso di canoni* che tendono, nella loro essenza, ad assoggettare l'azione di *ogni potere* (sia esso pubblico che privato) a *vincoli eteronomi*, posti a protezione degli altri componenti della collettività, resi *effettivi* mediante il sindacato di un apparato giudiziario effettivamente imparziale, e capaci di dimostrare in modo pubblico e trasparente che ogni potere di governo (ovvero di coazione autoritativa), da chiunque sia esercitato, si svolga *senza abusi* e *nel rispetto di principi di giustizia*, ovvero consenta il mantenimento di un regime di rapporti proporzionato, equo, in una sola parola "sopportabile" da parte di ogni parte o consociato»[303]. Pertanto, purché siano questi i fini, poco importa se le modalità ricalchino o meno quelle classicamente previste dallo Stato di diritto.

Infatti, l'Unione si caratterizza anzitutto per essere una comunità nella quale tutti i suoi Stati membri, sì, condividono, al loro interno, il valore dello Stato di diritto, nei suoi classici principi cardine, per l'individuazione dei quali vale il riferimento all'ultima Relazione della Commissione sullo Stato di diritto nell'Unione: «*Nel concetto di Stato di diritto rientrano principi come la legalità, in base alla quale il processo legislativo deve essere trasparente, responsabile, democratico e pluralistico; la certezza del diritto; il divieto di esercizio arbitrario del potere esecutivo; una tutela giurisdizionale effettiva da parte di organi giurisdizionali indipendenti e imparziali, e un controllo giurisdizionale effettivo anche per quanto riguarda il rispetto dei diritti fondamentali; la separazione dei poteri; e l'uguaglianza davanti alla legge*»[304].

Il rispetto di questo valore, nel complesso dei suoi principi, all'interno degli ordinamenti degli Stati membri garantisce il buon funzionamento dell'architettura sovranazionale: «*L'UE si fonda sullo Stato di diritto: le sue basi giuridiche, politiche ed economiche sono messe a repentaglio laddove è minacciato lo Stato di diritto. Ogni carenza in uno Stato membro influisce sugli altri Stati membri e sull'UE nel suo insieme*»[305]. In tal senso, infatti, «*for the EU to function effectively as a political and legal edifice, it is essential that both the EU and individual Member States can reasonably rely on the efficacy of the justice systems of other Member States*»[306].

Ma tale valore, in sé, ancorché comune agli Stati membri, non esaurisce né definisce propriamente la *EU rule of law*.

Infatti, accanto a questa comunanza tra gli Stati membri, la comunità di diritto si caratterizza per un aspetto peculiare che la rende molto differente dagli Stati – e su cui, da ultimo, si gioca il

[303] G. SALERNO, *European Rule of Law*: un principio in cerca d'autore, in *Federalismi*, 17 giugno 2020, p. 5.
[304] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Relazione sullo Stato di diritto 2020 – *La situazione dello Stato di diritto nell'Unione europea*, COM(2020) 580 final, 30.09.2020, p. 1.
[305] Ibidem, p. 3.
[306] MAGEN A. PECH L., The rule of law and the European Union, in MAY C., WINCHESTER A. (Eds), *Handbook on the Rule of Law*, Elgar, 2018, p. 256.

"dilemma" della sovranità – che emerge bene dal discorso di Hallstein: l'assoluta assenza di potere coercitivo. Anche per questo (e in ciò a differenza delle altre organizzazioni internazionali) essa trova la sua forza nel *potere normativo*, che riesce a imporre grazie ai meccanismi giuridici che performano gli Stati membri attraverso l'utilizzo degli apparati amministrativi e giudiziari di questi ultimi, consentendo l'effettiva applicazione delle proprie norme e dunque anche contribuendo «in misura significativa al governo delle comunità territoriali dei propri Stati membri»[307] (si dirà, peraltro, anche del c.d. *normative/regulatory power Europe* come influenza esterna dell'Unione, specie nel settore della protezione dei dati personali, cfr. Parte IV).

Da ciò, infatti, deriverebbero le "caratteristiche specifiche" del diritto dell'Unione e che, pertanto, consideriamo come elementi peculiari ulteriori per definire la *EU rule of law*: «*come rilevato più volte dalla Corte, il diritto dell'Unione si caratterizza per il fatto di derivare da una fonte autonoma, costituita dai Trattati, per il suo primato sul diritto dei singoli Stati membri (...) nonché per l'effetto diretto di tutta una serie di disposizioni applicabili ai cittadini di detti Stati membri nonché agli Stati stessi*»[308]. Dunque, ribadita l'autonomia della sua fonte, i principi del primato e dell'effetto diretto regolerebbero gli equilibri con gli Stati membri, ai quali inevitabilmente si aggiunge il meccanismo del *rinvio pregiudiziale* che ne consente l'effettiva operatività.

Inoltre, nell'esercizio di "poteri e funzioni", come abbiamo detto, a differenza della "separazione di poteri" propria dello Stato di diritto negli ordinamenti degli Stati membri, l'ordinamento dell'Unione si caratterizza per il *principio dell'equilibrio istituzionale*, che bilancia i rapporti di intervento tra le istituzioni sovranazionali, e quello delle *competenze di attribuzione*, che regola i rapporti di intervento con gli Stati membri.

Pertanto, come ha ben argomentato Rojas-Hutinel (ma anche, in qualche modo, riprendendo Majone), il *diritto* come *potere* dell'Unione, che consente alla stessa di modellarsi, all'interno, e affermarsi, all'esterno come *Unione di diritto*, è la caratteristica centrale della *EU rule of law*. E l'affermazione di questo diritto, tanto rispetto agli Stati membri che nell'ottemperanza delle istituzioni sovranazionali, quanto ancora nell'esercizio dell'azione esterna e dunque nella sua manifestazione rispetto agli Stati terzi, si conferma massimamente attraverso la tutela *effettiva* dei diritti fondamentali, ossia *propri* di quell'ordinamento. L'effettiva tutela di quei diritti, alla cui conformità deve rispondere l'operato dell'intera Unione, e la corretta applicazione del suo diritto, all'interno e nell'azione esterna, vengono garantiti dal sofisticato apparato giurisdizionale

[307] E. CANNIZZARO, *Diritto internazionale*, cit., p. 330.
[308] Corte di giustizia, Parere 2/13 (*Adesione alla CEDU*), 18 dicembre 2014, punto 172.

predisposto dai Trattati che trova in prima fila i giudici comuni degli Stati membri e il suo presidio ultimo nella Corte di giustizia.

Dunque, tutto questo insieme si intende quando ci riferiamo al concetto di *EU rule of law*, concetto che, nel suo c.d. "ruolo pluridimensionale", risponderebbe quindi infine a uno specifico disegno: «nell'ordinamento dell'Unione la finalità ultima della *European rule of law* è quella dell'inveramento e del mantenimento dell'Unione medesima»[309].

Così intesa la *EU rule of law*, se ne capisce giocoforza il rilievo quando si pongono questioni di legittimazione dell'Unione, ma, soprattutto, se ne propone spontaneamente il *nesso* con la protezione dei dati personali, quando si tenta di indagare la tendenza alla sovranità digitale come possibile risposta alle suddette crisi di legittimazione: la protezione dei dati personali nella dimensione digitale altro non sarebbe che la conferma, in quella dimensione, delle peculiarità della *EU rule of law*.

Prima di indagare tale nesso, è indispensabile dunque presentare le caratteristiche del diritto europeo alla protezione dei dati personali. A ciò dedicheremo la Parte II del presente lavoro.

[309] G. SALERNO, *European Rule of Law*: un principio in cerca d'autore, cit., p. 6, sottolineato aggiunto. Ibidem, p. 9, per "ruolo pluridimensionale".

PARTE II

Queste pretese tanto rapaci
sono state sostenute
dall'assenza di leggi in grado di fermarle,
dalla comunione di interessi
tra i primi capitalisti della sorveglianza
e le agenzie di servizi segreti,
e dalla tenacia con la quale le corporation
hanno subito difeso i territori conquistati.

S. Zuboff, Il Capitalismo della sorveglianza

PARTE II

SOMMARIO: I. Sulla protezione dei dati personali. – 1. Assumere una prospettiva. – 2. Origini ed evoluzione tra *privacy* e protezione dei dati personali. – 3. L'emersione di un diritto…a partire dalla *privacy* – 4. Il diritto alla protezione dei dati personali nelle sue diverse accezioni. – II. La protezione dei dati personali in Europa. – 1. Un'analisi cronologica a partire dall'esterno, seguendo (ancora) "*la spinta dello spazio sulla forma*". – 2. I principali interventi in seno al Consiglio d'Europa. – III. Il diritto alla protezione dei dati personali nell'Unione europea. – 1- Cenni introduttivi. – 2. L'evoluzione del quadro normativo. – 3. Il quadro istituzionale dedicato alla protezione dei dati. – IV. Tra Strasburgo e Lussemburgo: i *grands arrêts* europei sull'evoluzione della protezione dei dati personali. – 1. Alle origini delle tutele a livello sovranazionale: la contaminazione dei modelli interpretativi. – 2. Accostamenti e divergenze.

CAPITOLO I

SULLA PROTEZIONE DEI DATI PERSONALI

1. Assumere una prospettiva

«Poiché il trattamento di informazioni personali a mezzo dell'elaboratore accresce il potere di chi è in grado di avvantaggiarsi, direttamente o indirettamente, della nuova tecnologia, la prospettiva da considerare non può essere soltanto quella di una maggiore efficienza di strutture (pubbliche o private) tradizionali, bensì quella di *nuove forme di organizzazione del potere*: di conseguenza, non è possibile affrontare la nuova dimensione sociale individuata dagli elaboratori elettronici senza mettere a punto *tecniche di regolamentazione adeguate*»[1].

Così scriveva Rodotà nel 1973, ponendo l'attenzione su un problema tanto inesplorato allora quanto attuale oggi: la protezione dei dati personali. Eppure, le considerazioni profeticamente esposte in "*Elaboratori elettronici e controllo sociale*" appaiono particolarmente lucide nell'individuare i confini effettivi della questione che si pone ancora oggi. Riportando a mo' di esempio la vicenda del *National Data Center* statunitense, l'istituzione del quale fu impedita ("*ma questa fu – come è stato giustamente osservato – una vittoria di Pirro*"), l'autore precisava: «questo specifico esempio conferma che l'unica via corretta per affrontare i problemi sociali discendenti dall'impiego degli

[1] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Il Mulino, 1973, p. 35, enfasi aggiunta.

elaboratori elettronici è quella che muove *dall'analisi delle trasformazioni dell'uso e della distribuzione del potere nelle strutture pubbliche e private*»[2].

Quest'opera "risalente" assume particolare rilievo ai nostri fini perché, nonostante le imponenti evoluzioni e riforme intercorse nel tempo che la separa da noi (e nonostante, pur coi dovuti riferimenti a ordinamenti europei e americani, improntata ad un'analisi eminentemente nazionale), fornisce un paradigma che risulta ancora (forse, ancora di più) appropriato all'analisi sul tema. Essa, infatti, pone in luce il nesso tra raccolte di dati e potere, da un lato, e necessità di regolazione, dall'altro, che si rende oggi più che mai evidente, tanto che è frequente il riferimento a «uno statuto di regole funzionale alla stessa economia digitale» e si riconosce che «il nuovo quadro giuridico europeo muove dalla consapevolezza della nuova geografia dei poteri»[3]. A partire da questa prospettiva, e dunque con questo paradigma di fondo, si condurrà in questa Parte II un'analisi ricognitiva/ricostruttiva del c.d. diritto alla protezione dei dati personali nell'Unione europea.

2. Origini ed evoluzione, tra *privacy* e protezione dei dati personali

Qualsiasi studio che aspiri a precisare i termini della protezione dei dati personali non può prescindere da un introduttivo, per quanto breve, riferimento alla relazione con il concetto di *privacy*, il suo sviluppo e la necessità di chiarirne i contorni.

Per quanto affini, infatti, il diritto alla riservatezza o al rispetto della vita privata (che si intende con il più generico termine "*privacy*") va distinto dal diritto alla protezione dei dati personali (a cui pure, in maniera non del tutto corretta, il termine "*privacy*" parrebbe spesso riferirsi). Così, anche,

[2] Ibidem, p. 37, in cui l'autore continua: «Al contrario, denunciare singoli inconvenienti, prospettare un'apocalisse orwelliana, riaprire i dossier delle "due culture", può servire soltanto per qualche frettolosa panacea o per dibattiti consolatori, mentre gli elaboratori proliferano senza alcun controllo nella nostra società. L'ideologia del laisser-faire tecnologico e la superbia dei tecnici concorrono ad oscurare i nessi con il quadro istituzionale a cui riferire l'azione dei soggetti che si servono degli elaboratori elettronici; e ad accreditare ulteriormente l'opinione che la nostra società non possa sottrarsi ad un "inquinamento da elaboratore". L'umanità sembra ad un bivio tra una mostruosa efficienza e la difesa delle libertà individuali: negli stessi titoli dei libri si parla, con toni da battaglia di "assalto alla privacy". Non si sottolineerà mai abbastanza la unilateralità di questa impostazione, che fa perder di vista i vantaggi sociali dell'impiego degli elaboratori elettronici. Ed è opportuno aggiungere subito che non si tratta tanto di vantaggi su piano dell'efficienza (come negli esempi ricordati in precedenza), quanto piuttosto della possibilità di realizzare forme nuove di gestione del potere, offrendo alle stesse libertà individuali possibilità di espansione fino ad oggi sconosciute».
Si segnala, peraltro, un articolo precedente dell'autore in tal senso: ID., Elaboratori elettronici, strutture amministrative e garanzie per la collettività, in Rivista trimestrale di diritto pubblico, 1971, pp. 1842-1852.

[3] Così, molto di recente, A. SORO, La tutela di un diritto fondamentale: un primo bilancio applicativo – *Prefazione*, in (a cura di E. Tosi) *Privacy Digitale – Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè, 2019, XXVI.

emerge dal *Manuale sul diritto europeo in materia di protezione dei dati* (edizione 2018), curato dall'Agenzia dell'Unione europea per i diritti fondamentali di concerto con il Consiglio d'Europa e il Garante europeo della protezione dei dati[4]. Invero, ogni ipotetica perplessità al riguardo dovrebbe ritenersi fugata – almeno, nell'ordinamento dell'Unione – vent'anni or sono dalla precipua scelta del legislatore europeo di sancire la previsione di entrambi i diritti nella Carta dei diritti fondamentali dell'Unione europea, dedicando a ciascuno una specifica norma (com'è noto, rispettivamente, l'articolo 7 sul rispetto della vita privata e della vita familiare; l'articolo 8 sulla protezione dei dati di carattere personale). D'altronde (come si avrà modo di analizzare), sono ben note le conclusioni dell'Avvocato Generale Sharpston nel riconoscere due diritti distinti: quello "classico" alla tutela della vita privata (che, fuori dell'ordinamento comunitario, viene individuato nell'articolo 8 CEDU) e quello "moderno" alla tutela dei dati personali (con riferimento, sempre in seno al Consiglio d'Europa, alla Convenzione n. 108 del 1981; cfr. *infra,* par. 4)[5]. Ciononostante, l'effettiva demarcazione tra i due non è facilmente definibile[6], mentre non si può escludere un'inevitabile contaminazione, tanto che, com'è stato notato, pur nella consapevolezza delle previsioni della Carta sono stati molteplici e variegati gli interventi delle "Corti europee" (*rectius*, a fini del presente lavoro, della Corte di giustizia dell'Unione europea e della Corte europea dei diritti umani) nel senso di ribadirne il reciproco legame tra i due diritti: «*the jurisprudence has justifiably considered privacy to be at the core of data protection*»[7]. Di tale giurisprudenza si dirà diffusamente nel prosieguo; qui preme essenzialmente spiegare il contesto e le dinamiche che hanno portato all'emersione del diritto al rispetto della vita privata, quindi, alla protezione dei dati personali.

[4] FRA-COE-EDPS, *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, 2018.

[5] Conclusioni AG E. SHARPSTON, presentate il 17 giugno 2010, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Harmurt Elfert c. Land Hessen,* punto 71.

[6] Ciò, in particolare, quanto al contesto della Convenzione europea dei diritti umani, in cui l'unica previsione di riferimento per entrambi è l'articolo 8 CEDU, e rispetto al quale, dunque, la necessità di demarcazione ha avuto maggior rilievo. Cfr., *ex multis,* A. TERRASI, *Protection of Personal Data and Human Rights between the ECHR and the EU Legal Order*, in A. CALIGIURI (ed.), *Legal Technology Transformation. A Practical Assessment*, Editoriale Scientifica, 2020, che, nell'esaminare gli interventi più rilevanti della Corte di Strasburgo al riguardo, sviluppava la sua analisi a partire da considerazioni di tale tenore: «*One could wonder whether the gap existing among right to privacy and right to data protection can be filled up or not. As already seen, it is not a theoretical question as such. On the contrary, the effectiveness of data protection can be affected by the abovementioned gap. In recent years, the Strasbourg Court has moved towards a more data-oriented approach*», p. 24.

[7] J. KOKOTT, C. SOBOTTA, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International data privacy law*, 2013, Vol. 13, No. 4, p. 223.

Ex multis, e come si dirà meglio: Corte di giustizia, C-275/06, *Promusicae*, 29 gennaio 2008; Corte europea dei diritti umani (GC), nn. 30562/04 e 30566/04, *S&Maper c. Regno Unito*, 4 dicembre 2008.

3. L'emersione di un diritto…a partire dalla *privacy*

Com'è noto, l'affermazione conclamata di un *right to privacy* può farsi risalire al 1890 con la seminale pubblicazione di Warren e Brandeis che per la prima volta rivendicavano un diritto alla riservatezza e al rispetto della vita privata – inteso come "diritto ad essere lasciati soli" –, ponendo l'accento sul legame tra l'emersione di tale prerogativa individuale e l'evoluzione tecnologica (in particolare, della stampa e della fotografia). Gli autori, infatti, nel sottolineare come proprio i mutamenti politici, economici e sociali implicassero l'individuazione di nuovi diritti, notavano che il proliferare della stampa giornalistica nel contesto americano di fine Ottocento – pur indicativo della libertà di espressione – provocasse il rischio un'invasione della sfera privata degli individui[8]. Dunque, risulta preponderante la considerazione del contesto in cui emerse la necessità di una tutela della sfera privata. Whitman ci viene d'ausilio in tal senso, per una "rilettura" del saggio di Warren e Brandeis (non la sola, in verità) che coglie le peculiarità del contesto americano e le differenti connotazioni del contesto europeo.

Invero, un'interessante analisi (tra le molteplici) della letteratura dedicata alla *privacy* è stata condotta da González Fuster, la quale ha rintracciato le più comuni accezioni del termine distinguendole in principali categorie, peraltro facendo anche riferimento alla disarticolazione proposta da Prosser delle quattro possibili fattispecie di *torts* nel caso di invasione della *privacy*[9]. L'economia del presente lavoro non consente di approfondire tali aspetti, per i quali si rinvia allo scritto segnalato. Qui ci si limiterà a riferimenti all'analisi di Whitman, in quanto utile a descrivere il passaggio, in Europa, dalla necessità di tutela della riservatezza a quella relativa ai dati di carattere personale, che mantiene ancora oggi la medesima radice.

Partendo dalla diffusa considerazione della *privacy* come nucleo essenziale di ogni ambizione di integrità della persona, fondamento di tutti gli altri diritti individuali, l'autore poneva anzitutto l'accento sulla necessità di norme a tutela della stessa: «*privacy matters so much to us that laws protecting it must be a basic element of human rights*»[10]. Cò non suonerebbe, invero, troppo risalente, se si considera la recente "*Risoluzione sulla privacy come diritto umano fondamentale e prerequisito per l'esercizio di altri diritti fondamentali*" approvata nell'ambito della Conferenza

[8] S. D. WARREN, L D. BRANDEIS, The right to privacy, *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), in part. p. 193-196: «*The press is overstepping in every direction the obvious bounds of propriety and of decency*» p. 196.
[9] G. GONZÁLEZ FUSTER, *The emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014, p.22 ss. Il riferimento è inoltre al famoso W.L. PROSSER, Privacy, in *California Law Review*, 1960, pp. 383-423 (su cui si sofferma particolarmente anche S. RODOTÀ, op. cit., pp. 130-131).
[10] J. Q. WHITMAN, The Two Western Cultures of Privacy: Dignity Versus Liberty, *The Yale Law Journal*, Vol. 113, 2003, p. 1153.

internazionale delle Autorità per la protezione dei dati (ICDPCC) a Tirana nell'ottobre 2019[11]. Tornando all'autore, focalizzandosi sui sistemi occidentali (in cui particolarmente tale esigenza si propose), egli evidenziava l'esistenza di due diverse "culture" della riservatezza tra Europa e Stati Uniti che condurrebbero inevitabilmente a due diversi apparati normativi di tutela[12]. Riprendendo quanto elaborato da Post, l'autore spiegava queste due culture avendo riguardo ai differenti sistemi valoriali di ciascun contesto e dunque chiarendo che il concetto di riservatezza va ricondotto a valori diversi e rispettivamente: alla *libertà*, nel contesto americano; alla *dignità*, nel contesto europeo. Tale assunto merita qualche commento quanto a contenuti e implicazioni.

In Europa la tutela della riservatezza esprimerebbe un peculiare profilo del più ampio valore della *dignità* della persona, in quanto tale riconducibile a ciò che i tedeschi chiamerebbero "*diritto all'autodeterminazione informativa*" – così concepito, invero dalla Corte costituzionale tedesca negli anni Ottanta[13]–, ossia possibilità di controllare le informazioni sul proprio conto, come l'immagine pubblica, la reputazione che ciascuno ha nell'ambiente che lo circonda. Così intesa, la riservatezza subirebbe una grave minaccia dall'esposizione mediatica. Nel contesto americano, invece, la riservatezza sarebbe piuttosto considerata come declinazione della *libertà* degli individui nei confronti dello Stato, dunque la principale minaccia sarebbe costituita da possibili intrusioni da parte di questo nella propria "casa", in quella sfera di proprietà in cui l'individuo esercita la "propria sovranità"[14]. L'autore, nondimeno, precisava come questa differenza non possa dirsi affatto assoluta e come siano ravvisabili diversi esempi in cui entrambi i contesti arrivano alle medesime conclusioni; tuttavia, è proprio il punto di partenza che si assume diverso e che vede, essenzialmente, il sistema europeo orientato da considerazioni su dignità e reputazione e quello americano orientato dai valori della libertà rispetto a intromissioni della pubblica autorità[15].

---

[11] Conferenza mondiale dei Garanti Privacy, novembre 2019, cfr. https://www.privacy.it/2019/11/28/conferenza-mondiale-garanti-privacy-2019/ .

[12] J. Q. WHITMAN: «*What we must acknowledge, instead, is that there are, on the two sides of the Atlantic, two different cultures of privacy, which are home to different intuitive sensibilities, and which have produced two significantly different laws of privacy*», p. 1160.

[13] Cfr. Corte costituzionale federale tedesca, sentenza del 1983, *Volkszählungsurteil*, BVerfGE Vol. 65, pagg. 1 e segg Cfr. al riguardo, *ex multis*, M. TZANOU, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Hart Publishing, 2017, laddove insiste, tra i valori a fondamento della data protection, su quello della dignità: «*With human dignity as an underpinning value, data protection can be seen as informational autonomy rather than a mere claim for information management. 204 Data protection as informational autonomy fi nds its legal description in the right to 'informational self-determination ' (informationelle Selbstbestimmung), as pronounced by the German Constitutional Court (Bundesverfassungsgericht) in its landmark Census decision (Volksz ä hlungsurteil)*», p. 29.

[14] J. Q. WHITMAN, pp. 1160-1162, in cui si legge chiaramente: «*To the continental way of seeing things, what matters is the right to control your public image (…). To the American mind, by contrast, what matters is sovereignty within one's own home*».

[15] Ibidem, pp. 1163-1164, in cui ancora: «*The comparative law of privacy is not about the intuitive preconditions of personhood, but about contrasting political and social ideals. In the United States those political and social ideals revolve, as they have for generations, primarily around our suspicions of the police and other officials, while on the*

Ciò potrebbe sembrare, a prima vista, stridere con quanto detto sopra rispetto al saggio di Warren e Brandeis che, rivolto com'era ad insistere sulle minacce della divulgazione di fatti privati per mezzo della stampa, raffigurava nel contesto americano una prerogativa individuale "nuova" proprio nell'insistenza sulla reputazione e sulla necessità di un limite/bilanciamento rispetto alla libertà di espressione. In realtà, però, Whitman aiutava a leggere il saggio dei due bostoniani spiegando che esso andrebbe inteso come il più grande "tentativo di introdurre un diritto alla riservatezza in stile continentale nel sistema americano", che l'autore riteneva essere stato non tanto una "innovazione americana, ma un trapianto continentale senza successo" [16]. Precisamente, Whitman evidenziava come il contesto proprio dei due autori non rispecchiasse tanto quello generale americano, quanto piuttosto quello specifico della "rispettabilità" propria di Boston, molto più affine all'alta società continentale di fine Ottocento. Whitman dunque segnalava non solo l'evidente tenore di "alto livello" dell'articolo, nell'indignazione rispetto ai giornali che divulgavano aspetti della vita privata, ma soprattutto il fatto che nel fare ciò – nel rivendicare quel "nuovo" *right to privacy* – i due autori trovassero manforte proprio in ordinamenti e autori continentali, da cui già allora compariva l'appello verso una tutela della reputazione (il riferimento è in particolare a tradizioni in Francia e Germania sul punto, oggetto di fervente dibattito verso la fine del XIX secolo). Così, per esempio, il riferimento alla legge francese della seconda metà dell'Ottocento («*The right to privacy, limited as such right must necessarily be, has already found expression in the law of France*»)[17], in parte alla giurisprudenza inglese[18], nonché, più in generale, agli interventi di studiosi anche tedeschi: «*Yet let us note that, even in their account of common law evolution, Warren and Brandeis did not sound all that different from their continental, and especially German, predecessors. As we have seen, French and German writers held that privacy had emerged as a limitation on property, and an evolutionary outgrowth of the growing sensitivity to the needs of "personality" Warren and Brandeis echoed these ideas. (…) All of this made for an inspired contribution to the international literature on the protection of privacy--one that Europeans themselves still cite. But what Warren and Brandeis could not do was bring the European structure of values to the United States*»[19].

Continent they revolve unmistakably around one's position in society, one's "dignity" and "honor"». Nello stesso senso anche da p. 1203.

[16] Ibidem, così letteralmente: «*This is indeed how we should understand the fate of "that most influential law review article of all" Warren and Brandeis's The Right to Privacy. Warren and Brandeis undertook the seminal, and still most cited, effort to introduce a continental-style right of privacy into American law. In theory, their right is still part of the law almost everywhere in America. Nevertheless, it is generally conceded that, after a century of legal history, it amounts to little in American practice today. The story of the relative failure of Warren and Brandeis is precisely a study in how poorly continental ideas do in the American climate. In fact, it is best to think of the Warren and Brandeis tort not as a great American innovation, but as an unsuccessful continental transplant*», p. 1204.

[17] S. D. WARREN, L.D. BRANDEIS, *op. cit.*, p. 214. Il riferimento è alla "*Loi relative à la Presse*", 11 Mai 1868.

[18] Così nota anche G. GONZÁLEZ FUSTER, *op. cit.*, p. 27.

[19] J. WHITMAN, *op. cit.*, pp. 1207-1208,sottolineato aggiunto.

Nell'insistere quindi sulle differenze di contesto valoriale, ben oltre l'apparente commistione ravvisabile dal saggio discusso, l'autore contribuiva alla migliore comprensione delle peculiarità di ciascuno, anche chiarendo il preponderante legame con la "santità della casa", come espressione massima di libertà nei confronti dello Stato, nel contesto americano: «*To Americans, the starting point for the understanding of the right to privacy is of course to be sought in the late eighteenth century, and especially in the Bill of Rights, with its vigorous circumscription of state power. In particular, "privacy" begins with the Fourth Amendment: At its origin, the right to privacy is the right against unlawful searches and seizures. It is thus a right that inheres in us as free and sovereign political actors, masters in our own houses, which the state is ordinarily forbidden to invade. Over time, to the American mind, the early republican commitment to "privacy" has matured into a much more far-reaching right against state intrusion into our lives*»[20].

Peraltro, González Fuster ci ricorda che a partire dalla metà degli anni Sessanta il termine "*privacy*" acquisì negli USA due significati principali: sotto il profilo prettamente civilistico, utilizzato come un sintetico riferimento al sistema degli illeciti (*torts*); dal punto di vista pubblicistico (di diritto costituzionale), considerato come il diritto riconosciuto agli individui di respingere interferenze della pubblica autorità[21]. Quanto, invece, alle peculiarità del contesto europeo, Whitman attribuirebbe al retaggio storico la rilevanza di *rispetto* e *dignità* come caratteristiche proprie della concezione della riservatezza. La sua analisi è peculiare nel fornire una risposta che si allontana da quelle solitamente volte a spiegare la centralità del concetto di *dignità* nel contesto europeo, che spesso pongono l'accento sulle reazioni ai sistemi totalitari, dalle cui aberranti violazioni sarebbe derivata la necessità di attenzionarne la tutela.

L'autore sosteneva che la rilevanza del concetto di dignità abbia radici più complesse e vada rintracciata nel Diciottesimo, se non Diciassettesimo, secolo. La derivazione da società fortemente gerarchiche e aristocratiche, di cui la Francia di Luigi XIV è modello (dunque, dove era forte la rilevanza delle "etichette"), spiegherebbe come fosse forte sin da allora la considerazione del rispetto e dell'onore, di cui però soltanto le persone di un certo status sociale potevano pretendere tutela. Ebbene, la storia europea da allora sarebbe quella di un percorso durante il quale si percepì sempre più inaccettabile che una tale tutela fosse privilegio di pochi (con il paradosso, evidenziato dall'autore, che proprio nel periodo fascista si ebbe una tendenza al livellamento e dunque estensione della tutela dell'onore a tutti i livelli della comunità)[22]. Senza potersi addentrare nel

[20] Ibidem, pp. 1211-1212.
[21] G. GONZÁLEZ FUSTER, op. cit., p. 28.
[22] J. WHITMAN, *op. cit.*, p. 1166: «*What we see in continental law today is the result of a centuries-long, slow-maturing revolt against that style of status privilege. Over time, it has come to seem unacceptable that only certain persons should enjoy legal protections for their "dignity" (…). The uncomfortable paradox, as I have tried to show, is that much*

ragionamento sviluppato dall'autore, ciò che emerge particolarmente è la c.d. "*society conception of privacy*" che caratterizzerebbe il contesto europeo e dunque la comprensione della riservatezza: «*What the continental law of privacy expresses is the fundamental social importance of a commitment to extend royal treatment to everyone. Indeed, we cannot understand our transatlantic conflicts if we do not recognize the authentically wide social application of "society" privacy in continental law*»[23]. In tal senso, la storia della riservatezza nel contesto europeo sarebbe stata fortemente plasmata dalla necessità, a partire dall'Ottocento, di resistere a due forze che potevano minacciare quel concetto di "onore", ossia l'eccesso di libera stampa e l'eccesso di libero mercato, entrambi espressivi del valore americano di libertà: «*Continental privacy law has been shaped by a longstanding battle waged against both. Indeed, the history of continental privacy law has been, in essence, the history of the resistance, in the name of "honor" to two of the fundamental values of American liberty: the value of free speech, and the value of private property as distributed through the market*»[24].

Peraltro, in una prospettiva storico-giuridica più ampia, svariati sono i riferimenti alla classicità greca e romana in cui la "*privacy*" assumeva una connotazione negativa nella misura in cui escludeva la partecipazione attiva del cittadino[25]. Mentre valutazioni comparabili sono state fatte per il periodo medievale, quando, nell'ambito del sistema feudale e del preponderante rilievo dei legami familiari dei gruppi sociali la riservatezza era vista quasi con sospetto, proprio un ribaltamento vi sarebbe stato con l'avvento dello Stato moderno e l'emersione dei bisogni di protezione dell'intimità: «La maggiore separazione tra pubblico e privato e, soprattutto, le discriminazioni religiose che seguono la fine dell'unità religiosa conducono, da un lato, a *reindividualizzare* l'aspirazione a proteggere la propria intimità e, da un altro lato, a far emergere il legame strettissimo tra l'aspirazione a proteggere la propria riservatezza ed il timore di vederla violata per i rischi connessi con lo svelamento delle proprie convinzioni più intime»[26]. Dunque, sarebbe proprio questo differente retaggio storico/culturale a spiegare il passaggio, tutto europeo, dalla riservatezza alla necessità di protezione dei dati personali.

---

of this leveling up took place during the fascist period (...). Infact, the fascist period, seen in proper sociological perspective, was one stage in a continuous history of the extension of honor throughout all echelons of continental society. This long-term secular leveling-up tendency has shaped continental law in a very fundamental way».

[23] Ibidem, p. 1170.

[24] Ibidem, p. 1171, vedi anche p. 1208.

[25] Così M. TZANOU, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Hart Publishing, 2017, p. 9, e gli studi ivi citati.

[26] M. OROFINO, Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione, *Rivista di diritto dei media*, n. 2/2018, p. 91, enfasi aggiunta.
Peraltro, si segnalano le riflessioni più generali sulla nozione di "dignità in senso oggettivo" nel contesto europeo proposte da P. DE SENA, Dignità umana in senso oggettivo e diritto internazionale, in *Diritti umani e diritto internazionale*, n. 3/2017, pp. 573-586.

Pur con qualche salto e inevitabile semplificazione, Pizzetti riconduceva infatti la distinzione nella differenza esistente (almeno sino all'11 settembre 2001, *sic!*) tra sistema americano ed europeo nella considerazione del ruolo dello Stato. Ribadendo, come già emerso da Whitman, la preponderanza dell'autonomia privata e della libertà individuale dei *cittadini* americani, Pizzetti sottolineava come invece, *mutatis mutandis*, il contesto europeo si caratterizzerebbe sempre e da sempre per la dialettica *sovrano-sudditi*. Ciò avrebbe performato un ambiente che assume come caratteristica peculiare proprio il controllo costante dello Stato nei confronti dei cittadini: «un controllo apparentemente finalizzato a garantire il rispetto delle regole e a tutelare lo Stato dai nemici interni ed esterni, ma sostanzialmente orientato a tenere costantemente sotto controllo la lealtà dei cittadini verso lo Stato. Dunque, il fenomeno che in Europa è all'origine del diffondersi di forme sempre più penetranti di controllo sulla vita dei cittadini è prima di tutto di carattere storico-politico»[27]. Queste considerazioni parrebbero ricondurre ancora alla dicotomia libertà/dignità che differenzia i contesti sulle due sponde dell'Atlantico, consentendo anche di accompagnare il passaggio dal concetto di riservatezza *tout court* alla necessità di una protezione dei dati personali. Mentre la libertà americana è un valore a fondamento stesso della costruzione dell'apparato pubblico, l'esasperazione del controllo statale nella realtà europea avrebbe addirittura portato alle derive autoritarie del Novecento. Qui, mentre si ribadisce quanto evidenziato da Whitman sull'emersione del rilievo della dignità (come concetto) già in secoli precedenti, è anche da rilevarsi che però la considerazione della stessa come valore fondamentale sia stata «legata soprattutto al personalismo cattolico francese del secolo scorso»[28] e che un ruolo preponderante ha effettivamente giocato la reazione agli oltraggi perpetrati nell'era dei totalitarismi. Così, nell'analisi già richiamata sulla riservatezza nel contesto prettamente nazionale: «sistemi come quello italiano non riuscivano ad apprestare neppure una ragionevole cornice garantista ai diversi aspetti della personalità, anche a causa del taglio netto operato tra versante "privatistico" e versante "pubblicistico" della disciplina. Il quadro complessivo subisce alcuni notevoli mutamenti in questo dopoguerra. (…) alcune

[27] F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali – Dalla Direttiva 95/46 al nuovo Regolamento europeo – I –*, Giappichelli, 2016, pp. 50-52. L'autore, ripercorrendo molto sinteticamente le tappe salienti, spiega: «Negli USA sono i cittadini e i loro rappresentanti che trasformano le precedenti colonie in singoli Stati e poi i rappresentanti dei cittadini organizzati in Statiche costruiscono la Federazione. (…) in Europa, al contrario di quanto accaduto in USA, il Sovrano, Monarca o Stato che fosse a seconda delle epoche, ha sempre avuto un ruolo predominante, del tutto staccato e anzi sovrapposto al popolo, non a caso fino alla Rivoluzione francese definito suddito. La supremazia dello Stato è rimasta e anzi si è accresciuta anche quando, con la Rivoluzione francese, i sudditi sono diventati cittadini. Infatti i cittadini, attraverso i loro rappresentanti sono diventati prima Nazione e subito dopo essi stessi si sono identificati nello Stato (la France), aprendo coì il via alla successiva deriva napoleonica. La successiva tradizione delle Costituzioni post-rivoluzionarie e prevalentemente *octroyées* ha elaborato ulteriormente questa trasformazione, trovando un equilibrio instabile tra la figura del Sovrano, ora costituzionalizzato, e la partecipazione del popolo, attraverso i suoi rappresentanti, all'esercizio della funzione legislativa e alla legittimazione del potere esecutivo. Questo equilibrio instabile si è successivamente ancor più indebolito nel passaggio dal XIX al XX secolo, specialmente nei Paesi a più tenue intensità democratica (…)», p. 51.
[28] Ibidem, p. 7.

dichiarazioni internazionali esplicitamente dedicate ai diritti della personalità, nelle quali comincia ad emergere proprio la necessità di dedicare una autonoma tutela alla riservatezza. Queste dichiarazioni sono pure il frutto diffuso del giusnaturalismo dell'epoca, attraverso il quale si esprime la reazione alle violazioni dei diritti dell'uomo consumate dal nazismo e dal fascismo»[29]. Dunque, il "controllo totale" nel periodo dei totalitarismi avrebbe avuto a suo fondamento sicuramente l'esigenza di individuare e "distinguere" i cittadini per finalità profondamente malsane e lesive dell'autentico significato di dignità umana – che dopo, quindi, a ragione pretese una forte tutela –, ma accanto a ciò anche, ancora una volta, l'evoluzione tecnologica.

Pizzetti ci fa notare, infatti, che così come nella Boston di fine Ottocento Warren e Brandies sentirono l'esigenza di rivendicare apertamente un *right to privacy*, emergendo tale esigenza di riservatezza come contraltare delle profonde innovazioni legate alla stampa, così nell'Europa del Novecento si sarebbe sviluppata la "tecnologia del controllo", che, «con la sua sempre più penetrante capacità di raccogliere, trattare, archiviare dati sui comportamenti delle persone, riporta i cittadini alla condizione di sudditi dello Stato totalitario»[30]. Appare molto più chiara l'emersione di un'esigenza di tutela dei dati personali, particolare e quindi differenziata rispetto alla riservatezza, se la si comprende come conseguenza dello sviluppo di "trattamenti automatizzati" e "tecniche di archiviazione, conservazione e trattamento dei dati".

Dunque, per chiudere l'*excursus* che ci ha consentito di comprendere l'emersione dell'esigenza di riservatezza – nelle sue diverse concezioni – e il passaggio alla tutela dei dati personali, sottolineiamo quanto enfatizzato da Pizzetti, ossia la necessità di legare entrambi gli sviluppi all'evoluzione tecnologica. In particolare, egli rintracciava un parallelismo tra: riservatezza e tutela della vita privata/libertà di espressione e manifestazione del pensiero, da un lato (rispetto alle innovazioni di stampa e fotografia); protezione dei dati personali/controllo generalizzato (rispetto ai trattamenti automatizzati, realizzati in particolare con schede perforate), dall'altro[31]. Ciò spiegherebbe, infatti, non solo i primi interventi legislativi nel contesto regionale europeo – a partire dagli anni Settanta – essenzialmente riferiti proprio al trattamento dei dati (il riferimento è a leggi

[29] S. RODOTÀ, op. cit., p. 126.
[30] F. PIZZETTI, op. cit., p. 53. Ibidem anche i riferimenti a "controllo totale" e "tecnologia del controllo".
[31] Ibidem, pp. 54-55. Peraltro, l'autore precisa: «Sul piano delle tecnologie che resero possibile le più pervasive forme di controllo globale, un posto centrale spetta infatti ai trattamenti automatizzati, basati in quel tempo essenzialmente sulle schede perforate e sui sistemi di elaborazione messi a punto, per prima, dalla IBM. (…) È diffusa la convinzione che proprio gli archivi automatizzati, insieme ad altre tecniche di raccolta di informazioni, già da tempo messe a punto, come le intercettazioni telefoniche, abbiano svolto un ruolo molto importante a favore degli apparati di controllo nazisti». Su questo ultimo aspetto, l'autore aggiunge una nota riferita ai rapporti tra la Germania nazista e le grandi imprese USA collaborative con il regime.
Tra i primi, in Italia, ad insistere sull'incidenza dell'evoluzione tecnologica, S. RODOTÀ, nei suoi vari scritti. Oltre a quanto già citato, si ricorda, *ex multis*, *Tecnopolitica – La democrazia e le nuove tecnologie della comunicazione*, Laterza, 1997.

nazionali e soprattutto alla Convenzione n. 108, di cui si dirà), ma anche le considerazioni dottrinali del tempo che, pur non distinguendo ancora nettamente tra riservatezza e protezione dei dati personali, a ciò facevano essenzialmente riferimento: «una tutela della riservatezza, adeguata all'ambiente in cui viviamo, richiede soprattutto la possibilità di controllare la stessa attività di raccolta delle informazioni, il modo del loro trattamento, le sedi in cui le informazioni sono raccolte. Nella definizione della riservatezza, quindi, entra come parte integrante non solo il diritto di respingere le invasioni della sfera privata, ma soprattutto il diritto di controllare il flusso di informazioni riguardanti un determinato soggetto»[32].

4. Il diritto alla protezione dei dati personali nelle sue diverse accezioni

L'ultima citazione riportata ci consente di ribadire il fondamentale nesso tra riservatezza e protezione delle informazioni personali, ma anche di spiegare la necessità, posta in tempi molto più recenti (e dunque espressiva di un contesto socioeconomico completamente mutato rispetto agli anni Settanta, soprattutto nel rapporto con la tecnologia) di individuare profili di autonomia della protezione dei dati come diritto fondamentale in quanto tale.

Un'analisi esaustiva dell'ampio e ancora aperto dibattito al riguardo esula dalla presente trattazione, ma si darà conto degli aspetti fondamentali del ragionamento esposto di recente dalla Tzanou e fondato su ulteriori precedenti teorie, che quindi verranno brevemente esposte. Inoltre, si introdurrà (ma si avrà modo di approfondire nel prosieguo) la considerazione della protezione dei dati come un vero e proprio sistema giuridico nel contesto ordinamentale europeo, il cui significato può meglio comprendersi guardando alle sue ragioni di fondo: «*Data protection regulation does not protect us from data processing, but from unlawful and/or disproportionate data processing*»[33]. Questa affermazione appare di fondamentale importanza per capire il significato – e dunque gli sviluppi – della regolazione europea sulla protezione dei dati, quindi per palesarne la duplice natura di diritto individuale e branca dell'ordinamento.

[32] S. RODOTÀ, *op. cit.*, p. 130.
[33] P. DE HERT, S.GUTWIRTH, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, IN S. GUTWIRTH, Y. POULLET, P. DEHERT, J, NOUWT, C. DE TERWANGNE (Eds), *Reinventing data protection?*, Springer Science, Dordrecht, 2009, p. 3. E ancora: «*data protection regulation does a lot more than echoing a privacy right with regard to personal data. Rather, it formulates the conditions under which processing is legitimate*», p. 4.

Il diritto alla protezione dei dati personali come diritto fondamentale…

Per definire la protezione dei dati personali come avente una propria specificità di diritto fondamentale (sulla quale, peraltro, sono state avanzate interessanti perplessità)[34] rispetto alla *privacy*, dell'amplissima letteratura al riguardo faremo essenzialmente riferimento alla teoria esposta da Tzanou, la quale, nel proporla, richiamava (e confutava) altre due teorie fondamentali che così ci consente di presentare.

La prima delle due teorie era considerata dall'autrice riconducibile a un "modello separatista": sarebbe quella sostenuta da De Hert e Gutwirth[35], volta a proporre un'analisi del ruolo che *privacy* e *data protection* svolgerebbero nella società come strumenti di controllo del potere, distinti ma complementari. In particolare, la *privacy* sarebbe vista come uno strumento di *opacità*, tale da influire sulle scelte normative relative ai limiti del potere, proteggendo gli individui rispetto a un uso illegittimo o eccessivo di questo (dunque, uno strumento di *non interferenza*); la protezione dati come strumento di *trasparenza*, influirebbe invece dopo che le scelte normative sono intervenute e quindi con lo scopo di canalizzare l'uso legittimo del potere.

Il gran merito di questo approccio, secondo l'autrice, sarebbe quello di cercare di comprendere il ruolo della *data protection* in un sistema giuridico attraverso il contenuto dei suoi principi («*designed to promote procedural justice, rather than normative (or substantive) justice*»)[36], che non opererebbe in senso "proibitivo", come invece è tra le funzioni della *privacy*: «*Due to these different functions, de Hert and Gutwirth explain, for the first time, why data protection is needed alongside privacy in a democratic constitutional state. Its added value in a democratic constitutional framework can be seen, according to these authors, in the clear separation of the two rights, which implies a distinction between the legal tools of opacity, on the one hand, and transparency, on the other*»[37]. Se da un lato, dunque, la Tzanou riconosceva agli autori il merito di aver evidenziato l'esigenza della protezione dei dati accanto a quella di riservatezza in una società democratica, dall'altro criticava questo approccio per il fatto di concentrarsi troppo poco sulla protezione dati in quanto tale e di definirla, invece, troppo in rapporto alla *privacy*[38].

[34] Il riferimento è in particolare a B. VAN DER SLOOT, Legal Fundamentalism: Is Data Protection Really a Fundamental Right?, in R. LEENES, R. VAN BRAKEL- S. GUTWIRTH, P. DE HERT (editors), *Data Protection and Privacy: (In)visibilities and Infrastructures*, Springer, 2017, pp. 3-30.
[35] Il riferimento specifico è al contributo del 2006, Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power, in *E*. Claes, A. Duff, S. Gutwirth (Eds), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, p. 61-104; ma lo stesso viene ripreso dagli autori nell'*op. cit*. del 2009.
[36] M. TZANOU, *op. cit*., p. 32.
[37] Ibidem, p. 33.
[38] Ibidem: «*There is, however, a paradox in their line of thinking: their theory, while it aims to be a theory on data protection, does not focus on data protection itself. Rather, the added value of data protection is demonstrated through*

La seconda teoria proposta, sostenuta da Rouvroy e Poullet, veniva definita dall'autrice espressione di un "modello strumentalista": sia *privacy* che *data protection* avrebbero un valore intermedio piuttosto che finale, come strumenti attraverso i quali valori "più fondamentali" e diritti "più basilari" sarebbero perseguiti ("*namely human dignity and individual personality right*")[39]. I due autori ribadirebbero, come abbiamo già avuto modo di notare da altri, l'imprescindibile nesso tra l'evoluzione tecnologica e l'emersione di tali nuovi diritti, ma insisterebbero sulla necessità di non porli sullo stesso piano – cosa che deriverebbe peraltro dalla Carta dei diritti fondamentali UE, che li riconosce distintamente – poiché ciò, secondo loro, potrebbe comportare il rischio di oscurare la relazione tra essi esistente e dunque distogliere il riferimento, per la *data protection*, ai valori di dignità e autonomia individuale.

Nel criticare questa teoria, Tzanou la considerava confusa soprattutto laddove non spiegherebbe chiaramente perché la *data protection* perderebbe il carattere strumentale rispetto a quei valori fondamentali se concepita sullo stesso piano della *privacy*, così negando alla prima un effettivo valore: «*Rouvroy and Poullet make a valid point about the uniqueness of the final goals of the two rights (be that autonomy or dignity or the right to individual personality), but they do not provide convincing reasons why the constitutional entrenchment of data protection is so harmful*»[40].

Analizzate le due teorie, l'autrice elaborava la propria partendo dal punto che esse hanno in comune: entrambe guardano alla protezione dei dati attraverso la *privacy* e dunque tentano di costruire una teoria della protezione dei dati fondandola sul rapporto con la *privacy*. Il punto della "nuova" teoria proposta dall'autrice sarebbe, invece, di mantenere il focus sulla protezione dei dati personali, dunque considerarla in maniera isolata, scevra dai pur esistenti legami con la riservatezza, proprio per poterne apprezzare il valore aggiunto. La domanda che quindi l'autrice si poneva era, quindi, la seguente: può considerarsi la *data protection* capace di "stare da sola", di essere intesa come diritto fondamentale? O c'è qualche lacuna che la rende incapace di ciò e dunque comprensibile solo nel nesso con la *privacy*?

A tal proposito richiamava il modello separatista, che considera la protezione dei dati personali solo in termini affermativi (come una libertà positiva), dunque come uno strumento di trasparenza (l'autrice nota che una simile connotazione deriverebbe dal disposto dell'articolo 8 della Carta oltre che da un approccio della Corte di giustizia che per parecchio tempo l'avrebbe così intesa, nel

---

its distinction from privacy. By preaching separation, they strive to show the indispensability of data protection. But, their very argument proves them wrong. (...) Data protection, as a transparency tool, merely describes the permitted processing; the limits will then be set on the basis of privacy. This, however, means that data protection is not indispensable: we could live well without it».

[39] Ibidem, p. 34.

[40] Ibidem, p. 35.

definirne i connotati partendo dalla *privacy*), mentre la privacy sarebbe delineata come strumento di opacità e non interferenza. Ebbene, secondo l'autrice il problema starebbe proprio in questo: diventa impossibile considerare la protezione dei dati personali come un diritto fondamentale in quanto tale se esso può operare solo come strumento di trasparenza, mentre le interferenze illegittime vengono determinate dal diritto alla riservatezza: «*I argue that this approach to data protection obstructs the right itself to operate independently from privacy. Contrary to what de Hert and Gutwirth contend, the value, of a fundamental right to data protection, thus interpreted, is limited: it can operate only as a transparency tool, but illegitimate interferences will have to be determined on the basis of privacy*»[41]. Inoltre, la Tzanou riteneva che ulteriore elemento a limitare un'autonoma considerazione della *data protection* fosse la sua relazione con il diritto derivato, di cui è stata oggetto esclusivo per parecchio tempo[42]. Alla luce di ciò, l'autrice sosteneva che per poter, invece, considerare la protezione dei dati personali come un diritto fondamentale dotato di un valore proprio dovrebbero essere soddisfatte tre condizioni: che ne sia ravvisabile un contenuto "autonomo"; che sia bilanciato con altri diritti e/o interessi in quanto tale, non attraverso il filtro della *privacy*; che possa funzionare sia in senso positivo che negativo, nel senso non solo di canalizzare e controllare il potere, ma anche di proibirlo. Senza potersi soffermare sulla specificità delle tre condizioni, basti dire brevemente che l'autrice: quanto alla prima, riteneva il contenuto della protezione dei dati come diritto fondamentale ravvisabile nell'articolo 8 della Carta considerato nel suo complesso (nonostante da interventi della Corte sembrerebbe delimitato al solo primo paragrafo); quanto alla seconda, ribadendo che il diritto alla protezione dei dati può essere sottoposto a restrizioni, ne riconosceva il necessario bilanciamento con altri interessi confliggenti, ma ciò senza il bisogno di ricorrere al diritto alla privacy; quanto alla terza, che il c.d. *essential core* di tale diritto non può essere scalfito, come deriva da paragrafo 1 dell'articolo 52 della Carta dei diritti fondamentali, al fine di poter funzionare sia in termini positivi che negativi[43]. Per spiegare questa condizione, l'autrice faceva riferimento in particolare alla pronuncia della Corte di giustizia sul famoso caso *Digital Rights Ireland* (di cui si dirà ampiamente): «*This pronouncement indeed confirms that the CJEU has recognised that data protection is a fully fledged fundamental right that operates both positively and negatively, and has an inviolable core*»[44].

[41] Ibidem, p. 36.
[42] Ibidem, pp. 37-38.
[43] Su questo aspetto, si veda in particolare la recente analisi di M. BRKAN, The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU's Constitutional Reasoning, *German Law Journal*, vol. 20, no. 6, 2019, p. 864-883.
[44] M. TZANOU, *op.cit*., p. 43. Sullo stesso aspetto, commentando la pronuncia, così M. BRKAN, *op. cit*.: «*this approach makes the essence of this right a minimum standard rather than a maximum one and places the threshold for compliance with the essence rather low*», pp. 878-879.

Che si tratti, dunque, di un diritto fondamentale riconosciuto come tale nell'ordinamento dell'Unione europea, aldilà delle speculazioni sulla sua connotazione più o meno autonoma rispetto al diritto alla riservatezza, risulta evidente non solo dall'importante giurisprudenza che ha concorso a definirlo (che si avrà ampio modo di analizzare), ma oramai dalle disposizioni di diritto primario e derivato che così lo definiscono: l'articolo 8 della Carta dei diritti fondamentali, anzitutto; l'articolo 16 TFUE, che costituisce peraltro base giuridica del GDPR; quest'ultimo, che sin dal suo *incipit*, al Considerando n. 1, dichiara lapidariamente che "la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale". Si tornerà frequentemente su questo aspetto; per il momento, basti soffermarsi a considerare la peculiarità dell'oggetto del nostro studio che, oltre ad essere pacificamente considerato un diritto fondamentale, assume anche una più ampia connotazione.

…e come branca dell'ordinamento giuridico europeo

Non soltanto, infatti – come può già in qualche modo evincersi dalle considerazioni sostenute dal "modello separatista" – esso è stato ampiamente considerato come interesse collettivo: in termini di «*un interesse primario della società, lo è proprio perché esso appare strumentale, da un lato, alla garanzia dei diritti e, dall'altro lato, alla tenuta complessiva degli ordinamenti democratici*»[45].

Ancor di più, addirittura, nello spazio giuridico europeo esso si è evoluto e definito talmente tanto da istituire uno specifico apparato normativo, in parte emerso dalla prassi, e istituzionale che connota una specifica branca dell'ordinamento giuridico europeo. Va precisato, invero, che ciò che viene definito "diritto europeo per la protezione dei dati personali" è inteso essenzialmente come «un sistema molto complesso (…) insieme di regole e di principi che incrociano tra loro atti normativi appartenenti a due diversi ordinamenti»[46], intendendo in tal senso quello del Consiglio d'Europa, da un lato, e quello dell'Unione europea, dall'altro. L'esposizione dettagliata dei molteplici atti che lo caratterizzano (alcuni, pur parecchio rilevanti, di valore non normativo), come anche dell'importante e copiosa giurisprudenza delle due corti europee, esula dallo scopo di questo studio, che vorrebbe concentrarsi essenzialmente sugli aspetti – normativi, giurisprudenziali e istituzionali – propri dell'ordinamento UE. Nondimeno, e anche in funzione di quello scopo, un riferimento anche breve ai principali strumenti predisposti in seno al Consiglio d'Europa (e, più in generale, ad interventi internazionali di impatto settoriale e/o comunque non prettamente regionale – come le famose linee guida OCSE o alcune risoluzioni ONU) si ritiene indispensabile proprio per

[45] M. OROFINO, *op.cit.*, p. 104.
[46] Così F. PIZZETTI, *op. cit.*, p. 27.

agevolare la comprensione degli interventi assunti nell'ordinamento sovranazionale, mentre il riferimento alla giurisprudenza di Strasburgo risulterà nondimeno fondamentale, anche per intendere al meglio quella di Lussemburgo. Procediamo, dunque, a delineare i caratteri fondamentali di questo contesto.

CAPITOLO II

LA PROTEZIONE DEI DATI PERSONALI IN EUROPA

1. Un'analisi cronologica a partire dall'esterno, seguendo (ancora) "*la spinta dello spazio sulla forma*"

Un'esposizione che voglia fornire, anche sommariamente, gli elementi basilari per avere contezza del contesto al quale presteremo attenzione non può prescindere dagli interventi internazionali in materia.

Primo tra tutti, l'articolo 12 della Dichiarazione Universale dei Diritti Umani proclamata, com'è noto, dall'Assemblea Generale delle Nazioni Unite nel 1948, che prevedeva all'indomani del Secondo Conflitto Mondiale un esplicito riferimento alla tutela della vita privata[47]. Questa norma, come si sa, è stata poi sostanzialmente ripresa dall'articolo 17 del Patto sui Diritti Civili e Politici, adottato dall'Assemblea Generale ONU nel 1966[48], del quale il Comitato dei diritti umani ha dato specificazioni nel 1988 con il *General Comment* n. 16: «*Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour and reputation*»[49]. Sempre nel periodo del secondo dopoguerra, ma con specifico riferimento al contesto regionale europeo, il riferimento fondamentale – che accompagnerà l'intera trattazione – è al celeberrimo articolo 8 della Convenzione europea sui diritti umani (di seguito anche CEDU), firmata nel 1950 in seno al Consiglio d'Europa, dedicato al rispetto della vita privata e familiare[50]. Per quanto questi interventi

[47] Dichiarazione Universale dei Diritto Umani, Articolo 12: «*Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge, contro tali interferenze o lesioni*». Si noti, peraltro, il riferimento alla duplice accezione di "privacy", sia come "casa" e "corrispondenza" che come "onore" e "reputazione" (cfr. *supra*, Capitolo I, par. 3). Disponibile sul sito ufficiale UN: https://www.un.org/en/universal-declaration-human-rights/

[48] Article 17, *International Covenant on Civil and Political Rights, adopted by the General Assembly of the United Nations on 19 December 1966*: https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

[49] UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, available at: https://www.refworld.org/docid/453883f922.html .

[50] Articolo 8 CEDU: https://www.echr.coe.int/Documents/Convention_Ita.pdf . Un'interessante comparazione linguistica tra questi atti viene svolta da G. GONZÁLEZ FUSTER, *op. cit.*, pp. 37-38, che nota come l'articolo 8, pur basandosi sulla Dichiarazione ONU, non faccia – nella vesione inglese – riferimento al termine "privacy" ma "private life" e non menzioni minimamente il richiamo a "onore" e "reputazione". Peraltro, a ulteriore esempio delle

intendessero salvaguardare la riservatezza e la dignità umana, mancava un chiaro riferimento alla necessità di protezione rispetto ai rischi legati all'evoluzione tecnologica, come testimonierebbero anche le Costituzioni europee dei primi anni del dopoguerra[51]. Invero, nella sua importante monografia già richiamata, González Fuster ci ricorda che il nesso tra computers e privacy cominciò ad emergere negli Stati Uniti a partire dalla metà degli anni Sessanta (periodo nel quale, com'è noto, si ebbe la celeberrima sentenza della Corte Suprema degli Stat Uniti che riconosceva espressamente il *right to privacy*)[52] e che, nonostante gli elaboratori elettronici fossero presenti nel mercato già da una decina d'anni, prima di quel tempo non si prestava particolare attenzione a quel possibile nesso con la riservatezza: «*it was only in the 1960s when computers began to be highlighted as a potentially important societal threat; more particularly, what was put forward as a threat was the automated processing of information on individuals that computers were capable of sustaining, and of trivialising*»[53].

Intanto l'attenzione su questi aspetti iniziava a presentarsi anche altrove come per esempio nell'ambito della Commissione Internazionale dei Giuristi (organizzazione non governativa fondata nel 1952 con l'intento di promuovere e proteggere i diritti umani attraverso lo stato di diritto, di seguito: ICJ)[54] che nel 1967 tenne una sessione a Stoccolma denominata "*Nordic Conference of Jurists on the Right to Respect for Privacy*" che elaborò un ampio *working paper* con studi comparativi sul tema. In seno alle Nazioni Unite, poi, la questione si faceva sempre più rilevante: l'anno dopo, infatti, una prima Conferenza mondiale sui diritti umani si tenne a Teheran "*per esaminare i progressi compiuti nei venti anni successivi all'adozione della Dichiarazione universale dei diritti dell'uomo e per formulare un programma per il futuro*". In quell'occasione, si riconosceva apertamente che l'evoluzione tecnologica, pur stimolando lo sviluppo economico e sociale, presentava rischi per i diritti e le libertà dell'individuo, che dovevano dunque essere monitorati[55]. Da lì, l'Assemblea Generale invitò il Segretario Generale ad affrontare uno studio sulle relazioni tra diritti umani ed evoluzione tecnologica, in particolare, per quel che qui interessa,

---

"*convoluted relations*" tra i termini "privacy, private life and *vie privée* in international law" l'autrice cita la Convenzione americana sui diritti umani del 1969 (San José, Costa Rica), p. 38.

[51] Al riguardo, infatti, PIZZETTI ci fa notare: «malgrado le esperienze fatte, nel periodo immediatamente successivo alla seconda guerra mondiale non furono immediatamente percepite la portata e le conseguenze delle innovazioni tecnologiche in genere, e di quelle legate alla archiviazione e al trattamento automatizzato dei dati, in particolare», *op.cit.*, pp. 56-57.

[52] Il riferimento è al noto caso *Griswold c. Connecticut* del 1965, in cui la Corte riconobbe la libertà per le coppie sposate di usare contraccettivi senza restrizioni governative, ritenendo che la legge che ne vietava espressamente l'utilizzo fosse lesiva del "*right to marital privacy*"; cfr. U.S. Supreme Court, *Griswold v. Connecticut*, 381 U.S. 479 (1965).

[53] G. GONZÁLEZ FUSTER, *op. cit.*, p. 29.

[54] *International Commission of Jurists* – per ulteriori informazioni: https://www.icj.org/ .

[55] Così emerge dal punto 18 del Proclama di Teheran, adottato il 13 maggio 1968 dalla Conferenza internazionale sui diritti umani (disponibile in italiano qui: http://ospiti.peacelink.it/cd/docs/1206.pdf).

con riguardo a*: «respect for the privacy of individuals and the integrity and sovereignty of nations in the light of advances in recording and other techniques; (…) uses of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society; (…) more generally, the balance which should be established between scientifical and technological progress and the intellectual, spiritual, cultural and moral advancement of humanity»*[56]. Ancora, González Fuster segnalava che nel 1970 le medesime esigenze si palesarono anche in ambito UNESCO (UN *Educational, Scientific and Cultural Organisation*), affidando inoltre alla suddetta ICJ il compito di svolgere una nuova indagine comparativa internazionale sul tema, poi pubblicato nel 1972 che, specie rispetto al primo del 1967, poneva l'accento sulla particolare minaccia derivante ai dati personali dalla raccolta, conservazione e diffusione tramite l'utilizzo dei computers: «*According to the ICJ, this particular threat required not laws on a general right to privacy, but rather ad-hoc legislation, which should guarantee the right of individuals to know which data about them are being processed, and to have them rectified if necessary, as well as strict control of the access to information, compliance with a general purpose limitation principle, and the existence of an authority analogous to an ombudsman with technical means allowing it to monitor the observance of the rules, and which would have the power to receive and examine complaints. (…) In its search for a modern approach to the protection of privacy, the ICJ had encountered privacy as (shared) control over the use of personal data, and had embraced this notion as the concrete desired target*»[57]. In quegli anni, peraltro, venne pubblicato il seminale lavoro di Westin, *Privacy and Freedom*, che rappresentò un fondamentale faro rispetto all'attenzione da dedicare alla protezione dei dati[58].

È a partire dagli anni Settanta, dunque, che emersero delle riflessioni a livello internazionale sulle esigenze che solo di recente stanno trovando compimento e che cominciò, quindi, a diffondersi l'idea della necessità – tra le varie rivendicazioni a tutela della riservatezza – di un controllo sull'utilizzo dei dati personali da parte dei nuovi "elaboratori elettronici" (di cui il lavoro di Rodotà citato, tra gli altri, in apertura, costituisce uno tra i primissimi esempi italiani)[59]. Il richiamo a

[56] General Assembly UN – Twenty-third Session, Resolution 2450 (XXIII), *Human rights and scientific and technological developments*, 19 december 1968, disponibile qui: https://undocs.org/en/A/RES/2450(XXIII) .
[57] G. GONZÁLEZ FUSTER, *op.cit*., pp. 40-41, con riferimento al Report ICJ del 1972, p. 578. L'autrice, peraltro, riporta anche esemplari interventi che si ebbero, a partire da quel periodo, in Canada.
[58] Al punto che, ci ricorda la GONZÁLEZ FUSTER, venne utilizzato come base per i lavori della ICJ; cfr. *op. cit*., p. 40. Il riferimento è a A. F. WESTIN, *Privacy and Freedom*, New York, 1967. Il fondamentale lavoro aveva peraltro delle anticipazioni nel succitato ID., Science, Privacy, and Freedom: Issues and Proposals for the 1970's, in *Columbia Law Review*, Jun., 1966, Vol. 66, No. 6 (Jun., 1966), pp. 1003-1050.
[59] L'autore, infatti, nel 1973, apriva in premessa: «preceduta da prudenti assaggi e preparata da una sommaria divulgazione sociologica, si annuncia in Italia la fortuna di un genere letterario che, negli Stati Uniti, ha fatto sfiorare anche i giuristi dal brivido del best-seller: prodi cavalieri si accingono a scendere in campo a difesa dei diritti individuali minacciati dagli elaboratori elettronici», *op. cit.*, p. 7.

quest'epoca ci consente di focalizzare l'attenzione sul contesto regionale europeo, perché è da allora che cominciarono a presentarsi i primi timidi interventi legislativi a livello nazionale: «*in the 1970s started to see the light in various European countries different provisions regulating the automated processing of data. They basically took two distinct forms: they were either ad-hoc acts, or constitutional-level provisions*»[60].

Come si suole riportare in questi casi, il primissimo riferimento è alla "*legge sulla protezione dei dati*" del 1970 del Land dello Hesse, ossia parte della Repubblica Federale Tedesca, quale normativa precipuamente dedicata alla *data protection,* che si applicava quindi solo in quel territorio[61]. Pizzetti ne sottolineava l'importanza «non solo perché essa tutelava esplicitamente i lavoratori dalle schedature ma anche perché voleva avere un chiaro significato politico specialmente nei confronti della Repubblica democratica di Germania. La D.D.R. era all'epoca, come è noto, governata da un sistema fortemente autoritario (…). Dunque, che un Land della Germania Federale disciplinasse, tutelasse e limitasse il trattamento dei dati personali operato attraverso banche dati, e introducesse anche i divieti di schedature di massa, assumeva un valore politico particolarmente forte»[62]. Anche in Francia, invero, lo stesso anno veniva emanata una legge (Legge sul rafforzamento della garanzia dei diritti individuali dei cittadini, n. 70-643 del 17 luglio 1970) che interveniva a modificare i codici civile e penale per tutelare apertamente la "vita privata", ma essa non riguardava specificamente la protezione dei dati, per la quale si dovette aspettare il 1978 con la Legge istitutiva del CNIL (*Commission Nationale de l'informatique et des Libertés*) che per la prima volta tutelava rispetto alle possibili invasioni derivanti dall'informatica[63], mentre in Germania una legge di protezione dei dati a livello federale si ebbe solo nel 1977 (sostituita poi nel 1990). Dunque, la prima legislazione nazionale in Europa (o meglio, addirittura, "al mondo"[64]) a protezione dei dati può essere considerata quella svedese del 1973[65]. Proprio in quegli anni, peraltro, anche a livello sovranazionale iniziò a palesarsi l'attenzione verso il trattamento di dati personali. Il riferimento è essenzialmente alla Comunicazione della Commissione del 1973 su

[60] G. GONZÁLEZ FUSTER, *op. cit.*, p. 55.
[61] Cfr. Manuale sul diritto europeo in materia di protezione dati, *cit.*, p. 21.
[62] F. PIZZETTI, *op. cit.*, p. 59, dove continua: «Con questa legge si affermava, infatti, una idea di democrazia e di tutela delle persone opposta a quella propria della Germania dell'Est, basata invece su forme di controllo vecchie e nuove che in quel Paese si praticavano ampiamente». Ad essa anche G. GONZÁLEZ FUSTER, op. cit., dedica attenzione, pp. 56-58.
[63] Il riferimento al testo di legge del 1970 ancora su S. RODOTÀ, *op. cit*., pp. 175-176.
Il distinguo con l'esperienza tedesca e la legge del 1978 vengono riportati da Pizzetti, *op. cit*., p. 59.
[64] Così Manuale sul diritto europeo in materia di protezione dati, *cit*., p. 21, nota 2.
[65] Come ricorda O. LYNSKEY, *The foundations of EU Data Protection Law*, Oxford University Press, 2015, p. 47, ma anche G. GONZÁLEZ FUSTER, *op. cit.*, pp. 58-59. La stessa autrice, invece a pp. 42-44 offre un riferimento all'evoluzione del tema nel Regno Unito (a partire dalla proposta del 1969 – *Data Surveillance Bill*).

"*Community policy on data processing*"[66] nonché alle successive Risoluzioni del Parlamento europeo, rispetto alle quali si è notato «*One of the reasons why the European Parliament initially called for data protection legislation in the mid-1970s was a reaction to the emergence of a data processing industry in the EU*»[67]. Dunque, ancora una volta, fu lo sviluppo della tecnologia e l'emergere dell'industria sul trattamento dei dati a spingere verso interventi anche da parte delle istituzioni europee. Si avrà modo di approfondirne cause e sviluppi; qui basti menzionare, per completare il contesto che contorna l'oggetto del nostro studio e dunque, con le sue 'spinte', concorre a modellarne la 'forma', gli ulteriori e più rilevanti interventi sino a tempi recenti.

Ci riferiamo anzitutto alle famose Linee Guida dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE, organizzazione internazionale che promuove a livello globale politiche per migliorare il benessere economico e sociale dei cittadini)[68] del 1980 "*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*", che costituirono la prima dichiarazione di principi relativi al trattamento dei dati condivisa livello internazionale. Esse rilevano particolarmente ai nostri fini perché presentano il merito di avere tra i loro obiettivi, oltra a quello di tutelare la *privacy* e le libertà ad essa correlate, quello di evitare disparità tra legislazioni nazionali che possano ostacolare il libero flusso di dati personali oltre le frontiere ("*across national frontiers, and indeed across continents*")[69]. Queste linee-guida sono state poi riviste e aggiornate nel 2013, mentre l'organizzazione continua a lavorare sul tema, come risulta anche dalla pagina dedicata: «*Since the mid-1970s, the OECD has played an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders. The OECD's Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data are the cornerstone of OECD's work on privacy. In 2013 the OECD revised the Privacy Guidelines for the first time since their launch in 1980. The revised text modernised the OECD*

[66] Commission of the European Communities, *Community Policy on Data Processing* (Communication of the Commission to the Council), SEC(73) 4300 final, Brussels, 21 November 1973; available here: http://aei.pitt.edu/6337/1/6337.pdf

[67] O. LYNSKEY, *The foundations of EU Data Protection Law*, Oxford University Press, 2015, p. 3.

[68] Come si legge dalla pagina del Ministero degli Esteri, che la descrive: l'OCSE è stata istituita con la Convenzione sull'Organizzazione per la Cooperazione e lo Sviluppo Economico, firmata il 14 dicembre 1960 ed entrata in vigore il 30 settembre 1961, sostituendo l'OECE, creata nel 1948 per amministrare il cosiddetto "Piano Marshall" per la ricostruzione postbellica dell'economia europea». Per ulteriori informazioni: https://www.esteri.it/mae/it/politica_estera/organizzazioni_internazionali/ocse.html ; nonché il sito ufficiale: www.oecd.org

[69] Così nota, infatti, G. GONZÁLEZ FUSTER, *op. cit*, p. 80. Per un suo approfondimento sulle Linee guida OCSE, da p. 75 ss. Si veda anche O. LYNSKEY, *op. cit*., p. 48: «*The aim of these Guidelines was therefore clearly to ensure that national data protection laws would develop in a way that would not disrupt cross-bordar data flows and consequently international trade. However, as these Guidelines were non-binding, their effectiveness was limited and divergences persisted between existing national laws*».
Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980, disponibili qui: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm .

approach in many important respects and reinforced its integration with more recent work on privacy law enforcement co-operation. In 2020 the OECD is continuing to work with countries and experts to scope developments and provide practical recommendations on the implementation of the Guidelines in today's digital environment»[70].

Richiamando i più importanti interventi adottati in materia in seno alle Nazioni Unite, anzitutto ricordiamola Risoluzione del 2013 su "*The right to privacy in the digital age*" sul rapporto tra lo sviluppo tecnologico e le rivelazioni relative alla sorveglianza di massa (caso Snowden) che, palesando preoccupazioni, chiedeva all'Alto Commissariato per i diritti umani di preparare un report "*on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale*" [71], poi presentato al Consiglio per i diritti umani. In quell'occasione, il Consiglio adottò la Risoluzione 28/16 del 2015 istitutiva dello *Special Rapporteur sul diritto alla privacy*[72]. Vale, peraltro, la pena di riprendere al riguardo le considerazioni di Della Morte che, nell'analizzare la Risoluzione 57/239 del 2003 (iscrivendola nel solco di altri atti analoghi adottati nello stesso periodo) e quella n. 68/198 de 2013 ha notato "un'evoluzione del tema e delle sue articolazioni" e una "sostanziale differenza di approccio" nell'arco dei dieci anni, riscontrando prima – all'indomani dell'11 settembre – una certa diffidenza degli Stati rispetto alla rete; dopo, un'ampia fiducia verso le potenzialità delle tecnologie dell'informazione e della comunicazione[73].

Inoltre, una nuova Risoluzione, fondata sugli atti richiamati, ancora dedicata al *"right to privacy in the digital age*" venne adottata dall'AG nel novembre 2016, ribadendo l'importanza degli impegni internazionali rispetto al tema e notando che «*while metadata can provide benefits, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an*

[70] Così alla pagina web su *OECD work on privacy*: https://www.oecd.org/sti/ieconomy/privacy.htm .
Va detto anche che importanti obiettivi comuni correlati al tema sono stati individuati, dalla stessa OCSE, e articolati in principi in una Dichiarazione adottata nel 2011 nel corso di un *High Level Meeting* su "*The Internet Economy: Generating Innovation and Growth"* e che tra quei principi rileva, ai nostri fini, quello (il quarto) dedicato alle barriere che ostacolano il libero flusso transfrontaliero di dati, che dovrebbero essere minimizzate purché siano implementati i sistemi di sicurezza e protezione dei dati e assicurato il bilanciamento tra diritti; così ricorda G. DELLA MORTE, *Big Data e protezione internazionale dei diritti umani – regole e conflitti*, Editoriale Scientifica, 2018, pp. 122-128 (in part. p. 125).

[71] UN General Assembly, Resolution 68/167. *The right to privacy in the digital age*, 18 December 2013: https://undocs.org/A/RES/68/167 , part. punto 5. Rispetto a questa Risoluzione, nel Manuale sul diritto europeo in materia di protezione dati, *cit.*, p. 24, si legge: «Tali risoluzioni condannano fermamente la sorveglianza di massa ed evidenziano l'impatto che tale sorveglianza può avere sui diritti fondamentali alla vita privata e alla libertà di espressione nonché sul funzionamento di una società democratica e dinamica. Sebbene non giuridicamente vincolanti, esse hanno suscitato un importante dibattito politico internazionale di alto livello in materia di vita privata, nuove tecnologie e sorveglianza».

[72] Sullo UN Special Rapporteur on the right to privacy: https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx .

[73] Così G. DELLA MORTE, *op. cit.*, pp. 117-118.

individual's behaviour, social relationships, private preferences and identity. Expressing concern that individuals often do not provide their free, explicit and informed consent to the sale or multiple resale of their personal data, as the collecting, processing and sharing of personal data, including sensitive data, have increased significantly in the digital age»[74]. Su questa del 2016, come anche su un intervento del 2017[75], il Manuale della FRA fa notare per esempio l'importante sviluppo che essi rappresentano, rispetto agli atti precedenti, nel dibattito sulla vita privata in seno alle Nazioni Unite: «oltre alla responsabilità delle autorità statali, le risoluzioni sottolineano la responsabilità del settore privato nel rispetto dei diritti umani e invitano le imprese a informare gli utilizzatori in merito alla raccolta, all'utilizzo, alla condivisione e alla conservazione dei dati personali nonché a prevedere politiche di trattamento trasparenti»[76].

Tutto ciò, per dare contezza della sensibilità palesata in seno alle Nazioni Unite rispetto a questi temi in vista dell'evoluzione tecnologica e socioeconomica e, così, dell'impatto di queste riflessioni sugli interventi degli Stati e degli altri attori internazionali in materia.

Assumendo tali premesse, è quindi possibile passare all'analisi più specifica del contesto regionale europeo, nella consapevolezza che la regolamentazione del fenomeno gode di inarrestabili contaminazioni tra sistemi differenti e così, evolvendosi con il fenomeno stesso, si connota di dinamicità: "Nell'ambiente tecnologico in cui convergono le odierne attività di trattamento dei dati personali non potrebbe quindi esservi altra connotazione se non «dinamica» degli istituti che consentono alle persone il controllo sui propri dati, nel bilanciamento con altri interessi"[77].

2. I principali interventi in seno al Consiglio d'Europa

Preciseremo a seguire il quadro predisposto in seno a un'organizzazione internazionale che tipicamente si occupa di tutela dei diritti umani a livello regionale europeo, passaggio indispensabile prima di presentare quello previsto nell'ordinamento dell'Unione europea, posto che tutti gli Stati membri di quest'ultima sono anche parti della prima.

[74] UN General Assembly, Resolution A/C.3/71/L.39/Rev.1, *Revised draft resolution on the right to privacy in the digital age*, New York, 16 novembre 2016: https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1
[75] Il riferimento è a: ONU, Consiglio per i diritti umani, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 22 marzo 2017.
[76] FRA, Manuale, *cit.*, p. 25.
[77] Così R. D'ORAZIO, La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, 2019, p. 63.

Il riferimento è al Consiglio d'Europa, organizzazione internazionale a carattere regionale istituita nel 1949 da dieci Stati europei, e che conta oggi quarantasette Stati, con l'intento di proteggere e promuovere i diritti umani, la democrazia e lo stato di diritto.

CEDU

Il primo e principale intervento di attuazione di quegli obiettivi è, com'è noto, la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (di seguito anche CEDU), trattato multilaterale firmato a Roma nel 1950, di cui fanno parte tutti gli Stati del Consiglio d'Europa, tra cui, come si è detto, i 27 membri dell'UE. La Convenzione presenta un catalogo di diritti umani di cui promuove la protezione a livello internazionale – in ciò ispirandosi alla suddetta Dichiarazione Universale delle Nazioni Unite – ma con l'importante peculiarità di avere valore giuridico vincolante e soprattutto di aver istituito «un vero e proprio "sistema" di protezione dei diritti fondamentali, amministrato attraverso procedure di carattere "giurisdizionale", azionabili non solo su iniziativa degli Stati parti, ma anche (e ormai primariamente, com'è noto) ad impulso di privati. Nello spirito originario dei padri fondatori, dunque, la Convenzione di Roma nasceva come trattato internazionale di tutela dei diritti dell'uomo corredato di una struttura di controllo essenzialmente giudiziaria»[78].

Orbene, come si è anticipato, la CEDU prevedeva sin dagli esordi una norma dedicata alla materia in oggetto: il celebre articolo 8, rubricato "diritto al rispetto della vita privata e familiare" [79]. Tuttavia – e a differenza dell'articolo 12 UDHR – questa norma non faceva alcun cenno alla *privacy*, né ciò derivava da interpretazioni della Corte di Strasburgo, come notava González Fuster, che intercettava primi mutamenti in tal senso solo a partire dalla fine degli anni Sessanta. In quel periodo, infatti, il Consiglio d'Europa cominciò a mostrare mutamenti nell'affrontare la considerazione della "vita privata" degli individui, in particolare rispetto agli sviluppi tecnologici e alla necessità di regolare l'uso dei computer "*very much echoing formally the framing of the issue in the US, therefore*"[80]. L'esigenza (che portò il Comitato dei Ministri all'adozione di una Raccomandazione sulle banche dati elettroniche nel settore privato, del 1973, e poi nel settore

[78] Così ci ricorda A. DI STEFANO, *Convenzione europea dei diritti dell'uomo e principio di sussidiarietà – contributo ad una lettura sistematica degli articoli 13 e 35*, ed.it, 2009, p 23.
Sul carattere "innovativo" di tale sistema, *ex multis*, R. SAPIENZA, I 50 anni della Convenzione europea dei diritti dell'uomo, in *Aggiornamenti Sociali*, 6, 2000, pp. 515-523.
[79] Per alcuni commenti si vedano, *ex multis*: V. ZENO-ZENCOVICH , Articolo 8 – Diritto al rispetto della vita privata e familiare, in S. BARTOLE, B. CONFORTI, G. RAIMONDI (a cura di), Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali, Padova, 2001, pp. 307-318; C. PITEA, L. TOMASI , Articolo 8 – Diritto al rispetto della vita privata e familiare, in S. BARTOLE-P. DE SENA, V. ZAGREBELSKY (a cura di), *Commentario breve alla CEDU - Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali*, CEDAM, 2012, p. 297-369.
[80] G. GONZÁLEZ FUSTER, *op. cit.*, p.84, nonché, per i vari interventi in quel periodo, pp. 81-86.

pubblico, del 1974) si pose non solo per sopperire alle mancanze dell'articolo 8 CEDU, ma anche per l'urgenza di evitare divergenze tra le legislazioni nazionali in materia: «*By the end of 1974, experts at the Council of Europe considered that the body of law created across Europe for the protection of individuals against computerised records has acquired a name of its own, and that such name was 'data protection'*»[81]. Da qui, dunque, le basi per il principale intervento del Consiglio d'Europea al riguardo: una Commissione di esperti venne riunita nel 1976 con il compito di preparare (peraltro potendosi giovare di consulti con l'OCSE) una Convenzione precipuamente dedicata alla protezione rispetto al trattamento dei dati, compito che coinvolse anche l'interesse delle istituzioni comunitarie.

Convenzione 108 (e protocollo addizionale). Si tratta della *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, n. 108 del 1981[82], ispirata all'articolo 8 CEDU e ad oggi unico strumento giuridicamente vincolante di portata internazionale in materia. Va precisato, infatti, che la peculiarità della Convenzione 108 sta proprio nella sua apertura: pur essendo stata adottata in seno al Consiglio d'Europa, essa consente anche la ratifica di Stati che non partecipano all'organizzazione regionale, e conta infatti oggi 51 parti. Nel 1999 la Convenzione venne emendata per consentire alle (allora) Comunità europee di accedervi[83]. La *ratio* di tale peculiare apertura al mondo starebbe proprio nella necessità di consentire il flusso transfrontaliero di dati personali: «*Convention 108 was conceived, and delivered, with the idea that data protection should respect the principle of international free flow of information*»[84]. E difatti, ai lavori preparatori della Commissione parteciparono, da osservatori (oltre all'OCSE), anche quattro Paesi terzi (USA, Australia, Canada e Giappone), che però hanno instaurato relazioni formali sono in tempi recenti[85].

[81] Ibidem, p. 86, ove continua: <*This body of law was nevertheless portrayed as an element of 'privacy', a term sometimes linked to its understanding as 'information(al) privacy' (Hondius, 1975, p. 4) but sometimes used to refer the content of Article 8 of the ECHR*>, enfasi aggiunta.

[82] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, n. 108 del 28 gennaio 1981, Strasburgo: (versione italiana) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078c45

[83] Cfr. G. GONZÁLEZ FUSTER, *op. cit*., p.87.

[84] S. KWASNY, Convention 108, a Trans-Atlantic DNA?, in D. SVANTESSON, D. KLOZA (Eds), *Trans-atlantic data privacy relations as a challenge for democracy*, Intersentia, 2017, p. 533, ove, peraltro, l'autrice arriva a questa conclusione a seguito della domanda: «*Is this opening to the world, aimed at affording protection to individuals when data concerning them flow across borders and oceans, with a particular focus on the trans-Atlantic dimension examined here, the result of genetic instructions which guided its development? Or is it instead the result of a genetic mutation or the result of the use of genetic engineering techniques?* ».

[85] *Ibidem*, pp. 535-537.

Dall'articolo 1 della Convenzione si evince: «*Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»)*», mentre l'articolo 3 precisa che "*le Parti si impegnano ad applicare la presente Convenzione alle collezioni automatizzate di dati a carattere personale e all'elaborazione automatica di tali dati nei settori pubblico e privato*". Dunque, sono compresi anche i trattamenti effettuati da autorità giudiziarie e polizia (che esulano, invece, come si vedrà, dalla previsione del GDPR)[86]. Particolarmente rilevante ai nostri fini è il Capitolo III rubricato "Flussi internazionali di dati" a cui dedica il solo Articolo 12, rubricato *Flussi internazionali di dati a carattere personale e diritto interno*, che al paragrafo 1 statuisce che le disposizioni della Convenzione si applicano ali trasferimenti attraverso confini nazionali e poi, al paragrafo 2, che una Parte non può proibire i flussi destinati al territorio di un'altra parte, prevedendo però in tal caso delle al paragrafo 3, il quale (alla lett. a) dispone "*salvo che la regolamentazione dell'altra Parte fornisca una protezione equivalente*". L'*Explanatory Report* spiegava da subito, infatti, che la Convenzione fosse volta a sopperire alle difficoltà derivanti dall'adeguata protezione degli individui da parte delle legislazioni nazionali dedicate, quando i loro dati venissero trasferiti oltre i confini. Inoltre, commentando l'articolo 12 suddetto, il *Report* chiariva che le deroghe al divieto di proibire il flusso di dati verso un altro Stato parte non sarebbero consentite, appunto, se quest'ultimo garantisce una "protezione equivalente", e che quindi «*a Contracting State which subjects transborder data flows to special authorisation may not deny such authorisation on the ground of protection of privacy if the recipient country provides equivalent protection*»[87].

Questo passaggio si ritiene di rilievo poiché, ancorché limitato ai flussi di dati tra Stati parti della Convenzione (e, dunque, soggetti che ne condividono le disposizioni e i principi sottesi), ci consente di introdurre un concetto che costituirà il *leitmotiv* della nostra ricerca e che pare essere nucleo portante dell'azione del Consiglio d 'Europa, che in tal modo ha condizionato (in ossequio a ciò che è stato intercettato da alcuni come c.d. *Strasbourg effect*, di cui diremo) quella dell'attuale Unione europea (come, infatti, le previsioni del GDPR – sul flusso dei dati verso Stati terzi – confermano): *il principio della tutela equivalente*. A tal riguardo, risalta particolarmente il famoso Protocollo addizionale del 2001 (entrato in vigore nel 2003), specie considerandone le due rilevanti

[86] FRA, Manuale diritto europeo, *cit*., p.27.
[87] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 21.1.1981, par. 69; cfr. anche par. 8.

novità: l'istituzione di autorità nazionali di controllo per garantire la corretta applicazione delle disposizioni della Convenzione all'interno degli Stati parti (previsione che risente dell'influsso della direttiva comunitaria 95/46/CE, di seguito anche: direttiva madre)[88]; la necessità della garanzia di una "tutela adeguata" da parte di un Paese terzo o organizzazione internazionale verso i quali il flusso di dati da Stati parti è destinato[89]. Qui, un'ulteriore conferma dello spessore del principio, che dopo il 2001 (dunque, in piena coerenza con le nuove strategie di intervento facenti seguito agli eventi dell'11 settembre) veniva esteso ai flussi di dati verso Stati terzi e organizzazioni internazionali e, dunque, assumeva una portata centrale nelle dinamiche dei rapporti verso l'ambiente "esterno" rispetto a quello determinante il "territorio" della Convenzione.

Per chiudere sulla Convenzione 108, un intervento di fondamentale rilievo (che, come nel caso del Protocollo addizionale, segue importanti mutamenti socio-sistemici – tra cui il GDPR in EU – nonché la consueta necessità, tipica del settore, di stare al passo coi tempi) va ravvisato nella modifica apportata dal Protocollo emendativo del 2018, volto alla c.d. *modernizzazione della Convenzione 108*, che infatti dopo di esso è denominata "*Convenzione 108+".* Il Protocollo contiene parecchie novità, tra cui il rafforzamento delle autorità garanti e la previsione del Comitato della Convenzione, nonché l'irrobustimento di alcuni principi già inseriti. L'aspetto peculiare, ai nostri fini, riguarda sempre il flusso di dati: la Convenzione rappresenta così "un punto di raccordo importante tra i diversi approcci regionali", laddove, per esempio, il GDPR considera l'adesione di Stati terzi alla stessa come un criterio per valutare l'adeguatezza della protezione garantita a tali dati (al loro interno)[90].

Convenzione cybercrime

Sorvolando su alcuni altri interventi minori – come le Raccomandazioni del Consiglio correlate all'ampio settore della protezione dei dati[91], o la Dichiarazione del Comitato dei Ministri su "*Internet Governance Principles*" del 2011[92] –, deve darsi invece atto dell'importante intervento in materia di polizia sicurezza e giustizia, consistente nella nota Convenzione n. 185 "*sulla criminalità informatica*", firmata a Budapest nel 2001 (pertanto, c.d. Convenzione di Budapest). Si tratta del primo strumento di carattere internazionale che interviene a disciplinare i "nuovi reati" legati alla

[88] Cfr. FRA, Manuale, *cit.*, p. 33.
[89] Cfr. per le due innovazioni G. DELLA MORTE, *op. cit.*, pp. 92-93.
[90] Così dal sito web del Garante italiano per la protezione dei dati personali, Protezione dati: approvato il Protocollo che aggiorna la Convenzione 108, 21 maggio 2018: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9102006 .
[91] Cfr. F. PIZZETTI, cit., p. 28.
[92] Per cui si veda G. DELLA MORTE, op.cit., 120 ss.

realtà informatica, volta a perseguire una politica criminale comune contro la cybercriminalità[93]. I principi sui quali essa si fonda sono stati ispirati da un gruppo di Garanti europei, che puntualizzavano come lo scambio di dati derivasse anche e inevitabilmente dalle attività di cooperazione internazionale e dalle difficoltà derivanti da una non totale armonizzazione delle legislazioni degli Stati parti sul punto[94]. Anche la Convenzione 185 è corredata di un Protocollo addizionale, adottato nel 2003 e volto essenzialmente ad estenderne l'ambito di applicazione ai reati legati alla propaganda a sfondo razziale o xenofobo. Ciò, sia per muovere verso una sempre maggiore armonizzazione, sia per «fornire agli Stati parte la possibilità di utilizzare gli strumenti di cooperazione internazionale stabiliti dalla Convenzione in questo campo»[95].

Ciò brevemente detto, è possibile focalizzare l'attenzione sulla specifica realtà propria del contesto ordinamentale comunitario – nostro centro di indagine – tenendo sempre in conto, nel farlo, il contesto, sin qui delineato, all'interno del quale esso si inserisce.

[93] Qui riferimento alla Convenzione a ella parte di essa che prevede questo obiettivo.
[94] Così nota A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, Torino, 2018, pp. 7-8, che riporta anche gli sviluppi, nello specifico caso italiano, della legge di ratifica: "implementazione di alcune disposizioni del codice di procedura penale già esistenti; con espresso riferimento all'ambito informatico e introduzioni di disposizioni *ex novo*".
[95] Così G. DELLA MORTE, op. cit., p. 96.

CAPITOLO III

IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI NELL'UNIONE EUROPEA

1. Cenni introduttivi

"*While in generic terms the objective is still the same as in the eighties of the past century, namely warranting a European-wide high level of protection of personal data in order to ensure the free circulation of personal data and stimulating business in the digital single market, the points of discussion and disagreement are still manifold*"[96].

Se a partire dagli anni Settanta e poi, ancor più, negli anni Ottanta si ebbero i primi timidi interventi sulla protezione dei dati personali sia a livello domestico che a livello internazionale, l'intermedio livello sovranazionale fece attendere prima di fornire strumenti in materia. Eppure, già a quei tempi le istituzioni comunitarie palesavano una certa sensibilità sul punto.

Si è già fatto cenno, infatti, alla Comunicazione della Commissione dei primi anni Settanta "*Community policy on data processing*" stimolata dai suddetti interventi nazionali (, rispetto alla quale è stato notato che «*it optimistically hoped that if common ground rules were established there would be no need to enact legislation in order to harmonize conflicting national laws*»[97]. Sempre al fine di rintracciare regole di base comuni, la Commissione europea assunse poi un ruolo proattivo nei confronti della Convenzione n. 108, adottando una Raccomandazione (81/679/CEE)[98] per stimolare gli Stati membri a ratificarla entro il 1982, intervento che ebbe un esito infausto ma che così stimolò l'istituzione comunitaria ad agire direttamente per un'armonizzazione delle legislazioni nazionali[99]. Ancora, alla Convenzione n. 108 si riferiva la Risoluzione "*sulla tutela dei diritti degli individui di fronte al crescente sviluppo tecnico nel settore dell'informatica*"[100] del Parlamento

[96] S. GUTWIRTH, R. LEENES, P. DE HERT (Eds), *Data Protection on the Move – Current Developments in ICT and Privacy/Data Protection*, Springer, 2015, Preface, V.
[97] Così O. LYNSKEY, op. cit., p. 47.
[98] Raccomandazione della Commissione, del 29 luglio 1981, *concernente una convenzione del Consiglio d'Europa sulla protezione delle persone per quanto riguarda l'elaborazione automatica dei dati a carattere personale*, 81/679/CEE, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.1981.246.01.0031.01.ITA&toc=OJ:L:1981:246:TOC
[99] O LYNSKEY, *cit.*, p. 48.
[100] Parlamento europeo (Commissione giuridica), *Risoluzione sulla tutela dei diritti degli individui di fronte al crescente sviluppo tecnico nel settore dell'informatica*, GU C 87/39 del 5.4.1982, pag. 39, 51981IP0548 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:JOC_1982_087_R_0031_01&from=IT

europeo del 1982, che riportava preoccupazioni per i tempi di ratifica della Convenzione da parte degli Stati membri. In essa inoltre emergeva la constatazione che "*in vari Stati della Comunità non esistono ancora normative che disciplinino la tutela del cittadino europeo contro l'abuso della memorizzazione e dell'elaborazione di dati, o che quanto meno esse differiscono l'una dall'altra sotto il profilo del livello di protezione, dei criteri procedurali e delle fattispecie contemplate*", richiamando quindi la norma sul ravvicinamento delle legislazioni (l'allora articolo 100 del Trattato CEE, oggi corrispondente all'articolo 114 TFUE) e rimarcando che "*essendo una comunità economica e commerciale, la Comunità europea deve poter escludere gli effetti secondari che ne derivano, tutelando i cittadini europei con disposizioni generali, equivalenti ed efficaci in materia di informatica*"[101]. Difatti, proprio quando la vocazione economica dell'integrazione europea si scontrò con la necessità di garantire il funzionamento del sistema, attraverso le quattro libertà economiche fondamentali, risultò evidente che l'effettiva circolazione delle merci, delle persone, dei servizi e dei capitali non poteva avvenire in maniera efficiente senza una circolazione dei dati correlati. Non è un caso, quindi, che la prima normativa al riguardo – che trovava proprio fondamento giuridico nella suddetta norma sul ravvicinamento delle legislazioni nazionali ai fini del funzionamento del mercato interno – sia datata, com'è noto, alla metà degli anni Novanta, ossia all'indomani del Trattato di Maastricht.

Questa considerazione ci impone di confermare l'approccio scelto nel condurre la parte iniziale di questa ricerca – ossia quello che parte dalle spinte dell'esterno che modellano la 'forma', per poi, in un secondo momento, verificarne il moto opposto – e prendere atto che quella revisione subì un grande influsso dalla caduta del muro di Berlino, evento di portata internazionale (per le cui implicazioni rispetto al processo di integrazione europea si veda *supra*, Parte I), e dalla fine della Guerra fredda. Col Trattato di Maastricht, come si sa, si realizzò un'importante spinta all'integrazione europea, con la creazione dell'Unione europea, l'istituzione della cittadinanza europea, la struttura a tre pilastri che (per quanto interessa ai nostri fini) nel primo collocava la realizzazione del Mercato Unico. Ciò, ci ricorda Pizzetti, aveva un preciso legame con la protezione dei dati personali; anzi due. Ci riferiamo al ruolo non irrilevante giocato al riguardo dalla Convenzione di Schengen del 1990, che integrava l'Accordo di Schengen avvenuto nel 1985 tra 5 Paesi della CEE riguardo alla graduale abolizione dei controlli sulle persone alle frontiere interne (c.d. *acquis di Schengen*)[102]. Più precisamente: «Il primo, immediatamente connesso al Trattato di

[101] Ibidem, punti 2, 5, 6 e 10.
[102] Acquis di Schengen - Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni – Gazzetta ufficiale n. L 239 del 22/09/2000, p. 0019-0062.

Maastricht, è la caduta di ogni controllo doganale per le merci alle frontiere, che si verificò appunto a partire dal 1° novembre 1993. Il secondo fu l'abbattimento dei controlli di frontiera anche per le persone. Abbattimento, questo, che fu legato alla sottoscrizione della Convenzione di Schengen (…) integrata dal successivo Trattato di Amsterdam del 1999. (…) *come conseguenza del Trattato di Maastricht e dell'abbattimento delle dogane, avvenuto il 1° novembre 1993, divenne essenziale per i paesi dell'Unione superare anche le frontiere immateriali costituite dalle diverse leggi nazionali in materia di protezione dei dati personali*. Frontiere immateriali esistenti di fatto, sia per i Paesi che se ne erano dotati che per quelli che ancora non avevano provveduto a farlo. L'abbattimento delle dogane per le merci, infatti, aveva un effetto inevitabilmente limitato dal fatto che per ogni Paese, fornitore o destinatario della merce, potessero valere regole diverse relativamente all'uso dei dati personali connessi agli scambi. Ben consapevoli di tutto questo, i Paesi membri della Comunità preesistenti al Trattato sull'Unione del 1992, avviarono, a partire dalla firma dell'Atto Unico Europeo (…), le trattative necessarie per cercare di addivenire a una normativa europea uniforme in materia di protezione dei dati personali, che fosse in grado di appianare ogni differenza di trattamento, e facesse quindi cadere anche questa frontiera immateriale»[103]. Il riferimento è alla predisposizione della famosa Direttiva 95/46/CE che costituì sino a poco tempo fa la normativa comunitaria fondamentale nel settore, della quale si avrà modo di parlare. Qui basti dire che essa consentì l'armonizzazione delle diverse legislazioni nazionali in materia di protezione dei dati, introducendo anche in tale settore il principio del mutuo riconoscimento[104] (emerso, com'è noto, proprio nell'ambito della libera circolazione delle merci, dalle necessità imposte dall'unione doganale, cfr. sentenza *Cassis de Dijon*, 1979)[105].

Quanto esposto, peraltro, non esclude anche altre considerazioni: così, infatti, Lynskey richiamava il noto *caso FIAT*, sull'intervento dell'autorità francese di protezione dati (CNIL) circa il trasferimento dei dati di un impiegato da Parigi a Torino, palesante la mancanza di una legislazione di protezione adeguata in Italia, quale *casus belli* che stimolò la Commissione a proporre un regime armonizzato di protezione dei dati[106]. Tutto ciò concorre, quindi, a considerare la libera circolazione dei dati personali come una "costola" delle quattro libertà fondamentali, dunque a sua volta funzionale alla "centralità"[107] del funzionamento del mercato interno: «*Although the merits of free*

Sull'incidenza rispetto allo sviluppo del sistema di protezione dei dati nell'ordinamento comunitario, si veda GONZÁLEZ FUSTER, *op. cit*., p. 122 ss.

[103] F. PIZZETTI, *op. cit*., pp. 65-66.

[104] Ibidem.

[105] Corte di giustizia, causa 120/78, *Rewe-Zentral AG c. Bundesmonopolverwaltung für Branntwein*, sentenza 20 febbraio 1979.

[106] O. LYNSKEY, *op. cit*., p. 49.

[107] Così la esprime, precisamente, A. TERRASI, *La protezione dei dati personali tra diritto internazionale e diritto dell'Unione europea*, Giappichelli, 2008, p. 141.

trade in personal data have been contested, the logic underpinning this objective is the same as that underpinning the EU's Internal Market and, as such, is the familiar logic of trade liberalization between EU Member States»[108].

Così brevemente delineato il percorso eziologico della protezione dei dati personali nell'ordinamento comunitario, prima di passare alla disamina del contesto normativo va intanto ricordato che l'intervento successivo alla Direttiva 95/46, rilevante ai nostri fini, fu proprio l'adozione a Nizza nel 2000 della Carta dei diritti fondamentali dell'Unione europea, che (ancorché sino a Lisbona non giuridicamente vincolante), come si è accennato, introdusse un'apposita norma dedicata alla protezione dei dati personali (articolo 8) così enfatizzandone la natura di diritto fondamentale. Inoltre, un notevole incremento dell'attenzione dell'Unione nel settore è testimoniato dagli interventi successivi all'entrata in vigore del Trattato di Lisbona (che pure, come si vedrà, apportò significative novità), oltre che per la necessaria riforma della normativa esistente (risale al 2012 la proposta della Commissione, ancorché una comunicazione che discuteva su ciò può riscontrarsi già anni prima), anche per la costruzione di un Mercato Unico Digitale (*Digital Single Market*, di seguito anche: DSM).

Prospettato dalla Commissione già nel 2010 nella Comunicazione "*Europa 2020, una strategia per una crescita intelligente, sostenibile e inclusiva*"[109], il DSM è stato oggetto di una specifica strategia esposta dall'esecutivo europeo nel 2015 con la Comunicazione sulla "*Digital Single Market Strategy for Europe"*[110]. Esso consiste in un «mercato in cui è garantita la libera circolazione dei dati personali: quinta libertà oltre alle tradizionali (…). Un mercato unico in cui – indipendentemente da cittadinanza, nazionalità o luogo di residenza – persone e imprese non incontrano ostacoli all'accesso e all'esercizio delle attività on line in condizioni di concorrenza leale, potendo contare su un livello elevato di protezione dei consumatori e dei dati personali. La realizzazione del DSM consentirà all'UE di mantenersi tra i leader mondiali dell'economia digitale, sostenendo la crescita delle imprese europee su scala mondiale»[111]. L'integrazione digitale è

[108] O. LYNSKEY, *op. cit*., p. 9.
[109] COMUNICAZIONE DELLA COMMISSIONE, *EUROPA 2020 – Una strategia per una crescita intelligente*, sostenibile e inclusiva, COM(2010) 2020 definitivo, Bruxelles, 3.3.2010.
[110] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, disponibile qui: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN
Per riflessioni generali sul "nuovo quadro giuridico dell'Unione europea per la (progressiva) costruzione di un mercato unico digitale" si veda in particolare F. ROSSI DAL POZZO, La tutela dei dati personali nella giurisprudenza della Corte di giustizia, in *Eurojus*, 2018, pp. 3-4.
[111] E. TOSI, *Privacy Digitale*, cit.., p. 15.

divenuta pertanto, consideratone l'impatto, una priorità anche delle altre istituzioni dell'Unione[112]. Nella strategia, la Commissione individuava sedici azioni chiave per realizzare il DSM, raggruppate in tre pilastri (*access, environment, economy and society*)[113].

La predisposizione di una regolamentazione armonizzata in materia (di cui il GDPR costituisce il fiore all'occhiello) si iscrive dunque in questo contesto, mentre di recente la nuova Commissione, come avremo modo di illustrare, ha incrementato il suo impegno nel settore, tra le priorità dell'agenda 2019-2024. Il riferimento è alla Comunicazione del 19 febbraio 2020, "*Shaping Europe's Digital Future*" che presenta, come prima tra le azioni chiave prospettate, una "*European Data Strategy - to make Europe a global leader in the data-agile economy (February 2020), announcing a legislative framework for data governance (Q4 2020) and a possible Data Act (2021)*"[114]. Le azioni previste sono, ancora, raggruppate in tre pilastri (tecnologia al servizio delle persone; economia digitale equa e competitiva; società aperta, democratica e sostenibile) e la strategia mira proprio a rendere l'Unione europea un modello di riferimento mondiale per l'economia digitale, sostenendo le economie invia di sviluppo nella digitalizzazione e promuovendo norme digitali a livello internazionale[115]: così, definendo standard a livello globale, "*The EU (...) will remain the most open region for trade and investment in the world, provided that anyone who comes to do business here accepts and respects our rules*"[116]. Degli importanti interventi assunti recentemente dalla Commissione in attuazione della sua Strategia volta a *Plasmare il Futuro Digitale dell'Europa* si avrà modo di discutere.

Qui basti rilevare che pare ancora (ossia, pur trascorso un lustro) condivisibile l'arguta analisi di Lynskey (ancorché, inevitabilmente, inconsapevole degli ultimi sviluppi) sulle caratteristiche del regime di protezione dei dati personali nell'ordinamento sovranazionale europeo. In breve, l'autrice argomentava che si tratterebbe di un:

- *omnibus regime*, come sarebbe confermato da tre caratteristiche: «*the application of data protection rules to public and private sectors, the sector-neutral nature of data protection*

[112] Così, infatti, si evince dalla pagina del Parlamento europeo dedicata (e relativi collegamenti): https://www.europarl.europa.eu/italy/it/il-nostro-ufficio/il-mercato-unico-digitale-in-europa .
[113] Come si evince dalla Comunicazione già citata, i tre pilastri sono: 1) Migliorare l'accesso ai beni e servizi digitali in tutta Europa per i consumatori e le imprese; 2) Creare un contesto favorevole e parità di condizioni affinché le reti digitali e i servizi innovativi possano svilupparsi; 3) Massimizzare il potenziale di crescita dell'economia digitale. Così si legge dal comunicato stampa della Commissione del 6 maggio 2015, in cui sono disponibili i diversi collegamenti per i necessari approfondimenti: https://ec.europa.eu/commission/presscorner/detail/it/IP_15_4919 .
[114] Così dal testo della Comunicazione: Communication - *Shaping Europe's digital future*, 19 February 2020, https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf
[115] Così si legge nella pagina in italiano della Commissione a ciò dedicata: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_it#leuropa-leader-mondiale .
[116] Ibidem.

rules, and the enforcement of data protection rules by independent supervisory authorities»[117];

- *legitimizing regime*, cioé un regime che, in sostanza, (e come si è già detto *supra*, citando De Hert) legittimerebbe il trattamento dei dati personali: «*Once it can be demonstrated that a legal basis for personal data processing exists and that this processing complies with specified data protection safeguards, then this processing is in principle legitimate*»[118];
- *rights-based regime*, che, secondo l'autrice, può essere così considerato da due punti di vista: «*first, (...) if it is right-conferring, in other words if it grants rights to individuals. Secondly (...) if it 'gives expression to' a fundamental right or if its design and interpretation are consistent with its underlying conception as a fundamental right*»[119];
- *regime with an extraterritorial impact*, con ciò, evidentemente, intendendo che: «*Data protection is one of the rare fields in which the EU could be said to exercise global regulatory supremacy; the EU rules have now been used as a blueprint for regulatory regimes across 0the Western world*»[120].

La portata di ciascuna di queste caratteristiche veniva compiutamente analizzata dall'autrice, alla quale dunque si rimanda. Nondimeno, abbiamo voluto illustrarne brevemente i contenuti per tenerli in considerazione poiché molti aspetti, soprattutto l'ultimo, torneranno più volte nell'analisi che segue, sia nelle teorie che in pratica, fornendo manforte alla tesi che vogliamo sostenere.

Questo, quindi, per grandi linee, il contesto che caratterizza il settore della protezione dei dati nell'ordinamento sovranazionale, rispetto al quale è necessario, per poter sviluppare l'analisi che segue, esporne gli aspetti essenziali del quadro normativo e di quello istituzionale.

2. L'evoluzione del quadro normativo

La Direttiva 95/46/CE

Come si è accennato, la prima normativa in materia di protezione dei dati personali rinvenibile nell'ordinamento comunitario è la Direttiva 95/46/CE, del 24 ottobre 1995, *relativa alla tutela delle*

[117] O. LINSKEY, *op. cit.*, p. 15, ma per la compiuta esplicazione si veda pp. 15-30.
[118] Ibidem p. 30, ma per una compiuta esposizione v. pp. 30-35.
[119] Ibidem, pp. 35-36, ma per una compiuta esposizione si veda pp.35-40.
Di ciò si avrà modo di parlare nelle Parti III e IV.
[120] Ibidem, p. 41 (enfasi aggiunta), ma per una compiuta esposizione si veda pp. 41-44.

persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[121]. Si tratta, evidentemente, di un atto di diritto derivato, non direttamente applicabile e dunque richiedente norme interne di attuazione negli ordinamenti nazionali, che trovava la sua base giuridica nell'allora articolo 100 del Trattato CE, dedicato al ravvicinamento delle legislazioni nazionali aventi ad oggetto l'instaurazione e il funzionamento del mercato interno (corrispondente all'attuale articolo 114 TFUE). Ebbene, la valenza costituzionale della base giuridica di un atto, sovente ribadita dalla Corte di giustizia[122], palesa la *ratio* sottesa all'adozione della Direttiva, che si è in qualche modo introdotta nel paragrafo precedente.

In particolare, si è detto che la necessità di un ravvicinamento delle differenti legislazioni nazionali divenne sempre più impellente a seguito del Trattato di Maastricht, ossia dell'abbattimento delle barriere doganali tra Stati membri, e dunque essa si pose come strumentale al funzionamento del mercato interno. Così, ancora, riprendendo Pizzetti: «Soltanto nel 1995, infatti, la Direttiva 95/46 adottata nell'ambito della Comunità europea, e dunque nel quadro di quello che, fino al Trattato di Lisbona del 2009, è stato il primo pilastro dell'Unione, fu possibile addivenire a una normativa europea comune. (…) L'effetto maggiore di questa Direttiva fu però che, pur restando le legislazioni nazionali differenti anche se armonizzate, *si affermò il principio del mutuo riconoscimento tra i diversi Paesi membri*. La conseguenza del mutuo riconoscimento consiste nel fatto che in ogni Paese dell'Unione si applica la legge di protezione dati del Paese in cui ha sede lo stabilimento principale del titolare del trattamento. (…) In questo modo, da un lato si rinunciò all'obiettivo (…) di giungere a una regolazione vincolante comune. dall'altro, si ottenne egualmente che, grazie al principio del mutuo riconoscimento, *fossero abbattute le frontiere immateriali, legate alla protezione dei dati personali*»[123]. Invero, l'articolo 1 della Direttiva, rubricato "*oggetto della direttiva*", presentava espressamente "*la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali*", da un lato (par. 1), e "*la libera circolazione dei dati personali tra Stati membri*", dall'altro (par. 2), che non poteva essere ristretta o vietata dagli Stati membri per motivi connessi al paragrafo 1[124]. Così venivano individuati i due obiettivi della Direttiva: uno "economico" e l'altro

[121] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, GU L 281 del 23.11.1995, pagg. 31–50 (non più in vigore, dal 24.05.2018).
[122] *Ex multis*, Corte di giustizia, parere 2/00, *Protocollo di Cartagena*, 6 dicembre 2001.
[123] F. PIZZETTI, op. cit., pp. 65-66, enfasi aggiunta.
[124] Direttiva 95/46/CE, cit., Articolo 1: Articolo 1 – *Oggetto della direttiva*
1. Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.
2. Gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela garantita a norma del paragrafo 1.

"basato sui diritti": «*these two goals are intrinsically linked*. (…) *However (…) there is also an apparent tension between the Directive's economic and rights-based orientation*»[125]. Tensione che, ai tempi in cui la Direttiva fu adottata, si poteva ben comprendere in assenza di un catalogo di diritti tutelati espressamente a livello sovranazionale (la Carta dei diritti fondamentali sarà adottata nel 2000 e assumerà valore vincolante solo dopo Lisbona). Nondimeno, in questo settore – come, più in generale, in tutti quelli in cui si poneva l'impellenza di una tutela dei diritti fondamentali – fu, com'è noto, l'intervento pretorio della Corte di giustizia a soddisfare, poco a poco, le istanze di tutela. Si darà conto di ciò nel prosieguo, ma una cosa va subito chiarita: «*there is a stark difference between data protection past and data protection present: data protection now continues to serve its integrationist purpose but its fundamental rights objective is no longer overlooked*»[126].

Interessante è anche l'ambito di applicazione della normativa, che veniva individuato dall'articolo 3 della Direttiva, specie rispetto all'unico strumento allora comparabile, ossia la Convenzione 108: esso risultava più esteso nella misura in cui era rivolto anche al trattamento non automatizzato di dati personali (art. 3, par. 1), ma più ristretto nella misura in cui escludeva le "*attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale*" (art. 3, par. 2)[127], estromettendo così quelli che erano allora il secondo e il terzo pilastro. Sulla rilevanza di questa previsione, in particolare, insisteva Della Morte: «la Direttiva 95/46/CE presenta uno dei momenti regolamentativi più significativi. Essa segna il passaggio da una disciplina di stampo marcatamente minimo e settoriale, come quella sancita dalla Convenzione 108 (…) a un approccio caratterizzato da una visione più ampia, ancorché circoscritto dal contesto comunitario. (…) il principio cardine riconosciuto nel contesto della Direttiva dati è quello, strettamente connesso con il principio di proporzionalità, della cd. finalità limitata, ai sensi della quale i dati personali devono essere rilevati per finalità che siano determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità»[128]. Tuttavia, proprio questa previsione si rivelerà problematica col passare del tempo, specie a seguito dell'eliminazione della struttura a pilastri avvenuta con il Trattato di Lisbona. Sull'ambito di applicazione, peraltro, è intervenuta poi la Corte di giustizia in seminali sentenze, prima della rimodulazione avvenuta con il GDPR, come diremo ampiamente (cfr. *infra*, Capitolo I, Parte IV).

[125] Così li descrive O. LINSKEY, op. cit., p. 46.
[126] Ibidem, p. 47.
[127] Direttiva 95/46/CE, cit., Articolo 3.
[128] G. DELLA MORTE, op. cit., pp. 102-103.

Un ultimo aspetto da segnalare sin d'ora sulla direttiva madre, non più in vigore, è quello relativo al Capo IV, rubricato "*Trasferimento di dati personali verso Paesi terzi*" che, composto da soli due articoli, all'articolo 25 ne definiva i principi e all'articolo 26 ne stabiliva le deroghe. Analizzeremo parecchio questo settore e le sue evoluzioni (*infra*, Capitolo II, Parte IV), ma qui ricordiamo che già l'articolo 25 prevedeva proprio la necessità che gli Stati membri assoggettassero il trasferimento di dati personali verso Paesi terzi alla condizione che questi ultimi garantissero "un livello di protezione adeguato", spiegando come gli Stati membri e la Commissione dovessero atteggiarsi in caso di riscontrata inadeguatezza[129]. Queste considerazioni, innovative nel contesto comunitario come l'intera disciplina introdotta dalla direttiva, venivano sicuramente mutuate dalla Convenzione 108, nella quale, si è detto, emerge chiaramente il principio di protezione equivalente (declinato, nell'ordinamento comunitario, in termini di "adeguatezza"), e dunque in qualche modo espressive di ciò che spiegheremo verrà chiamato "*Strasbourg effect*". Così infatti, ancora, notava Pizzetti, rilevando che la Direttiva addirittura "rovesciò l'impostazione" della Convenzione 108 nello specificare che il trasferimento può essere consentito *soltanto se* lo Stato terzo garantiva la condizione richiesta: «In questo modo, se è certamente vero che si rafforzarono ulteriormente le garanzie di protezione dei dati personali assicurate dall'Unione, è vero anche che quelle frontiere immateriali prima esistenti all'interno dell'Unione furono spostate tutte ai suoi confini, favorendo così il fenomeno della protezione dei dati personali come parte integrante della c.d. "fortezza Europa"»[130].

Orbene, se è vero che la Direttiva ha costituito per più di un ventennio il "principale strumento legislativo per la protezione dei dati personali in Europa" pertanto considerata una "pietra miliare"[131], è vero anche che essa pose sin da subito alcuni problemi, che divennero sempre più pressanti e numerosi con il passare del tempo e il sempre più veloce sviluppo delle tecnologie. Anzitutto, essa presentava sin da subito diverse lacune, che furono parzialmente colmate con ulteriori interventi normativi che si elencheranno a breve. Ma soprattutto, essa risultò inadeguata a seguito dell'entrata in vigore del Trattato di Lisbona. Al riguardo, infatti, Passaglia ci ricorda quali furono i principali elementi di criticità: "Un primo elemento da prendere in considerazione è la discrasia «operativa» venutasi a creare, dopo il Trattato di Lisbona, tra la direttiva e il diritto primario dell'Unione: l'avvenuta eliminazione della struttura a pilastri dell'Unione ha reso, infatti, obsoleta la distinzione su cui la Direttiva del 1995 si imperniava (…). Ancor più rilevante, peraltro, appare la circostanza che la Direttiva del 1995, (…) fosse stata concepita con il preciso intento di

[129] Direttiva 95/46/CE, articolo 25, parr. 1,2,3.
[130] F. PIZZETTI, *op. cit.*, p. 66.
[131] A. PISAPIA, *op. cit.*, p. 16.

favorire un ravvicinamento delle legislazioni nazionali. (…) L'affacciarsi prepotente della tutela dei dati personali come diritto individuale nell'ambito del diritto primario creava dunque una frattura rispetto alla filosofia di fondo della direttiva, che indubbiamente ha contribuito a comportarne la senescenza"[132]. Ma, in aggiunta a questi aspetti, l'autore rilevava come fattore preponderante di criticità della Direttiva proprio la sua "finalità basilare", ossia, appunto, il ravvicinamento delle legislazioni. «Ciò ha influito sulla sorte della direttiva sotto due punti di vista. Il primo si collega alle difficoltà incontrate in diversi paesi nella fase di recepimento della direttiva. (…) Dal secondo punto di vista, il superamento delle difficoltà di attuazione non ha fatto velo, peraltro, ad un limite strutturale della direttiva, che non poteva non tradursi in una sua congenita provvisorietà: perseguendo un *ravvicinamento* delle legislazioni, la direttiva poteva raggiungere uno scopo che poteva essere soltanto parziale. (…) Altrimenti detto, la direttiva, una volta raggiunti i suoi obiettivi, non poteva non mostrare i suoi limiti, consistenti nell'impossibilità oggettiva di creare una uniformità compiuta di disciplina tra gli Stati membri»[133]. Condividendo queste considerazioni, che paiono sufficienti per spiegare la necessità di riforma, prima di passare all'analisi degli interventi risolutivi da Lisbona in poi, occorre dare brevemente conto della normativa che integrava la direttiva colmando le lacune *ratione materiae*. Va detto, nondimeno, che la Direttiva ha comunque assunto un rilievo "centrale", non solo nell'ordinamento comunitario, ma anche (già allora) – come ricorda Della Morte – in termini di influenza delle legislazioni di Stati terzi[134], vocazione che sarà ancora più spiccata nel GDPR.

Altri atti di diritto derivato

Tra gli altri atti di diritto derivato che già facevano da cornice alla Direttiva del 1995, più o meno direttamente correlati alla protezione dei dati personali, vanno annoverati gli interventi che incidono sul diritto d'autore e sui diritti connessi (rispetto ai quali si è passati dal riferimento alla "società dell'informazione" al riferimento al "mercato unico digitale"). Si tratta della Direttiva 96/9/CE[135] del marzo 1996 sulla tutela giuridica delle banche dati e della Direttiva 2001/29/CE che riguarda l'armonizzazione di alcuni aspetti relativi alla "tutela giuridica del diritto d'autore e dei diritti connessi nell'ambito del mercato interno, con particolare riferimento alla società

[132] P. PASSAGLIA, Il sistema delle fonti normative in materia di tutela dei dati personali, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I Dati personali nel diritto europeo*, Giappichelli, 2019, pp. 92-93.
[133] *Ibidem*, pp. 93-94.
[134] Così, G. DELLA MORTE, richiama il Rapporto concernente i lavori condotti dalla Commissione di diritto internazionale nel corso del 2006, individuando tutti i Paesi che sono stati direttamente influenzati dalla Direttiva; *op. cit.*, p. 104.
[135] Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati – GU L 77 del 27.3.1996, pagg. 20–28.

dell'informazione"[136]. Importanti interventi di riforma, rispetto a tali atti, sono ravvisabili in due recenti direttive: la Direttiva (UE) 2017/1564, del settembre 2017, che invero interviene solo sulla Direttiva del 2001, e, più di recente, nell'aprile 2019, la Direttiva (UE) 2019/790[137], che modifica entrambi gli atti precedenti (e che è stata poco dopo rettificata)[138], avendo appunto riguardo alle esigenze del mercato unico digitale.

In particolare, la direttiva e-privacy

Il secondo "blocco" di interventi rilevanti riguarda gli atti dedicati al settore delle comunicazioni elettroniche. Il riferimento è alla c.d. Direttiva *ePrivacy* del 2002 (che interveniva, in verità, a sostituire la Direttiva 97/66/CE sulle telecomunicazioni; cfr. considerando 4), che, come si legge dal suo Articolo 1, "armonizza le disposizioni degli Stati membri necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità", aggiungendo al paragrafo 2 che a tali fini "le disposizioni della presente direttiva *precisano e integrano la direttiva 95/46/CE*. Esse prevedono inoltre la tutela dei legittimi interessi degli abbonati che sono persone giuridiche"[139]. La direttiva, tutt'ora in vigore, è stata modificata nel 2006 (Direttiva 2006/24/CE)[140] e poi nel 2009 (Direttiva 2009/136/CE)[141] con ulteriori interventi nel 2013 e poi nel 2017[142]. È ben noto, peraltro, che in questo settore è

[136] Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione - GU n. L 167 del 22/06/2001 pag. 0010-0019. Si ricorda, comunque, che è ancora in vigore la Direttiva direttamente riferita ai diritti di proprietà intellettuale: DIRETTIVA 2004/48/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 29 aprile 2004 sul rispetto dei diritti di proprietà intellettuale – GU L 157 del 30.4.2004, pagg. 45–86.

[137] Direttiva (UE) 2017/1564 del Parlamento europeo e del Consiglio, del 13 settembre 2017, relativa a taluni utilizzi consentiti di determinate opere e di altro materiale protetto da diritto d'autore e da diritti connessi a beneficio delle persone non vedenti, con disabilità visive o con altre difficoltà nella lettura di testi a stampa, e che modifica la direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione – GU L 242 del 20.9.2017, pagg. 6–13.

[138] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32019L0790R(02) .

[139] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), Articolo 1.

[140] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE – GU L 105 del 13.4.2006, pagg. 54–63, non più in vigore.

[141] Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori (Testo rilevante ai fini del SEE), GU L 337 del 18.12.2009, pagg. 11–36.

[142] Si veda https://eur-lex.europa.eu/legal-content/IT/TXT/?qid=1602237351736&uri=CELEX:02002L0058-20091219 nonché, per l'ultima rettifica del 2017: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32009L0136R(03)

intervenuta una proposta della Commissione nel 2017 per modificare la Direttiva 2002/58/CE promuovendo il c.d. Regolamento *ePrivacy*[143], ancora tanto atteso, per regolare e rimodulare alcuni aspetti relativi alla tutela nelle comunicazioni elettroniche, settore che sarà oggetto di particolare analisi poiché quello rispetto al quale si è sviluppata la casistica che coinvolge i sistemi di sicurezza nazionale (cfr. *infra*, Parte IV).

Vale la pena, in particolare, ricordare che la suddetta Direttiva 2006/24/CE: c.d. *Data retention Directive*, assume rilevanza perché, non più in vigore, è stata interamente annullata dalla Corte di giustizia nel famoso caso *Digital Rights Ireland*, riscontrando un eccesso dei "limiti imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta" [144]. Su questo aspetto, proprio di recente la Corte è intervenuta di nuovo, ribadendo che «la proporzionalità resta, dunque, la chiave per affrontare l'emergenza, in ogni campo, secondo lo Stato di diritto»[145]. Il riferimento è alle attese pronunce del 6 ottobre 2020 sul caso *La Quadrature du Net e a*. (cause riunite C-511/18, C-512/18, C-520/18) e sul caso *Privacy International* (C-623/17)[146], in cui la Corte è tornata proprio sulla normativa succitata (sia Direttiva 2002/58 che 2009/36), che avremo modo di commentare.

Interventi nell'ambito della cooperazione giudiziaria e di polizia in materia penale

Ancora, di particolare rilievo, gli interventi normativi volti a sopperire la lacuna *ratione materiae* della Direttiva 95/46/CE, che espressamente non copriva i settori riconducibili all'allora secondo (PESC) e terzo (GAI) pilastro. Il riferimento è quindi, chiaramente, alla Decisione Quadro 2008/977/GAI, relativa alla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale[147]. Come si può notare, la Decisione arrivò parecchi anni

[143] Commissione europea, COM(2017) 10 final, 2017/0003 (COD), Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni
elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), disponibile qui: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017PC0010&from=MT .

[144] Cause riunite C-293/12 e 594/12, *Digital Rights Ireland Ltd*, sentenza 8 aprile2014, p. 69, ma si veda anche p. 38.
Su questo aspetto e sugli sviluppi successivi, si veda ex multis: A. VEDASCHI-G. MARINO NOBERASCO, From DRD to PNR: Looking for a New Balance Between Privacy and Security, in D. D. COLE, F. FABBRINI AND S. SCHULHOFER (Eds), *Surveillance, Privacy and Transatlantic Relations*, Oxford: Hart Publishing, 2017, pp. 67–88.
88. Hart Studies in Security and Justice. Bloomsbury Collections

[145] Così ha commentato il Garante italiano rispetto alla pronuncia della Corte di giustizia del 6 ottobre 2020, cfr. *Data retention: Garante privacy su sentenza Corte di giustizia Unione europea*, 6 ottobre 2020, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9464165 .

[146] Cause riunite C-511/18, C-512/18, C-520/18, *La Quadrature du Net e a*., 6 ottobre 2020;
Causa C-623/17, *Privacy International*, 6 ottobre 2020.

[147] Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, GU L 350 del 30.12.2008, pagg. 60–71.

dopo la direttiva-madre (più di dieci), comportando inevitabilmente una tutela dei dati molto più blanda in quel settore, che divenne ancora più minacciata a seguito degli eventi dell'11 settembre 2001, quando diversi Stati inevitabilmente introdussero «sulla spinta di una politica tuta incentrata sull'esigenza securitaria, delle legislazioni particolarmente invasive della privacy»[148]. La Decisione Quadro del 2008 veniva dunque a sanare il "disordine normativo" rispetto alle materie rientranti nel terzo pilastro, pur palesando a sua volta perplessità che la recente riforma del c.d. *Pacchetto protezione dati* ha cercato di sistemare. Infatti, la Decisione dal 2018 non è più in vigore, abrogata dalla Direttiva del 2016/680 dell'aprile 2016, sulla protezione dei dati personali trattati dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali[149], di cui si dirà.

Trattamenti di dati effettuati da istituzioni, organi e organismi dell'Unione

Va infine segnalata la normativa relativa alla tutela dei dati personali trattati dalle istituzioni e agli organismi dell'Unione europea: il primo atto di riferimento è il Regolamento (CE) 45/2001[150], cui si riferisce espressamente anche la *Spiegazione relativa all'articolo 8* della Carta dei diritti fondamentali, ora non più in vigore perché abrogato e sostituito a partire dal dicembre 2018 dal Regolamento (UE) 2018/1725[151].

Una regolamentazione, dunque, frastagliata e dissonante, ma che cercava di colmare lacune e coprire quanti più ambiti fossero coinvolti nella necessità di tutelare i dati personali. L'esigenza di un intervento di diritto primario si faceva sempre più impellente.

L'avvento del Trattato di Lisbona e l'articolo 16 TFUE

Il Trattato di Lisbona ha rappresentato una rivoluzione anche con riguardo alla protezione dei dati personali. Anzitutto, com'è noto, riconoscendo valore vincolante alla Carta dei diritti fondamentali,

[148] Così ricorda G. DELLA MORTE, *op. cit.*, p. 105 nonché l'ampia dottrina a ciò dedicata, indicata alla nota 300, tra cui si richiama in particolare M. NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, Napoli, 2012.
[149] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio – GU L 119 del 4.5.2016, pagg. 89–131.
[150] Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati – GU L 8 del 12.1.2001, pagg. 1–22.
[151] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (Testo rilevante ai fini del SEE.) PE/31/2018/REV/1 – GU L 295 del 21.11.2018, pagg. 39–98.

ha consentito di ammetterla come parte del diritto primario dell'Unione, al pari dei Trattati (articolo 6 TUE)[152]. Dunque, le norme ivi inserite dalla prima previsione a Nizza nel 2000 e poi riadattate a Strasburgo nel 2007, possono considerarsi dopo Lisbona aventi tale rango. Ai nostri fini, la Carta è stata considerata «il punto di svolta dell'andamento evolutivo del sistema multilivello di protezione dei dati»[153]: essa, infatti, contiene l'articolo 8, espressamente dedicato alla protezione dei dati personali, cosa che da subito rappresentò un elemento "di anomalia, o quantomeno di differenziazione"[154] specie rispetto ai cataloghi di diritti fondamentali nel contesto europeo (come si è detto, tra tutti, la CEDU, non prevedeva alcun riferimento esplicito a tale diritto, che venne dalla giurisprudenza di Strasburgo inglobato nell'articolo 8 dedicato alla tutela della vita privata e familiare).

Delle implicazioni di tale previsione sotto alcuni dei molteplici e variegati profili che essa presenta, nonché del ruolo della Corte di giustizia nel plasmarne la sua configurazione, si avrà modo di parlare. Qui basti fare riferimento alla individuazione della genesi della norma. Considerato, cioè, lo "sdoppiamento" avvenuto attraverso la Carta dei diritti UE, specie rispetto alla CEDU, nella previsione di un articolo specificamente dedicato alla vita privata (articolo 7, comparabile all'articolo 8 CEDU) e un altro specificamente riferito alla tutela dei dati personali (articolo 8), sicuramente non si esclude l'influenza data dall'evoluzione non indifferente del concetto di *privacy* durante l'arco di tempo che separa i due cataloghi di diritti. Ma in realtà, più incisivamente, deve riconoscersi che «l'art. 8 CDFUE rappresenta il culmine del percorso di emersione e di costituzionalizzazione del diritto europeo alla protezione dei dati personali. (…) apparentemente realizza la codificazione di un diritto fondamentale già parte dell'*acquis* comunitario e sotteso a una molteplicità di documenti legislativi»[155]. Ciò, invero, si evincerebbe proprio della Spiegazione della Carta ad esso dedicata, che pure richiama un'altra norma di diritto primario, fondamentale ai nostri fini.

Il riferimento è all'articolo 16 TFUE[156], intervenuto (insieme con l'articolo 39 TUE) a sostituire l'articolo 286 TCE[157], che costituisce attualmente base giuridica, tra gli altri, degli atti normativi

[152] Si veda, *ex multis*, L.S. ROSSI, Rango, primato ed effetti diretti della Carta dei diritti fondamentali dell'Unione europea, in *Il Diritto dell'Unione europea*, n. 2/2019, pp. 329-356; N. LAZZERINI, La Carta dei diritti fondamentali dell'Unione europea – I limiti di applicazione, Franco Angeli, 2018, pp. 1-314. Sui recenti sviluppi delle implicazioni della Carta rispetto agli ordinamenti interni, con particolare riguardo a quello italiano, R. MASTROIANNI, Sui rapporti tra Carte e Corti: nuovi sviluppi nella ricerca di un sistema rapido ed efficace di tutela dei diritti fondamentali, in *European Papers*, Vol. 5, 2020, No. 1, pp. 493-522.
[153] R. D'ORAZIO, *op. cit.*, p. 75.
[154] O. POLLICINO-M. BASSINI, *Articolo 8*, in R. MASTROIANNI, O. POLLICINO, ALLEGREZZA, F. PAPPALARDO, RAZZOLINI (a cura di), *La Carta dei diritti fondamentali dell'Unione europea*, Giuffré editore, 2016, p. 134.
[155] O. POLLICINO-M. BASSINI, *op. cit.*, pp. 135-136.
[156] *Articolo 16 TFUE*:
1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

previsti dal c.d. pacchetto di protezione dati (GDPR e due direttive). Anche su questa norma torneremo[158]; quii diciamo, a titolo introduttivo, che essa «costituisce al tempo stesso l'enunciazione di un diritto dell'individuo *erga omnes*, e la previsione di una base giuridica generale, espressione di una competenza dell'Unione a legiferare circa la tutela delle persone in materia di trattamento dei dati personali»[159].

Nel commentare l'articolo, infatti, Cortese ci ricorda su quest'ultimo aspetto che prima di Lisbona un intervento normativo comunitario in materia di dati personali poteva aversi solo (come si è detto) in quanto legato al perseguimento degli obiettivi del mercato interno; la previsione dell'articolo 16 TFUE, attribuendo una specifica competenza all'Unione in materia, non solo consentirebbe di slegare la competenza da quegli obiettivi ma addirittura si spingerebbe anche oltre la previsione dell'articolo 8 della Carta (che resta, pur sempre, limitata all'ambito di applicazione previsto dall'articolo 51 CDFUE): «Di conseguenza, l'intervento dell'Unione può estendersi fino al punto di privare gli Stati membri di qualsiasi margine di manovra in tale ambito, potendo al limite stabilire un livello inderogabile di tutela, tanto *in melius* quanto *in peius*, e ciò a prescindere da considerazioni legate alla necessità di assicurare la circolazione dei dati personali»[160]. E dunque, rispetto a ciò, non si esclude lo scopo già perseguito in precedenza di circolazione dei dati (previsto, infatti, al paragrafo 2), ma si aggiunge (e si privilegia, proprio in quanto previsto al paragrafo 1) l'affermazione del diritto fondamentale garantito anche dall'articolo 8 della Carta[161]. Le Dichiarazioni allegate ai Trattati specificano, poi alcuni aspetti relativi alle implicazioni rispetto a questioni di sicurezza nazionale nonché rispetto ai settori della cooperazione giudiziaria penale e di

---

2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le *norme relative alla libera circolazione di tali dati*. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.
Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea.

[157] *Articolo 286 TCE*:
1. A decorrere dal 1o gennaio 1999 gli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati si applicano alle istituzioni e agli organismi istituiti dal presente trattato o sulla base del medesimo.
2. Anteriormente alla data di cui al paragrafo 1 il Consiglio, deliberando secondo la procedura di cui all'articolo 251, istituisce un organo di controllo indipendente incaricato di sorvegliare l'applicazione di detti atti alle istituzioni e agli organismi comunitari e adotta, se del caso, tutte le altre pertinenti disposizioni.

[158] Peraltro, la dottrina al riguardo è sconfinata. Per il momento, si consideri, *ex multis*: H. HIJMANS, *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU*, (PhD Thesis), 2016.

[159] B. CORTESE, Articolo 16 TFUE, in A. TIZZANO (a cura di), *I Trattati dell'Unione europea*, Giuffré, 2014, p.445.

[160] *Ibidem*, p. 446.

[161] Cfr. F. BALDUCCI ROMANO, La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo, in *Rivista Italiana di Diritto Pubblico Comunitario*, Fasc. 6-2015, che peraltro nota: «La portata innovativa della riforma, al contrario, appare evidente sin dalla scelta sistematica, dato che la collocazione della norma tende ad attribuire fondamentale rilievo al diritto in parola», p. 1627.

polizia[162]. In questo senso, devono considerarsi integrative le norme contenuti negli articoli 87 e 88 del TFUE. Dunque, quanto detto può ritenersi sufficiente per comprendere la discrasia tra tali previsioni di diritto primario e il mantenimento in vigore della Direttiva 95/46 e della logica ad essa sottesa. L'esigenza di una riforma si faceva impellente.

La riforma del sistema di protezione dei dati personali

Una volta predisposta una nuova base giuridica, la possibilità di procedere ad una riforma del sistema di protezione dei dati venne da sé. Se già, infatti, era già possibile ravvisare alcuni segnali in tal senso della Commissione in comunicazioni relative al programma di Stoccolma del 2009 e 2010[163], la proposta di riforma arrivò nel gennaio 2012 e si sostanziò in un duplice intervento: uno finalizzato al regolamento per la tutela nel trattamento dei dati, l'altro sulla direttiva relativa alla tutela nel trattamento dei dati i fini penali. Quanto a questa differenziazione, che giustificava la scelta di un regolamento per un settore già armonizzato in precedenza, mentre la direttiva per coprire le distanze tra Stati ancora esistenti in quello che era il terzo pilastro, si è notato: «La scelta di questo doppio canale ha rappresentato un bilanciamento tra l'obiettivo più volte enunciato di dare un quadro unitario al sistema di protezione dei dati e l'esigenza di tener conto della situazione concreta in cui la nuova legislazione euro-unitaria si sarebbe calata»[164].

A seguito di tali proposte, l'*iter* fu abbastanza travagliato[165] e condusse al c.d. *pacchetto protezione dati*, che, volto a "dare un assetto compiuto ed organico alla materia"[166], era composto da: il Regolamento Generale sulla Protezione dei Dati, Regolamento (UE) n. 679/2016[167]; la Direttiva (UE) n. 2016/680, sulla protezione dei dati personali trattati dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali,

[162] 20. *Dichiarazione relativa all'articolo 16 del trattato sul funzionamento dell'Unione europea*
La conferenza dichiara che, ogniqualvolta le norme in materia di protezione dei dati personali da adottare in base all'articolo 16 possano avere implicazioni dirette per la sicurezza nazionale, si dovrà tenere debito conto delle caratteristiche specifiche della questione. Rammenta che la legislazione attualmente applicabile (vedasi in particolare la direttiva 95/46/CE) prevede deroghe specifiche al riguardo.
21. *Dichiarazione relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia*
La conferenza riconosce che potrebbero rivelarsi necessarie, in considerazione della specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, in base all'articolo 16 del trattato sul funzionamento dell'Unione europea.
[163] Così rileva P. PASSAGLIA, *op. cit*., p. 95-96 ss.
[164] *Ibidem*, p. 97.
[165] Per cui si rinvia a P. PASSAGLIA, *op. cit*., pp 97-101.
[166] *Ibidem*, p. 101.
[167] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

nonché alla libera circolazione di tali dati[168]; la Direttiva (UE) n. 681/2016, sull'uso del codice PNR per la prevenzione, accertamento, indagine e azione penale per reati di terrorismo reati gravi[169]. A tale ultimo proposito, basti per ora solo richiamare, che l'Unione ha già concluso accordi con Paesi terzi sul trasferimento dei dati PNR, in particolare con gli USA e l'Australia, mentre si sta finalizzando la revisione di quello con il Canada (a seguito del famoso parere della Corte di giustizia al riguardo) ed è stato di recente autorizzato l'avvio dei negoziati con il Giappone[170].

Le normative brevemente esposte, e il loro impatto, verranno adeguatamente commentate via via che esporremo la concreta interazione tra le questioni legate ai dati personali e il sistema valoriale dell'Unione. Qui di seguito, dunque, ci si limiterà ad una presentazione introduttiva di aspetti rilevanti che è bene tener subito presente.

Il GDPR

Quanto al GDPR[171], anzitutto le disposizioni generali (Capo I, articoli 1-4) assumono un rilievo preponderante nel definire oggetto e finalità, ambito di applicazione materiale e territoriale, nonché le definizioni dei termini utilizzati, specifici del settore. Di particolare rilievo, specie rispetto alle previsioni della direttiva madre, l'articolo 3 dedicato all'*ambito di applicazione territoriale*, la cui previsione dovrebbe considerarsi innovativa in vista dell'ampliamento di tale ambito a operazioni di trattamento dei dati che si svolgono in Paesi terzi. Invero, si è detto che l'articolo «riveste particolare importanza, da un lato, perché costituisce il frutto di un dialogo tra legislatore, giudice ed autorità preposte alla vigilanza sul trattamento dei dati personali; dall'altro lato, la norma esprime il preciso indirizzo politico che caratterizza l'approccio seguito, in questa materia,

[168] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, cit. Per un commento si veda, *ex multis*, G. RUGANI, La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della Direttiva (UE) 2016/680: frammentazione ed incertezza applicative, in *Freedom, Security & Justice: European Legal Studies*, 2019, n. 1, pp. 75-92.

[169] Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

[170]Si vedano: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en ; https://www.consilium.europa.eu/it/policies/fight-against-terrorism/passenger-name-record/
Cfr. in particolare Capitolo III, paragrafo 5.2.

[171] A commento del quale è già vastissima la dottrina appositamente dedicata. Ricordiamo, per ora, solo il recente commentario: C. KUNER, L.A. BYGRAVE, C. DOCKSEY , *General Data Protection Regulation (GDPR) -A Commentary*, Oxford, 2020.

dall'Unione europea nelle sue varie articolazioni»[172]. Si comprende subito, dunque, la portata della norma e le inevitabili questioni che essa ha (ri)proposto[173].

Rinviando al prosieguo per i riferimenti all'assetto istituzionale previsti dal Regolamento, l'altro aspetto di fondamentale rilievo ai nostri fini riguarda l'attuale Capo V, rubricato "*Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*". In particolare, anzitutto l'articolo 44 contiene il principio generale per cui ogni trasferimento di dati, legato al trattamento degli stessi, verso un Paese terzo o un'organizzazione internazionale «ha luogo *soltanto se* il titolare del trattamento e il responsabile del trattamento *rispettano le condizioni* di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che *il livello di protezione* delle persone fisiche garantito dal presente base di una decisione di adeguatezza da parte della Commissione, che sarà oggetto approfondito della nostra analisi, specie nella parte in cui, al paragrafo 2, stabilisce: «nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione in particolare i seguenti elementi: a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (…)»[174]. L'articolo 46 prevede, invece, le ipotesi di trasferimento quando manchi una decisione di adeguatezza della Commissione *ex* art. 45, par.3 (ossia quando valuti l'adeguatezza del Paese terzo medianti atti di esecuzione), richiedendo che il titolare o responsabile del trattamento forniscano "garanzie adeguate" e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi". Tra le varie garanzie adeguate, la norma annovera: le norme vincolanti d'impresa in conformità dell'articolo 47; le *clausole tipo di protezione dei dati* adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione[175]. Proprio su questi aspetti si è pronunciata di recente la Corte di giustizia, annullando la decisione della Commissione sul c.d. *Privacy Shield* ma ritenendo adeguate, ai fini del trasferimento, le clausole contrattuali tipo (cfr. *Schrems II*), su cui si avrà modo di commentare lungamente.

[172] A. NERVI, Il perimetro del Regolamento europeo: portata applicativa e definizioni, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 169.
[173] Su cui qui si consideri, *ex multis*: P. DE HERT, M. CZERNIAWSKI, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, in *International Data Privacy Law*, Vol. 6(3), 2016, pp. 230-243; D. J. SVANTESSON, *Article 3 – Territorial scope*, in 2018 Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019), Oxford, 2018, pp.1-18; M. GOMANN, The new territorial scope of EU Data protection law: deconstructing a revolutionary achievement, in *Common Market Law Review*, 54: 567–590, 2017.
[174] GDPR, *cit.*, Articolo 45, paragrafo 2.
[175] GDPR, *cit.*, Articolo 46 (in part. par. 2).

Altri atti normativi sulla protezione dei dati

Oltre al suddetto "pacchetto di protezione dati", pur esulando dall'oggetto di questa trattazione, è bene dare conto del Regolamento (UE) 2018/1807, entrato in vigore nel maggio 2019, concernente la libera circolazione dei dati non personali nell'Unione europea[176], nonché la c.d. *Direttiva NIS*, Direttiva (UE) 2016/1148, relativa a misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione[177].

Il resto della normativa rilevante è stato, in qualche modo, anticipato: ci si riferisce al Regolamento (UE) 2018/1725, sulla tutela dei dati trattati da istituzioni e organismi dell'Unione; alla Direttiva (UE) 2019/790, sul diritto d'autore e diritti connessi nel mercato unico digitale.

Si resta ancora in attesa, invece, del prospettato Regolamento *ePrivacy* sulla tutela nelle comunicazioni elettroniche (settore, nel quale, si è detto, è intervenuta proprio di recente la Corte di giustizia, cfr. sentenze 6 ottobre 2020), che, come si è detto, dovrebbe sostituire la Direttiva 2002/58/CE e la cui proposta è arrivata dalla Commissione nel 2017, iscrivendosi a pieno nella prospettiva di costruzione di regole uniformi di tutela per chi si muove nel mercato unico digitale[178].

Inoltre, nell'ambito della Strategia per il Mercato Unico Digitale, accennata, nell'aprile 2018 la Commissione ha avanzato la proposta di un "Pacchetto sulle prove elettroniche", composto dal c.d. Regolamento *eEvidence* e dalla Direttiva sulla *nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali*[179]. In particolare, il Regolamento su *gli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* sarebbe volto ad agevolare l'assistenza giudiziaria e la cooperazione tra autorità di Stati membri e i prestatori di servizi con sede in Paesi terzi[180].

Fa parte della stessa Strategia anche l'adozione, nel 2019, della c.d. *Direttiva Open Data*, n. 2019/1024, sull'apertura dei dati e il riutilizzo nel settore pubblico, che è intervenuta a modificare

[176]REGOLAMENTO (UE) 2018/1807 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.
[177] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione – GU L 194 del 19.7.2016, pagg. 1–30.
[178] Commissione, COM(2017) 10 final, Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), 10.1.2017.
[179] Commissione, Proposta di DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali, COM/2018/226 final - 2018/0107 (COD): https://eur-lex.europa.eu/legal-content/it/TXT/?uri=COM:2018:226:FIN
[180] Commissione, Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, COM/2018/225 final - 2018/0108 (COD), disponibile qui: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018PC0225 .Su questa si veda O. POLLICINO, M. BASSINI, La proposta di Regolamento e-Evidence: osservazioni a caldo e possibili sviluppi, in *MediaLaws*, 26 ottobre 2018.

quella adottata nel 2003 (e già editata nel 2013) per adattare la normativa ai cambiamenti tecnologici intercorsi[181]. Prendendo atto di queste misure assunte nell'ambito della Strategia DMS, va comunque tenuto in debito conto quanto da qualcuno osservato di recente: «l'ordinamento UE, appare, con riguardo al completamento del mercato unico digitale, ancora in mezzo al guado: se da un lato, infatti, molte sono le misure già adottate sia per quanto concerne la tutela della concorrenza, sia sotto il profilo delle libertà economiche fondamentali, sia, ancora, per quanto concerne i profili internazionalprivatistici, dall'altro è evidente come l'impianto normativo così predisposto rimanga comunque ancora incompleto»[182].

Infine, nell'ambito della nuova anticipata Strategia *Plasmare il Futuro Digitale dell'Europa*, la Commissione ha anzitutto avanzato l'importante proposta di *Data Governance Act* nel novembre 2020 per la condivisione di dati nell'Unione, e che modifica in parte la Direttiva Open Data. Si tratta della prima proposta di Regolamento che chiaramente espone la scelta di orientare l'Unione verso una propria governance di dati che risponde ai connotati tipici delle tradizioni giuridiche europee, palesando di voler adottare un approccio antropocentrico[183].

Nell'ambito delle priorità 2019-2024 di detta Strategia, quella dedicata a "un'Europa pronta per il Digitale" ha visto già avanzare due nuove proposte lo scorso dicembre 2020: *Data Services Act* e *Digital Markets Act* (ovvero, "Regolamento sui servizi digitali" e "Regolamento sui mercati digitali") essenzialmente per regolamentare le piattaforme digitali e tutelare i consumatori[184].

Infine, anche se fuoriesce dal nostro oggetto di indagine, facciamo solo un cenno, per completezza, alla recente proposta di regolamento per regole armonizzate sull'Intelligenza Artificiale[185].

Così esposto il quadro normativo nei suoi aspetti fondamentali, che si approfondiranno laddove la trattazione lo richiederà, si rinvia alle Parte IV per illustrare i rilevanti accordi internazionali conclusi dall'Unione che coinvolgono trattamenti dei dati personali

Adesso illustreremo, invece, il quadro istituzionale dedicato a tale settore.

---

[181] DIRETTIVA (UE) 2019/1024 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, PE/28/2019/REV/1.

[182] Così. G. M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Cacucci editore, 2021, p. 228.

[183] Commissione europea, Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo alla governance europea dei dati (*Atto sulla governance dei dati*), 25 novembre 2020, COM(2020) 767 final.

[184] Commissione europea, Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo a un mercato unico dei servizi digitali (*legge sui servizi digitali*) e che modifica la direttiva 2000/31/CE, 15 dicembre 2020, COM(2020) 825 final.
Commissione europea, Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo a mercati equi e contendibili nel settore digitale (*legge sui mercati digitali*), 15 dicembre 2020, COM(2020) 842 final.

[185] Commissione europea, Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE (*LEGGE SULL'INTELLIGENZA ARTIFICIALE*) E MODIFICA ALCUNI ATTI LEGISLATIVI DELL'UNIONE, 21 aprile 2021, COM(2021) 206 final.

3. Il quadro istituzionale dedicato alla protezione dei dati personali

È bene ricordare che per il buon funzionamento delle previsioni relative al diritto alla protezione dei dati personali è fondamentale il controllo indipendente realizzato sulla loro attuazione. A questo riguardo, infatti, lo stesso articolo 8 della Carta dei diritti prevede al paragrafo 3 che il rispetto delle regole previste nei paragrafi precedenti "*è soggetto al controllo di un'autorità indipendente*".

Analizziamo, dunque, in ordine cronologico, gli interventi previsti a tal fine.

Invero, il quadro normativo sin qui individuato, nelle sue evoluzioni, ha portato con sé anche mutamenti nel quadro istituzionale dedicato al settore. In particolare, il Capo IV della Direttiva 95/46/CE era rubricato "*Autorità di controllo e gruppo per la tutela delle persone con riguardo al trattamento dei dati personali*" e conteneva tre articoli: l'articolo 28, dedicato alle autorità di controllo; l'articolo 29, dedicato al *Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali*, da cui quello che sarà (sino al 2018) il famoso "Gruppo di Lavoro Articolo 29 (WP29)"; l'articolo 30, che specificava i compiti del Gruppo.

Quanto alle autorità di controllo *ex* articolo 28, si tratta di autorità amministrative indipendenti volte a sorvegliare l'applicazione della direttiva nel territorio di ciascuno Stato membro, da consultare nell'elaborazione di misure correlate al trattamento dei dati personali, dotate di specifici poteri[186] e alle quali i singoli possono rivolgere domande per la tutela dei propri diritti con riguardo al trattamento dei dati personali. Veniva prevista altresì una collaborazione tra le autorità dei vari Stati membri, specie attraverso scambio di informazioni. In Italia, in particolare, il c.d. Garante per la protezione dei dati personali (comunemente denominato Garante privacy) è stato istituito con la legge 31 dicembre 1996, n. 675[187].

[186] In particolare, Articolo 28, par. 3: Ogni autorità di controllo dispone in particolare:
- di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;
- di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 20, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali;
- del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette violazioni le autorità giudiziarie.
È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio.

[187] Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali

Quanto, poi, al Gruppo di Lavoro "Articolo 29", si trattava di un gruppo europeo di lavoro istituito dalla suddetta norma, con carattere consultivo e indipendente, composto dai rappresentanti delle autorità degli Stati membri, dal rappresentante dell'autorità comunitaria e da un rappresentante della Commissione. Tra i compiti assegnati dall'articolo 30, di rilievo quello di intervenire per contribuire all'applicazione omogenea delle norme nazionali di attuazione, formulare pareri, consigliare la Commissione su opportunità di modifica o integrazione della normativa dedicata, nonché formulare raccomandazioni. Inoltre, particolarmente rilevante ai nostri fini, la previsione già allora contenuta al paragrafo 2, sulla necessità di constatare "divergenze che possano pregiudicare *l'equivalenza della tutela delle persone* in materia di trattamento dei dati personali *nella Comunità*", nonché quella al paragrafo 6: "Il gruppo redige una relazione annuale sullo stato della tutela delle persone fisiche con riguardo al *trattamento dei dati personali nella Comunità e nei paesi terzi* e la trasmette alla Commissione, al Parlamento europeo e al Consiglio. La relazione è oggetto di pubblicazione". L'articolo 31 prevedeva, inoltre, un Comitato per assistere la Commissione nell'adozione di misure di esecuzione. Il gruppo di lavoro articolo 29 ha funzionato sino al 25 maggio 2018, data di entrata in vigore del GDPR che, come si dirà a breve, ha invece istituito un Comitato europeo per la protezione dei dati.

Ancora, l'articolo 286 TCE, al paragrafo 2, prevedeva l'istituzione a livello sovranazionale di un organo di controllo indipendente per sorvegliare sull'applicazione degli atti comunitari sulla protezione dei dati nelle istituzioni e negli organismi comunitari. Ebbene, il suddetto Regolamento n. 45/2001, sulla tutela dei dati da parte di istituzioni e organismi comunitari, istituiva a tal fine un'autorità indipendente: il Garante europeo per la protezione dei dati personali (GEPD, per il cui statuto si veda Decisione n- 1247/2002/CE), con funzioni consultive, di controllo e di cooperazione, nonché la possibilità di adire la Corte di giustizia o di intervenire in cause pendenti dinanzi ad essa e il potere di accedere a tutti i dati e le informazioni necessari per le indagini (così, articolo 47 del Regolamento). Pur senza considerare le successive modifiche di cui si dirà, nel senso del rafforzamento del ruolo di questa figura, già il Regolamento istitutivo lo delineava nel senso che « *son action participe au maintien d'un exercice régulier du pouvoir des institutions et des organes de l'Union dans le domaine qui les concerne* »[188].

Questo quadro ha subito un mutamento con l'entrata in vigore del GDPR.

(testo consolidato con il d.lg. 28 dicembre 2001, n. 467) - Legge abrogata ai sensi dell'articolo 183, comma 1, lettera a), del Codice in materia di protezione dei dati personali.
Di seguito la pagina dedicata: https://www.garanteprivacy.it/home/autorita .

[188] Così N. ROJAS-HUTINEL, *La séparation du pouvoir dans l'Union européenne*, mare&martin, 2017, p. 354.

Infatti, molteplici sono le disposizioni consacrate al quadro istituzionale dedicato alla protezione dei dati, che risulta così ridefinito: il Capo VI è interamente dedicato alle "*Autorità di controllo indipendenti*", mentre il Capo VII, rubricato "*Cooperazione e coerenza*" dedica la Sezione terza alla nuova figura del Comitato per la protezione dati (*European Data Protection Board*, EDPB). L'articolo 51 del GDPR, che apre il Capo VI, stabilisce infatti che ogni Stato membro dispone di tali autorità, incaricate di sorvegliare la corretta applicazione del Regolamento e agevolare la libera circolazione dei dati all'interno dell'Unione, a tali fine cooperando con le autorità degli altri Stati membri. Le norme a seguire ne dispongono la composizione e l'istituzione, mente la Sezione 2 (articoli 55-59) ne definisce competenze, compiti e poteri, che risultano ampliati e rafforzati, oltre che specificamente definiti.

L'articolo 68 prevede l'istituzione del Comitato europeo per la protezione dei dati (di seguito anche nella sigla inglese: EDPB), quale organismo dell'Unione dotato di personalità giuridica[189]. Composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal Garante europeo della protezione dei dati (o dai rispettivi rappresentanti, di seguito anche nella sigla inglese: EDPS), il Comitato coadiuva la coerente applicazione delle norme sulla protezione dei dati nell'UE, promuovendo a tal fine la cooperazione tra le autorità degli Stati membri[190].

Questa figura, peraltro, non esclude ma si aggiunge al Garante europeo di cui si è detto, che, una volta abrogato il Regolamento 45/2001, trova ora espresso riferimento, oltre che in alcune disposizioni del GDPR, nel Regolamento 2018/1725 relativo alla tutela dei dati trattati da istituzioni e organismi dell'Unione. in particolare, il Considerando 60 prevede: "*Il regolamento (UE) 2016/679 ha istituito il comitato europeo per la protezione dei dati quale organo indipendente dell'Unione dotato di personalità giuridica. Il comitato dovrebbe contribuire all'applicazione coerente del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680 in tutta l'Unione, fornendo anche consulenza alla Commissione. Nel contempo il Garante europeo della protezione dei dati dovrebbe continuare a esercitare le proprie funzioni di controllo e consulenza in relazione a tutte le istituzioni e tutti gli organi dell'Unione, di propria iniziativa o su richiesta. Per garantire la coerenza delle norme sulla protezione dei dati in tutta l'Unione, la Commissione, all'atto della*

[189] Regolamento Europeo per la Protezione dei Dati, Articolo 68, par. 1.

[190] Si veda il sito dedicato: https://edpb.europa.eu/about-edpb/about-edpb_it , che specifica: "Il comitato europeo per la protezione dei dati è composto da rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati (GEPD). Ne fanno altresì parte le autorità di controllo degli Stati EFTA/SEE per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati (GDPR), senza però che i loro rappresentanti godano del diritto di voto o di essere eletti presidente o vicepresidenti. Il comitato è istituito dal regolamento generale sulla protezione dei dati e ha sede a Bruxelles. La Commissione europea e, per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati, l'Autorità di vigilanza EFTA hanno titolo a partecipare alle attività e alle riunioni del comitato senza diritto di voto. Il comitato si avvale di un segretariato, fornito dal GEPD".

preparazione di proposte o raccomandazioni, dovrebbe sforzarsi di consultare il garante europeo della protezione dei dati"[191].

Va ricordato per completezza, inoltre, che (fuori dell'ordinamento dell'Unione) la Convenzione 108, come modernizzata (c.d. Convenzione 108+) a seguito del Protocollo di emendamento adottato dal Comitato dei Ministri nel maggio 2018, prevede a sua volta, come detto, un espresso riferimento alle autorità di controllo (Capitolo IV, articolo 15) e alla loro cooperazione (Capitolo V, articoli 16-21), nonché l'istituzione di un Comitato convenzionale (Capitolo VI, articoli 22-23)[192].

Fondamentale, inoltre, come vedremo (*infra*, Parti III e IV), soprattutto per quanto interessa ai fini di questa indagine circa il flusso di dati verso Paesi terzi, il ruolo della Commissione. Oltre che, come si è detto, nella collaborazione con le autorità nazionali ed europea di controllo, così come con il Comitato europeo, la Commissione assume un ruolo centrale non solo quanto alla *valutazione di adeguatezza* circa il livello di protezione garantito dal Paese terzo o dall'organizzazione destinatari del trasferimento di dati dall'Unione ai fini delle relative decisioni (articolo 45 GDPR), ma spesso anche rispetto alle altre garanzie adeguate (articolo 46 GDPR).

Infine, il GDPR espressamente richiama anche il ruolo della Corte di giustizia. Infatti, come si evince dal Considerando 143, "Qualsiasi persona fisica o giuridica ha diritto di proporre un ricorso per l'annullamento delle decisioni del comitato dinanzi alla Corte di giustizia, alle condizioni previste all'articolo 263 TFUE. In quanto destinatari di tali decisioni, le autorità di controllo interessate che intendono impugnarle, devono proporre ricorso entro due mesi dalla loro notifica, conformemente all'articolo 263 TFUE", che si aggiunge, ovviamente, al riferimento alla possibilità di adire la Corte con rinvio pregiudiziale.

Così succintamente esposta la composizione del quadro istituzionale di riferimento, e avendo fornito le premesse essenziali per una generale comprensione della materia, possiamo procedere adesso ad esporre l'evoluzione giurisprudenziale del diritto alla protezione dei dati personali, per come ha trovato sviluppo nel contesto regionale europeo.

[191] Regolamento (UE) 2018/1725, *cit.*, Considerando 60.
[192] Convention 108 +, *Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel*, https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726

CAPITOLO IV
TRA STRASBURGO E LUSSEMBURGO.
I *GRANDS ARRÊTS* EUROPEI
SULL'EVOLUZIONE DELLA PROTEZIONE DEI DATI PERSONALI

1. Alle origini delle tutele a livello sovranazionale: la contaminazione dei modelli interpretativi

Premessa

Ancora oggi, ogni dissertazione che voglia esporre, anche per grandi linee, l'evoluzione della dottrina dei diritti fondamentali nell'Unione europea non manca di esordire con un riferimento alla sentenza *Stauder*. Eppure, se è ben noto che con essa, pronunciata il 12 novembre 1969, venne fatto per la prima volta espresso riferimento a «*i diritti fondamentali della persona, che fanno parte dei principi generali del diritto comunitario, di cui la Corte garantisce l'osservanza*»[193], non è altrettanto diffuso riferire che essa riguardasse proprio questioni legate ai dati personali.

Si trattava, infatti, di un rinvio pregiudiziale tedesco che interrogava la Corte sulla compatibilità con in principi generali del diritto comunitario di una decisione della Commissione relativa alla fornitura di burro a prezzo ridotto nei confronti di beneficiari di forme di assistenza pubblica. Sulla base di quella decisione, delle direttive tedesche consentivano la distribuzione di tesserini con tagliandi, convalidabili solo se presentavano nome e indirizzo del beneficiario, nome che doveva risultare anche dal libretto da mostrare al dettagliante al fine di ottenere il burro a prezzo ridotto. Ebbene, il signor Stauder lamentava proprio l'obbligo di esibire il suo nome sul tagliando, ritenendolo illegittimo (specie alla luce dei diritti fondamentali riconosciuti dalla Costituzione tedesca); pertanto (oltre a proporre un ricorso costituzionale) citava la città di Ulm (per ottenere un provvedimento che abolisse provvisoriamente tale obbligo) dinanzi al giudice tedesco, il quale rinviava alla Corte di giustizia.

Nel presentare le sue osservazioni in sede pregiudiziale, la Commissione sosteneva tra le altre cose, «*Per quanto riguarda il diritto comunitario non scritto, (...) che, nei confronti del diritto costituzionale tedesco, la costituzionalità materiale dell'obbligo di rivelare la propria identità può essere messa in dubbio solo sotto il profilo del principio della proporzionalità tra mezzo e fine, che deriva dal principio dello Stato di diritto. La giurisprudenza della Corte di giustizia ha più volte*

[193] Caso 29/69, *Erich Stauder contro città di Ulm-Sozialamt*, 12 novembre 1969, p. 7.

applicato questo principio a proposito di taluni aspetti degli atti delle istituzioni comunitarie, senza tuttavia affermare ch'esso si applichi a tutte le attività della Comunità ed in particolare agli atti normativi del Consiglio e della Commissione»[194], introducendo così l'argomento per cui non vi fosse violazione nel caso specifico in considerazione dell'obiettivo della decisione. Quest'ultima, infatti, aveva un preciso obiettivo legato alle esigenze del mercato comune, in linea con la struttura e le finalità dell'embrionale integrazione europea, che la Corte precisava in quella sede: «*destinata a tutti gli Stati membri, autorizza questi ultimi, onde favorire lo smercio nel mercato comune delle eccedenze di burro, a porre a disposizione di determinate categorie di consumatori, assistiti dalla pubblica beneficienza, del burro a un prezzo inferiore al normale. Questa autorizzazione è accompagnata da determinate condizioni, intese a garantire fra l'altro che il prodotto immesso sul mercato non sarà sviato dalla sua destinazione*»[195].

Aldilà dell'esito della questione nel caso di specie (in cui la Corte prospettava un'interpretazione della decisione comunitaria che non consentiva di ritenere le misure nazionali ad essa contrarie), da questi tre passaggi della breve e risalente sentenza possono già evincersi i tratti essenziali dell'intero discorso sui dati personali nell'Unione europea, e persino di come esso si declina nell'attuale era digitale.

Non va sottovalutato, intanto, il riferimento della Commissione al principio di proporzionalità degli atti come parte dei principi dello Stato di diritto, non solo caratteristico dell'ordinamento tedesco ma applicato anche dalla Corte di giustizia e quindi già condiviso a livello sovranazionale, pur in maniera ancora timida e limitata (*senza tuttavia affermare ch'esso si applichi…agli atti normativi del Consiglio e della Commissione*), in considerazione dell'ancora contenuto livello di integrazione dell'allora Comunità economica europea.

Inoltre, emerge per la prima volta un riferimento alla necessità che gli Stati membri, nell'adottare le misure per attuare l'obiettivo dell'atto comunitario, scelgano quelle meno pregiudizievoli dei diritti della persona (tra i quali quindi rientrerebbe anche quello alla "riservatezza"), così venendo tali diritti riconosciuti espressamente come parte dei principi generali del diritto comunitario[196]. È stato notato al riguardo: «I diritti fondamentali assurgono, dunque, a parametro di legittimità dei comportamenti degli Stati membri in attuazione del diritto comunitario e in questo quadro prende forma il diritto alla protezione dei dati personali quando il loro utilizzo si riverbera e interferisce sulla vita privata dell'individuo. Nondimeno, la tutela dei dati personali appare, attraverso una possibile lettura di questa pronuncia, indissolubilmente connessa alle misure adottate per la

[194] *Ibidem*, p. II.3 (in fatto).
[195] *Ibidem*, p. 2 (in diritto).
[196] F. ROSSI DAL POZZO, La tutela dei dati personali nella giurisprudenza della Corte di giustizia, *Eurojus*, n.1/2019, p. 5.

realizzazione del mercato interno»[197]. E da qui si trae il terzo interessante aspetto caratteristico che, con i due precedenti, trova un seme in quella pronuncia che ancora oggi produce frutti.

Ci riferiamo al legame inestricabile tra dati e mercato (interno, ma non solo) che deriva dalla necessità della circolazione dei primi per l'effettivo funzionamento del secondo, ma che al contempo ha sollevato sempre maggiori istanze di tutela nella circolazione dei dati, tali da assurgere, nel tempo, a diritto fondamentale riconosciuto nell'ordinamento dell'Unione europea. Quest'ultimo aspetto, potenziato per un certo periodo (specie quello che ha accompagnato e seguito il Trattato di Lisbona) non ha però reciso il legame con le esigenze di mercato interno, che si palesano più chiaramente nelle urgenze dell'attuale era digitale.

Ecco, dunque, che questi aspetti, alternativamente posti in risalto nell'evoluzione della disciplina dei dati personali a livello sovranazionale, erano già *in nuce* identificabili in quella questione trattata dalla Corte di giustizia più di cinquant'anni fa, da allora da quest'ultima costantemente sviluppati e rafforzati. Pur proponendo nel prosieguo più approfondite analisi dei casi legati alle specifiche tematiche che tratteremo, pare opportuno qui di dare conto delle tappe fondamentali di tale evoluzione, anche alla luce degli interventi della Corte europea dei diritti umani su materie affini, proprio per consentire una migliore comprensione degli sviluppi (non solo giurisprudenziali, ma anche normativi e istituzionali) dell'attuale quadro sovranazionale di disciplina dei dati personali e quindi illustrare le pronunce che concorrono a formare l'*acquis* su cui si è costruito (il GDPR in particolare, ma più in generale) l'attuale impianto europeo di protezione dei dati.

Primo periodo

A partire da questo primordiale ed emblematico intervento, è comprensibile che negli anni immediatamente successivi la giurisprudenza sul tema non sia stata particolarmente copiosa (specie se la si confronta con l'attuale attivismo). Ciò sicuramente (ma non esclusivamente) perché mancavano appigli di diritto positivo a cui riferirsi. Tuttavia, e in virtù di tali considerazioni, proprio casi legati a questioni di riservatezza hanno concorso a consentire alla Corte di giustizia di sviluppare quella famosa casistica che porterà all'emersione (come si suole dire, "pretoria" e "nel silenzio dei Trattati") delle esigenze di tutela dei diritti a livello sovranazionale. Ci si riferisce al fatto che, com'è noto, per sviluppare la dottrina dei diritti fondamentali, quali riconosciuti nell'ordinamento comunitario, la Corte ha fatto riferimento alle tradizioni costituzionali degli Stati membri e anche alla Convenzione europea dei diritti umani che, come si è detto, risaliva al 1950.

[197] *Ibidem*, pp. 5-6.

Pertanto, nel caso *National Panasonic* del 1980 la Corte richiamava per la prima volta in una sua argomentazione la CEDU, in particolare l'articolo 8 dedicato alla tutela della vita privata.

Il caso riguardava la società suddetta, con sede in Regno Unito, che, avendo subito un accertamento da parte della Commissione, chiedeva l'annullamento della relativa decisione nonché la restituzione delle copie dei documenti e il divieto per la stessa di utilizzare le informazioni assunte in quell'occasione. La richiesta di annullamento si fondava su diversi motivi, tra i quali la "violazione dei diritti fondamentali", in particolare con riguardo all'articolo 8 CEDU, sostenendo che potesse ritenersi applicabile alle persone giuridiche. A ciò la Corte rispondeva: "in proposito è il caso di rilevare che l'art. 8 della convenzione europea, supposto che si applichi a persone giuridiche, pur enunciando il principio della non ingerenza delle autorità pubbliche nell'esercizio dei diritti indicati nel suo primo paragrafo, ammette, nel secondo paragrafo, che un'ingerenza del genere è possibile soltanto se «prevista dalla legge e se costituisce un provvedimento che, in una società democratica, è necessario alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine ed alla prevenzione delle infrazioni penali, alla protezione della salute o della morale, alla protezione dei diritti e delle libertà altrui»"[198].

Anzitutto, è bene sottolineare che sia in questo caso che nel precedente *Stauder* la Corte, nel riconoscere la rilevanza dei diritti che così timidamente iniziavano a farsi strada nell'ordinamento comunitario, ribadiva la necessità di prediligere le esigenze del mercato comune, precipuo obiettivo del Trattato. Così, nel caso *National Panasonic* la Corte rigettava il ricorso anche in considerazione della funzione dei poteri della Commissione, posti a presidio delle regole della concorrenza volte al funzionamento del mercato comune[199].

Questo aspetto, che abbiamo già accennato, merita di essere ribadito a più riprese: le origini della regolamentazione europea in materia di dati personali, ad uno con la particolare attenzione per la protezione di questi ultimi, sono profondamente radicate nell'esigenza di stabilire il mercato interno e garantirne il funzionamento. Ogni conseguenza, in termini di emersione di una peculiare tutela, al punto da assurgere a diritto fondamentale dell'ordinamento sovranazionale[200], ovvero in termini di esternalizzazione dei relativi standard[201], conserva il suo effettivo intento nelle esigenze di funzionamento del mercato interno. Si tratta di quello stesso intento che oggi, dopo un periodo di particolare insistenza sulla rilevanza della protezione dei dati come diritto fondamentale, comporta

[198] Causa 136/79, *National Panasonic c. Commissione*, sentenza del 26 giugno 1980, punto 19 (in diritto).
[199] Ibidem, punto 20.
[200] *Ex multis*, G. GONZÁLEZ FUSTER, *The emergenc*, cit.; M. TZANOU, op. cit.
[201] Su tutti, si veda A. BRADFORD, *The Brussels Effect – how the European Union Rules the World*, Oxford, 2019, part. p. 18-24 e pp. 131-169.

che «la attenzione della UE alla tutela dei dati si sia spostata dalla pura tutela dei dati personali (che è rimasta comunque essenziale per conquistare la fiducia delle persone nella società dei dati) alla tutela e regolazione dei dati come asse portante della economia digitale»[202].

Proprio questo percorso (in qualche modo, circolare) e queste evoluzioni hanno traccia nella giurisprudenza lussemburghese, la cui analisi è perciò indispensabile, e per questo le pronunce appena descritte sono emblematiche tanto del funzionalismo che caratterizzava l'orientamento dell'epoca, da non sottovalutare proprio perché palesato dall'esito delle pronunce, quanto però anche delle prime attenzioni nell'ordinamento comunitario a questioni che implicavano in qualche modo la tutela di diritti fondamentali. Pertanto, l'importanza della sentenza *National Panasonic*, ai nostri fini, risiede – oltre che nel riconoscimento del rispetto della vita privata come principio generale del diritto comunitario[203] – nel richiamo effettuato dalla Corte di giustizia all'articolo 8 CEDU, ancorché sollecitato dal ricorrente e con i limiti suddetti.

Esso, peraltro, consente di volgere lo sguardo a Strasburgo per constatare già presente la giurisprudenza sull'articolo 8 CEDU[204]. Va detto che, in questo caso, la casistica che ha da subito coinvolto (anche o solo) l'articolo 8 è proprio quella che ha assunto particolare importanza per l'elaborazione da parte della Corte EDU della rinomata *dottrina del margine di apprezzamento*[205]. Ciò, ovviamente, in virtù della stessa «tecnica redazionale di quegli articoli che giustificano eventuali limitazioni di diritti»[206], di cui l'articolo 8 fa parte (in particolare, ci si riferisce agli articoli 8-11 della Convenzione, ma anche all'articolo 1 del Protocollo n. 1) e che presentano la seguente struttura: nel primo paragrafo è enunciato il diritto garantito; nel secondo paragrafo sono

[202] Così F. PIZZETTI, Il futuro dell'Europa di regge sui dati. Pizzetti: "Così l'UE ha cambiato approccio", in *Agenda Digitale*, 5 agosto 2020.
[203] J. KOKOTT, C. SOBOTTA, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International data privacy law*, 2013, Vol. 13, No. 4, p. 223.
[204] L'articolo 8 si compone di due paragrafi:
1. *Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza*.
2. *Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute e della morale, o alla protezione dei diritti e delle libertà altrui*.
[205] Per la quale si veda, *ex multis*: R. ST. J. MACDONALD, The margin of appreciation in the Jurisprudence of the European Court of Human Rights, in *Il Diritto internazionale al tempo della sua codificazione. Studi in onore di Roberto Ago*, Milano, 1987, pp. 187-208; R. SAPIENZA, Sul margine di apprezzamento statale nel sistema della Convenzione europea dei diritti dell'uomo, in *Rivista di diritto internazionale*, LXXIV, 1991, pp. 571-614; E. BENVENISTI, Margin of appreciation, consensus, and universal standards, in *Journal of International law and politics*, 1999, pp. 843-854.
[206] P. TANZARELLA, Il margine di apprezzamento, in M. CARTABIA (a cura di), *I diritti in azione – Universalità e pluralismo dei diritti fondamentali delle Corti europee*, Bologna, 2007, p. 150.

previste le condizioni alle quali uno Stato può adottare misure per limitare il godimento di quel diritto[207].

Facendo solo cenno al primo esempio in cui poteva ravvisarsi un'ancora implicita applicazione di tale dottrina, risalente a una pronuncia del 1968, esso già coinvolgeva, con altri, anche la violazione dell'articolo 8: il celebre caso *Belgian linguistic* consentiva infatti alla Corte di sottolineare che il rispetto della Convenzione fosse compatibile con il mantenimento delle diversità proprie degli Stati parti, riservandosi essa un controllo sulla conformità delle scelte statali[208]. Si suole però riferire la prima indicazione esplicita di tale dottrina a qualche anno più tardi, con riguardo al caso *De Wilde, Ooms, Versyp*, relativo proprio al controllo della corrispondenza in una situazione di detenzione per vagabondaggio. Sull'asserita violazione dell'articolo 8, la Corte rispondeva infatti che: «*the competent Belgian authorities did not transgress in the present cases the limits of the power of appreciation which Article 8 (2) (art. 8-2) of the Convention leaves to the Contracting States: even in cases of persons detained for vagrancy, those authorities had sufficient reason to believe that it was "necessary" to impose restrictions for the purpose of the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others*»[209].

Dello stesso orientamento, volto a giustificare le misure statali limitative del diritto previsto al primo paragrafo, è la celebre pronuncia del 1978 sul caso *Klass*, particolarmente rilevante ai nostri fini perché apre il sempre più copioso filone relativo alla sorveglianza di massa, che proprio riguardo al delicato bilanciamento tra esigenze di pubblica sicurezza e tutela della riservatezza delle comunicazioni ha assunto un certo rilievo (cfr. *infra*, Parte IV). In quel caso, infatti, i ricorrenti criticavano la legislazione tedesca non tanto per la previsione di misure di sorveglianza quanto perché essa consentiva alle autorità di controllare corrispondenza e comunicazioni elettroniche senza obbligarle a notificare il controllo agli interessati nonché laddove non prevedeva rimedi giurisdizionali contro l'ordinanza e l'esecuzione di tali misure.

Ebbene, la Corte escludeva una violazione dell'articolo 8 CEDU perché, da una valutazione complessiva del sistema di sorveglianza, riteneva che, nonostante le mancanze indicate dai

[207] Cfr. R. SAPIENZA, *op. cit.*, p. 589.
[208] Corte europea dei diritti umani, *Belgian linguistic*, ricorsi n. 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64, decisione 23 luglio 1968. Si ricorda che i ricorrenti erano cittadini belgi di lingua francese, residenti nella regione di lingua tedesca, i cui figli frequentavano istituti scolastici dove l'insegnamento del francese veniva sottovalutato, motivo per cui lamentavano una violazione dell'articolo 2 del Protocollo n. 1 (diritto all'istruzione) e dell'articoli 8 e 14 (divieto di discriminazione).
[209] Corte europea dei diritti umani, *De Wilde, Ooms, Versyp c. Belgio*, ricorsi n. 2832- 2835- 2899/66, decisione 18 giugno 1971, punto 93.

ricorrenti, venissero comunque previste esigenze adeguate di tutela[210]. Tuttavia, proprio nell'effettuare tale valutazione ammetteva che la discrezionalità di cui godono gli Stati non è illimitata, specie in virtù della delicatezza delle misure di sorveglianza segreta per la tenuta del sistema democratico, indicando a tal fine, per la prima volta, "*minimum standards*"[211] quanto agli elementi da prendere in considerazione per la legittimità di simili misure[212]. Peraltro, più garantista si mostrava la Corte qualche anno dopo, in un altro caso riguardante l'articolo 8 ma relativo ad un altro dei molteplici aspetti da esso contemplati: il riferimento è al famoso caso *Dudgeon* in cui il ricorrente contestava la rigida normativa irlandese che incriminava pratiche omosessuali, ritenendola in violazione di una sfera particolarmente intima della vita privata. Nella sua pronuncia del 1981, la Corte infatti stabiliva che «*the present case concerns a most intimate aspect of private life. Accordingly, there must exist particularly serious reasons before interferences on the part of the public authorities can be legitimate for the purposes of paragraph 2 of Article 8 (art. 8-2)*»[213], non ravvisate presenti nel caso di specie.

L'accostamento dei due casi appena citati ci consente (soprattutto alla luce dell'impossibilità di accennare alle molteplici e variegate pronunce sull'articolo 8) di sottolineare l'ampiezza della nozione di "vita privata" elaborata dalla Corte di Strasburgo, condividendo che «sebbene la Corte abbia preferito seguire un approccio di tipo casistico in luogo di definire in modo generale e astratto in che cosa consiste precisamente il contenuto del par. 1 dell'art. 8, se si esamina lo sviluppo della giurisprudenza nel corso del tempo è possibile registrare una notevole estensione del concetto di diritto al rispetto della vita privata e familiare. Le direttive principali di tale evoluzione sono quelle che dall'ambito dello spazio privato si estendono alla vita di relazione; o ancora che dall'identità personale si ampliano alla raccolta e utilizzo di dati da parte delle pubbliche autorità e che dalla tutela dei dati sanitari si allargano agli orientamenti sessuali *et alia*»[214]. A partire dai casi riferiti, infatti, è possibile ravvisare una sempre più fitta giurisprudenza volta ad allargare l'ambito dell'articolo 8, al punto da comprendere, come è stato sottolineato, l'autonomia personale e ancor

[210] Corte europea dei diritti umani, *Klass e a. c. Germania*, ricorso n. 5029/71, decisione 6 settembre 1978, punti 49 e 60 (in seguito: caso *Klass*).
[211] Cfr. E. PSYCHOGIOPOULOU, The European Court of Human Rights, privacy and data protection in the digital era, in M. BRKAN, E. PSYCHOGIOPOULOU (Eds), *Courts, privacy and data protection in the digital environment*, Elgar, 2017, pp. 53-54.
[212] Caso *Klass*, *cit*., punti 50-59. Sulla rilevanza del caso con riguardo specifico al rapporto tra terrorismo e protezione dei dati personali si veda, *ex multis*, M. NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, Editoriale Scientifica, 2012, part. p. 66.
[213] Corte europea dei diritti umani, *Dudgeon c. Regno Unito*, ricorso n. 7525/76, decisione del 22ottobre 1981, punto 52.
[214] G. DELLA MORTE, *Big Data e protezione internazionale dei diritti umani – regole e conflitti*, Editoriale Scientifica, 2018, pp. 86-87.
Per una disamina abbastanza esaustiva della portata dell'articolo 8 CEDU e della giurisprudenza al riguardo si veda la recente *Guida sull'articolo 8 CEDU*, del CoE, aggiornata al 31 agosto 2020, disponibile qui: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (ultimo accesso 3.03.2021).

più specificamente la "autodeterminazione informativa"[215] (di cui si era fatto cenno *supra*, Capitolo I). Ciò basti a segnalare l'estensione della nozione e, da qui, la necessità di limitare l'attenzione alle questioni che rilevano ai nostri fini, soprattutto in termini di influenza e successivo possibile dialogo con la Corte di Lussemburgo[216].

Tralasciando, dunque, i pur numerosi e interessanti esempi di bilanciamento tra tutela della vita privata e altri diritti individuali, su tutti la libertà di espressione[217], e/o i casi in cui detta tutela si declina in termini di tutela della reputazione e dell'immagine[218], la nostra attenzione si concentrerà sulla giurisprudenza da cui emerge la comprensione della protezione dei dati personali nell'alveo dell'articolo 8, con particolare riguardo a quella relativa alle misure di sorveglianza, intercettazione di comunicazioni e conservazione di dati da parte di autorità pubbliche per esigenze di sicurezza.

Così, sulla spinta del caso *Klass*, tra gli anni Ottanta e inizio Duemila importanti casi hanno dato alla Corte l'occasione di precisare i margini entro i quali consentire sistemi di sorveglianza e di conservazione dei dati da parte di pubbliche autorità in virtù del paragrafo 2 dell'articolo 8. Vi è una notevole casistica, in questo primo periodo, che ha visto elaborare la precisazione dei requisiti necessari, tra cui vanno annoverati almeno i casi *Malone*, *Leander*, *Kruslin*, *Kopp*, *Amann e Rotaru*[219]. Seguendo questa giurisprudenza, già in tempi risalenti (precisamente nel 1987, ossia all'indomani della stipula della Convenzione n. 108) la Corte sussumeva nel paragrafo 1 dell'articolo 8 la protezione dei dati personali, in termini di informazioni su persone acquisite e conservate dalle autorità: «*Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference*

[215] Così, in particolare, rilevano P. DE HERT, S. GUTWIRTH, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, in S. GUTWIRTH, Y. POULLET, P. DEHERT, J, NOUWT, C. DE TERWANGNE (Eds), *Reinventing data protection?*, Dordrecht, 2009, richiamando il famoso caso *Pretty c. Regno Unito*, ricorso n. 2346/02, decisione del 29 aprile 2002, part. p. 61: «*In Pretty autonomy is considered a 'principle' and physical and social identity are issues of which 'aspects' are sometimes protected by the right to private life. In their joint dissenting opinion to Odièvre v. France judges Wildhaber, Bratza, Bonello, Loucaides, Cabral Barreto,Tulkens and Pellonpää consider autonomy and identity to be 'rights'*», p. 10, nota 64. Quanto al riferimento specifico a "*informational self-determination*" si veda p. 12, in cui gli autori fanno riferimento a diversi casi, tra i quali rileva ai nostri fini: Corte europea dei diritti umani, *Gaskin c. Regno Unito*, ricorso n. 10454/83, decisione del 7 luglio 1989.

[216] Sebbene in tempi abbastanza recenti, è comunque da segnalare sin da ora un interessante esempio di dialogo tra le due Corti europee quanto a questioni di sorveglianza e protezione dei dati, suggerendo a tal fine la puntuale analisi di M.D. COLE, A. VANDENDRIESSCHE, From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR made of the deep pass by the CJEU in the recent cases on mass surveillance, in (2016) *European Data Protection Law Review* 121.

[217] Un'interessante disamina dei casi relativi a tale bilanciamento viene effettuata da E. PSYCHOGIOPOULOU, *op. cit*., pp. 35-49.

[218] Per una ricognizione dei casi più importanti si vedano i seguenti *factsheets* dedicati: per la tutela della reputazione, https://www.echr.coe.int/Documents/FS_Reputation_ENG.pdf ; per la tutela della propria immagine, FS_Own_image_ENG (coe.int)

[219] Corte europea dei diritti umani, *Malone c. Regno Unito*, ricorso n. 8691/79, decisione del 2 agosto 1984; *Leander c. Svezia*, ricorso n. 9248/81, decisione del 26 marzo 1987; *Klusin c. Francia*, ricorso n. 11801/85, decisione del 24 aprile 1990; *Kopp c. Svizzera*, ricorso n. 23224/94, decisione del 25 marzo 1998; *Amann c. Svizzera*, ricorso n. 27798/95, decisione del 16 febbraio 2000; *Rotaru c. Romania*, ricorso n. 28341/95, decisione del 4 maggio 2000.

with his right to respect for private life as guaranteed by Article 8 § 1 (art. 8-1)»[220]. La stessa Corte poi precisava, nell'ambito della sua ampia interpretazione della norma, la definizione di dati personali da tutelare, facendo espresso richiamo alla Convenzione n. 108 (per cui si veda *supra*, Capitolo II): «*The Court reiterates that the storing of data relating to the "private life" of an individual falls within the application of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48). It points out in this connection that the term "private life" must not be interpreted restrictively (...) That broad interpretation corresponds with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2)*»[221]. Il richiamo alla Convenzione 108 è dirimente (e lo sarà anche per la sua influenza nell'ordinamento comunitario), poiché è proprio tramite questo che la Corte di Strasburgo può perorare la sua tendenza ad interpretare estensivamente l'articolo 8 e così, oltre le righe, farvi rientrare la tutela dei dati oggetto di trattamento automatizzato.

Quanto alla giustificabilità delle misure, seguendo il paragrafo 2 dell'articolo 8 è necessario anche in questi casi soddisfare i "tre test": previsione legislativa; scopo legittimo; necessarietà in una società democratica[222]. Ebbene, lo scrutinio della Corte in questi casi partiva anzitutto dalla constatazione di un'ingerenza insita nella stessa previsione statale di sistemi di sorveglianza: «*As the Commission pointed out in its report (paragraph 115), the existence in England and Wales of laws and practices which permit and establish a system for effecting secret surveillance of communications amounted in itself to an "interference ... with the exercise" of the applicant's rights under Article 8 (art. 8), apart from any measures actually taken against him*»[223]. Constatata quindi l'ingerenza, occorre valutare se essa sia "prevista dalla legge", per uno scopo legittimo e "necessaria in una società democratica".

---

[220] Caso *Leander*, cit., punto 48.

[221] Caso *Amann*, cit., punto 65. Sul richiamo effettuato dalla Corte europea (guardiana della sola CEDU) alla Convenzione 108, è stato detto: «*Through its references to the 1981 Data Protection Convention, the Strasbourg Court has endorsed and spread the idea that data protection is more than just technical regulation*», così P. DE HERT-S. GUTWIRTH, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, cit., p. 17.

[222] Per un'esaustiva analisi della giurisprudenza sui "*tre test*" in materia di protezione dei dati, si veda su tutti la nuova Guida appositamente dedicata: *Guide sur la jurisprudence de la Convention européenne des droits de l'homme – Protection des données*, Première édition – 31 décembre 2020 (part. *Les trois « tests » en matière de protection des données*), pp. 24-32, disponibile qui : https://www.echr.coe.int/Documents/Guide_Data_protection_FRA.pdf .

[223] Caso *Malone*, cit., punto 64. Dello stesso tenore anche, tra le altre, le successive: *Amann*, cit., punti 69-80; *Rotaru*, cit. punto 46.

Con riferimento particolare al criterio di legalità, la Psychogiopoulou ci ricorda che «*the legality criterion also requires an element of* quality of the law *in question: the law must be in accordance with the rule of law and adequately* accessible *and* foreseeable. *Legislation is considered to be adequately accessible when the person concerned has an indication that is adequate in the circumstances of the legal rules applicable to a given case. (…) A rule is generally foreseeable if it is formulated with sufficient precision to enable an individual (…) to regulate his conduct*»[224]. Basti al riguardo richiamare il celebre caso *Rotaru*, in cui il ricorrente lamentava l'impossibilità di poter confutare la veridicità di informazioni sul proprio conto conservate dai servizi di intelligence rumeni. In tal caso la Corte (che riteneva applicabile l'articolo 8 anche se le informazioni riferibili al ricorrente erano parecchio risalenti nel tempo) non solo ribadiva, richiamando la propria giurisprudenza (*Amann* in particolare) la necessità della "qualità" delle previsioni legislative (in termini di accessibilità e prevedibilità), ma insisteva sulla loro precisione, quanto per esempio all'indicazione del tipo di informazioni registrate e della categoria di soggetti cui applicare tali misure nonché le circostanze per la loro adozione e i limiti di durata di conservazione delle informazioni[225]. Peraltro, negli anni successivi e con l'affinarsi delle tecnologie, la Corte ha insistito sempre più sulla necessità di una legislazione sufficientemente chiara quanto alle condizioni in presenza delle quali l'autorità può procedere alla sorveglianza[226].

Circa gli altri due aspetti e, in particolare, la necessarietà in una società democratica, vale richiamare il famoso caso *S. e Marper c. Regno Unito* (relativo alla conservazione di campioni cellulari, profili DNA e impronte digitali), su cui la Corte si pronunciò nel 2008 precisando: «*An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim*

---

[224] E. PSYCHOGIOPOULOU, *op. cit*., pp. 52-53.

[225] Caso *Rotaru*, cit., punti 56-57: «*The "quality" of the legal rules relied on in this case must therefore be scrutinised, with a view, in particular, to ascertaining whether domestic law laid down with sufficient precision the circumstances in which the RIS could store and make use of information relating to the applicant's private life. The Court notes in this connection that section 8 of Law no. 14/1992 provides that information affecting national security may be gathered, recorded and archived in secret files. No provision of domestic law, however, lays down any limits on the exercise of those powers. Thus, for instance, the aforesaid Law does not define the kind of information that may be recorded, the categories of people against whom surveillance measures such as gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed. Similarly, the Law does not lay down limits on the age of information held or the length of time for which it may be kept.* Section 45 of the Law empowers the RIS to take over for storage and use the archives that belonged to the former intelligence services operating on Romanian territory and allows inspection of RIS documents with the Director's consent. The Court notes that this section contains *no explicit, detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that may be made of the information thus obtained*». Sull'applicabilità dell'articolo 8 con riguardo a informazioni risalenti nel tempo v. punto 44.

[226] Ibidem, p. 53, laddove vengono citate diverse pronunce, tra cui vanno richiamate qui: Corte europea dei diritti umani, *Liberty e a. c. Regno Unito*, ricorso n. 58243/00, decisione del 1 luglio 2008 (p. 62; *Roman Zakharov c. Russia*, ricorso n. 47143/06, decisione del 4 dicembre 2015 (p. 229); *Szabó e Vissy c. Ungheria*, ricorso n. 37138/14, decisione del 12 gennaio 2016 (p. 62). V. anche *M.M. c. Regno Unito*, ricorso n. 24029/07, decisione del 13 novembre 2012, pp. 202-207.

pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient". While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention» e così sottolineando l'importanza del suo scrutinio a riguardo, pur riconoscendo alle autorità nazionali un margine di apprezzamento[227].

Ma questa pronuncia è di particolare importanza ai nostri fini soprattutto rispetto all'esplicito riconoscimento della protezione dei dati personali come aspetto della tutela della vita privata: «*The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention*»[228]. Questo passo è, infatti, emblematico dell'approccio tipico della Corte di Strasburgo rispetto al rapporto tra riservatezza e protezione dei dati, in termini di considerazione della seconda come contenuta nella prima. Ovviamente, non vanno trascurate più generali considerazioni circa il fatto che sia l'ex Commissione che la Corte hanno considerato non tutti gli aspetti del trattamento dei dati come coperti dalla protezione della CEDU (così come la distinzione tra dati che rientrano e dati che non rientrano nell'ambito di applicazione dell'articolo 8)[229]. E difatti, in questo senso qualcuno ha rilevato criticamente che nella pronuncia sul caso *Marper* «*the Court kept a privacy-oriented approach, without taking into proper account the peculiarities of data protection. In other words, the data protection substantive principles violation did not absorb the proportionality assessment but were just one element in such an assessment*»[230]. Pertanto, parrebbe ritenersi valida in via generale la seguente considerazione: «*In essence, the protection of personal data is treated as a subset of the right to respect for private life. This differs from the approach followed under European Union (EU) law, that is, the recognition of a* separate *fundamental right to personal data protection, enshrined in Article 8 of the Charter of Fundamental Rights (Charter or CFR) of the EU, which is distinct from the right to respect for private (and family) life, safeguarded under*

[227] Corte europea dei diritti umani, *S. e Marper c. Regno Unito*, ricorso n. 30562/04, decisione del 4dicembre 2008, punto citato 101 e punto 102 sul margine di apprezzamento.
[228] Ibidem, punto 103, dove continua: «*The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article (…). The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes*».
[229] Così rilevano P. DE HERT, S. GUTWIRTH, Data Protection in the Case Law of Strasbourg and Luxemburg, *cit*., pp. 15-16: «*Both the former Commission and the Court have held that not all aspects of the processing of personal data are protected by the ECHR. (…) Also, the Court made a distinction between personal data that fall within the scope of Art. 8 ECHR and personal data that do not. In the eyes of the Court there is processing of personal data that affects private life and processing of personal data that does not affect the private life of individuals*».
[230] Così A. TERRASI, *Protection of Personal Data and Human Rights between the ECHR and the EU Legal Order*, in A. CALIGIURI (ed.), *Legal Technology Transformation. A Practical Assessment*, Editoriale Scientifica, 2020, p. 25.

Article 7 CFR»[231]. Ciò ci riporta, così, ad analizzare la giurisprudenza di Lussemburgo, che ha adottato un approccio in qualche misura diverso da quello qui esposto, pur ad esso inevitabilmente ispirandosi.

2. Accostamenti e divergenze

Secondo periodo

Nell'ambito della giurisprudenza comunitaria, infatti, se è vero che la comprensione del rapporto tra *privacy* e protezione dei dati ha assunto un approccio diverso, ciò non significa che non siano ravvisabili perplessità quanto alla effettiva delimitazione dei due diritti ugualmente tutelati nell'ordinamento di riferimento. Per procedere all'analisi della giurisprudenza occorre rammentare che, dopo gli ultimi casi precedentemente citati, un'importante innovazione intervenne nell'ordinamento comunitario: la Direttiva 95/46/CE (c.d. direttiva madre, per cui si rinvia *supra*, Capitolo II), quale normativa di diritto derivato a tutela delle persone fisiche quanto al trattamento dei dati personali nonché della circolazione di tali dati e rispondente, come sottolineava anche la Commissione, a una duplice logica intrinsecamente legata alle più antiche ambizioni del processo di integrazione: esigenze di mercato interno; tutela i diritti degli individui coinvolti. Per ammissione della stessa Commissione, "Nella Direttiva entrambi gli obiettivi assumono pari importanza. In termini giuridici tuttavia la direttiva trae origine da motivi di mercato interno"[232].

Ebbene, nel caso *Fisher*, un rinvio pregiudiziale che non riguardava direttamente detta normativa ma quella relativa al regime di pagamenti compensativi a favore dei produttori di taluni seminativi, nonché quella che istituiva a tal fine un sistema integrato di gestione e controllo per prevenire frodi e così richiedeva banche dati informatizzate negli Stati membri, la Corte di giustizia richiamava comunque la direttiva madre, statuendo: «*Tuttavia, i rispettivi interessi delle persone coinvolte con riguardo ai dati di natura personale devono essere valutati nel rispetto della tutela delle libertà e dei diritti fondamentali. A questo proposito, le norme della direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al*

[231] E. PSYCHOGIOPOULOU, *op. cit.*, p. 33.
[232] Commissione delle Comunità europee, Prima Relazione sull'applicazione della Direttiva sulla tutela dei dati (95/46/CE), COM (2003) 265 def, punto 1.1, disponibile qui: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:IT:PDF .

trattamento dei dati personali, nonché alla libera circolazione di tali dati (...), forniscono criteri che si prestano ad essere applicati dall'autorità competente all'atto di tale valutazione. Infatti, anche se detta direttiva non era ancora entrata in vigore all'epoca dei fatti della causa principale, dal decimo e dall'undicesimo 'considerando' risulta ch'essa riprende, a livello comunitario, i principi generali che facevano già parte, in questa materia, del diritto degli Stati membri»[233]. Da questa pronuncia (insieme con le due analizzate precedentemente) possono sollevarsi due aspetti di rilievo, utili a condurre la breve analisi sulla casistica più importante nell'evoluzione del diritto alla protezione dei dati personali nell'Unione europea.

Il primo consiste nella riconducibilità di tale diritto ai principi generali del diritto comunitario, specie prima di formali riconoscimenti normativi, quali la Direttiva e soprattutto la Carta dei diritti fondamentali (proclamata per la prima volta a Nizza nel 2000)[234], e nella conseguente possibilità di individuarne una distinzione (come poi verrà effettuata dalla Carta) nella giurisprudenza della Corte. Tale questione è stata affrontata, tra gli altri, da Brkan (della quale seguiremo l'analisi), che infatti al riguardo affermava: «*The question is, however, whether the CJEU already recognized the nature of data protection as a general principle of the EU law in its pre-Charter jurisprudence. From the* Fisher *case it seems that Directive 95/46/EC codifies existing principles of EU law, but it is not entirely clear whether those existing principles enshrine merely the protection of privacy or the protection of personal data. Moreover, data protection could be considered as a general principle of EU law on the basis of its recognition by the ECtHR*»[235].

Il secondo aspetto deriva dalle esigenze conseguenti all'entrata in vigore di quella prima previsione normativa (la Direttiva madre), tra le quali, soprattutto, quella di definirne l'ambito di applicazione. Pertanto, si suole indicare il riferimento alle sentenze della Corte del 2003 *Österreichischer Rundfunk* e *Linqvist* quale punto di partenza per l'interpretazione del diritto alla protezione dei dati personali nell'ordinamento comunitario e che assumono rilevanza fondamentale ai fini della nostra analisi. Non solo, infatti, entrambe servono per indagare i primi orientamenti sull'ambito di

[233] Corte di giustizia, C-369/98, *The Queen contro Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher*, 14 settembre 2000, punti 32-34, enfasi aggiunta.
[234] Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza, dicembre 2000, riproclamata a Strasburgo 2007, di seguito Carta o CDFUE.
[235] M. BRKAN, The Court of Justice of the EU, privacy and data protection: Judge-made law as a leitmotif in fundamental rights protection, in M. BRKAN-E. PSYCHOGIOPOULOU (Eds), *Courts, privacy and data protection in the digital environment*, Elgar, 2017, p. 12. Sulla punto si veda anche J. KOKOTT, C. SOBOTTA, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *cit*, pp. 222-228.

applicazione della normativa (questioni non certo sopite, neppure dopo l'entrata in vigore del GDPR)[236], ma anche ciascuna presenta qualche elemento aggiuntivo di non poco conto.

Il caso *Österreichischer Rundfunk,* per esempio, sulla compatibilità di misure interne imponenti raccolta di dati sui redditi di dipendenti di enti pubblici per l'inserimento in una relazione della Corte dei Conti destinata alla pubblicazione, risalta ai nostri occhi per essere il primo in cui espressamente la Corte di Lussemburgo fece esplicito richiamo alla giurisprudenza di Strasburgo sull'articolo 8 CEDU per costruire e giustificare il proprio ragionamento in risposta alle questioni pregiudiziali, sollevate con riguardo all'interpretazione della direttiva 95/46/CE. Nel fare ciò, la Corte richiamava l'ampia interpretazione data dai giudici di Strasburgo rispetto alla nozione di "vita privata" nonché le valutazioni suesposte (i c.d. "tre test") circa la giustificabilità di misure statali di ingerenza: "*Occorre anzitutto considerare che la raccolta di dati nominativi relativi ai redditi professionali di un individuo, per comunicarli a terzi, rientra nel campo di applicazione dell'art. 8 della CEDU. La Corte europea dei diritti dell'uomo ha dichiarato, al riguardo, che l'espressione «vita privata» non deve essere interpretata in modo restrittivo e che «nessun motivo di principio consente di escludere le attività professionali (...) dalla nozione di "vita privata"» (v., in particolare… Amann/Svizzera… e 4 maggio 2000, Rotaru/Romania…). È giocoforza constatare che, se è vero che la semplice registrazione, da parte del datore di lavoro, di dati nominativi relativi alle retribuzioni corrisposte al suo personale non può, in quanto tale, costituire un'ingerenza nella vita privata, la comunicazione di tali dati ad un terzo, nel caso di specie un'autorità pubblica, arreca pregiudizio al diritto al rispetto della vita privata degli interessati, quale che sia l'ulteriore utilizzazione delle informazioni così comunicate, e presenta il carattere di un'ingerenza ai sensi dell'art. 8 della CEDU. Per accertare l'esistenza di una simile ingerenza (…) È sufficiente constatare che i dati relativi ai redditi percepiti da un lavoratore o da un pensionato sono stati comunicati dal datore di lavoro ad un terzo. Un'ingerenza come quella menzionata al punto 74 della presente sentenza viola l'art. 8 della CEDU, salvo se, «prevista dalla legge», essa persegue uno o più finalità legittime previste al n. 2 di tale disposizione ed è «necessaria in una società democratica» per la realizzazione di tale o tali finalità*"[237]. Nondimeno, è stato altresì notato che in tale occasione la Corte non faceva affatto riferimento, pur potendo, all'articolo 8 della

[236] In questo senso v. ROSSI DAL POZZO, *op. cit.*: «Rimane, certo, un'ambiguità di fondo della norma, peraltro non fugata, ma anzi, per un verso, acuita dalle analoghe disposizioni del Regolamento (UE) n. 2016/679 dal quale sarebbe stato lecito attendersi una maggiore precisione linguistica», p. 7.

[237] Corte di giustizia, cause riunite C-465/00, C-138/01 e C-139/01, *Rechnungshof c. Österreichischer Rundfunk e a. e Christa Neukomm e Joseph Lauermann c. Österreichischer Rundfunk*, sentenza del 20 maggio 2003, punti 73-77. Inoltre, ai punti 78 ss. continua puntando sulla necessità della precisione della previsione legislativa nazionale e sul principio di proporzionalità.

già proclamata Carta dei diritti fondamentali[238]. Peraltro, come si diceva, il caso assume rilievo, insieme con il caso *Lindqvist*, proprio quanto all'ambito di applicazione della direttiva.

Come si usa ricordare, infatti, la base giuridica della direttiva (l'allora articolo 100A del TCE, corrispondente all'attuale articolo 114 TFUE) riguardava il ravvicinamento delle legislazioni statali sull'instaurazione e funzionamento del mercato interno e quindi non rispondeva totalmente ai due obiettivi della stessa, non fornendo effettivamente alla Comunità una specifica competenza in materia di protezione dei dati personali[239]. Ciò implicava perplessità circa l'ambito di applicazione della normativa, che vennero affrontate nei due casi, in modo divergente, dall'Avvocato Generale Tizzano e dalla Corte. Nel caso *Österreichischer Rundfunk*, infatti, l'AG riteneva indispensabile per risolvere le questioni proposte stabilire se l'attività di controllo prevista da quelle misure rientrasse nel campo di applicazione della direttiva (definito dall'articolo 3 della stessa)[240]. Nel caso *Lindqvist,* relativo alla pubblicazione di dati propri e di alcuni colleghi su una *home page* appositamente creata su Internet da una catechista svedese a fini informativi per i parrocchiani, era proprio uno dei quesiti pregiudiziali a interrogare la Corte sulla portata dell'ambito di applicazione (nella specie, se in esso rientrasse l'indicazione di nomi e numeri di telefono di quelle persone nella home page, accessibile anche tramite link dal sito della parrocchia). Ebbene, in entrambi i casi l'AG proponeva un'interpretazione restrittiva al riguardo: «*La promozione del progresso economico e sociale e la salvaguardia dei diritti fondamentali rappresentano dunque importanti valori ed esigenze di cui il legislatore comunitario ha tenuto conto nel delineare la disciplina armonizzata necessaria per l'instaurazione ed il funzionamento del mercato interno, ma non autonomi obiettivi della direttiva. Diversamente, si dovrebbe ritenere che la direttiva intenda tutelare gli individui rispetto al trattamento dei dati personali anche a prescindere dall'obiettivo di favorire la libera circolazione di tali dati, con l'incongrua conseguenza di far rientrare nel suo campo di applicazione pure trattamenti effettuati per l'esercizio di attività che abbiano qualche rilevanza sociale ma che non presentino alcun rapporto con l'instaurazione ed il funzionamento del mercato interno*»[241].

Di diverso avviso la Corte, che in entrambi i casi sostanzialmente stabiliva che «*l'applicabilità della direttiva 95/46 non può dipendere dalla soluzione del problema se le situazioni concrete di cui*

[238] Così denota H. HIJMANS, *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU*, (PhD Thesis) University of Amsterdam, 2016, p. 180.
[239] Così F. BALDUCCI ROMANO, La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo, in *Rivista Italiana di Diritto Pubblico Comunitario*, Fasc. 6-2015, p.1624.
[240] Caso *Österreichischer Rundfunk, cit*., punto 42. Dello stesso identico tenore, e richiamando proprio il punto appena citato dell'altra pronuncia, Corte di giustizia, causa C-101/01, *Bodil Lindqvist c. Åklagarkammaren i Jönköping*, 6 novembre 2003, punti 40-41.
[241] Conclusioni AG Tizzano, causa C-101/01, *Bodil Lindqvist c. Åklagarkammaren i Jönköping*, presentate il 19 settembre 2002, punto 41 (ma v. pp. 40-44). Assolutamente dello stesso tenore le Conclusioni proposte nella causa C-465/00, *Rechnungshof c. Österreichischer Rundfunk e a.* e cause riunite C-138/01 e C-139/01, *Neukomm e Lauermann c. Österreichischer Rundfunk*, presentate il 14 novembre 2002, punti 51-56.

trattasi nelle cause principali presentino un nesso sufficiente con l'esercizio delle libertà fondamentali garantite dal Trattato e in particolare, nelle dette cause, con la libera circolazione dei lavoratori. Infatti, un'interpretazione in senso contrario rischierebbe di rendere particolarmente incerti ed aleatori i limiti del campo di applicazione della detta direttiva, il che sarebbe contrario al suo obiettivo essenziale, che è quello di ravvicinare le disposizioni legislative, regolamentari, ed amministrative degli Stati membri per eliminare gli ostacoli al funzionamento del mercato interno derivanti proprio dalle disparità esistenti tra le normative nazionali»[242]. Senza poter indugiare sul punto, ciò basti ad evidenziare l'importanza dei due casi per la definizione, effettuata dalla Corte, dell'ambito materiale e personale di ciò che iniziava a consolidarsi come diritto alla protezione dei dati nell'ordinamento sovranazionale, secondo un approccio "sostanziale"[243] che veniva poi confermato anche successivamente[244].

Inoltre, è bene fare cenno a un altro intervento quanto alla definizione dell'ambito di applicazione materiale della direttiva 95/46: il famoso caso finlandese *Satamedia*, rilevante sotto diversi profili, diede alla Corte l'occasione di stabilire nel 2008 che rientra nel "trattamento di dati personali" anche l'attività di estrazione da documenti pubblici dell'amministrazione fiscale e la pubblicazione di dati sul reddito e sul capitale di persone fisiche[245].

Si consenta, poi, di segnalare ancora due aspetti sul caso *Lindqvist.* Anzitutto, che esso viene di solito indicato come il primo in cui la Corte specificò la nozione di "trattamento di dati personali interamente o parzialmente automatizzato dei dati personali" ai sensi dell'articolo 3 della direttiva[246]. Inoltre, che esso rileva ai nostri fini perché pone le basi della questione del trasferimento di dati verso Paesi terzi, che così veniva per la prima volta affrontato dalla Corte di giustizia. Il giudice *a quo* chiedeva, tra le varie questioni, se l'inserimento di dati nella pagina Internet (così accessibili a chiunque, anche da Paesi terzi) costituisse un "trasferimento verso Paesi terzi" ai sensi dell'articolo 25 della Direttiva. La Corte ebbe l'occasione di precisare che operazioni come quelle dei fatti di causa (che consentiva il mero accesso su internet a quei dati) non

[242] Corte di giustizia, *Österreichischer Rundfunk, cit*., punto 42; dello stesso tenore in *Lindqvist*, cit., p. 41.
[243] Così lo definisce F. BALDUCCI ROMANO, *op. cit*.: «un approccio sostanziale, volto a rendere più chiare e prevedibili le regole in materia di protezione dei dati personali. Come si vedrà, infatti, la prevedibilità delle norme assume particolare rilevanza proprio perché il diritto alla protezione dei dati personali costituisce un diritto fondamentale», p. 1626.
[244] Per esempio, pochi anni dopo: Corte di giustizia, C-524/06, *Huber*, 16 dicembre 2008.
[245] Corte di giustizia, causa C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy e Satamedia Oy*, sentenza del 16 dicembre 2008. Cfr. B. CORTESE, Articolo 16 TFUE, in A. TIZZANO (a cura di), *I Trattati dell'Unione europea*, Milano, 2014, p. 449.
[246] Caso *Lindqvist*, cit. p. 27. Vedi, a tal proposito: FRA-COE-EDPS, *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, 2018, p. 112; Corte di giustizia dell'Unione europea – Direzione della ricerca e documentazione, *Scheda tematica – tutela dei dati personali*, 2017, p. 12.

costituissero di per sé trasferimenti verso Paesi terzi, seguendo un'interpretazione della norma che rintracciava le intenzioni del legislatore comunitario[247].

Dato conto di due pronunce particolarmente salienti poiché tra le prime sulla normativa in materia, cosa accadde di interessante a condurre l'evoluzione giurisprudenziale in quegli anni? Come si è accennato, nel 2000 venne proclamata la Carta dei diritti fondamentali dell'Unione europea quale catalogo che, ancorché non vincolante, raccoglieva e formalizzava il riconoscimento a livello sovranazionale di diritti fondamentali. E, come si sa, nella nostra materia essa assume particolare rilievo perché si caratterizza per delle previsioni che la distinguono nettamente dall'analoga CEDU: essa, infatti, contiene l'articolo 7 precipuamente dedicato al *rispetto della vita privata e familiare*, che quindi corrisponde effettivamente all'articolo 8 CEDU (e che, ai sensi dell'articolo 52, paragrafo 3 della Carta, dee essere interpretato in conformità con esso)[248]; ma contiene anche l'articolo 8, specificamente dedicato alla "*protezione dei dati di carattere personale*". La Carta, dunque, esplicitava il riconoscimento di un diritto, quale era stato in qualche modo estrapolato dalla Corte, che a sua volta lo riconduceva ai principi generali del diritto comunitario attraverso il riferimento anche all'articolo 8 CEDU e alla giurisprudenza di Strasburgo che, nel definirlo, richiamava la Convenzione n. 108, alla quale infatti la *Spiegazione relativa all'articolo 8* fa espresso richiamo[249].

Vale la pena valutare, dunque, l'impatto che tale innovazione ebbe nella giurisprudenza di Lussemburgo. È nota, infatti, la cautela della Corte nel riferirsi alla Carta nel primo periodo successivo alla sua proclamazione[250].

Il primo caso in cui ciò avvenne nella materia che ci interessa è il noto *Promusicae*, su cui la Corte si pronunciò nel 2008, conosciuto anche come quello nel quale per la prima volta essa

[247] Caso *Lindqvist*, cit. pp. 56-71. Si veda anche *Scheda tematica*, cit., p. 17.
[248] V. *Spiegazione relativa all'articolo 7- Rispetto alla vita privata e familiare*.
V. anche *ex multis* Article 7 CFR, in M. KELLERBAUER, M. KLAMERT, AND J. TOMK (Eds), *The EU Treaties and the Charter of Fundamental Rights – A Commentary*, Oxford University Press, 2019, pp. 2215-2216.
[249] *Spiegazione relativa all'articolo 8 – Protezione dei dati di carattere personale* (per come aggiornata a seguito della riproclamazione della Carta nel 2007).
Sulla questione definitoria del diritto alla protezione dei dati personali nei sistemi, rispettivamente, dell'Unione europea e del Consiglio d'Europa si è soffermato di recente, tra gli altri, A. TERRASI, Protection of Personal Data and Human Rights between the ECHR and the EU Legal Order, *cit*., che, nel condurre un'analisi della giurisprudenza più rilevante delle Corti di Lussemburgo e Strasburgo al riguardo (peraltro, sino alle recenti "saghe" che hanno interessato *Google* e *Facebook*), è addivenuto alla conclusione per cui «(…) *there is one thing that brings together Luxembourg and Strasbourg in dealing with data protection: neither the former nor the latter have shaped, up to now, a coherent definition of the individual right to data protection. And none of them succeeded in, or even tried to, drawing up a distinction between right to private life scope and right to data protection scope. As a consequence, it remains unclear whether the latter can be implemented autonomously or an interference in the right to data protection always amount to an interference in the right to private life as well*», pp. 31-32.
[250] Cfr. G. GONZÁLEZ FUSTER, *op. cit*., p. 226, che ricorda che i primi timidi riferimenti provenivano da pareri degli Avvocati Generali (es. AG Tizzano in BERTU) o dal Tribunale (es. T-377/00).

espressamente riconobbe la tutela dei dati personali come diritto fondamentale (prima di allora, infatti, riferendosi unicamente al diritto al rispetto della vita privata)[251]. Occorre rammentare che nel frattempo vi furono diversi interventi normativi rilevanti in materia (per cui si veda *supra*, Capitolo III), tra cui la direttiva sul commercio elettronico (2000/31/CE) e la direttiva relativa alla vita privata e alle comunicazioni elettroniche (2002/58/CE) oggetto di interpretazione in quel caso (originato da una controversia mossa dal rifiuto della società telefonica di comunicare alla *Promusicae* dati personali sull'utilizzo di Internet tramite connessione predisposta dalla prima).

Si riportano di seguito i punti della sentenza da cui si evincono i diversi aspetti di interesse, la cui ambiguità è stata oggetto di diverse riflessioni che saranno condivise di seguito. Stabiliva la Corte: «*Tuttavia, occorre rilevare che nella controversia in relazione alla quale il giudice del rinvio ha sollevato tale questione risulta coinvolto, oltre ai due suddetti diritti, anche un altro diritto fondamentale, vale a dire quello che garantisce la tutela dei dati personali e, quindi, della vita privata. Ai sensi del secondo 'considerando' della direttiva 2002/58, quest'ultima mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla Carta. Segnatamente, essa mira a garantire il pieno rispetto dei diritti delineati agli artt. 7 e 8 di tale Carta. L'art. 7 di quest'ultima riproduce in sostanza l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950, il quale garantisce il diritto al rispetto della vita privata, mentre l'art. 8 della Carta proclama espressamente il diritto alla tutela dei dati personali. Pertanto, la domanda di pronuncia pregiudiziale in esame solleva la questione della necessaria conciliazione degli obblighi connessi alla tutela di diversi interessi fondamentali: da una parte, il diritto al rispetto della vita privata e, dall'altra, i diritti alla tutela della proprietà e ad un ricorso effettivo*»[252].

Da questi pochi passi si evince che, se è vero che «*The Court thus innovatively used the EU Charter as a direct source for the identification of a fundamental right never before recognised as integral to the general principles of the EU law (Groussout 2008, p. 1755) – and this despite the fact that, at that time, the Charter was not legally binding*»[253], è vero anche che ciò «*did not have a particular impact on the reasoning of the Court*»[254]. Si denota, insomma, una propensione da parte della Corte a considerare (ancora) la protezione dei dati come inscindibilmente legata alla tutela della vita privata, nonostante i due diritti godano di specifica e autonoma previsione nella Carta (ancorché non ancora vincolante).

[251] Come ricorda F. BALDUCCI ROMANO, *op. cit.*, p. 1643.
[252] Corte di giustizia, causa C-275/06, *Productores de Música de España (Promusicae) e Telefónica de España SAU*, 26 gennaio 2008, punti 63-65.
[253] . G. GONZÁLEZ FUSTER, *op. cit.*, p. 227.
[254] Ibidem.

Ciò riconduce alle riflessioni sull'approccio delle Corti nella comprensione del rapporto tra riservatezza e protezione dei dati e consente, in particolare, di richiamare l'analisi proposta dalla Brkan quanto a quello della Corte di giustizia. L'autrice, rilevando una qualche confusione nell'approccio della giurisprudenza sovranazionale al riguardo, individuava tre categorie di casi: quelli in cui una distinzione risulta chiaramente; quelli in cui una distinzione non è chiara; quelli in cui la protezione dei dati è considerata come un sub-contenuto del diritto alla riservatezza. Ebbene, anche se l'autrice non annoverava il caso di specie in nessuna delle suddette categorie, dai passi testé riportati si ritiene che esso a buon diritto possa rientrare nella terza, definita come contenente «*those where the CJEU seems to consider the fundamental right to data protection as a part of the fundamental right to privacy*»[255]. Queste considerazioni, peraltro, ci consentono di riportare un altro caso particolarmente rilevante in materia e riferibile all'incirca allo stesso periodo, che l'autrice espressamente riconduce a questa terza categoria.

Il riferimento è al celebre caso *Volker und Markus Schecke*, relativo alla pubblicazione dell'indicazione di beneficiari di finanziamenti agricoli, su cui la Corte si pronunciò nel 2010. Nel risolvere la questione pregiudiziale, la Corte affermava: «*Quanto alla necessità della misura, si deve rammentare che l'obiettivo della pubblicazione in questione non può essere perseguito senza tener conto del fatto che esso deve essere conciliato con i diritti fondamentali sanciti dagli artt. 7 e 8 della Carta (v., in tal senso, sentenza 16 dicembre 2008, causa C-73/07, Satakunnan Markkinapörssi e Satamedia, Racc. pag. I-9831, punto 53). Occorre dunque verificare se il Consiglio dell'Unione europea e la Commissione abbiano effettuato un contemperamento equilibrato tra, da un lato, l'interesse dell'Unione a garantire la trasparenza delle proprie azioni e un utilizzo equilibrato delle finanze pubbliche e, dall'altro, la lesione del diritto dei beneficiari interessati al rispetto della loro vita privata, in generale, e alla protezione dei loro dati personali, in particolare. A tale riguardo la Corte ha già dichiarato che le deroghe e le limitazioni alla protezione dei dati personali devono operare entro i limiti dello stretto necessario*»[256]. Il caso merita inoltre considerazione anche per l'attenzione della Corte al principio di proporzionalità per la valutazione delle misure statali di ingerenza e per il richiamo, a tal fine, della giurisprudenza della Corte di Strasburgo[257]. Nello stesso anno, inoltre, una sovrapposizione tra i due diritti veniva in

[255] M. BRKAN, The Court of Justice of the EU, privacy and data protection, *cit*., p. 16 e, più gen. da 13 a 17.
[256] Corte di giustizia, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, 9 novembre 2010, punti 76-77, enfasi aggiunta.
[257] Ibidem: «Infine, quanto alle persone giuridiche beneficiarie di aiuti del FEAGA e del FEASR, e nei limiti in cui esse possono invocare i diritti riconosciuti dagli artt. 7 e 8 della Carta (v. punto 53 della presente sentenza), si deve considerare che l'obbligo di pubblicazione derivante dalle disposizioni della normativa dell'Unione della cui validità si discute non supera i limiti imposti dal rispetto del principio di proporzionalità. Infatti, la gravità della lesione del diritto alla protezione dei dati personali si presenta in maniera differente per le persone giuridiche e per le persone fisiche. Si deve rilevare, a tale riguardo, che le persone giuridiche sono già soggette a un obbligo più gravoso di pubblicazione dei

qualche modo prospettata dalla Corte nella pronuncia di appello sul caso *Bavarian Lager*, discostandosi così dall'approccio suggerito dal Tribunale[258].

Orbene, che le pronunce riferibili a questa categoria risalgano perlopiù al primo decennio Duemila non è un caso, mentre le altre due categorie vengono esemplificate dall'autrice con casi ben più recenti (a partire, essenzialmente, dal 2014)[259]. Ciò si spiega chiaramente col fatto che sarà l'entrata in vigore del Trattato di Lisbona a stimolare "un'evoluzione interpretativa"[260] della Corte al riguardo. Infatti, non solo Lisbona renderà la Carta dei diritti fondamentali giuridicamente vincolante (ai sensi dell'articolo 6 TUE essa "ha lo stesso valore giuridico dei trattati"), ma l'introduzione dell'articolo 16 TFUE attribuirà espressamente una competenza all'Unione in materia di protezione di dati personali, fornendo così nuova base giuridica a ciò che da lì verrà eretto come "nuovo" diritto europeo alla protezione dei dati personali.

Quanto esposto si ritiene momentaneamente sufficiente per un'esaustiva panoramica delle pronunce essenziali che hanno provocato e accompagnato l'evoluzione del diritto europeo alla protezione dei dati personali. A partire da queste consapevolezze, i successivi interventi giurisprudenziali, soprattutto di Lussemburgo, ma anche in vista di quelli di Strasburgo, costituiranno i passaggi salienti del lavoro che si propone e pertanto verranno trattati con riferimento alle argomentazioni da affrontare e sostenere di volta in volta per una comprensione critica dello stato dell'arte sulla protezione dei dati e, perché no, per uno stimolo per prospettive future.

---

dati che le riguardano. Peraltro, l'obbligo per le autorità nazionali competenti di esaminare, prima della pubblicazione in questione, per ogni persona giuridica beneficiaria di aiuti del FEAGA e del FEASR, se la denominazione di quest'ultima identifichi persone fisiche graverebbe tali autorità di un onere amministrativo eccessivo (v., in tal senso, Corte eur. D.U., sentenza K.U. c. Finlandia del 2 marzo 2009, ricorso n. 2872/02, non ancora pubblicata, § 48)», punto 87, enfasi aggiunta.

[258] M. BRKAN, *op. cit.*, p. 14: «*In its judgment, the General Court stressed that 'not all personal data are by their nature capable of undermining the private life of the person concerned', which seems to imply that the fundamental right to data protection has a wider scope of application (…). This seems to be in line with a theoretical approach that Article 8 CFR is to be considered as* lex specialis *in relation to Article 7 CFR. However, at the appeal level the CJEU did not follow this reasoning and again seemed to treat the two rights as overlapping*». Il riferimento è a Tribunale, T-194/04, *Bavarian Lager*, 8 novembre 2007; Corte di giustizia, C-28/08 P, *Bavarian Lager*, 29 giugno 2010, punti 59-61. Tuttavia, si segnala sugli stessi punti la riflessione di senso equivocamente opposto di J. KOKOTT, C. SOBOTTA, op. cit., P. 222: «*The Court of Justice of the European Union in Luxembourg (the Luxembourg Court or CJEU) in the Bavarian Lager case reasoned that compared with the right to privacy, the EU rules on data protection create a specific and reinforced system of protection*».

[259] M. BRKAN, *op. cit.*, laddove riconduce alla prima categoria, per esempio, i casi *Tele2 Sverige* e *Watson* (2016); alla seconda categoria, i casi *Digital Rights Ireland* (2014), *Google Spain* (2014) e *Schrems I* (2015), cfr. pp. 14-17.

[260] Così, infatti, F. BALDUCCI ROMANO, cit.: «Una certa evoluzione interpretativa, comprensibilmente, si registra nella giurisprudenza successiva alla riforma di Lisbona, ove però sovente si continua ad affermare che il diritto alla protezione dei dati personali sarebbe strettamente connesso al diritto al rispetto della vita privata. Tale connessione, per la verità, non appare soltanto sostanziale, cioè relativa al contenuto dei due diritti: essa è anche strumentale, nel senso che serve al giudice comunitario per potersi avvalere del rinvio all'art. 8 della CEDU, relativo al diritto al rispetto della vita privata. Ciò perché, in base alla Carta, laddove essa contenga diritti corrispondenti a quelli garantiti dalla CEDU, il significato e la portata degli stessi devono essere uguali a quelli conferiti da quest'ultima», p 1644. Cfr. anche C. DOCKEY, H. HIJMANS, The Court of Justice as a Key Payer in Privacy and Data Protection: an overview of recent trends in case law at the start of a new era of data protection law, in *European Data Protection Law Review*, n. 3/2019, p.302.

PARTE III

(...) l'uomo
che si sposta
modifica le forme
che lo circondano.

J.L.Borges, Tlön, Uqbar, Orbis Tertius

PARTE III

SOMMARIO: I. Dalla "spinta dello spazio sulla forma" al "moto opposto", e viceversa, in continuo intervallo armonico. Verso una sovranità digitale dell'Unione europea? – 1. Dinamiche di un "ente senza forma". – 2. Il "moto opposto". – 3. …e viceversa, in continuo intervallo armonico. – II. *EU Rule of Law* e protezione dei dati personali. – 1. Il quadro predisposto a partire da Lisbona. – 2. Le autorità indipendenti: portata e implicazioni del controllo. – 3. Il ruolo della Commissione europea. – III. La coerenza tra azione interna ed esterna dell'Unione quanto al rispetto *della EU Rule of Law* nella protezione dei dati personali. – 1. Il principio generale di coerenza nell'azione dell'Unione. – 2. Il meccanismo di coerenza tra le autorità di controllo (e la Commissione).

CAPITOLO I

DALLA "SPINTA DELLO SPAZIO SULLA FORMA" AL "MOTO OPPOSTO", E VICEVERSA, IN CONTINUO INTERVALLO ARMONICO.

VERSO UNA SOVRANITÀ DIGITALE DELL'UNIONE EUROPEA?

1. Dinamiche di un "ente senza forma"

Concluse le premesse indispensabili per l'argomentazione utile a sostenere la nostra tesi, che, lo ripetiamo, indaga se la tendenza verso una sovranità digitale dell'Unione europea possa costituire una plausibile soluzione alle sue crisi di legittimazione, è necessario procedere alla comprensione delle dinamiche che muovono attualmente il complesso congegno costituito dal processo di integrazione europea e della sua affermazione a livello globale.

Molti spunti introdotti in precedenza verranno quindi spesso ripresi e sviluppati, per poter meglio definire il *milieu* della nostra ricerca, che si palesa come punto di partenza, e non di arrivo, da cui necessariamente emanciparci per rivelare ciò che rappresenta quasi un paradosso, ossia l'ostinazione di voler costringere in una "forma" ciò che per sua stessa natura non ha, e dunque ontologicamente non è, forma: il processo di integrazione europea. Un processo, in quanto tale, in *moto perpetuo*, che subisce spinte esterne e produce importanti pressioni verso l'esterno, e rispetto al quale tali spinte e pressioni da/verso l'esterno si sono alternate nel tempo e si producono ora anche simultaneamente, richiamando così l'idea di intervalli armonici, in un andamento che continua a plasmare e rimodellare l'ente, che, nel frattempo, continua a "muoversi" e così a mutare.

Così inteso, il processo produce e subisce inevitabilmente e fisiologicamente delle "crisi" che, come abbiamo detto, pongono sempre in ultima analisi dubbi sulla legittimazione dell'ente. Per questo motivo, considerate le continue spinte e rotture, pare più corretto indicare l'Unione come *un ente senza forma*: non solo perché, come detto, si tratta di un ordinamento *sui generis* nel panorama internazionale, ma anche, e soprattutto, perché proprio nel cercare di definire, e dunque 'stabilire', le caratteristiche specifiche di tale "nuovo" ente, queste stanno intanto mutando.

Prendere atto di questi aspetti è molto utile, trattandosi di dinamiche non semplici e neppure del tutto assodate, dunque anche suscettibili di confutazione. Tuttavia, per quanto necessaria, l'eziologia delle crisi di legittimazione dell'Unione europea non parrebbe, in quanto tale, sufficiente per suggerire possibili scenari di soluzione rispetto alla questione che essa pone e che si sostanzia in: *perché* (oggi, e soprattutto domani) l'Unione, perché dovremmo averne (ancora) bisogno.

Qui, dunque, emerge l'importanza della dimensione digitale.

L'attenzione verso un altro "nuovo" spazio, squisitamente privo di forma, sfornito di regole e definizioni, ma soprattutto di tutele (perlomeno ai pur recenti albori), si presterebbe ad essere la dimensione in cui l'Unione, oggi, potrebbe effettivamente trovare una possibile risposta alla sua crisi di legittimazione. L'Unione, ente privo di forma, troverebbe cioè nella dimensione digitale un'occasione per *dare forma* a uno spazio che, ampliandosi ed intricandosi sempre di più, sembrerebbe esigere regole e definizioni per favorire e perfezionare il suo stesso funzionamento.

Utilizzando le peculiarità proprie della *EU rule of law*, ossia il *diritto* come *potere*, e in particolare la *regolamentazione* fondata su certi *valori*, dunque insistendo sulla necessità di predisporre *tutele* nello spazio digitale, l'Unione si è candidata per prima a "modellarne" in questo senso gli orientamenti e così, a partire da questo, starebbe cercando in quello spazio dei modi per conferire a sé stessa legittimazione.

Intesa così, a nostro parere la "sovranità digitale dell'Unione europea" si spiegherebbe allora come il tentativo, per l'ente, di legittimarsi, di trovare una soluzione all'attuale crisi di legittimazione, in uno 'spazio' nel quale il suo intervento può essere effettivamente riconosciuto come indispensabile.

Questo non significa che tale intervento non porti con sé contraddizioni o sia scevro da perplessità, che infatti verranno di seguito esposte, nel verificare l'effettività di tale ragionamento nonché nel presentare prospettive nel prossimo futuro; tuttavia, significa semplicemente che l'anelito verso la "sovranità" di un ente che per definizione ne sarebbe privo può comprendersi massimamente (almeno, per cominciare) nel digitale, ovvero in uno spazio che in quanto "nuovo" è privo di "sovrano" ed è quindi, al netto delle dinamiche di mercato, da conquistare.

2. Il "moto opposto"

A sostegno del ragionamento esposto, prima di passare alla dimostrazione degli elementi che già conducono verso un'idea di "sovranità digitale dell'Unione europea", occorre ancora soffermarsi a condividere le elaborazioni di studiosi che si sono rivelate particolarmente utili a tal fine.

Il riferimento è proprio al "moto opposto" rispetto a quello presentato nella Parte I, ossia quello che si riferiva alla "*spinta dello spazio sulla forma*" e che costituirebbe il primo tassello del nostro ragionamento, per la comprensione del quale abbiamo considerato calzante il riferimento iconico alla natura morta di Cezanne. Da lì, il secondo tassello che andremo ora a delineare, è un "moto" che partirebbe invece proprio dall'interno – e per l'interno – di quella "forma" (impropriamente intesa) e che, più o meno consapevolmente (per nulla, in verità, agli esordi) avrebbe delle ripercussioni sempre più notevoli verso lo spazio esterno, tali da influenzare soggetti e fenomeni terzi non altrimenti coinvolti. Il diritto alla protezione dei dati personali è, come si vedrà, uno (ma non l'unico) tra i settori in cui più chiaramente è ravvisabile l'operatività di tale moto. Per comprenderlo, ci serviremo senz'altro di ciò che è stato individuato come c.d. *normative power* dell'Unione europea, ma soprattutto, e più ampiamente, del già accennato c.d. *Brussels effect* elaborato da Anu Bradford.

Va subito precisato che non è errato intravedere una qualche sequenza cronologica tra i moti che stiamo presentando come performativi dell'Unione europea, per quanto li consideriamo anche attualmente simultanei. Come si è cercato di delineare nella Parte I, infatti, le spinte esterne volte a modellare il processo di integrazione europea dal di fuori sembravano più pressanti e più incisive nel primo periodo della storia dell'integrazione rispetto a quelle che dall'interno potevano avere delle influenze verso l'esterno. Ciò non significa che delle dinamiche interne non esistessero sin dall'inizio, anzi. Significa piuttosto che esse erano rivolte consapevolmente alla *sola* definizione del processo di integrazione in quanto tale, per la costruzione e il funzionamento di un mercato unico europeo che consentisse un'armonizzazione tra le differenziate normative degli Stati membri[1].

[1] A. BRADFORD, *The Brussels Effect – How the European Union Rules the World*, Oxford, 2020, p. 7. «*For a long time, the Brussels effect was an ancillary and largely unintended by-product of a regulatory agenda that was driven by internal motivation. Only more recently, a conscious external agenda has emerged alongside this internal one*».

Il c.d. Brussels effect: origini ed evoluzione

Prima di definire quello che la Bradford ha chiamato "effetto Bruxelles" e che rappresenta la più chiara spiegazione, tra le varie che indicheremo, di ciò che qui vogliamo intendere con '*moto opposto*', è molto utile chiarire ciò che l'autrice puntualizzava essere l'origine di questo moto, tutt'altro che intenzionalmente volto a provocare esternalizzazioni. Prospettando a fondamento del proprio discorso l'attenzione verso la costruzione del mercato interno in un modo peculiare, che è divenuto *il modo* comunitario, ossia "*promoting European integration via regulation*", l'autrice mostrava (affinando considerazioni sviluppate da altri, specie quanto alla concezione di *Regulatory State*) che elemento essenziale in questa costruzione sia stata (e sia ancora) *l'armonizzazione degli standard* tra i diversi Stati membri, senza la quale la stessa idea di un mercato interno non potrebbe chiaramente esistere, costringendo imprese a confrontarsi con diverse legislazioni per ogni Stato e quindi modificare le proprie offerte di conseguenza, con tutti i costi che ciò comporterebbe[2].

Tale armonizzazione sarebbe, in particolare, avvenuta tramite il *mutuo riconoscimento* (a partire dalla giurisprudenza *Cassis de Dijon*) degli standard nazionali e la "*minimum harmonisation*"[3], in particolare nel senso di "*upward harmonization*" ossia volta al rialzo degli standard con conseguente previsione di meccanismi (quali i fondi strutturali) per allineare gli Stati membri dotati di garanzie meno elevate[4]. Peraltro, da questi propositi di integrazione economica interna sempre più fitta derivarono anche le attenzioni verso dei *valori non-economici comuni* da preservare e porre a fondamento della stessa integrazione, anche per le istituzioni europee al fine di legittimare il proprio operato[5].

Ciò chiarito, come sarebbe avvenuto allora che da questi moti interni, da queste attenzioni rivolte alla costruzione di un sistema integrato che funzionasse in quanto tale, si sarebbero via via

[2] Ibidem, p. 9: «*harmonized standards became a key goal for European integration early on, serving both the specific substantive goal (such as environmental protection) and the broader economic and political goal of achieving greater market integration*».

[3] Ibidem, p. 10, in cui l'autrice continuava: «*Minimum harmonisation calls for a common EU standard only to the extent that is necessary to ensure the functioning of the single market, while preserving the flexibility for member states to enact more stringent standards domestically*», o ancora «*Because these national regulations risk fragmenting the single market, the EU is prompted to harmonize standards at the EU level in an effort to preserve the integrity of the common market*».

[4] Ibidem: «*Notably, the EU has tended not to pursue "downward harmonization", which would entail letting the member states with low levels of regulation set the common standard for everyone. Instead, (…), it has typically pursued "upward harmonization"and regulated toward more stringent standards of its member states – something which (…) has been a key factor in extending the Brussels Effect*», pp. 10-11.

[5] Ibidem, p. 11: «*As economic integration deepened, Europeans began to resist the liberalization agenda that was seen as a threat to these non-economic values. To defend the continued economic integration and to vest themselves with greater legitimacy, EU institutions thus set out to expand the integration agenda to these other values, adopting stringent standards – in areas such as environmental protection, food safety, or data privacy – to ensure that economic gains from integration are not pursued without protecting quality of life. Thus, upward harmonization of regulatory standards was seen as necessary to ensure continuing political support for economic liberalization*», enfasi aggiunta.

realizzate delle pulsioni anche verso l'esterno? «*It has been sufficient to simply generate regulations to strengthen its single market, with external influences emerging as incidental by-products of this internal goal*»[6].

Sarebbero, dunque, le stesse ragioni che hanno spinto verso l'armonizzazione interna delle legislazioni tra Stati membri, attraverso la regolamentazione sovranazionale, a produrre spontaneamente le condizioni per l'esternalizzazione degli standard così generati: man mano che il mercato interno andava incrementandosi, le stesse regole e logiche volte a proteggerlo facevano emergere corrispondenti esigenze sempre in ragione del suo funzionamento (quali quella di evitare distorsioni della concorrenza) anche nella dimensione esterna. Gli standard comuni predisposti dalle istituzioni sovranazionali per gestire il mercato unico avrebbero, così, subìto un'esternalizzazione non tanto per volontà delle istituzioni stesse, bensì primariamente da parte degli operatori di quel mercato (perlopiù imprese multinazionali) tenuti a conformarsi alle sue regole per potervi operare e che così hanno poi "trascinato", via via, quegli standard anche a livello globale: «*This internally driven, passive externalization of the EU rules has been particularly effective in that the EU institutions have only had to generate the consensus to pursue a goal that lies at the heart of the EU project: European integration and the establishment of the single market. Often, EU standards have been externalized as a by-product of that mission, not by the EU institutions but by market participants who need to comply with EU rules and who often decide to apply the EU standard globally*»[7].

Che le esigenze di mercato e gli interventi degli operatori privati abbiano stimolato questo spontaneo e involontario effetto esternalizzante rappresenta però solo una parte del moto individuato nella sua interezza come "effetto Bruxelles". Le istituzioni europee divennero infatti sempre più consapevoli dell'impatto esterno della regolamentazione interna, in connessione con la più generale accresciuta sensibilità rispetto allo sviluppo del commercio globale a partire dagli anni Novanta, «*where the external effects of countries' regulatory policies began to occupy the global trade agenda*»[8].

[6] Ibidem, p. 19.
[7] Ibidem, p. 20.
[8] Ibidem, p. 18, dove continua: «*Various domestic regulations were increasingly seen as non-tariff barriers, promoting multilateral efforts to abolish them. These negotiations culminated in the establishment of the WTO in 1995. Partly for this reason, the external effects of the EU's regulatory policies became a more salient issue, both within and outside the EU*».

In particolare, il riferimento è ad alcuni interventi della Commissione soprattutto del primo decennio Duemila[9]. Vero è che quel periodo è legato al Trattato di Lisbona che, come vedremo a breve (cfr. *infra*, Capitolo II), si caratterizza rispetto alle precedenti revisioni per una spiccata vocazione verso l'esterno, e ciò non solo in termini di regole legate a interessi economici e commerciali ma anche e soprattutto con riferimento ai valori fondanti[10]. Nondimeno, queste consapevolezze a livello istituzionale arrivarono a seguito delle spontanee influenze del mercato.

In tal senso, dunque, la Bradford distingueva chiaramente tali due momenti identificandoli come "*de facto Brussels Effect*" e "*de jure Brussels Effect*" che insieme costituirebbero nel complesso l'Effetto Bruxelles: «*The de facto Brussels Effect explains how global corporations respond to EU regulations by adjusting their global conduct to EU rules. No regulatory response by foreign governments is needed; corporations have the business incentive to extend the EU regulation to govern their worldwide production or operations. The de jure Brussels Effect – which refers to the adoption of EU-style regulations by foreign governments – builds directly on the de facto Brussels Effect: after multinational companies have adjusted their global conduct to conform to EU rules, they have the incentive to lobby EU-style regulations in their home jurisdictions. This ensures that they are not at the disadvantage when competing domestically against companies that do not export to the EU and that, therefore, have no incentive to conform their conduct or production to costly EU regulations*»[11]. Dunque, soprattutto alla luce di questi due momenti consequenziali, è possibile chiarire che il "*Brussels effect*" viene definito come «*the EU's unilateral ability to regulate the global marketplace*»[12] che si realizzerebbe quindi quale risultato dell'interazione tra la normativa posta dall'Unione e la capacità delle forze di mercato di "esternalizzare" quelle norme in altri mercati[13]. Inoltre, per la realizzazione del *Brussels Effect*, la Bradford specificava che

[9] In particolare, l'autrice individua un cambio di prospettiva da parte della Commissione, con acquisizione di maggiore consapevolezza al riguardo e la volontà di incrementarne la portata, palesato dal 2007, tra gli altri, per esempio con lo *staff working document* su "*The external dimension of the single market review*" in occasione della Comunicazione dedicata a "Un mercato unico per il XXI secolo"cfr. Commission staff working document - *The external dimension of the single market review - Accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A single market for 21st century Europe* {COM(2007) 724 final}.
Per ciò che rileva ai nostri fini legati alla protezione dei dati personali, la stessa autrice nota, cfr. p. 22, come ciò si fece evidente sin dalle prime Comunicazioni della Commissione al riguardo, quali quella del 2009 "*Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini*"[9] e soprattutto quella del 2010 "*Un approccio globale alla protezione dei dati personali nell'Unione europea*", cfr. COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI - *Un approccio globale alla protezione dei dati personali nell'Unione europea* /* COM/2010/0609 def. */.
[10] La stessa autrice rileva infatti, al riguardo: «*the 2007 Lisbon Treaty vests the EU with an explicit mandate to project its internal norms and values externally, emphasizing the importance of those values in the EU's relations with the wider world*», op. cit., p. 23.
[11] Ibidem, p. 2.
[12] Ibidem, p. 1.
[13] Ibidem, p. 2, letteralmente: «*the interplay between EU regulations and the market forces' ability to externalize those regulations in different markets*».

interverrebbero cinque precise condizioni, che qui possiamo solo indicare: *market size*; *regulatory capacity*; *stringent regulations*; *inelastic targets*; *non-divisibility*[14].

Orbene, un effetto Bruxelles operante in entrambe le accezioni parrebbe chiaramente ravvisato nel diritto alla protezione dei dati personali e, in particolare, nel GDPR. Il suo sviluppo avrebbe, infatti, manifestato proprio quelle dinamiche, dimostrando come in principio proprio l'opportunità sovranazionale di regolamentare il mercato interno avrebbe stimolato, come anche in altri settori funzionali, l'armonizzazione delle normative nazionali sulla circolazione e protezione dei dati[15], (come si è visto, peraltro, trattando l'evoluzione storica di tale diritto; cfr. *supra*, Parte II). Inoltre, e come si vedrà (*infra*, Parte IV), esso confermerebbe gli ulteriori passaggi nell'attuale consapevolezza dell'importanza dell'esternalizzazione degli standard europei sulla protezione dei dati personali.

In particolare, la Bradford riconosceva l'operatività del *de facto Brussels Effect*, arrivando ad affermare che «*today many multinational companies have only one company-wide privacy policy – and it is that of the EU*»[16], nonché del *de jure Brussels Effect*, illustrando le ragioni della fortuna della diffusione di "*EU-style privacy regimes*" che avverrebbe anche, tra le altre, per l'esigenza di Paesi terzi di ottenere una "decisione di adeguatezza" ai fini del trasferimento di dati dall'Unione europea (*ex* art. 45 GDPR), che così incentiverebbe i primi ad emulare il regime predisposto dalla seconda[17].

Limitandoci a questi tratti essenziali ma sufficienti per comprendere l'operatività della teoria della Bradford ai nostri fini, va detto che la stessa autrice riconosceva il rilievo anche di altri meccanismi attraverso i quali l'Unione eserciterebbe la propria influenza verso l'esterno e che andrebbero distinti dall'effetto Bruxelles, pur potendosi considerare ad esso complementari e/o supplementari.

---

[14] Ibidem, pp. 25-65. In breve, l'autrice descrive le singole condizioni come segue: «*market size, as a proxy for the jurisdictions' ability to exercise regulatory authority over foreign entities. (…) sufficient regulatory capacity to exercise global regulatory authority. This entails having in place institutional structures hat are capable of adopting and enforcing regulations effectively. In addiction, these regul6atory institutions must promulgate stringent regulatory standards, reflecting the preferences of key stakeholders in the jurisdiction. A global regulatory authority is also tied to a choice of regulating inelastic targets (…). Only stringent standards aimed at targets that cannot flee the jurisdiction ensure that a country's regulations will not be constrained by market forces or other jurisdiction's regulatory responses. Finally, unilateral standards become global standards only when (…) a target's conduct or production is non-divisible across global markets*», pp. 25-26.

[15] Ibidem, p. 137: «(…) *it was politically more feasible for the EU to harmonize upward than downward, elevating the data protection standards in low-regulation member states rather than forcing high-regulation member states to weaken the data protection laws already governing their domestic markets. While these internal motivations to integrate the European market provided the initial impetus for regulating data privacy, the EU's current regulatory pursuits are also shaped by external motivations. Given the global nature of data processing and the importance of cross-border transfer of data – not just within the EU but across global markets – the EU has recognized the importance of promoting international standards for the protection of personal data*».

[16] Ibidem, p. 143.

[17] Ibidem, pp. 149-150. Ma anche, p. 140: «*many US companies are adjusting their global business practices to reflect European norms, making data privacy one of the most powerful examples of the Brussels Effect*».

È indispensabile ai nostri fini richiamarli, sia per come delineati in rapporto all'effetto Bruxelles, sia considerati in quanto tali (e per come esposti dai relativi studiosi), proprio perché anch'essi concorrono a spiegare e comporre ciò che qui chiamiamo "moto opposto" e che, insieme col primo, partecipa a configurare le dinamiche attuali del processo di integrazione europea.

Orbene, gli altri canali di influenza dell'Unione verso l'esterno, a livello globale, che interverrebbero a completare, ampliare o sostituire l'effetto Bruxelles, sarebbero dunque sia unilaterali che non: ciò che è stato teorizzato da Manners come "*normative power Europe*"; tecniche legislative come extraterritorialità o estensione territoriale della normativa europea; l'armonizzazione "*treaty-driven*" opposta a quella "*market-driven*" realizzata con l'effetto Bruxelles *de facto*[18]. Come si capisce, ad eccezione della "*treaty-driven harmonization*" che, avendo il suo fondamento nella cooperazione, esprime la possibile influenza bilaterale o multilaterale dell'Unione, gli altri fenomeni esprimerebbero l'influenza unilaterale dell'Unione oltre i suoi propri confini verso l'esterno e quindi sono stati intesi insieme da alcuni studiosi come il c.d. "*Global reach of the EU law*": «*What do we mean by the global reach of EU law? It includes the extraterritorial application of EU law, the presence of territorial extension, and the so-called 'Brussels Effect', all phenomena concerned with the effects of unilateral legislative instruments and regulatory action beyond the EU's borders*»[19].

Ebbene, nella nostra proposta, il "moto opposto" sarebbe proprio l'insieme di tutti questi fenomeni, sia unilaterali, che bilaterali o multilaterali (ancorché meno incisivi dei primi), che dimostrano come l'Unione possa essere più o meno capace di esercitare un'influenza verso l'esterno. Procediamo, pertanto, ad illustrare gli aspetti caratterizzanti tali fenomeni, per come teorizzati dai vari autori, al fine di poterne poi rinvenirne, o meno, traccia nella successiva analisi pratica (*infra*, Parte IV).

Il c.d. Normative Power Europe

Quanto al primo fenomeno, risale agli inizi del nuovo millennio la teorizzazione di Manners del "*Normative Power Europe*", presentato nel pieno dibattito sul ruolo internazionale dell'Unione europea in contrapposizione a certe visioni di "*Civil or Military Power Europe*" che l'autore considerava errate essenzialmente per «*their unhealthy concentration on how much like a state the EU looks. The concept of normative power is an attempt to refocus analysis away from the empirical emphasis on the EU's institutions or policies, and towards including cognitive processes,*

[18] Ibidem, p. 67.
[19] M. CREMONA, J. SCOTT, Introduction - EU Law Beyond EU Borders, in M. CREMONA, J. SCOTT (Eds), *EU Law Beyond EU Borders – The Extraterritorial Reach of EU Law*, Oxford University Press, 2019, p. 1.

with both substantive and symbolic components»[20]. Il "potere normativo dell'Unione" consisterebbe dunque nella capacità persuasiva che l'ente rivela nelle sue relazioni internazionali e, più in generale, nella sua azione verso l'esterno[21].

Proprio perché anche funzionale alla comprensione dell'identità internazionale dell'Unione, l'autore ha concepito il "*normative power*" dell'Unione a partire dalla sua "differenza normativa" data dalle "norme costituzionali" come elementi distintivi della sua identità internazionale[22]: «*The EU is founded on and has as its foreign and development policy objectives the consolidation of democracy, rule of law, and respect for human rights and fundamental freedoms*»[23]. Pur insistendo sulla "differenza normativa" dell'Unione che riposerebbe proprio nella sua base normativa costituita dai predetti principi/valori fondanti (proprio come dicevamo *supra,* Parte I), ciò sarebbe però solo il punto di partenza (di per sé, non sufficiente) per indicare l'Unione quale "*normative power*". Lo scarto fondamentale a tal fine risiederebbe proprio nella *diffusione* di quelle norme dell'Unione nel contesto internazionale, che avverrebbe secondo l'autore attraverso sei fattori: "contagio", ossia diffusione involontaria di idee dall'Unione agli altri attori politici; "*informational diffusion*" come conseguenza di comunicazioni strategiche; "*procedural diffusion*", tramite accordi internazionali o partecipazione ad altre organizzazioni o interventi nell'ambito delle politiche di allargamento; "*transference*" che avviene negli scambi che intercorrono tra l'Unione e terze parti; "*overt diffusion*" che discenderebbe dalla presenza fisica dell'Unione in Paesi terzi; "*cultural filter*" che ivi stimolerebbe ulteriori consapevolezze[24].

Dunque, il "*normative power Europe*" veniva delineato come quell'attitudine dell'Unione di performare il sistema internazionale, proprio in virtù di ciò che la identifica[25]: «*the most important factor shaping the international role of the EU is not what it does or what it says, but what it is. Thus my presentation of the EU as a normative power has an ontological quality to it – that the EU can be conceptualized as a changer of norms in the international system; a positivist quantity to it –*

[20] I. MANNERS, Normative Power Europe: A Contraddiction in Terms?, in *Journal of Common Market Studies*, 2002, Vol 40. No 2, p. 239; per "*Civil or Military Power Europe*" si veda p. 236 ss. L'autore, infatti, specificava la sua posizione criticando le altre come segue: «*Thus both Duchêne and Bull shared an interest in the maintenance of the status quo in international relations which maintained the centrality of the Westphalian nation-state*», p. 238.
[21] Ibidem, p. 239: «(…) *the notion of a normative power Europe is located in a discussion of the 'power over opinion', idée force, or 'ideological power', and the desire to move beyond the debate over state-like features through an understanding of the EU's international identity*».
[22] Ibidem, p. 241, laddove si legge precisamente: «(…) *its constitutional norms represent crucial constitutive factors determining its international identity*».
[23] Ibidem.
[24] Ibidem, pp. 244-245.
[25] Performare al punto da incidere su ciò che in quel sistema può considerarsi "normale", cfr. ibidem, p 253: «*Thus the different existence, the different norms, and the different policies which the EU pursues are really part of redefining what can be 'normal' in international relations. Rather than being a contradiction in terms, the ability to define what passes for 'normal' in world politics is, ultimately, the greatest power of all*».

that the EU acts to change norms in the international system; and a normative quality to it – that the EU should act to extend its norms into the international system»[26].

La propensione dell'Unione ad influenzare attraverso questa capacità di persuasione è stata messa in evidenza anche da Anu Bradford per distinguerla dal *de facto Brussels effect* e rilevarla come fonte di attrazione ed emulazione da parte di Paesi terzi quando l'effetto Bruxelles da lei evidenziato, per mancanza delle condizioni (essenzialmente, relative alle logiche di mercato), non riesce ad operare[27].

Extraterritorialità ed estensione territoriale del diritto dell'Unione

Queste considerazioni conducono, poi, al carattere di *extraterritorialità* del diritto dell'Unione, quale ulteriore fenomeno attraverso cui l'ente influenza l'esterno e dunque ulteriore espressione del 'moto opposto', che va analizzato con il concetto di "*estensione territoriale*", proposto dalla Scott in confronto con il primo e della cui analisi su entrambi pertanto ci serviremo[28], anche al fine di introdurre riflessioni, nello specifico settore di nostro interesse, sulla misura dell'attuale ambito di applicazione territoriale della normativa europea sulla protezione dei dati personali (art. 3 GDPR), che saranno poi utili per la comprensione dell'analisi della giurisprudenza dedicata (*infra*, Parte IV).

La questione della extraterritorialità del diritto (in senso lato), che qui non può neppure sufficientemente accennarsi nelle sue grandi linee, è tra le più controverse del diritto internazionale riguardando essenzialmente la portata del principio di territorialità. Per introdurre la nostra breve analisi al riguardo, valgano, tra tutti, le riflessioni seguenti, particolarmente utili ai nostri fini proprio perché rimarcano il legame tra questi temi e questioni di legittimazione del potere: «sempre di più gli Stati tendono a muoversi con disinvoltura oltre i confini territoriali della propria giurisdizione, al punto che siamo indotti a chiederci se la legittimazione di queste ipotesi di esercizio dei poteri statali non debba ravvisarsi in qualcosa di diverso dal territorio e dalla signoria che su di esso lo Stato esercita. Intendo riferirmi ai numerosi esempi di giurisdizione

[26] Ibidem, p. 252, sottolineato aggiunto.
[27] A. BRADFORD, *op. cit.*, p. 81: «*The normative appeal of EU rules may explain the willingness of foreign courts to cite and emulate EU laws and ECJ judgments, even in instances where no Brussels Effect takes places. (…) Amedeo Arena reached the same conclusion, observing that EU principles are seen as having worked well for Europe and therefore can serve as an example for other regions pursuing deeper integration. In addition to the EU model's normative appeal, several commentators note how the EU actively promotes the replication of its institutional structures. The Eu provides legal and technical expertise and financial support to many third states implementing their rules. Notably, studies of the EU's influence over foreign courts reveal no coercion, but rather persuasion*».
[28] Il riferimento è a J. SCOTT, Extraterritoriality and Territorial Extension in EU Law, in *American Journal of Comparative Law*, Vol. 62, 2014, pp. 87-126, in cui si legge infatti: «*This focus on the EU as a global regulatory power has been accompanied by a shift in perspective on extraterritoriality in EU law*», p. 88.

extraterritoriale, alla complessa fenomenologia della giurisdizione universale e da ultimo al diffuso convincimento che la società globale nella quale oggi viviamo sarebbe una società all'interno della quale la dimensione territoriale non rivesta il ruolo di canone preferenziale di legittimazione del potere. Insomma *una società deterritorializzata o nella quale la legittimazione del potere sovrano non si fonderebbe più o comunque non in maniera esclusiva sulla sua dimensione territoriale*»[29]. Di questo, evidentemente, la "*sovranità digitale*" alla quale l'Unione tenderebbe, nel senso che abbiamo brevemente illustrato e che cercheremo meglio di dimostrare con questo lavoro, rappresenta la testimonianza attualmente più evocativa; pertanto, è opportuno analizzare le peculiarità dell'extraterritorialità ai nostri fini.

La professoressa Scott ha elaborato la concezione di "estensione territoriale" distinguendola dall'extraterritorialità di una certa normativa come segue: nell'ultimo caso, non vi sarebbe una connessione territoriale tra il soggetto e l'ente regolatore, la cui normativa si applica però al primo in virtù di elementi *diversi*; nel primo caso, sussiste una rilevante connessione territoriale tra il soggetto e l'ente regolatore ma l'applicazione della determinata misura avverrebbe, per previsione di legge, in virtù del realizzarsi di determinate condotte o circostanze all'estero[30]. Successivamente alle prime elaborazioni, più di recente l'autrice ha precisato che si avrebbe estensione territoriale quando «*Although the application of a measure is triggered by a territorial connection, evaluation of compliance with the measure requires an assessment of foreign conduct and/or third country law*»[31], dunque ridefinendo la nozione con la necessità di una valutazione della condotta straniera e/o del sistema del Paese terzo di riferimento.

Sin dai suoi primi studi, invero, l'autrice rilevava rispetto all'Unione europea che raramente potessero riscontrarsi situazioni di extraterritorialità, potendo invece all'opposto notarsi un sempre maggiore incremento della pratica di "estensione territoriale"[32], che si rivelava particolarmente "pervasiva": sia nel senso che si avrebbe quando una certa normativa tiene conto della condotta o delle circostanze al di fuori dei confini dell'Unione, modellandone di conseguenza il perimetro di intervento; ma anche nel senso che consentirebbe talvolta di promuovere l'effettiva applicazione

[29] R. SAPIENZA, Oltre i territori. Diritto internazionale, giurisdizioni e "nuove geografie", in A. DI STEFANO (a cura di), *Un diritto senza terra? Funzioni e limiti del principio di territorialità nel diritto internazionale e dell'Unione europea*, Atti e contributi del X Incontro di Studio fra i giovani cultori delle materie internazionalistiche – Catania, 24-25 gennaio 2013, I, Giappichelli, 2015, p. 139, corsivo aggiunto.

[30] J. SCOTT, Extraterritoriality and Territorial Extension in EU Law cit., p. 90: «*Extraterritoriality The application of a measure triggered by something other than a territorial connection with the regulating state. Territorial Extension: The application of a measure is triggered by a territorial connection but in applying the measure the regulator is required, as a matter of law, to take into account conduct or circumstances abroad*».

[31] J. SCOTT, The Global Reach of the EU Law, in M. CREMONA, J. SCOTT (Eds), *EU Law Beyond EU Borders – The Extraterritorial Reach of EU Law*, Oxford University Press, 2019, p. 22.

[32] J. SCOTT, Extraterritoriality and Territorial Extension in EU Law, *cit*., pp. 89, 94, 113-114; ID., The Global Reach of the EU Law, *cit*., p. 24.

delle norme stesse dei Paesi terzi; e ancora nel senso che in qualche modo stimolerebbe anche la conclusione di accordi internazionali e quindi incoraggerebbe gli Stati in tale direzione, influenzando di conseguenza l'evoluzione del diritto internazionale[33].

Da simili valutazioni, l'autrice rilevava che l'estensione territoriale del diritto dell'Unione si caratterizzerebbe per il suo "*orientamento internazionale*", per questa specifica vocazione che la distinguerebbe (e, dunque, giustificherebbe le critiche rivolte dall'Unione) dalle analoghe pratiche attuate dagli USA[34], per arrivare così a concludere che «*the EU's preference for territorial extension over extraterritoriality is significant because it reflects a commitment on the part of the EU to respect the limits on rescriptive jurisdiction laid down by public international law. As such, and notwithstanding the unilateral nature of many of the measures at stake, it forms part of the broader international orientation which pervades EU measures of this kind*»[35].

Nei suoi più recenti studi sul tema, poi, l'autrice ha avanzato degli sviluppi molto interessanti, di cui due in particolare risaltano ai nostri fini. Il primo è dato dalla chiara differenza tra la totale assenza di riferimento alla *data protection* nei primi studi sull'estensione territoriale e, al contrario, l'ammissione espressa, negli ultimi studi, che la protezione dei dati personali nell'Unione europea e il correlato trasferimento verso Paesi terzi ne costituiscano uno dei principali esempi: «*Some examples of territorial extension are well known and highly controversial. Among these, I would include the EU's (…) well-known practice of rendering the transfer of personal data to third countries contingent upon the country in question having adequate data protection policies in place*»[36]. Peraltro, proprio rispetto al trasferimento dei dati si notava l'emersione di perplessità quanto al criterio del collegamento territoriale: «*The existence of a territorial connection cannot be considered conclusive, given that there will often be disagreement about what constitutes a territorial connection and such connections vary considerably in type and degree. The example of data protection is telling in this respect. Here, the EU is relying upon a novel and flimsy territorial connection, namely the fact that data processors are using computer equipment located within the*

[33] J. SCOTT, Extraterritoriality and Territorial Extension in EU Law, cit., pp. 106 e 108. Il richiamo al carattere "pervasivo" è a p. 114 e verrà spiegato nel prosieguo.
[34] J. SCOTT, Extraterritoriality and Territorial Extension in EU Law, cit., pp. 114-115: «*An international orientation is inherent in the EU's very preference for territorial extension. This preference reflects the EU's often repeated conviction that prescriptive jurisdiction must be exercised in a manner that is consistent with public international law, and its belief that territorial extension complies with this standard*», sottolieato aggiunto. Nello stesso senso, per esempio, l'autrice continuava: «*An international orientation is also reflected in the EU practice of territorial extension in that it is oriented towards the enforcement of international standards and/or towards contributing to the attainment of objectives that have been internationally agreed*.», p. 116. Si veda su questo anche p. 125.
[35] Ibidem, sott. aggiunto.
[36] J. SCOTT, The Global Reach of the EU Law, in M. CREMONA, J. SCOTT (Eds), *EU Law Beyond EU Borders – The Extraterritorial Reach of EU Law*, Oxford University Press, 2019, p. 21.

EU; for example, by collecting data from EU-located computers by means of 'cookies', JavaScript, ad banners and spyware»[37].

Il secondo sviluppo di rilievo è dato dall'analisi della relazione tra l'effetto Bruxelles teorizzato dalla Bradford[38] e la concezione dell'estensione territoriale. «*there is no necessary relationship between territorial extension and the Brussels Effect. Some measures that generate the Brussels Effect may be imbued with territorial extension, but many others will not. And similarly, not all measures that give rise to territorial extension will give rise to the Brussels Effect. Nonetheless, despite the absence of any inherent relationship between territorial extension and the Brussels Effect, it does appear that territorial extension is a phenomenon that can sometimes serve to promote the emergence of the Brussels Effect. If this is accepted, it has implications for our understanding, and indeed the operation, of the Brussels Effect*»[39]. Secondo la Scott, insomma, l'estensione territoriale potrebbe in qualche misura "alimentare" l'effetto Bruxelles, essenzialmente stimolando l'emersione delle condizioni per il suo realizzarsi e pertanto «*it is therefore a mistake to overlook the concept of territorial extension when developing an account of the Brussels Effect*»[40]. Nondimeno, secondo le più recenti analisi della Bradford, che distingue l'effetto Bruxelles da extraterritorialità ed estensione territoriale, questi ultimi sarebbero più che altro meccanismi alternativi: «*These mechanisms just mentioned, while reflecting different dynamics, offer pathways other than the Brussels Effect for the EU to shape regulatory environment unilaterally*»[41].

Invero, ai fini del nostro lavoro non è indispensabile stabilire i termini precisi del rapporto tra questi fenomeni, che possono apparire per certi versi complementari e per altri sovrapposti. Sicuramente, per ciò che ci interessa, tutti rappresentano manifestazioni di quel "moto opposto" che stiamo cercando di mostrare, quale capacità dell'UE di influenzare l'esterno, in tali casi "unilateralmente". Ciò è tanto più vero se si considera il settore da noi prediletto, ossia quello della protezione dei dati personali, rispetto al quale la definizione dell'ambito di applicazione territoriale della normativa dedicata (la Direttiva madre, prima; il GDPR, adesso) è stata ed è ancora oggetto di ampi dibattiti anche istituzionali oltre che di interventi giurisprudenziali particolarmente rilevanti per la materia, di cui si dirà meglio. Qui ci limiteremo a porre le basi per le successive valutazioni al riguardo, tenendo in considerazione che esperti già da qualche tempo considerano di lana caprina la questione

[37] Ibidem, p. 39.
[38] L'autrice espose la sua teoria per la prima volta in una pubblicazione del 2012 per poi svilupparla in altri scritti, prima di perfezionare i risultati con la monografia già citata. Il riferimento è ad A. BRADFORD, The Brussels Effect, 107 *Northwestern Uiversity Law Review* 1 (2012), pp. 1-68; ID., Exporting Standards: The Externalization of the EU's Regulatory Power via Markets, 42 *International Review of Law and Economics* (2015) 158-173.
[39] J. SCOTT, *The Global Reach*, cit., pp. 32-33, sott. aggiunto.
[40] Ibidem, p. 35. Più in generale, si vedano pp. 33-34.
[41] A. BRADFORD, *op. cit.*, p. 68.

delle possibili differenziazioni tra extraterritorialità dell'ambito o degli effetti ovvero estensione territoriale quando si tratta di *EU data protection law*[42].

Il GDPR dedica, com'è noto, l'articolo 3 a delineare "l'ambito di applicazione territoriale" della normativa, come segue: "1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento *da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*. 2. Il presente regolamento si applica *al trattamento dei dati personali di interessati che si trovano nell'Unione*, effettuato da un titolare del trattamento o da un responsabile del trattamento che *non è stabilito nell'Unione, quando le attività di trattamento riguardano*: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) *il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione*. 3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in *un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico*"[43].

Vogliamo riportare l'intero testo dell'articolo proprio per riconoscerne l'importanza, ad uno con i Considerando 22-25 (e il 24 in particolare), nel complesso sistema di protezione dei dati personali, sia in quanto punto di partenza per la corretta applicazione del Regolamento, sia in considerazione del suo inscindibile legame, evidentemente, con le norme che costituiscono particolare oggetto del nostro interesse, ossia quelle del Capo V relative al trasferimento dei dati personali verso Paesi terzi o organizzazioni internazionali. In generale, risalta senz'altro dal GDPR un ridimensionamento del principio di territorialità[44] e, in particolare, «(…) *Article 3 outlines what types of contact with the EU's territory will activate the application of the GPDR, and it does so in a manner that is partly*

[42] Così infatti C. KUNER, Extraterritoriality and International Data Transfers in EU Data Protection Law, in *Legal Studies Research Paper Series* – Paper No. 49/2015, University of Cambridge, laddove, riprendendo la distinzione di Poullet tra "extraterritoriality in scope" e "in effect", già allora affermava: «*In my view, this has become a distinction without a difference, and use of the term "extraterritorial" should encompass both the explicit territorial scope of legislation and its effects in other countries, so that at least in EU data protection law, fine distinctions between extraterritorial jurisdiction, extraterritorial impact, and extraterritorial triggers no longer matter*.», p. 8. Nello stesso senso, più di recente l'autore affermava: «*With regard to EU data protection law, it is less important to categorize the exact form of extraterritoriality used, than to recognize that it exerts its influence in different ways on persons and activities in third countries*», in The Internet and the Global Reach of the EU Law, in M. CREMONA, J. SCOTT (Eds), *EU Law Beyond EU Borders – The Extraterritorial Reach of EU Law*, Oxford, 2019, p. 124.

[43] Regolamento Generale per la Protezione dei Dati (di seguito GDPR), n. 679 del maggio 2016, Articolo 3, enfasi aggiunta.

[44] Come viene notato, tra gli altri, da P. DE HERT M. CZERNIAWSKI, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, in *International Data Privacy Law*, 2016, Vol. 6, No. 13, pp. 230-243, part. 237.

territoriality-dependent and partly territoriality-independent. (…) it must be emphasised that a key purpose of Article 3 is to position the GDPR within the international system»[45].

Rinviando al prosieguo l'analisi delle complesse problematiche sollevate dalla definizione dell'ambito territoriale del diritto alla protezione dei dati personali, e degli sviluppi avutisi con l'articolo 3 del GDPR rispetto all'articolo 4 della Direttiva madre anche in virtù dei fondamentali interventi giurisprudenziali, va detto sin d'ora, e proprio in questa sede dedicata all'extraterritorialità, che nonostante le aggiornate previsioni del Regolamento l'effettiva portata dell'ambito di applicazione rimane problematica. Si dirà anche degli interventi istituzionali volti a dare contributi chiarificatori; in ogni caso, sicuramente le previsioni del paragrafo 2 dell'articolo 3 hanno destato parecchio interesse[46], considerate da molti studiosi come uno tra i più importanti risultati della riforma anche, come rilevato da De Hert e Czerniawski, per la capacità di estendere l'ambito di applicazione ai soggetti e alle situazioni di cui alle lettere a) e b) senza utilizzare il termine "extraterritorialità" e secondo un approccio assolutamente nuovo che consiste nella "*jurisdiction based on targeting*"[47]: «*The territorial scope of the GDPR is (as before) still based on links with the EU territory, but indeed complemented with extraterritorial solutions. (…) The overall logic here is based on targeting:* if you target EU data subjects then the Regulation reaches out to you. *This targeting or destination approach proposed in the GDPR is, however, not absolute and Article 3(2) tries to set clear limits to the extraterritorial scope of the General Regulation*»[48].

Ciò basti, per il momento, ad evidenziare come proprio nella dimensione digitale, e, in particolare, con il diritto alla protezione dei dati personali, l'impatto dell'azione dell'Unione verso l'esterno risulta sempre più preponderante e incisivo. E di ciò, senza dubbio, e a differenza dei primi periodi, la stessa Unione diventa ormai sempre più consapevole: «*the EU tends to assert itself as a global regulatory power consciously and deliberately with regard to the Internet*»[49].

Cenni sulla cooperazione internazionale

[45] D.J.B. SVANTESSON, Article 3. Territorial scope, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020, p. 76.
[46] Il riferimento è, per esempio, a G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Cacucci editore, 2021, che, trattando di geolocalizzazione e mercato unico digitale, quindi commentando il Regolamento 2018/302 (sul c.d. *geoblocking*), comunque riconosceva che: «(…) l'estensione dell'ambito territoriale di applicazione dei diritto UE oltre i confini degli Stati membri è un trend che sta caratterizzando spesso le regolamentazioni relative alla disciplina di fattispecie online, sulla base di un modello costruito sulla base di un *template* contenuto nel GDPR, il regolamento generale sulla protezione dei dati(…)», così passando ad analizzare proprio l'articolo 3, par. 2 del GDPR; cfr. p. 225.
[47] P. DE HERT, M. CZERNIAWSKI, Expanding the European data protection scope beyond territory, *cit.*, p. 238.
[48] Ibidem, p. 242.
[49] C. KUNER, The Internet and the Global Reach of the EU Law, in M. CREMONA, J. SCOTT (Eds), *EU Law Beyond EU Borders – The Extraterritorial Reach of EU Law*, Oxford University Press, 2019, p. 125.

L'ultimo metodo da considerare nel 'moto opposto', anche in relazione all'effetto Bruxelles, è quello (l'unico) non unilaterale attraverso cui l'Unione espande la propria regolamentazione (ovvero il suo impatto): semplicemente, nella maniera classica del diritto internazionale, ossia attraverso la conclusione di accordi internazionali, bilaterali o multilaterali.

Orbene, nell'analisi della Bradford emerge in parallelo la *market-driven harmonization*, propria del *de facto Brussels effect*, e la *treaty-driven harmonization*, più attiva, guidata dal consesso e frutto di cooperazione, individuando pro e contro di ciascuna dinamica, ravvisando in particolare a favore della seconda alcune ragioni, tra cui: «*(…) to obtain greater legitimacy for EU regulations through globalization. If foreign companies and governments endorse EU standards, those standards may be seen as having wider appeal and thus greater legitimacy. (…) Less tangibly, being the global standard setter has the benefit of expanding the EU's soft power and validating its regulatory agenda, both at home and abroad*»[50]. Dunque la *treaty-driven harmonization* sarebbe talvolta alternativa rispetto all'effetto Bruxelles, specie nei casi in cui questo non opera perché si tratta di settori non legati al mercato, e dunque in tal senso utile anche a superare le criticità spesso rivolte all'influenza troppo unilaterale dell'Unione; nondimeno, talaltra sarebbe complementare a quell'effetto o in rapporto di consequenzialità: «*What sets the EU apart is that, unlike in many other jurisdictions, both market-driven and treaty-driven mechanisms can coexist, or even amplify one another, maximizing the influence EU regulations have over market outcomes worldwide*»[51].

Invero, qualche studioso, ha posto l'accento proprio sull'importanza della cooperazione per la diffusione, nello specifico, del diritto europeo alla protezione dei dati personali, cercando quindi di ridimensionare la portata unilaterale dell'intervento dell'Unione nel settore. Infatti, proprio rispetto alle considerazioni sull'effetto Bruxelles, Schwartz ha sollevato qualche perplessità, pur senza misconoscerne il contributo, e ha puntato piuttosto l'attenzione sulla rilevanza dell'intervento *non* unilaterale dell'Unione per la diffusione della sua regolamentazione nel settore della protezione dei dati personali: «(…) *contrary to the one-fell-swoop perception of EU influence evoked by GDPR Day, there has, in fact, been a varied range of nation-state, transnational, and corporate behavior that has helped spread EU data protection throughout the world*»[52].

L'autore analizzava le posizioni di altri studiosi al riguardo e in particolare quella della Bradford per evidenziare come in realtà il modello dell'effetto Bruxelles, nella sua duplice composizione *de facto-de jure*, non sarebbe perfettamente riscontrabile rispetto all'espansione della protezione dei dati; a tal fine, presentava due casi-studio, relativi a USA e Giappone, a sostegno di altri fattori e

[50] A. BRADFORD, *The Brussels Effect*, *cit.*, p. 89.
[51] Ibidem, p. 91, ma più in generale si vedano pp. 86-91.
[52] P. M. SCHWARTZ, Global Data Privacy: The EU Way, *New York University Law Review*, Vol. 94, No. 4, 2019, p. 773.

strategie rilevanti[53]. In particolare, da quei casi l'autore rilevava, quanto al Giappone, che l'effetto *de jure* della diffusione non seguirebbe necessariamente quello *de facto* ma sembrerebbe invece precederlo; inoltre, rispetto agli USA, sarebbe riscontrabile una viva flessibilità negoziale e cooperazione, piuttosto che unilateralità, da parte dell'Unione[54].

Invero, è da precisare che l'autore perveniva a tali conclusioni focalizzandosi precipuamente su aspetti quali l'adeguatezza, la capacità normativa dell'Unione e l'interazione istituzionale al suo interno; tutti aspetti che, come si è in parte esposto, sono pure (e non solo, se si ripensa al *normative power* di Manners) valorizzati dalla Bradford come parte integrante dell'effetto Bruxelles[55]. Nondimeno, il passaggio dirimente nell'esposizione di Schwartz va rintracciato in due fattori generali come preponderanti per la diffusione globale della protezione europea dei dati personali: "*accessible model*" e "*markeplace of ideas*".

Quanto al primo, la capacità europea di presentare un modello "accessibile" ossia facile da adottare in altri contesti sarebbe, secondo l'autore, un derivato dell'esperienza interna dell'integrazione europea, risalente al bisogno – emerso soprattutto negli anni Settanta – di armonizzare le legislazioni e le pratiche degli Stati membri dell'Unione rispetto alla protezione dei dati personali. È quanto abbiamo illustrato (*supra*, Parte II) rispetto all'emersione a livello sovranazionale della normativa sulla protezione dei dati personali (obiettivo principale della direttiva madre) e che, in realtà, consideriamo ravvisabile anche nel ragionamento esposto dalla Bradford (oltre che condiviso da altri autori) a fondamento dell'emersione dell'effetto Bruxelles (quale espressione di esternalizzazione che sarebbe derivata, nondimeno, dai necessari interventi interni di armonizzazione). Ma è molto interessante la constatazione effettuata da Schwartz sull'allargamento dell'Unione verso Stati dell'Est come trampolino per testare l'adattabilità del modello europeo di protezione dei dati anche altrove: «*The use of omnibus laws in Europe proved a key element in the global diffusion of EU data protection law. Consider the Data Protection Directive of 1995, which consolidated existing national European laws and established a requirement that member states*

[53] Ibidem, p. 783: «*Bradford's Brussels Effect does not fully capture the dynamic present in the global negotiations around data privacy*».

[54] Ibidem, p. 803: «(…) *the case studies cast doubt on the ideas that the EU exercises unilateral power and reaches only de facto results. Instead, they demonstrate that the EU employs a broad set of strategies that have encouraged the spread of its data protection law. Beyond these strategies, the EU has benefited both from elaborating a highly transplantable legal model and from developing concepts that have proved successful in a global marketplace of ideas*»; si vedano anche pp. 804-805.

[55] Semplicemente, mentre essi sono considerati aspetti delle cinque condizioni indispensabili perché possa realizzarsi l'effetto Bruxelles, almeno nella sua ultima e più raffinata elaborazione del 2019, l'autore preferisce vederli come elementi di dinamiche non unilaterali, pur riconoscendoli rilevanti anche per la Bradford: «*One of the most striking themes of this Article's case studies concerns the EU's regulatory capacity. Bradford is correct to emphasize this factor as a major element of her Brussels Effect*», in P. M. SCHWARTZ, Global Data Privacy: The EU Way, *cit.*, p. 807. Si veda anche p. 818.

harmonize their data protection laws according to the Directive's standards. With the fall of the Iron Curtain and the eastward expansion of the EU, each new member state was obliged to enact a harmonized national data protection law as part of the price of joining the EU. The general principles of the Directive and the harmonized EU data protection laws provided a relatively simple model first for the new member states of the EU and then for the rest of the world»[56].

Il secondo fattore individuato da Schwartz consisterebbe essenzialmente nell'importanza delle idee e, più specificamente, del fascino esercitato dagli elevati standard europei per la protezione dei dati, che provocherebbe una forte influenza a livello internazionale, per spiegare il quale, ben oltre il potere unilaterale dell'Unione e finanche le strategie di negoziazione, egli portava come esempio le vicende legate al *California Consumer Privacy Act*: «*The result has been widespread familiarity with EU-style data protection and, over time, buy-in to its ideals. This phenomenon represents another way the EU has not singlehandedly imposed its regime on nations, but rather reached important actors through the force of appealing ideas and a range of different kinds of interactions, which lead to a general process of acculturation to EU privacy concepts*»[57]. Anche su questi rilievi, tuttavia, va detto che, per quanto assolutamente condivisibili, essi appaiono non proprio distanti dalle considerazioni che sopra esposte, sia della Bradford sia (quanto, per esempio, all'importanza delle idee) della concezione elaborata da Manners per spiegare la peculiarità del *normative power Europe*. Nondimeno, l'intervento di Schwartz consente di bilanciare la considerazione dell'influenza esterna dell'Unione nel settore della protezione dei dati, ribadendo l'importanza del profilo collaborativo e del fattore culturale in tale processo. Pertanto, questa ulteriore analisi concorre, con le altre, a corroborare il 'moto opposto', riscontrabile nella generale diffusione verso l'esterno del "modo europeo" di protezione dei dati personali.

L'influenza della giurisprudenza

Infine, per chiudere su questo "moto", non va dimenticata l'importanza dell'influenza dei giudici di Lussemburgo rispetto alla "esportazione" delle norme dell'Unione, che peraltro anche la Bradford riteneva quale ulteriore incentivo all'effetto Bruxelles[58]. In effetti, dal Capitolo dedicato all'evoluzione del diritto alla protezione dei dati personali dalla giurisprudenza delle Corti europee (*supra*, Capitolo IV, Parte II) abbiamo visto emergere un orientamento volto ad enfatizzare l'aspetto

[56] Ibidem, pp. 811-812.
[57] Ibidem, p. 817 e più in generale da p. 816. Peraltro, sul punto l'autore conclude: «*EU-style data protection has proven to be an appealing idea that a large number of jurisdictions have adopted. The global diffusion of EU data protection reflects a success in the marketplace of ideas*», p. 818.
[58] A. BRADFORD, *The Brussels Effect*, *cit.*, p. 75: «(…) *the European courts have provided an institutional template for regional courts*»; si veda anche più ampiamente pp. 75-78.

di riconoscimento di diritto fondamentale, cosa che, come vedremo (*infra*, Capitolo II) ha poi influenzato gli interventi di riforma (anche a livello di diritto primario, tra Carta dei diritti e articolo 16 TFUE) del sistema europeo di protezione dei dati e massimamente il GDPR: «*The description of privacy through rights discourse is a core aspect of the EU approach to data privacy. Data protection in the EU is seen as a fundamental right, and one that rests on interests in dignity, personality, and informational self-determination*»[59]. Questo, evidentemente, e in considerazione della risonanza esterna di quella impostazione, ha influito sul modo di pensare la *privacy* in modo più generalizzato: «*The EU has taken an essential role in shaping how the world thinks about data privacy*»[60].

Abbiamo così illustrato per sommi capi i principali interventi, non solo unilaterali, che contribuiscono a realizzare il 'moto opposto' ossia, partendo dall'Unione, sempre più consapevolmente influenzano lo spazio ad essa esterno e così la rendono sempre più rilevante nello scacchiere internazionale. Come dicevamo, però, se è vero che questi stanno ultimamente divenendo preponderanti rispetto al primo periodo dell'integrazione europea, e l'evoluzione del diritto alla protezione dei dati personali ne è un esempio lampante, ciò non vuol dire che i moti esogeni non siano più rilevanti, quanto al settore prescelto. È quello che ci accingiamo a presentare.

3. …e viceversa, in continuo "intervallo armonico"

Che le dinamiche che modellano oggi il processo di integrazione europea siano sia esogene che endogene appare, come si diceva, particolarmente evidente nel settore che ci interessa: «*The relationship between EU law and the Internet is one of mutual influence. On the one hand, EU law has influenced the development of the Internet, and impacted countries and parties outside the EU's borders. On the other hand, the Internet raises important questions about the application, scope and normative values of EU law. In many ways the Internet is the ideal vehicle for examining the ambitions of EU law in an increasingly complex and globalized world*»[61].

Il c.d. Strasbourg effect

[59] P. M. SCHWARTZ, Global Data Privacy: The EU Way, cit., p. 773.
[60] Ibidem.
[61] C. KUNER, The Internet and the Global Reach of the EU Law, in M. CREMONA, J. SCOTT (Eds), *EU Law Beyond EU Borders – The Extraterritorial Reach of EU Law*, Oxford University Press, 2019, p. 112.

Condividiamo totalmente questa concezione dell'Internet come "veicolo ideale" (o meglio, "luogo" ideale) per esaminare le ambizioni del diritto (e non solo) dell'Unione. E proprio partendo dall'analisi appena effettuata dell'effetto Bruxelles con specifico riguardo alla *Digital economy*, notiamo subito che da alcune critiche ad esso sollevate emergono chiari i segnali di influenze che "viceversa" avrebbero stimolato quell'effetto (ancora, o di nuovo) dall'esterno.

Il riferimento è (anzitutto) a ciò che Bygrave ha voluto intendere con "*Strasbourg Effect*" rispetto all'impatto della nuova Convenzione 108+ (su cui *supra*, Parte II) e più in generale alla "europeizzazione delle norme sulla protezione dei dati personali nel mondo"[62] che si potrebbe in qualche misura ricondurre (l'autore farebbe un cenno in tal senso) anche alla contaminazione tra la giurisprudenza di Strasburgo e quella di Lussemburgo (a partire da quanto si è illustrato *supra*, Capitolo IV, Parte II, ma anche più di recente, come si dirà *infra*, Capitolo I, Parte IV).

La principale critica che l'autore muoveva alla teoria prospettata dalla Bradford, a cui pure riconosceva grandi meriti e sulla quale invero fondava il proprio ragionamento, è data dal fatto di sottovalutare, a suo modo di vedere, l'indispensabile lavoro in seno al Consiglio d'Europa (e quindi a una spinta esterna, data da un'organizzazione internazionale distinta, per quanto regionalmente contigua, dall'Unione) come fondamento della stessa emersione del sistema dell'Unione europea sulla protezione dei dati personali[63].

L'autore partiva proprio dalle caratteristiche che connotano l'effetto Bruxelles per individuare le peculiarità dell'effetto Strasburgo: quest'ultimo, a differenza del primo, sarebbe un processo "*treaty-based*" che coinvolge prevalentemente attori statali e con un apparato burocratico molto meno sofisticato e forte di quello proprio dell'Unione, nonché uno schema sanzionatorio – quale quello prospettato dalla Convezione 108+ – più debole di quello predisposto dal GDPR[64]. Ciò posto, l'autore focalizzava però l'attenzione – ed è questo il punto che ci interessa ai fini della nostra analisi che "viceversa" ci riporta alla 'spinta dello spazio sulla forma'– sui punti di forza del Consiglio d'Europa (prevalentemente concentrato sulla protezione dei diritti umani) e su quanto essi abbiano caratterizzato non solo il lavoro interno dedicato alla protezione dei dati ma anche e soprattutto su quanto abbiano influito nel modellare tale settore nell'Unione europea nel recente passato. E questo non tanto, e non solo, in maniera unilaterale, ma, e sempre di più ultimamente,

[62] L. A. BYGRAVE, The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2020, https://doi.org/10.1016/j.clsr.2020.105460, p. 2.
[63] Ibidem, p. 6: «*Bradford's account also fails to do justice to the CoE's work in laying many of the foundations for EU data protection law. Apart from acknowledging that the right to data protection in EU law builds on Article 8 ECHR, she ignores the important role played by C108 and other CoE instruments in shaping EU data protection norms*».
[64] Cfr. ibidem, pp. 6-7.

stimolando anche delle influenze, oltre a subirle, che a sua volta e di converso l'Unione eserciterebbe sugli interventi del Consiglio d'Europa nel settore.

Vale la pena riportare letteralmente i passaggi salienti di queste considerazioni dell'autore: «*the regulatory capacity and regulatory propensity inherent in BE is partly a reflection of CoE policy work. A well-established tradition of close cooperation between the CoE and EU exists across a wide range of regulatory fields.* (…) *This carries over into the area of data protection. (…)*. *The CoE and its various data protection codes, together with jurisprudence from the ECtHR pursuant to Article 8 ECHR, have had an enormous impact on EU policy development in the area. The basic principles of Convention 108 were the central point of departure for EU legislative efforts in the field, particularly the DPD, and they inform much of the backbone of the GDPR. They have also been an important benchmark for EU data protection rules in the area of policing and judicial cooperation. Conversely, the DPD catalysed and shaped work on the Additional Protocol to C108 adopted in 2001. Further, the recent process of modernising C108 in parallel with the drafting of the GDPR was a situation where Brussels and Luxembourg shaped the deliberations of Strasbourg. Yet influence also went the other way. For example, the provisions in C108+ on processing of biometric data shaped the trilogue discussions on how such data should be treated under the GDPR. Thus, SE is baked into BE to a significant extent, and vice-versa. (…) the EU and CoE share a broadly similar normative vision as projected onto the global stage*»[65].

Riprendendo alcune valutazioni che Schwartz aveva rilevato rispetto all'Unione europea e alla diffusione del suo modello di protezione dei dati (nonché il fondamento del *normative power* di Manners), Bygrave enfatizzava il c.d. "*ideational power*" del Consiglio d'Europa per rintracciare la caratteristica dello *Strasbourg Effect* nel c.d. *"regulatory appeal"*: «*The CoE's ideational power rests on the mechanics of persuasion tempered by processes of acculturation. This will continue to provide the basic 'fuel' for SE. As such, SE is an exemplary manifestation of what may be termed 'regulatory appeal' (…). By this is meant the degree to which a regulatory system or model developed in one jurisdiction (or set of jurisdictions) has an attractive aura for other jurisdictions. This appeal is a function (…) of the inherent cogency, integrity and reputation of the regulatory system/model concerned. It points to the capacity for legal norms to spread from one state to another due (at least partly) to the recipient state perceiving those norms as intrinsically sensible or as sufficiently 'fashionable' that adherence to them augments the recipient state's reputation or status vis-à-vis other states or actors with which it wants to identify. Such appeal is vital to SE*»[66].

[65] Ibidem, p. 7, sottolineato aggiunto.
[66] Ibidem, p. 13.

Ebbene, a noi qui interessa capire quanto questo *Strasbourg Effect* abbia influenzato e/o continui ad influenzare "dall'esterno" il sistema di protezione dei dati predisposto dall'Unione europea.

Al riguardo, l'autore indicava interventi della Commissione europea volti a riconoscere l'importanza della Convenzione 108 per la diffusione a livello globale della protezione dei dati personali, oltre che a enfatizzare l'impatto della Convezione 108+, così mostrando di considerare lo *Strasbourg Effect* anche come veicolo per il *Brussels Effect*[67]. Nondimeno, se l'influenza derivante dal Consiglio d'Europa è stata dirimente per la costruzione del sistema di protezione dei dati personali nell'Unione sin dai suoi (pur vicini) albori e nei suoi sviluppi principali, più di recente, e specie dopo le ultime riforme che hanno anche portato al GDPR, l'autore ravviserebbe una sorta di c.d. "*Byzantine Turn*", per cui l'attuale sistema in seno all'Unione europea costituirebbe un vero e proprio "impero", parecchio autoreferenziale, proceduralmente molto intricato e dunque anche più difficilmente influenzabile dall'esterno, e dal quale, piuttosto, lo *Strasbourg Effect* potrebbe trarre vantaggio nel prossimo futuro: «*C108+ has considerable potential to strengthen and expand SE. At the same time, the power of such an effect will depend on BE. While BE could undermine SE, history shows that the two processes are not necessarily at loggerheads but tend to be mutually reinforcing, both intentionally and incidentally. Hopefully, this mutuality will persist. Just as SE has helped BE in the past, BE could act as a vehicle for SE in the future, particularly by utilising the 'adequacy' mechanism provided by Articles 44–45 GDPR to encourage accession to C108+. Operationalised carefully, the strategy may help break part of the gridlock in which multilateralism at the global level is caught*»[68]. Questa "reciprocità" e "mutualità" tra i due sistemi europei, per quanto attualmente veda prevalere nel settore dei dati l'intervento dell'Unione (e dunque, il c.d. moto opposto'), comunque avvalora la constatazione di vicendevoli influenze che configurano la protezione dei dati (in senso lato) europea e caratterizzano il processo di integrazione sovranazionale.

Ulteriori influenze esterne

Per una comprensione più completa delle ulteriori influenze che "viceversa" hanno inciso sulla costruzione del sistema di protezione dei dati personali nell'Unione europea e che poi, 'in continuo

[67] Cfr. ibidem, p. 12. Il riferimento è a due atti della Commissione in particolare: Proposta di DECISIONE DEL CONSIGLIO che autorizza gli Stati membri a firmare, nell'interesse dell'Unione europea, il protocollo che modifica la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STE 108) COM/2018/449 final - 2018/0237 (NLE); COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO Scambio e protezione dei dati personali in un mondo globalizzato, COM/2017/07 final.
[68] Ibidem, p. 13.

intervallo armonico', si combinano con le seguenti spinte da quel sistema verso l'esterno, torna abbastanza utile l'analisi di Bygrave laddove pone l'accento sui sistemi esterni da cui proprio l'Unione europea avrebbe tratto ispirazione nel recente passato per la propria legislazione in materia di protezione dei dati: «(…) *EU legislative developments have not been exclusively 'home grown'; they have sometimes been inspired by regulatory ideas and traditions elsewhere. Security breach notification rules (which originated in the USA) are an example in point; requirements for data protection impact assessments (which have roots in the USA, Australia and New Zealand) are another example; rules on data protection by design and by default (which partly originated in Canada) and certification schemes (which first took widespread hold in the USA) are yet others. Thus, EU data protection rules are the result of a cross-fertilisation of regulatory traditions*»[69]. Proprio questa "fertilizzazione incrociata delle tradizioni normative" presentata da Bygrave, in uno con la contaminazione dei modelli interpretativi tra gli organi giurisdizionali di diversi ordinamenti giuridici (essenzialmente, nel contesto regionale europeo), costituisce il cuore pulsante di ciò che intendiamo qui con "*continuo intervallo armonico*" e che costituirebbe il fattore peculiare che contrassegna l'attuale stadio dell'evoluzione del processo di integrazione europea. Richiamando la metafora musicale già utilizzata in uno scritto che analizzava le dinamiche tra istituzioni europee in una certa materia[70], vogliamo intendere qui semplicemente che i "moti" che intervengono a modellare e influenzare l'attuale processo di integrazione europea risultano oggi tendenzialmente simultanei, sovrapponibili, ancorché non sempre e non in tutti gli ambiti con la stessa intensità, in considerazione della più spiccata rilevanza dell'Unione sia (verso l'interno) rispetto agli Stati membri che, soprattutto, (verso l'esterno) come attore globale.

Ciò è principalmente riscontrabile nel settore della protezione dei dati personali, di cui in particolare il meccanismo dei criteri di adeguatezza per il trasferimento dei dati verso Paesi terzi, sia che lo si intenda in senso unilaterale (come per alcune teorie) sia che lo si intenda come cooperazione bidirezionale (come per altre), rappresenta massima espressione. Si avrà modo di analizzarne le peculiarità (*infra*, Capitolo II, Parte IV), rispetto a cui, per esempio, sono stati fondamentali gli stimoli derivanti dalla celeberrima vicenda delle rivelazioni di Snowden che hanno fortemente

[69] Ibidem, pp. 5-6, sottolineato aggiunto.

[70] Il riferimento è a G. LO TAURO, Diritti fondamentali e misure antiterrorismo nell'Unione europea: intervalli melodici tra Consiglio e Corte di giustizia, in *Diritto pubblico comparato ed europeo*, n. 1/2020, pp. 151-182.
In particolare, in quell'occasione, analizzando gli interventi alternativi di Corte di giustizia e Consiglio rispetto a misure restrittive, usavamo la metafora musicale, spiegando: "L'intervallo misura la distanza tra due note musicali. Ai nostri fini rileva la distinzione tra intervalli melodici e armonici: «Si definiscono intervalli melodici quelli in cui le due note vengono suonate in successione, mentre si definiscono intervalli armonici quelli in cui le due note si suonano contemporaneamente», A. Zanchi, Teoria e armonia moderna, Lainate (Milano), 2010, 10. Ebbene, il rapporto tra gli interventi, di volta in volta, di Corte e Consiglio parrebbe svilupparsi come un intervallo melodico", p. 152, nota 2.
Nel caso di specie, invece, il riferimento agli "intervalli armonici" parrebbe più appropriato per spiegare i moti che stiamo descrivendo.

messo in discussione il sistema statunitense e, quindi, hanno costretto a ripensare le modalità di valutazione dell'adeguatezza; ma anche ulteriori fattori di influenza possono riscontrarsi attualmente: le vicende legate alla Brexit, per esempio, costituiscono un raffinatissimo esempio di moti sia endogeni (in questo caso potendosi parlare quasi, non a torto, di 'rotture'), prima, che esogeni, poi, il cui particolare atteggiarsi rispetto al settore dei dati personali (anche, per esempio, rispetto ai casi a Strasburgo e Lussemburgo quanto al sistema di sorveglianza) denota le peculiarità e fa emergere le criticità più generali dello stadio attuale del processo di integrazione europea; ancora, e com'è chiaro, preponderante è anche l'incidenza della crisi pandemica sull'approccio dell'Unione alla dimensione digitale, da cui sono emerse criticità e lacune specie rispetto agli interventi di Paesi terzi, ma anche nuovi stimoli e ripensamenti (*infra*, Capitolo III, Parte IV).

Il c.d. modello di integrazione senza sovranità

Ebbene, cosa ci consentono di desumere queste analisi sui diversi e simultanei moti caratterizzanti l'attuale processo di integrazione europea? Essenzialmente, essi confermerebbero che l'Unione è un ente *sui generis* in costante movimento e dunque, per questo, è *a*morfa. Ciò sarebbe invero connaturato al meccanismo dell'integrazione europea: «il meccanismo dell'integrazione europea appare piuttosto fondato su una concezione incrementale del potere politico, smembrato e ripartito fra più titolari che competono per allargare i confini delle proprie competenze, *creando un equilibrio in continua mutazione*»[71].

Questa constatazione, che descrive in definitiva l'Unione *a*morfa, assume particolare rilevanza ai fini della crisi di legittimazione, proprio perché stimola una provocazione rispetto a ciò che Cannizzaro ha, a ragione, indicato come "*il modello dell'integrazione senza sovranità*": «L'Unione europea è probabilmente il primo caso in cui gli Stati hanno accettato di trasferire all'esterno il potere di regolare su larga scala la vita sociale delle proprie comunità. Oggi sappiamo che questo fenomeno è capace di creare una comunità di individui che condividono interessi e valori comuni anche al di là dei confini statali. Difatti, per lo meno nei primi decenni della sua vita, il processo di integrazione europea è stato universalmente acclamato dai suoi sostenitori come il più avanzato esperimento sociale di limitazione, se non addirittura di trasformazione del modello dello Stato sovrano, idoneo ad affrontare le nuove sfide provenienti dai processi di mondializzazione dell'economia e dall'esigenza di difesa dello Stato sociale. Tuttavia, l'improvvisa accelerazione dei processi di mondializzazione ha svelato l'incompiutezza e la fragilità del disegno di integrazione

[71] Così E. CANNIZZARO, *La sovranità oltre lo Stato*, Il Mulino, 2020, p. 90, enfasi aggiunta.

che, producendo sostanzialmente una frammentazione dei poteri sovrani, ha finito per lasciare ciascun ente – sia gli Stati membri che l'Unione – privo della pienezza dei poteri necessari a far fronte alle conseguenze di tali processi»[72].

Ecco quindi, come traspare chiaramente da questi ultimi passaggi, che si (ri)propone la questione della crisi di legittimazione dell'Unione europea (da ultimo gravata dalla pandemia). Ed ecco, quindi, che entra in gioco la *dimensione digitale*, come spazio di plausibile soluzione.

La protezione dei dati personali in particolare rappresenta un esempio mirabile, nel più ampio ambito dell'economia digitale, perché attraverso di essa essenzialmente l'Unione manifesta la propria indispensabilità e dunque, in qualche modo, rivendica una "nuova" legittimazione: «*Beyond the concern over the competitiveness of the European industry, the EU may have additional incentives to project its regulatory power abroad. For one, the EU may be motivated by a desire to obtain greater legitimacy for its rules through globalizing them*»[73]. Ed è quindi in questa nuova dimensione digitale che l'Unione si candida, soprattutto attraverso la protezione dei dati personali, a definire delle regole volte a disciplinare le dinamiche che interessano il digitale ponendo l'accento (con una presa molto più incisiva di quella che potrebbero avere sia singolarmente gli Stati membri sia, come abbiamo visto, le iniziative in seno al Consiglio d'Europa) sulla necessità di *tutele* e quindi enfatizzando il proprio apparato valoriale e riconfermando la *EU rule of law* anche in quel settore e, più in generale, in quella dimensione.

In questo modo, quindi, l'Unione, quale ente amorfo e "modello di integrazione senza sovranità", cavalca la sfida di una sovranità *nuova*, o meglio "*rinnovata*", delimitata quanto al profilo materiale ma non quanto a quello territoriale, in una dimensione *nuova*, quella *digitale* appunto, che si presta come terreno fertile ad essere ordinata. Le dinamiche che abbiamo indicato come "moto opposto" sarebbero dimostrative in tal senso: «*Data protection is one of the rare fields in which the EU could be said to exercise global regulatory supremacy; the EU rules*»[74].

Questi profili, così ampiamente supportati in teoria, dovranno quindi essere riscontrati nella pratica. A questo sarà dedicatala trattazione della Parte IV. Da essa emergerà che, per quanto sotto il profilo regolatorio sembrerebbe possibile confermare ciò che emerso dalle teorie appena esposte, e dunque sembrerebbe possibile ravvisare degli indizi di sovranità digitale dell'Unione europea già operativa, nondimeno alcuni punti critici farebbero emergere degli ostacoli e dei freni a una compiuta realizzazione di tale sovranità nella dimensione digitale, e dunque manterrebbero alcuni aspetti

[72] Ibidem, pp. 90-91.
[73] A. BRADFORD, *op. cit.*, p. 23.
[74] O. LYNSKEY, *The Foundations of EU Data Protection Law*, Oxford University Press, 2015, p. 41.

problematici della legittimazione dell'Unione. Quella stessa analisi, infatti, ci farà rilevare come, per quanto la forza del *diritto* come *potere* rimanga una peculiarità dell'Unione, vi sono altri aspetti rispetto ai quali il suo intervento rimane ancora carente e che non possono più essere sottovalutati, come la dimensione digitale fa emergere chiaramente.

Prima di passare a detta analisi, è molto utile avere ben chiaro il quadro predisposto dal sistema di protezione dei dati personali dell'Unione europea, focalizzando l'attenzione sul ruolo assegnato, e via via perfezionato, alle istituzioni preposte al suo funzionamento. Ciò, infatti, costituirebbe una piena conferma, quantomeno nelle previsioni teoriche, del nesso tra *EU rule of law* e protezione dei dati personali. Inoltre, valuteremo anche l'importanza del principio di coerenza nell'azione dell'Unione, almeno nella sua presentazione teorica, rispetto alla protezione dei dati personali, per comprendere, poi, se sarà possibile o meno rintracciarlo nella pratica.

CAPITOLO II

EU RULE OF LAW E PROTEZIONE DEI DATI PERSONALI

1. Il quadro predisposto a partire da Lisbona

La portata innovativa del (attualmente ultimo) Trattato di riforma è largamente nota, specie se paragonata alle versioni precedenti, soprattutto in termini di vocazione verso l'esterno, quanto ai due aspetti che vogliamo qui prendere in considerazione: i valori su cui l'Unione si fonda e la protezione dei dati personali. Il legame tra questi due aspetti si connota essenzialmente dei seguenti postulati: «*fundamental rights are applicable in all situations, the Court of Justice's scrutiny of the European Union is strict, and the application in horizontal situations between private parties acquires a new dimension on the internet, including a duty for the European Union to ensure protection*»[75].

L'analisi degli elementi principali che, si ritiene, contribuiscono a palesare il legame tra *EU rule of law* e protezione dei dati, sarà condotta principalmente, ma non esclusivamente, dall'angolo privilegiato della giurisprudenza della Corte di giustizia, che ne consentirà una più agevole dimostrazione (sia in teoria che in pratica). Proseguendo con l'evoluzione a partire dal Trattato di Lisbona (per il periodo precedente si veda *supra*, Capitolo IV, Parte II), vedremo infatti che, per esempio, la giurisprudenza sulla Direttiva 95/46 non solo sarà applicabile nel periodo post GDPR, in virtù del fatto che i principi basilari rimarranno gli stessi, ma che in alcuni aspetti rilevanti essa venne proprio codificata dal GDPR[76]. Passiamo, dunque, a presentare i due aspetti il cui legame si vuole indagare, prima di procedere all'analisi degli elementi da cui questo emergerebbe in teoria.

---

[75] H. HIJMANS, *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU*, (PhD Thesis) University of Amsterdam, 2016, p. 30. Il ricco lavoro condotto dall'autore, a cui faremo spesso riferimento, aveva come fondamento la seguente domanda di ricerca: "*How does the constitutional mandate under Article 16 TFEU contribute to legitimate and effective privacy and data protection on the internet and what does and should the European Union do to make Article 16 TFEU work, through judicial review, legislation and control by (cooperating) independent authorities, taking into account that the mandate has external effect?*".

[76] C. DOCKEY, H. HIJMANS, The Court of Justice as a Key Payer in Privacy and Data Protection: an overview of recent trends in case law at the start of a new era of data protection law, *cit.*, p. 301 [*The case law on Directive 95/46 is applicable in the GDPR era because the basic principles of data protection did not fundamentally change between the GPR and the Directive. Moreover, in some important respects the Court's case law has actually been codified into the GDPR. For example, the elaboration of the right to be forgotten in Article 17, the safeguards for independence of*

Sul primo aspetto, di cui si è già detto (vedi *supra*, Capitolo IV, Parte I), ricordiamo che sebbene il riferimento a *rule of law* e diritti fondamentali fosse ravvisabile già nel Trattato di Amsterdam (art. 1 al punto 8, laddove modificava l'articolo F del precedente Trattato), a seguito della codificazione di principi operata da Maastricht, è solo con il Trattato di Lisbona che tali principi sono stati "ribattezzati come valori"[77]. Tralasciando la questione della non perfetta corrispondenza tra i valori sanciti all'articolo 2 TUE e quelli che fondano l'aziona esterna ai sensi degli articoli 3 e 21 TUE[78], è comunque indiscusso che: da un lato «*Article 2 TEU has created one "single 'homogeneity' clause", which may be understood as expressing both the "untouchable core" of the EU legal order and the core constitutional identity of the EU as a legal-political system*»[79]; e che, dall'altro, quanto alla dimensione esterna, non solo il Trattato di Lisbona ha formalmente rafforzato le condizioni per l'adesione all'Unione (in termini di impegno per i Paesi candidati al rispetto e alla promozione dei valori dell'Unione), ma soprattutto con riguardo alle disposizioni generali sull'azione esterna dell'Unione, ha previsto l'articolo 21 TUE, quale «*new, trasversal provision, which reflects one of the EU Member States' key priorities at the time of the Lisbon Treaty and which was to improve the coherence of the EU's external action*»[80].

Sul secondo aspetto, ossia la protezione dei dati personali, il Trattato di Lisbona è stato indubbiamente dirompente. Tra i vari "cambiamenti costituzionali" apportati alla struttura dell'Unione, infatti, i seguenti hanno riguardato o coinvolto lo specifico settore che ci interessa: «*introducing the right to data protection and a specific legal basis for data protection legislation in Article 16 of the Treaty on the Functioning of the European Union ('TFEU'); elimination of most aspects of the Maastricht Treaty's 'pillar' structure (meaning essentially that the same basic legal protections should apply to all types of data processing); increased oversight of and participation in data protection policy-making by the European Parliament; the elevation of the Charter of Fundamental Rights of the EU ('CFR'), which includes a specific right to data protection (Article 8 CFR), to constitutional status; and the obligation of the EU to accede to the European Convention*

---

supervisory authorities, ans the explanation that for data transfers an adequate level of protection 'essentially equivalent' to the level ensured within the EU].

[77] M. KLAMERT, Article 2 TEU, in M KELLERBAUER, M KLAMERT, J TOMKIN (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Oxford, 2019, p. 24. Peraltro, si considera al riguardo che «*there is also a connection with Article 4(2) TEU on the national identities of the MS, if we perceive Article 2 TEU as expression of a corresponding 'EU identity': outlining the constitutional core of the Union as a legal-political system*», ibidem.

[78] Per cui si segnala, *ex multis*, C. MORVIDUCCI, I valori dell'azione esterna nella prassi PESC, in E. SCISO, R. BARATTA, C. MORVIDUCCI (a cura di), *I valori dell'Unione europea e l'azione esterna*, Torino, 2017, pp. 58 ss.

[79] L. PECH, The Rule of Law in the EU: The Evolution of the Treaty Framework and Rule of Law Toolbox, *RECONNECT Working Paper* No. 7, March 2020, p. 14.

[80] Ibidem.

on Human Rights ('ECHR')»[81]. Si è già detto (*supra,* Capitolo III, Parte II) della duplice natura del nuovo articolo 16 TFUE, che è base giuridica generale della competenza dell'Unione a legiferare sulla protezione nell'ambito del trattamento dei dati personali[82]. L'importanza di tale innovazione è stata posta in risalto sotto il profilo constituzionale proprio quanto al nesso, che qui vogliamo enfatizzare, con i valori fondanti dell'Unione: «*The European Union acts, under Article 16 TFEU, as a constitutional guardian of privacy and data protection. In an information society, the fundamental rights of privacy and data protection remain essential values for our democracies that are subject to the rule of law. However, at the same time, this information society is challenging the enjoyment of these fundamental rights, with big data and mass surveillance as the most obvious illustrations*»[83]. Posto questo, va segnalato quanto non è stato enfatizzato in precedenza e completa la struttura del regime di protezione dati predisposto dal Trattato di Lisbona[84]: lo stesso articolo 16 TFUE, infatti, fa espresso richiamo all'articolo 39 TUE[85], introdotto precipuamente per fornire una base giuridica speciale in materia PESC, che si affianca a quella generale dell'articolo predetto.

A differenza di quest'ultimo, che trova un suo antecedente nell'articolo 286 TCE, l'articolo 39 TUE rappresenta una totale novità: prima della riforma, infatti, non esisteva alcuna base giuridica specifica sulla protezione dei dati personali nell'ambito PESC, pertanto, la questione era interamente lasciata agli ordinamenti nazionali[86]. Nondimeno, tale norma costituisce una previsione essenzialmente procedurale, volta a prospettare una procedura separata per l'adozione di norme in materia ma che mantiene nella sostanza gli stessi principi basilari sanciti nell'articolo 16 TFUE, confermando la "natura orizzontale" del diritto in esso riconosciuto[87].

Si è detto, peraltro, che con Lisbona questo diritto fondamentale è ritenuto come particolarmente meritevole di tutela non solo in virtù della previsione dell'articolo 16 TFUE ma anche in

[81] C. KUNER, L.A. BYGRAVE, C. DOCKSEY, Background and Evolution of the EU General Data Protection Regulation (GDPR), in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020, p. 3.
[82] B. CORTESE, Articolo 16 TFUE, in A. TIZZANO (a cura di), *I Trattati dell'Unione europea*, Giuffrè, 2014, pp.445-446.
[83] H. HIJMANS, *The European Union as Guardian of Internet Privacy, cit.*, p. 450.
[84] Su cui si vada in modo efficacemente conciso M. KLAMERT, Article 16 TFEU, in M KELLERBAUER, M KLAMERT, J TOMKIN (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Oxford University, 2019, pp. 406-407.
[85] *Articolo 39 TUE*
Conformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.
[86] Come si evince anche da B. CORTESE, Articolo 39 TUE, in A. TIZZANO (a cura di), *I Trattati dell'Unione europea*, Milano, 2014, pp. 290-291.
[87] Così F. PIZZETTI, Article 39 TEU [Protection of Individuals with Regard to the Processing of Personal Data by the Member States], in H.-J. BLANKE, S. MANGIAMELI (Eds), *The Treaty on European Union (TEU) – A Commentary*, Springer, 2013, pp. 1159-1160, si veda in part. il paragrafo su "*Relationship of Art. 39 TEU and Art. 16 TFEU*", p. 1160 ss.

considerazione del fatto che la Carta dei diritti fondamentali assume, *ex* articolo 6 TUE, lo stesso valore giuridico dei Trattati, conferendo maggiore risalto all'articolo 8 precipuamente dedicato alla protezione dei dati di carattere personale. La riforma di Lisbona è dunque di primaria importanza nell'esposizione del nostro lavoro proprio perché fa emergere in maniera palese il legame tra il sistema di valori dell'Unione (con ciò che esso comporta, in termini di affermazione e promozione) e il diritto alla protezione dei dati personali (nella duplice accezione di diritto fondamentale e settore dell'ordinamento giuridico da regolamentare). A corroborare questo legame, si condivide quanto segue: «*The values of democracy, the rule of law and human or – in an EU context – fundamental rights are at the basis of the existence of the European Union. Hence, privacy and data protection as fundamental rights in a developing information society are elements of the wider ambitions of the Union to promote the values laid down in Article 2 TEU*»[88].

Tutto ciò premesso, un indicatore evidente del legame che vogliamo indagare è sicuramente ravvisabile nella previsione dell'apparato istituzionale dedicato alla protezione dei dati, operante (in virtù di e) in conformità con i valori fondanti dell'Unione. L'importanza di tale apparato è stata ancor più enfatizzata dalle nuove previsioni del GDPR, che ha infatti tra i suoi principali obiettivi quello di «*providing a stronger institutional arrangement for the effective enforcement of the data protection rules*»[89]. Si sono descritti gli aspetti essenziali della struttura di tale apparato, dalla sua istituzione ai giorni nostri (dunque tenendo conto anche delle innovazioni del GDPR; cfr. *supra*, Capitolo III, Parte II); qui si vuole invece dimostrare in che termini la previsione di un simile apparato per la protezione dei dati consenta, in teoria, di spiegare il nesso con la *EU rule of law* e, ancor meglio, come la Corte di giustizia abbia contribuito a definire tale nesso. Ciò dovrebbe consentire in seguito (*infra*, Parte IV) di analizzare se, ed eventualmente come, questo nesso effettivamente funzioni in pratica.

A partire, infatti, proprio dalle suddette norme del Trattato di Lisbona, si è assistito a una qualche rimodulazione degli interventi delle istituzioni coinvolte nella protezione dei dati personali, con l'attribuzione della competenza generale *ex* articolo 16 TFUE (e contestuale ricorso alla procedura speciale quanto all'adozione di atti in ambito PESC) che ha trovato la sua principale evidenza (nel pacchetto di riforma e, in particolare) nell'adozione del Regolamento Generale per la Protezione dei Dati personali (GDPR). L'adozione di quest'ultimo ha consentito una rinnovata collaborazione tra

[88] H. HIJMANS, *The European Union as Guardian of Internet Privacy, cit*., p. 29.
[89] H. HIJMANS, Article 51. Supervisory Authority, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2020, p. 865. Qui l'autore precisa: «The GDPR strengthens this institutional framework at EU level, but at the same time respects the EU as a federal system based on executive fe0deralism, where implementation and enforcement takes places at the national level. It remains the responsibility of Member States to provide for supervisory authorities».

le tre istituzioni politiche, nell'ambito di un lungo e complesso processo (si ricorda che è del gennaio 2012 la proposta della Commissione mentre il prodotto finale entrò in vigore solo nel maggio 2016) che ha goduto anche delle influenze sia della Corte di giustizia che delle autorità indipendenti[90]. In tal senso, esso costituisce senz'altro un importante segnale del nesso sussistente tra sistema di valori e di protezione dei dati. L'attenzione istituzionale dedicata, specie nell'ultimo periodo, al settore della protezione dei dati, non solo dalla Commissione ma anche dal Parlamento europeo, e in virtù di soggetti specificamente dedicati – le autorità nazionali indipendenti, ma anche lo *European Data Protection Supervisor* e ancor di più lo *European Data Protection Board* – ne è principale testimonianza: «*There are sometimes distinct, sometimes collaborative, sometimes overlapping roles for these bodies, which has led to a complex and rich policy environment for developing data protection*»[91].

Dunque, e riprendendo il riferimento al Trattato di Lisbona, si vuole anzitutto dedicare attenzione alle istituzioni preposte al controllo sull'osservanza delle norme in materia, ossia le autorità indipendenti. L'importanza del loro ruolo per il buon funzionamento dell'apparato di protezione dati è palesata dal fatto che le tre norme del Trattato di Lisbona dedicate alla materia, ossia i suddetti articoli 16 TFUE, 39 TUE e 8 Carta, sono proprio accomunate da formulazioni pressocché identiche espressamente dedicate al controllo da parte di tali autorità. Passiamo, dunque, ad analizzare le origini e soprattutto gli sviluppi di una figura che è diventata sempre più centrale in tale apparato, anche grazie agli impulsi giurisprudenziali, per comprendere in che termini essa rappresenti parte integrante dell'accostamento *EU rule of law*-protezione dati; ciò anche e soprattutto in vista di quanto ci interesserà più da vicino, ossia il trasferimento di dati verso Paesi terzi.

Nella stessa ottica, verrà esaminato subito dopo anche il ruolo della Commissione.

2. Le autorità indipendenti: portata e implicazioni del controllo

Significati del controllo

[90] Per una dettagliata esposizione si rinvia a C. KUNER, L.A. BYGRAVE, C. DOCKSEY, Background and Evolution of the EU General Data Protection Regulation (GDPR), *cit.*, pp. 3-10.
[91] P. M. SCHWARTZ, Global Data Privacy: The EU Way, *cit.*, p. 782.

Proveremo in questo paragrafo a dimostrare in che termini la previsione di autorità indipendenti costituisca uno dei principali elementi emblematici del legame tra *EU rule of law* e protezione dei dati personali, essenzialmente in virtù di un aspetto particolare che le caratterizza, in senso bidirezionale: il controllo.

Infatti, il controllo che si iscrive nel sistema articolato di autorità a livello nazionale e sovranazionale (nonché nella cooperazione tra queste) è genuinamente espressivo della *EU rule of law*, sia quando esso opera in senso attivo, ossia quando viene effettuato dalle autorità rispetto alla corretta applicazione del diritto alla protezione dei dati personali (come ricorda l'adagio delle tre norme di diritto primario suddette, oltre che in virtù delle previsioni, sia risalenti che aggiornate, di diritto derivato), sia, anche, quando esso opera in senso passivo, ossia nella misura in cui il complesso apparato di protezione dei dati prevede la supervisione dell'attività di tali autorità, in ultima analisi attraverso rimedi giurisdizionali. Cerchiamo di spiegare questa duplice accezione.

Prime previsioni relative alle autorità di controllo

La previsione di autorità di controllo sulla protezione dei dati trova il suo concepimento, a dire il vero, a livello nazionale: oltre alla nota CNIL francese, che venne istituita nel 1978, anche altri Stati europei si dotarono di autorità durante gli anni Settanta (mentre, si ricorda, l'Italia istituì il Garante solo a seguito della necessità di dare attuazione alle previsioni della Direttiva madre)[92].

Un primo timido richiamo a livello internazionale regionale può rintracciarsi nell'*Explanatory Report* alla Convenzione n. 108, che, prendendo atto di alcune normative nazionali esistenti in materia, definiva il "*principio di controllo*" come quello in base al quale "*supervisory authorities as well as the individuals directly concerned by the information can require that the rights and*

[92] Legge n. 675 del 31 dicembre 1996 - *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*; essa prevedeva l'articolo 30, rubricato "Istituzione del Garante", che apriva il Capo VII interamente dedicato a "Garante per la protezione dei dati personali" e che all'articolo 31 (compiti del Garante) richiamava anche l'attività indicata nella Convenzione n. 108, nonché ai fini della cooperazione tra autorità da quest'ultima prevista. Una volta così istituita, tale autorità viene considerata, tra quelle indipendenti presenti in Italia, quella «che riceve dal diritto dell'Unione europea la legittimazione più forte», così A. E. BASILICO, *Le autorità indipendenti tra diritto dell'Unione e sistema interno dei poteri*, Università degli Studi di Milano – Scuola di dottorato in scienze giuridiche, XXV ciclo (IUS/08), AA. 2011/2012, p. 63.
Quanto alle leggi di alcuni Stati membri istitutive di autorità per la protezione dei dati già dagli anni Settata, il riferimento è anzitutto alla Germania che, dopo previsioni del genere in alcuni Lander (in particolare quello di Hesse), nel 1977 si dotò di una "Federal Data *Protection Law*" istitutiva anche di un'autorità a livello federale; in Francia, la legge del 1978 "*Informatique et Libertés*" istituì la famosa *Commission nationale de l'informatique et des libertés* (CNIL, www.cnil.fr); in Svezia, addirittura, l'autorità (IMY) venne istituita nel 1973 (www.imy.se). Per ulteriori approfondimenti sull'evoluzione storica, si veda G. GONZÁLEZ FUSTER, *The emergence of Personal Data Protection as a Fundamental Right of the EU*, pp. 55-71.

interests of those individuals are respected by the data users"[93]. Nessun obbligo, tuttavia, di istituire autorità di controllo veniva espressamente previsto dalla Convenzione per gli Stati parti.

Fu solo a livello sovranazionale, con la Direttiva 95/46, che si sancì per la prima volta l'obbligatorietà per tutti gli Stati membri di istituire autorità preposte alla vigilanza della corretta applicazione della normativa in essa prevista. La Direttiva madre dedicava alle autorità i considerando da 62 a 65 e soprattutto, come si è detto (*supra*, Parte II), il Capo IV rubricato "*Autorità di controllo e Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali*", che si componeva di "soli" tre articoli (esigui, se comparati a quelli che compongono oggi, *strictu sensu*, il Capo VI e, *lato sensu*, anche i Capi VII a VIII del GDPR).

Particolarmente esplicativo dell'intenzione di creare uno specifico apparato istituzionale dedicato alla protezione dei dati, avente il perno in tali autorità, era già il Considerando 62, che recitava: "*considerando che la designazione di autorità di controllo che agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali*", così immediatamente introducendo i due aspetti fondamentali di indipendenza e controllo (ribaditi, infatti, nel paragrafo 1 dell'art. 28, *infra*).

Quanto alle norme del Capo dedicato, mentre gli articoli 29 e 30 riguardavano il c.d. *Gruppo di Lavoro Articolo29*, solo l'articolo 28 si dedicava alle autorità di controllo, ancorché contenente già gli elementi essenziali caratterizzanti tali figure. Esso, infatti, si componeva di diverse norme, tra le quali indispensabili quelle di esordio: "*Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri. Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite*"[94]. Su queste disposizioni, in particolare, la Corte ebbe modo di intervenire e definirne la portata prima dell'entrata in vigore del GPDR. L'articolo continuava poi prevedendo, tra le altre cose, i poteri e i compiti e gli obblighi delle autorità (paragrafi 3, 5, 6 e 7), la necessaria collaborazione tra le stesse (paragrafo 6, comma 2) e inoltre, particolarmente, il diritto di ogni persona di rivolgersi alle autorità per tutelare i propri diritti

[93] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28.1.1981), punto 6 (su *National legislation*), inserisce questo tra i principi che "*all national laws recognise*".

[94] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, Articolo 28, paragrafo 1, commi 1 e 2. Lo stesso articolo recita al paragrafo 3, comma 2: "È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio". Peraltro, il riferimento alla possibilità di istituire più autorità di controllo, ribadito nel GDPR (articolo 51, par. 3), è in linea con la sensibilità verso la articolazione di alcuni Stati con caratteristiche più o meno federali in cui la responsabilità per la protezione dei dati viene esercitata a diversi livelli, come per esempio in Germania (a livello di Lander) o in Spagna (in cui si assiste alla presenza di autorità indipendenti specifiche in Catalogna e nei Paesi Baschi), cfr. H. HIJMANS, Article 51. Supervisory Authority, *cit*., p. 871.

sui dati (paragrafo 4), da un lato, e, dall'altro, quello di agire nei confronti di tali autorità, proponendo ricorso giurisdizionale avverso loro decisioni (paragrafo 3, comma 2).

A livello primario, invece, il primo espresso riferimento a questo tipo di figure si ebbe con la previsione, introdotta dal Trattato di Amsterdam, dell'articolo 286 TCE, relativa all'istituzione di "*un organo di controllo indipendente incaricato di sorvegliare l'applicazione di detti atti alle istituzioni e agli organismi comunitari e adotta, se del caso, tutte le altre pertinenti disposizioni*"[95]. Ciò diede base giuridica al regolamento (CE) n. 45/2001[96] che istituì (articolo 41) il *Garante europeo della protezione dei dati* (di seguito nella sigla inglese: EDPS), quale autorità di controllo sul corretto trattamento di dati personali da parte di istituzioni e organismi comunitari (regolamento, peraltro, poi abrogato e sostituito dal Reg. UE 2018/1725 del 23 ottobre 2018).

L'acquisizione di "*constitutional status*"[97] anche per le autorità nazionali avvenne, invece, come si è visto, nel 2009 con il Trattato di Lisbona, mentre (come si avrà modo di approfondire) il GDPR, con base giuridica nell'articolo 16 TFUE, solidificava e ribadiva il ruolo di primo piano di queste figure (anche forte della giurisprudenza pregressa) e, come noto, istituiva (in luogo del Gruppo di lavoro Articolo 29) il Comitato europeo per la protezione dei dati (di seguito con l'acronimo inglese EDPB), composto dai rappresentanti delle autorità garanti nazionali (anche degli Stati EFTA quanto all'applicazione del GDPR) e dall'EDPS, con il compito di contribuire alla corretta applicazione della normativa sui dati e agevolare la cooperazione tra le varie autorità. In tal senso, il GDPR costituisce un maggiore avanzamento in termini di cooperazione tra autorità di tale "inedito" sistema, a un tempo integrato e decentralizzato[98].

Peraltro, l'ambito di applicazione delle normative indicate incide anche sulla portata dell'intervento delle autorità. Infatti, come si evince dall'articolo 2 del GDPR (come si dirà meglio nel prosieguo), quest'ultimo non si applica al trattamento dei dati personali da parte di istituzioni, organi e organismi dell'Unione, per il quale vige il suddetto regolamento (CE) 45/2001, che prevede

---

[95] Articolo 286 (ex articolo 213 B) Trattato che istituisce la Comunità europea (versione consolidata) (97/C 340/03)
1. A decorrere dal 1° gennaio 1999 gli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati si applicano alle istituzioni e agli organismi istituiti dal presente trattato o sulla base del medesimo.
2. Anteriormente alla data di cui al paragrafo 1 il Consiglio, deliberando secondo la procedura di cui all'articolo 251, istituisce *un organo di controllo indipendente incaricato di sorvegliare l'applicazione di detti atti alle istituzioni e agli organismi comunitari e adotta, se del caso, tutte le altre pertinenti disposizioni*. (enfasi aggiunta)

[96] Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati.

[97] H. HIJMANS, *The European Union as Guardian of Internet Privacy*, *cit*., p. 290.

[98] A. BENSOUSSAN, *Règlement européen sur la protection des données - Textes, commentaires et orientations pratiques*, 2e édition, Bruyant, 2018, p. X: « *le règlement constitue une avancée majeure en terme de gouvernance des autorités de protection des données, à travers un système inédit de coopération entre elles, à la fois intégré sur le fond, et décentralisé sur la forme* ».

l'apposito EDPS. Ma il GDPR non si applica nemmeno al trattamento di dati personali effettuato da autorità nazionali ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, per il quale (in luogo della direttiva 2008/977/GAI) è stata introdotta con il pacchetto di riforma la Direttiva (UE) 2016/680[99] (*supra*, Capitolo III, Parte II, e *infra*, Parte IV).

Sono questi i tre strumenti normativi che coprono ormai l'intero impianto di intervento predisposto a livello sovranazionale per le autorità indipendenti, efficacemente descritto da De Hert e Sajfert come "*Three-Pillar Structure of the EU Data Protection Legal Framework*"[100]. Si ha così una struttura mantenuta "frammentata" che vedrebbe il GDPR coprire il settore commerciale e quello pubblico negli Stati membri, ad eccezione delle autorità di polizia e giustizia penale; la Direttiva 2016/680 coprire il settore relativo a dette ultime autorità negli Stati membri; il Regolamento 45/2001 coprire i trattamenti effettuati dalle istituzioni, organi e organismi dell'Unione, ad eccezione dei database Eurojust e Europol. Secondo gli autori, la scelta di frammentazione sarebbe giustificabile per diverse ragioni, tra cui essenzialmente la necessità di assolvere esigenze diverse, ossia quella di maggiore armonizzazione propria del settore commerciale e, dall'altro lato, quella di mantenere al minimo la salvaguardia di protezione dei dati per bilanciarla con le esigenze di sicurezza nel settore giustizia. Ciò assume rilievo ai nostri fini giusto per segnalare che l'intervento delle autorità garanti dipenderà dunque dal settore in cui operano (per esempio, si escluderebbe il controllo sulle autorità giurisdizionali degli Stati membri; cfr. articolo 45 della Direttiva 680)[101].

Delineato per sommi capi il quadro in cui si inseriscono le autorità, pare utile interrogarsi, aiutandoci con quanto elaborato da Hijmans, sulla necessità/giustificazione di tali figure. In particolare, l'autore individuava sei ragioni che spiegherebbero l'esistenza delle autorità.

La prima avrebbe proprio carattere storico, nel senso che, seguendo il percorso appena descritto, la necessità di armonizzare le pratiche esistenti negli Stati europei in materia di protezione dati avrebbe fatto delle autorità degli strumenti del diritto sovranazionale a tal fine. La seconda risiederebbe nella necessità di un "supporto strutturale" da fornire per garantire la protezione efficace dei diritti dei cittadini e l'effettiva applicazione del diritto dedicato. La terza risiederebbe nella complessa natura del trattamento dei dati e nella derivante necessità di competenze tecniche,

[99] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[100] P. DE HERT. J. SAJFERT, The Role of the Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data, in C. BRIÈRE and A. WEYEMBERGH (Eds), *The Needed Balances in EU Criminal Law: Past, Present and Future*, Oxford, 2018, p. 244.

[101] Ibidem, pp. 245-247 e sull'ultimo aspetto (relativo all'articolo 45 della Direttiva) pp. 248-250.

che verrebbero assolte dalla previsione di autorità specializzate. La quarta consisterebbe nella necessità di controllo, sotto il profilo del trattamento dei dati, tanto del settore privato quanto anche degli stessi governi, cosa che richiede un meccanismo efficace che può ben essere assolto dalla previsione di autorità indipendenti. A questo aspetto si lega la quinta ragione, che risiederebbe nella necessità di indipendenza rispetto a preferenze politiche (cosa che le distinguerebbe dalle agenzie). Quindi, la sesta ragione consisterebbe nei vantaggi derivanti dal connubio di esperienza e flessibilità, nel dedicare totalmente le proprie risorse a tale obiettivo e nel consentire una più agevole cooperazione tra le varie autorità[102]. Queste condivisibili considerazioni sono state in parte tratte dalle elaborazioni della giurisprudenza, soprattutto con riguardo al criterio dell'indipendenza, alle quali si è fatto cenno e che si possono adesso finalmente esaminare.

Prime pronunce della Corte di giustizia sulle autorità indipendenti: i casi di Commissione contro Germania, Austria e Ungheria

La Corte ebbe modo di pronunciarsi proprio sull'articolo 28 della Direttiva madre, anche se in realtà ciò non avvenne prima che arrivassero rinforzi di diritto primario, ovvero (e senza considerare l'articolo 8 della Carta dai tempi, più risalenti del Trattato, in cui quella fu proclamata a Nizza) con le norme contenute nei tre articoli suddetti del Trattato di Lisbona. È nel periodo che accompagna quest'ultimo, infatti, che sorsero i casi riguardanti le autorità, principalmente concentrati sul criterio dell'indipendenza, e che consentirono alla Corte di giustizia di sviluppare il loro ruolo. Si tratta di tre ricorsi per infrazione proposti, in anni diversi, dalla Commissione avverso Germania, Austria e Ungheria.

Nel primo caso, la Commissione lamentava un inadempimento della Germania rispetto alle previsioni della Direttiva per aver sottoposto le autorità indipendenti in essa previste alla vigilanza dello Stato, rintracciando un'erronea applicazione del requisito dell'articolo 28, n. 1, co.2 per cui esse devono essere "pienamente indipendenti". Nella specie, il diritto tedesco effettuava una distinzione nel controllo sul trattamento dei dati personali, prevedendo autorità dedicate (sia a livello federale che di Länder) al controllo su organismi pubblici, responsabili verso i rispettivi parlamenti e non sottoposti a vigilanza, e altre dedicate al controllo su privati, la cui struttura variava nei vari Lander ma presentava l'unico aspetto comune di assoggettamento alla vigilanza dello Stato. Nell'analizzare la questione, la Corte si soffermò per la prima volta sulla "portata dell'esigenza di indipendenza di cui all'art. 28, n. 1, co. 2" la cui interpretazione era essenziale per

[102] H. HIJMANS, *The European Union as Guardian of Internet Privacy, cit*., pp. 290-292.

stabilire la fondatezza del ricorso della Commissione. È nell'ambito di tale analisi che la Corte elaborò la celebre statuizione secondo cui le autorità in oggetto «*sono le custodi dei menzionati diritti e libertà fondamentali, e la loro designazione, negli Stati membri, è considerata, come rilevato dal sessantaduesimo 'considerando' della citata direttiva, un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali. Al fine di garantire detta protezione, le autorità di controllo devono assicurare un giusto equilibrio fra, da un lato, il rispetto del diritto fondamentale alla vita privata e, dall'altro, gli interessi che impongono una libera circolazione dei dati personali*»[103].

Concentrandosi poi, in particolare, sul requisito dell'indipendenza, la Corte chiarì che «*le autorità di controllo competenti per la vigilanza del trattamento dei dati personali nei settori diversi da quello pubblico devono godere di un'indipendenza che consenta loro di svolgere le proprie funzioni senza influenze esterne. Tale indipendenza esclude non solamente qualsiasi influenza esercitata dagli organismi controllati, ma anche qualsivoglia imposizione e ogni altra influenza esterna, diretta o indiretta, che possa rimettere in discussione lo svolgimento, da parte delle menzionate autorità, del loro compito, consistente nello stabilire un giusto equilibrio fra la protezione del diritto alla vita privata e la libera circolazione dei dati personali*»[104]. Interessante quindi l'obiezione sollevata dalla Germania, che riteneva che un'interpretazione ampia dell'indipendenza osterebbe al principio di democrazia, richiedente "una subordinazione dell'amministrazione alle istruzioni del governo, responsabile dinanzi al parlamento", cosa che quindi vorrebbe un controllo sulla legittimità dell'intervento delle autorità da parte di organi eletti. Rispetto a ciò, oltre a ricordare che il principio di democrazia appartiene anche all'ordinamento comunitario (*ex* articolo 6 TUE), la Corte precisò che esso comunque «*non osta all'esistenza di autorità pubbliche collocate al di fuori dell'amministrazione gerarchica classica e più o meno indipendenti dal governo*»[105] e che anzi sarebbe «*inconcepibile l'assenza di qualunque influenza parlamentare sulle autorità in parola. Occorre, tuttavia, rilevare che la direttiva 95/46 non impone affatto agli Stati membri una siffatta assenza di qualunque influenza parlamentare*»[106], stabilendo piuttosto che tali autorità possono essere nominate da parlamento o governo e che il legislatore può sia definirne le competenze che imporre alle stesse di rendere conto al parlamento della loro attività. Ciò, comunque, non osterebbe all'esistenza e al funzionamento di autorità che rispondano al suddetto grado di indipendenza, ma che comunque «*sono soggette al rispetto della legge sotto il controllo*

[103] Corte di giustizia, causa C-518/07, *Commissione c. Germania*, 9 marzo 2010, punti 23-24 (enfasi aggiunta).
[104] Ibidem, punti 25 e 30.
[105] Ibidem, punto 42.
[106] Ibidem, punto 43.

dei giudici competenti»[107]. Così la Corte definì che l'indipendenza di tali autorità nei settori diversi dal pubblico rispetto all'amministrazione centrale non vale «*a privare dette autorità della loro legittimità democratica*» ed è quindi «*un elemento essenziale alla luce degli obiettivi della direttiva (...) [e] imprescindibile al fine di realizzare, in tutti gli Stati membri, un livello egualmente adeguato di protezione (...) e il funzionamento del mercato interno*»[108].

Da questi passaggi pare emergere chiaramente che l'essenza del nesso tra *EU rule of law* e protezione dei dati personali passa inestricabilmente dall'articolazione istituzionale delle autorità indipendenti. Ciò sotto diversi profili, alcuni dei quali rilevati, per esempio, in primi commenti alla sentenza che si condividono di seguito.

Fabbrini, infatti, ritenendo la pronuncia come "un ulteriore passo avanti nello sviluppo di un diritto amministrativo europeo", ha sottolineato che «un ruolo rilevante è rivestito dai sistemi di pubblici poteri indipendenti, messi al riparo dalle istituzioni rappresentative nazionali ed attratte nell'orbita sovranazionale»[109]. Rinnovato risalto, dunque, ai pubblici poteri indipendenti, ma oltre a questo dalla pronuncia si denoterebbe chiaramente «come il diritto europeo plasmi significativamente il diritto amministrativo nazionale, introducendo figure organizzative innovative il cui asse istituzionale viene fatto gravitare sempre più in funzione comunitaria»[110], prosieguo dell'intervento di armonizzazione realizzato dalla Direttiva 95/46 che in alcuni Stati membri (come quello italiano) ha infatti imposto *ex novo* l'istituzione di simili figure.

Dal commento proposto, il profilo che si ritiene di voler maggiormente condividere è quello che (in senso un po' lato) vede nel rafforzamento dell'indipendenza delle autorità nazionali un ulteriore passo avanti della giurisprudenza comunitaria verso la tutela dei diritti fondamentali, specie nell'ambito della "tutela multilivello" che stava trapelando proprio in quegli anni. Ciò, in particolare, in virtù di quanto considerato dall'autore nell'ottica di un'analisi che guardava anche pronunce tedesche dello stesso periodo: «*la decisione dei giudici comunitari interviene ad una settimana di distanza dalla presa di posizione del Bundesverfassungsgericht, il quale, pronunciandosi sulla legge tedesca di recepimento della Direttiva 2006/24/CE sulla ritenzione dei dati per finalità di lotta al terrorismo, ne ha dichiarato l'illegittimità costituzionale - pur senza mettere in discussione la legittimità della Direttiva europea stessa*»[111].

[107] Ibidem punto 42. Poco prima il riferimento (non citazione) è ai punti 44 e 45.
[108] Ibidem, punti 46 e 50.
[109] F. FABBRINI, Il diritto dell'Ue e l'indipendenza delle autorità nazionali garanti della protezione dei dati, in *Giornale di diritto amministrativo*, n. 10/2010, p. 1032.
[110] Ibidem.
[111] Ibidem.

Di qui si potrebbe ben passare a considerazioni ulteriori (alcune, invero, sviluppate dall'autore) sulla Direttiva 2006/24/CE e sulla celeberrima pronuncia *Digital Rights Ireland* (di seguito anche *DRI*) della Corte di giustizia, di qualche anno successiva, che, com'è noto, dichiarò quella direttiva invalida; tuttavia, si andrebbe troppo lontano rispetto all'argomento oggetto di analisi in questa fase, ossia il ruolo delle autorità indipendenti. Si avrà largo modo di commentare la *DRI* e le importanti implicazioni nel nostro settore, ma tale minimo riferimento basti qui per riconoscere come effettivamente tutti gli aspetti relativi alla protezione dei dati personali, trattati spesso in maniera settoriale e parcellizzata anche dalla Corte (che tiene spesso a definire in maniera netta l'ambito dell'intervento rispetto al caso specifico), confluiscono comunque, infine, verso la stessa logica e sono trattati dalle istituzioni, e dalla Corte in particolare, con un approccio abbastanza armonizzato.

Proseguendo, quindi, l'analisi sulle pronunce seminali dedicate alle autorità indipendenti, le considerazioni sul caso tedesco vennero riprese nel secondo caso contro l'Austria, introdotto dalla Commissione per lamentare l'inadempimento rispetto alla medesima disposizione della direttiva nella misura in cui riteneva che l'autorità austriaca non rispondesse al requisito di piena indipendenza. In particolare, secondo la normativa austriaca, il membro amministratore dell'autorità doveva sempre essere un funzionario della cancelleria federale.

Ebbene, la Corte, dopo aver richiamato la suddetta interpretazione della norma circa il criterio di indipendenza, stabiliva chiaramente che, a differenza di quanto sostenuto dall'Austria, la c.d. «*indipendenza funzionale* [secondo cui i membri dell'autorità non sono vincolati da alcuna istruzione nell'esercizio delle loro funzioni] *da sola non è sufficiente per preservare la suddetta autorità di controllo da qualsiasi influenza esterna*»[112]. Quindi, la Corte rilevava che «*indipendentemente dall'autorità federale cui appartiene il membro amministratore della DSK, è pacifico che sussiste un legame di servizio tra quest'ultimo e la suddetta autorità federale, che consente al superiore gerarchico di detto membro amministratore di controllare le attività di quest'ultimo*»[113]. L'interpretazione della direttiva fornita dalla Corte contrasterebbe dunque con tale "controllo di servizio" cui il membro dell'autorità sarebbe soggetto[114]. Anche in questo caso, quindi, visti i legami tra l'autorità di controllo sui dati e la cancelleria federale consentiti dalla normativa austriaca, la Corte accolse il ricorso della Commissione, così ribadendo l'importanza della posizione di indipendenza delle autorità per la protezione dei dati.

Peraltro, come è stato commentato, questa pronuncia mette in risalto che il requisito di indipendenza delle autorità preposte, a livello nazionale, alla vigilanza del diritto alla protezione dei

[112] Corte di giustizia, causa C-614/10, *Commissione c. Austria*, sentenza del 16 ottobre 2012, punto 42.
[113] Ibidem, punto 48.
[114] Ibidem, punto 50, ma si vedano anche i punti 55-60.

dati non risponda – solo – ad obiettivi di mercato ma sia sempre più volto a preservare anche la tutela degli individui: «*the essential message of Commission v. Austria is that the independence of certain specific national authorities enforcing the various pieces of EU legislation, being comprehensively regulated in EU secondary legislation, reveals its importance now not only in some economic (market) areas, traditionally perceived as the typical fields of activity of independent regulators (e.g. network-bound sectors, financial markets), but also in certain social spheres, and in the sphere of private life of individuals. This visible trend seems to support the thesis that the objectives (and values) underlying the requirement of independence of national authorities supervising the economic and non-economic fields are in fact very similar, and indeed justify such a far-reaching institutional convergence*»[115].

Il terzo caso riguardava, infine, un ricorso avverso l'Ungheria, con il quale la Commissione riteneva che lo Stato fosse venuto meno agli obblighi derivanti dalla Direttiva, ancora una volta sotto il profilo dell'indipendenza dell'autorità di controllo sui dati, per aver posto fine al suo mandato prima della scadenza naturale del termine. La Corte si trovò a stabilire anzitutto se gli interventi incidenti sulla durata del mandato delle autorità di controllo rientrassero nel vincolo *ex* articolo 28 della direttiva (*rectius*, se il requisito di indipendenza in esso previsto implicasse l'obbligo per lo Stato di rispettare la durata del mandato sino al termine inizialmente previsto, cfr. punto50 sentenza). In quell'occasione, la Commissione e l'EDPS (intervenuto a sostegno della prima) riconoscevano che gli Stati effettivamente godessero di un margine di manovra quanto all'applicazione dell'articolo 28, anche con riguardo alla determinazione della durata del mandato delle autorità di controllo, ma ritenevano anche che, una volta stabilita, tale durata dovesse essere rispettata, salvo gravi e oggettivi motivi, anche in virtù di un paragone con le previsioni del regolamento istitutivo dell'EDPS[116].

Forte della sua giurisprudenza pregressa, la Corte anzitutto ribadì l'insufficienza di un'indipendenza funzionale, sottolineando che il mero rischio di influenze politiche delle autorità statali sulle decisioni delle autorità di controllo, in termini di "obbedienza anticipata" o di semplice sospetto di parzialità, basterebbe ad ostacolare lo svolgimento indipendente delle funzioni[117]. Quindi, con riguardo al problema specifico della durata, dedusse che «*se fosse consentito ad ogni Stato membro porre fine al mandato di un'autorità di controllo prima del relativo termine inizialmente previsto senza rispettare le norme e le garanzie prestabilite a tal fine dalla legislazione applicabile, la*

[115] M. SZYDŁO, Principles underlying independence of national data protection authorities: *Commission v. Austria*, in *Common Market Law Review*, 50, 2013, p. 1811.
[116] Corte di giustizia, causa C-288/12, *Commissione c. Ungheria*, sentenza del 8 aprile 2014, punto 38.
[117] Ibidem, punti 52-53.

minaccia di una tale cessazione anticipata incombente su detta autorità durante l'intero esercizio del suo mandato potrebbe condurre ad una forma di obbedienza al potere politico in capo alla stessa, incompatibile con detto requisito di indipendenza»[118]. Per consolidare questa posizione, la Corte accolse poi in quell'occasione una comparazione con l'EDPS, rilevando che le norme relative alla cessazione del mandato di quest'ultimo confermassero che il rispetto del termine sino alla scadenza è una "condizione imprescindibile di indipendenza" dell'autorità[119]. La Corte concluse quindi per la constatazione dell'inadempimento dell'Ungheria rispetto agli obblighi derivanti dalla direttiva 95/46, ravvisabile proprio nella fine anticipata del mandato dell'autorità di controllo.

A partire da queste pronunce, quindi, si fece sempre più chiaro che le autorità di controllo istituite presso gli Stati membri fossero «*no longer only part of the national administration, but also have become part of the EU administration*»[120], cosa soprattutto rinsaldata dalle previsioni del GDPR.

Caratteristiche peculiari delle autorità di controllo

Nondimeno, e anche in virtù di tale ultimo riferimento alla collocazione delle autorità nell'articolato apparato istituzionale di protezione dei dati, va detto che l'indipendenza è solo *uno* degli aspetti caratteristici di tali autorità, anche nell'ottica del legame che stiamo rintracciando. Almeno altri due elementi (peraltro rintracciabili nella giurisprudenza esposta) vanno infatti presi in considerazione per comprendere il ruolo di tali figure nel contesto in cui si collocano: effettività e responsabilità.

Hijmans li analizza specificamente, provando ad indagare «*how the independence and effectiveness of the DPAs can be best reconciled with requirements of accountability, in a democratic society under the rule of law*»[121]. Ci limiteremo ad alcuni richiami della sua analisi, tratti essenzialmente da valutazioni sulla suddetta giurisprudenza, per acquisire gli spunti funzionali al nostro discorso. Anzitutto, da quella giurisprudenza emergerebbero efficacia e affidabilità del controllo come finalità: «*La garanzia dell'indipendenza delle autorità nazionali di controllo è diretta ad assicurare l'efficacia e l'affidabilità del controllo del rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali e deve essere interpretata alla luce di*

[118] Ibidem, punto 54.
[119] Ibidem, punto 56.
[120] H. HIJMANS, Article 51. Supervisory Authority, *cit*., p. 869. Da notare che l'autore, mentre nel recente passo citato in commento all'Articolo 51 del GDPR (del 2020) pare abbastanza fermo nella sua affermazione, qualche anno prima (2016) nel precedente lavoro '*The European Union as Guardian of Internet Privacy*', *cit.*, riferiva in maniera più prudente che «*possibly, with a wide interpretation of Article 298 TFEU (…), the national DPAs can be regarded as part of the European Administration*», p. 288.
[121] H. HIJMANS, *The European Union as Guardian of Internet Privacy*, *cit*., p. 287.

tale finalità»[122]. Ciò si esprimerebbe anche nel compito riconosciuto alle autorità di effettuare un corretto bilanciamento tra interessi apparentemente contrastanti, ossia protezione dei dati e libera circolazione degli stessi[123]. Così, soprattutto dalla prima pronuncia sulla Germania, la Corte avrebbe enfatizzato il legame tra indipendenza ed effettività, sulla base del quale l'autore ritiene che proprio in quest'ultima debba rintracciarsi la fonte di legittimazione delle autorità indipendenti, intendendola come "*output legitimacy*" (che ricordiamo di aver esposto *supra*, Parte I).

Invero di "poteri effettivi d'intervento" delle autorità indipendenti parlava già il paragrafo 3 dell'articolo 28 della Direttiva, mentre l'autore ribadiva che «*Effectiveness is the second building block for a good functioning of the control by DPAs, in the same way as effectiveness is required for any government action. A democracy without adequate powers cannot function as a democracy and the case law of the Court of Justice constantly emphasises the principle of effectiveness as a cornerstone of EU law, including European administrative law to which the DPAs are also subjected. For DPAs, effectiveness is an important raison d'être. DPAs have added value, because they are expected to be an effective tool in the protection of personal data*»[124]. Ebbene, se da un lato l'autore poneva forte l'accento su questo requisito, come indispensabile in teoria per un corretto ed effettivo funzionamento del sistema predisposto dalla direttiva, dall'altro lato si doleva di riscontrarne talvolta in pratica una mancanza: «*At present, a presumed lack of effectiveness of DPAs is seen as a major deficiency of data protection in the European Union, with an emphasis on insufficiencies in the powers and resources of the DPAs*»[125]. Ciò veniva affermato dopo il Trattato di Lisbona, ma quando ancora il GDPR non era entrato in vigore. La Commissione europea, infatti, metteva in luce anche tali carenze nella proposta di regolamento (del 2012): «esistono difficoltà pratiche nell'attuare efficacemente la normativa in materia di protezione dei dati e occorre stabilire una cooperazione tra gli Stati membri e le autorità nazionali a livello di Unione, per garantire uniformità nell'applicazione del diritto dell'UE»[126]. Così, in effetti, il GDPR ha cercato proprio di aggiustare il tiro su questo aspetto, palesando una "tendenza" che è riscontrabile nelle disposizioni del Capo VI: «*Making DPAs stronger and more European*»[127]. Se e quanto ciò sia avvenuto a

[122] *Commissione c. Germania*, cit., p. 25.
[123] Ibidem, pp. 314-315. Il riferimento è alle sentenze: *Commissione c. Germania*, punti 30 e 50; *Commissione c. Ungheria*, punto 51.
[124] Ibidem, pp. 322-323.
[125] Ibidem, p. 323.
[126] Commissione europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, COM (2012) 11 final, p. 6.
[127] H. HIJMANS, Article 51. Supervisory Authority, *cit*., p. 867. L'autore scriveva infatti a quattro anni di distanza e commentando la norma di apertura del GDPR dedicata alle autorità, dunque ben consapevole delle pregresse criticità e con un rinnovato spirito critico, con cui precisava: «*Article 51 GDPR reflects an important underpinning for the reform of the EU data protection law: the role of the supervisory authorities needs to be strengthened, to ensure that data*

seguito dell'entrata in vigore del Regolamento, nonché soprattutto con le spinte della più recente giurisprudenza al riguardo, sarà oggetto dell'analisi delle autorità in pratica (v. *infra*, Parte IV).

Quanto all'ultimo elemento di rilievo, che si è in parte introdotto con l'analisi della giurisprudenza, emergerebbe che le autorità non sfuggono alla *responsabilità* nei confronti dei parlamenti eletti (si veda quanto detto sul principio di democrazia rispetto alla causa *Commissione c. Germania*, punti 41-46). Sebbene la discrezionalità degli Stati al riguardo risulti ridotta a seguito del GDPR, quest'ultimo consente la nomina dei membri delle autorità da parte dei parlamenti; «*Moreover, the case law gives some further indication on ensuring accountability in a more general sense, since the Court does not preclude that governmental bodies have a right to be informed*»[128]. Sul requisito della responsabilità, Hijmans ha anche sviluppato un interessante parallelo con le agenzie autonome (di cui si riporta di seguito solo un breve passaggio), oltre che un più generale inquadramento sistemico delle stesse che si ritiene utile condividere: «*The DPAs have a responsibility in supervising compliance that does not exist in most other areas of law, in any event not in the field of the protection of other fundamental rights. There is a similarity with autonomous agencies operating in a number of other areas, for instance where these bodies are set up to ensure supervision of the markets. The DPAs as well as these agencies are expert bodies exercising public tasks at a certain distance from the traditional governmental structures that are characterised by the separation of powers under the traditional trias politica or – in case of the European Union – the institutional balance. However, there are also significant differences, because of the DPAs' specific tasks –fundamental rights, not market supervision – and because of the fact that the DPAs do not exercise their tasks on the basis of powers delegated to them by governmental bodies. Their independent role results directly from the Treaties*»[129]. Questa preziosa descrizione ci aiuta a comprendere meglio, anche forti della giurisprudenza suddetta, il ruolo delle autorità nei due livelli di interazione (nazionale e sovranazionale) in cui si articola l'apparato istituzionale europeo di protezione dei dati personali e ci consente di avere un'idea della "distanza" rispetto alle altre istituzioni, nazionali ed europee. Ciò riguarda tanto la definizione della posizione che dei compiti delle autorità.

Quanto alla loro posizione, si condivide la classificazione proposta dall'autore, che le considera come una sorta di "ibrido", a metà tra il livello nazionale e sovranazionale, poiché da un lato riconosciute come "guardiane" della protezione dei dati in virtù del diritto primario dell'Unione,

---

protection is not only delivered in the books, but also on the ground. Strengthening their role has two features in the GDPR: DPAs themselves should be better equipped, and DPAs should work in a more European fashion».

[128] Ibidem, p. 322. Il riferimento è alle sentenze *Commissione c. Germania*, punti 25 e 41-46, e, più in generale, *Commissione c. Austria*.

[129] Ibidem, p. 286 (sottolineato aggiunto).

dall'altro pur sempre autorità nazionali e in quanto tali responsabili della corretta applicazione del diritto UE all'interno degli Stati membri[130]. Così intesa, la posizione delle autorità nel sistema istituzionale di protezione dei dati pare essersi mantenuta, ed anzi accentuata, anche dopo la riforma 2016. Tale posizione assumere un rilievo ancora maggiore proprio per le peculiarità del contesto in cui si colloca, ossia quello della "*internet society*", in cui elemento destabilizzante è proprio la *mancanza di controllo,* e rispetto alla quale i metodi tradizionali si rivelano in qualche modo inadeguati quanto a fenomeni «*like big data and mass surveillance, which reflect large asymmetries in knowledge and power. The DPAs are an additional tool for oversight on the use of information and are an additional instrument to regain trust in governments and in the European Union, provided that the DPAs operate in an independent, effective and accountable way*»[131].

Per tale ragione, anche in considerazione dell'importanza del controllo operato dalle autorità, un altro aspetto fondamentale che aiuta a definirne il ruolo (in aggiunta alla posizione che esse assumono) è dato dallo *svolgimento dei compiti e dall'esercizio dei poteri ad esse attribuiti,* che, oltre ad essere espressione dell'indipendenza e dell'effettività di tali figure, interviene anche a caratterizzarne la responsabilità.

Cooperazione tra autorità di controllo: il nuovo meccanismo dello sportello unico

Come si diceva, mentre la direttiva madre dedicava il solo articolo 28 ai poteri e compiti delle autorità, essi sono stati considerevolmente intensificati con il GDPR. Quest'ultimo, peraltro, se non ha inciso sulla posizione "ibrida" della autorità, ha sicuramente apportato un'importante innovazione in termini di cooperazione tra le autorità all'interno dell'Unione, non solo in virtù dell'istituzione del EDPB, *ex* articolo 68 (cui si è fatto cenno *supra*), ma anche tramite

[130] Ibidem, p 287: «*Their position is to a certain extent hybrid, as they are attached both to the constitutional frameworks of the Member States as well as to that of the European Union*».
Nello stesso senso continuava l'autore a p. 288: «*The Treaties have positioned the DPAs as independent bodies with a constitutional nature responsible for a specific aspect of EU law, namely the control on the rules on data protection. The DPAs have to fulfil their tasks within the constitutional frameworks of the Member States, based on a separation of powers or trias politica, but they are not part of it, and within the constitutional framework of the Union, which is characterised by a closed system of institutional balance of powers as intended by the Treaties, but they are equally not part of it*».
[131] Ibidem, p. 289.

l'introduzione del c.d. *meccanismo dello sportello unico*, richiamato dal Considerando 127 del GDPR come "*cooperazione tra l'autorità di controllo capofila e altre autorità interessate*"[132].

La figura di c.d. *autorità di controllo capofila* è infatti una totale novità prevista dall'articolo 56 del GDPR come fulcro del meccanismo di sportello unico, nella gestione di situazioni transfrontaliere tra Stati membri dell'Unione, identificata come "l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento"[133] (salvo i casi dell'articolo 55). Dalla nota informativa dedicata all'autorità di controllo capofila del Garante italiano si chiarisce inoltre che: «L'obiettivo della devoluzione di competenze a favore dell'autorità capofila è garantire l'esistenza di uno "sportello unico" per i trattamenti transfrontalieri di dati personali: principio sancito dal paragrafo 6 dell'art. 56 ("L'autorità di controllo capofila è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale titolare o responsabile")»[134]. Ciò vale in linea generale, ma sono previste eccezioni anche dal regolamento. Orbene, se il meccanismo di sportello unico, pur con alcune differenze, era ovviamente oggetto della proposta della Commissione[135], va detto che un importante intervento in tale ambito si ebbe già prima dell'entrata in vigore del regolamento da parte della Corte, nel noto caso *Weltimmo*.

---

[132] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati, in seguito: GDPR), Considerando (127).

[133] GDPR, Articolo 56 – *Competenza dell'autorità di controllo capofila*.
Si consideri anche il Considerando (124): «*Qualora il trattamento dei dati personali abbia luogo nell'ambito delle attività di uno stabilimento di un titolare del trattamento o di un responsabile del trattamento nell'Unione e il titolare del trattamento o il responsabile del trattamento sia stabilito in più di uno Stato membro o qualora il trattamento effettuato nell'ambito delle attività dello stabilimento unico di un titolare del trattamento o responsabile del trattamento nell'Unione incida o possa verosimilmente incidere in modo sostanziale su interessati in più di uno Stato membro, l'autorità di controllo dello stabilimento principale del titolare del trattamento o del responsabile del trattamento o dello stabilimento unico del titolare del trattamento o del responsabile del trattamento dovrebbe fungere da autorità capofila. Essa dovrebbe cooperare con le altre autorità interessate perché il titolare del trattamento o il responsabile del trattamento ha uno stabilimento nel territorio dei loro Stati membri, perché il trattamento incide in modo sostanziale sugli interessati residenti nel loro territorio o perché è stato proposto loro un reclamo. Anche in caso di reclamo proposto da un interessato non residente in tale Stato membro, l'autorità di controllo cui è stato proposto detto reclamo dovrebbe essere considerata un'autorità di controllo interessata. Nell'ambito del suo compito di rilascio di linee guida su qualsiasi questione relativa all'applicazione del presente regolamento, il comitato dovrebbe essere in grado di pubblicare linee guida in particolare sui criteri da prendere in considerazione per accertare se il trattamento in questione incida in modo sostanziale su interessati in più di uno Stato membro e su cosa costituisca obiezione pertinente e motivata*».

[134] Garante per la protezione dei dati personali, *Autorità di Controllo Capofila – L'Autorità di Controllo Capofila e la cooperazione prevista dal meccanismo di "sportello unico" nel Regolamento 2016/679*, disponibile qui: https://www.garanteprivacy.it/regolamentoue/acc .

[135] Per una breve ma efficace spiegazione dei passaggi fondamentali che scandirono la "costruzione" del meccanismo di sportello unico (anche noto con la locuzione inglese "*one-stop-shop mechanism*") si veda C. KUNER, L.A. BYGRAVE, C. DOCKSEY, Background and Evolution of the EU General Data Protection Regulation (GDPR), in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020, pp. 36-37.

Si trattava di un rinvio pregiudiziale sollevato dal giudice ungherese riguardante la società Weltimmo, registrata in Slovacchia e che gestiva un servizio web di annunci immobiliari relativi a beni situati in Ungheria e che utilizzava come lingua predefinita l'ungherese, consentendo la possibilità di inserire annunci gratuitamente per un mese, dopo il quale questi divenivano a pagamento. La società trattava i dati degli inserzionisti, molti dei quali scaduto il mese chiedevano la cancellazione degli annunci e dei dati, cosa che la Weltimmo non fece, fatturando i servizi forniti ed inviando, a seguito di mancato pagamento, i dati degli interessati ad agenzie di recupero crediti. Questi ultimi per la violazione subita si rivolsero all'autorità di controllo ungherese, la quale si ritenne competente e irrogò un'ammenda alla società per la violazione appurata. La Weltimmo agiva dinanzi al giudice ungherese contro la decisione dell'autorità di controllo nei suoi confronti, ritenendo che detta autorità fosse incompetente e che non si potesse applicare il diritto ungherese poiché la propria sede di stabilimento non era in Ungheria. Le due parti invocavano l'articolo 28, paragrafo 6 della Direttiva madre – che stabilisce che ogni autorità è competente ad esercitare i propri poteri, conferiti dal par. 3, sul territorio del proprio Stato membro e anche che ogni autorità può essere invitata ad esercitare tali poteri da un'autorità di un altro Stato membro – con due diversi e contrapposti propositi: la Weltimmo, per ritenere che l'autorità ungherese avrebbe dovuto inviare il caso alla collega slovacca; l'autorità, per confermare la propria competenza[136]. La Corte si trovò dunque a dover interpretare diverse disposizioni della Direttiva e, vista la delicatezza delle implicazioni, tale compito suscitò da subito perplessità[137].

Richiamando la propria recente e celeberrima giurisprudenza sull'ambito di applicazione territoriale della direttiva come "particolarmente esteso"[138] (il riferimento è al caso *Google Spain*; si avrà modo di tornare sull'argomento, anche alla luce del GDPR, *infra* Capitolo I, Parte IV), la Corte ha insistito sulla «*concezione flessibile della nozione di stabilimento, che si discosta dall'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata. Infatti, per determinare se una società, responsabile di un trattamento dei dati, dispone di uno stabilimento, ai sensi della direttiva, 95/46, in uno Stato membro diverso dallo Stato membro o dal paese terzo in cui è registrata, occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura*

[136] Corte di giustizia, causa C-230/14, *Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, sentenza del 1° ottobre 2015, punti 9-13. Sulle precise questioni pregiudiziali, punto 14.
[137] Cfr. E. GYŐZŐ SZABÓ, The Weltimmo case in light of the future General Data Protection Regulation. One-stop-shop – burden or catalyst among cooperating data protection authorities? – selected intervention from the PHAEDRA Final Conference, in P. DE HERT, D. KLOZA AND P. MAKOWSKI (Eds), *Enforcing privacy: lessons from current implementation and perspectives for the future*, Warszawa, 2015, che, per esempio, ammetteva: «*My fear is that the CJEU will come to the conclusion that registration plays a more important role than the place of activity. In turn, this will create a legal loophole which will make the DPA's work much more complicated*», p. 116.
[138] *Weltimmo*, cit., p. 27.

specifica delle attività economiche e delle prestazioni di servizi in questione. Ciò vale soprattutto per imprese che offrono servizi esclusivamente tramite Internet. (…) la nozione di «stabilimento», ai sensi della direttiva 95/46, si estende a qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile. Nel caso di specie, l'attività esercitata dalla Weltimmo consiste, quantomeno, nella gestione di uno dei vari siti Internet di annunci immobiliari riguardanti beni situati in Ungheria, scritti in lingua ungherese e i cui annunci diventano a pagamento dopo un mese. Occorre dunque affermare che tale società svolge un'attività concreta ed effettiva in Ungheria»[139]. Sull'aspetto, poi, che più ci interessa, la Corte precisò la portata dei poteri attribuiti alle autorità di controllo stabilendo che «*Si evince quindi dall'articolo 28, paragrafo 6, della direttiva 95/46 che l'autorità di controllo di uno Stato membro alla quale persone fisiche presentano un reclamo relativo al trattamento di dati personali che le riguardano, in base all'articolo 28, paragrafo 4, di tale direttiva, può esaminare tale reclamo indipendentemente dalla legge applicabile e, di conseguenza, anche se il diritto applicabile al trattamento dei dati interessati è quello di un altro Stato membro. Tuttavia, in tale ipotesi, i poteri di tale autorità non comprendono necessariamente tutti quelli di cui è investita secondo il diritto del suo Stato membro. Infatti (…) dalle esigenze derivanti dalla sovranità territoriale dello Stato membro, dal principio di legalità e dalla nozione di Stato di diritto discende che il potere sanzionatorio non può avere luogo, in linea di principio, al di fuori dei limiti legali entro cui un'autorità amministrativa è autorizzata ad agire secondo il diritto nazionale del suo Stato membro*»[140].

La pronuncia veniva subito accolta come avente un impatto presumibilmente forte sulla proposta di regolamento, essenzialmente sotto due aspetti: «*the external scope of that Regulation (…) and the powers of national data protection authorities and the relationships between them - particularly whether there should be a 'one-stop shop' for regulation (…)*»[141]. Dunque, la Woods, del commento, dava risalto essenzialmente alla riconferma da parte della Corte della reiterazione dell'approccio utilizzato in *Google Spain*, quanto all'applicazione territoriale della normativa e, più in generale, all'attenzione alla natura fondamentale del diritto alla protezione dei dati e «*the need to interpret legal concepts broadly to ensure an adequate protection for those rights. This trend has,*

[139] Ibidem, punti 29 e 31-32.
[140] Ibidem, punti 54-56, enfasi aggiunta. Inoltre, così continuava al punto 57: «*Così, quando ad un'autorità di controllo viene presentato un reclamo, secondo l'articolo 28, paragrafo 4, della direttiva 95/46, essa può esercitare i suoi poteri investigativi indipendentemente dal diritto applicabile e ancor prima di sapere quale sia il diritto nazionale che si applica al trattamento controverso. Tuttavia, essa, qualora giunga alla conclusione che si applica il diritto di un altro Stato membro, non può imporre sanzioni al di fuori del territorio del suo Stato membro. In una situazione del genere, essa è tenuta, in virtù dell'obbligo di collaborazione di cui all'articolo 28, paragrafo 6, di tale direttiva, a chiedere all'autorità di controllo di tale altro Stato membro di accertare un'eventuale violazione di tale diritto e di imporre sanzioni se questo lo consente, appoggiandosi, se del caso, sulle informazioni che essa le avrà comunicato*».
[141] L. WOODS, Data protection: the CJEU clarifies the applicable law and jurisdiction, in *EU Law Analysis*, 13 October 2015.

of course, since been confirmed by the subsequent judgment in Schrems»[142]. Tuttavia, a nostro avviso, l'aspetto che risulta predominante è proprio quello relativo alla definizione dei poteri e compiti delle autorità e alla gestione della cooperazione tra di loro. Cooperazione che, difatti, godette di particolare attenzione nel GDPR, e ciò non solo con riguardo al meccanismo di sportello unico.

Infatti, dopo aver elencato, in maniera molto più dettagliata rispetto alla Direttiva, i compiti delle autorità di controllo all'articolo 57 e i poteri all'articolo 58, il GDPR dedica il successivo Capo VII a "*cooperazione e coerenza*" (articoli 60-76, in particolare l'articolo 60 su "cooperazione" e il 68, come detto, sul EDPB). In queste previsioni (poteri e compiti delle autorità e cooperazione tra di esse) è stata ravvisata quella sempre maggiore "europeizzazione" delle autorità indipendenti cui si è fatto cenno, e che comprenderebbe anche la cooperazione in senso lato, ossia non solo tra autorità indipendenti e/o EDPB ma anche, ancorché nei limiti richiesti dall'indipendenza, con la Commissione europea[143].

A tal proposito, il GDPR dedica il Capo VII a "cooperazione e coerenza", prevedendo nella Sezione I il funzionamento del meccanismo di cooperazione, in particolare: la cooperazione tra l'autorità di controllo capofila e le altre autorità interessate (articolo 60); l'assistenza reciproca (articolo 61); le operazioni congiunte tra autorità (articolo 62). La Sezione II, invece, è dedicata alla coerenza (di cui si dirà meglio, *infra* par. 3) delle attività svolte dalla autorità e pertanto disciplina i necessari rapporti a tali fine con il Comitato (EDPB) e con la Commissione, prevedendo il c.d. meccanismo di coerenza (articolo 63), gli interventi dell'EDPB a tal fine (articoli 64 e 65), la procedura d'urgenza in circostanze eccezionali (articolo 66) e l'intervento della Commissione per specificare lo scambio di informazioni tra autorità (articolo 67).

L'insieme di queste importanti innovazioni apportate dal GDPR rispetto alle autorità nazionali di controllo è stato enfatizzato in termini condivisibili, che consentiranno anche successive riflessioni (*infra*, Capitolo III): «*The new competences and powers of DPAs under the GDPR are definitely putting national data protection authorities in a stronger position to enforce EU data protection law. The enlarged scope of application of the Regulation, a clear set of powers for DPAs, the one stop shop and the consistency mechanism coupled with DPAs' possibility to apply high fines in*

[142] Ibidem.

[143] Il riferimento è sempre a H. HIJMANS, Article 51. Supervisory Authority, *cit*., p. 869. Ivi, infatti l'autore precisa: "*cooperation as an instrument relating to the consistent application of the EU is closely linked to the task of the Commission as Guardian of the Treaties, as defined in TEU Article 17 (…). It is understandable in this context that the GDPR should specifically provide that DPAs should cooperate with the Commission. The right of the Commission to partecipate in the activities and meetings of the EDPB has the same backgroud. However, the cooperation between DPAs and the Commission also has limits in view of the independence of DPAs and the fact that this independence precludes any external inlfuence, as specified in the case law of the CJEU*", p. 869.

cases of infringements will ensure a higher and more consistent level of protection of EU residents in relation to both EU and non EU based companies. The A29 WP refers in its action plan for the implementation of the GDPR to a 'brand new governance model, consisting of distributed governance built on three pillars namely, national DPAs, their cooperation and the EDPB for ensuring consistency»[144].

Tutto questo corrobora le peculiarità che caratterizzano le autorità come espressive della *EU rule of law*, ed è anche funzionale alla comprensione delle complesse dinamiche che hanno interessato anche la c.d. *saga Schrems* (sin dagli esordi, come si vedrà, ma ancora anche dopo l'ultima pronuncia del luglio 2020), e che sono ancor più all'ordine del giorno proprio a causa delle complessità che il meccanismo dello sportello unico comporta in pratica. Il riferimento è al caso *Facebook Ireland*, su cui la Corte di giustizia si è pronunciata lo scorso giugno 2021, che si avrà modo di commentare meglio nel prosieguo (*infra*, Capitolo II, Parte IV). Qui basti anticipare che, in tale recente pronuncia, la Corte posto l'accento sulla necessità di una stretta cooperazione tra le autorità, in definitiva dimostrando di voler rafforzare, piuttosto che ridimensionare (come pure le criticità rilevate dal caso potevano far auspicare) il funzionamento del nuovo meccanismo previsto dal GDPR[145]

Le autorità come espressione del nesso tra EU rule of law e protezione dei dati personali

Tutte queste considerazioni ci consentono quindi di apprezzare il significato del nesso tra *EU rule of law* e protezione dei dati nella previsione delle autorità indipendenti.

Infatti, come abbiamo visto, la definizione della loro posizione "ibrida" nel contesto costituzionale dei livelli nazionali e sovranazionale rappresenta un *unicum* ma al contempo, e proprio per le sue peculiarità, completa e così connota la concezione di *EU rule of law*, specie attraverso il controllo esercitato nel particolare settore di base "incontrollato" dell'Internet. E ciò, come si è visto, avviene sia in virtù dell'indipendenza ad esse riconosciuta rispetto alle altre istituzioni (e che quindi, come chiarito dalla giurisprudenza, non è solo funzionale ma proprio istituzionale), sia anche in virtù della cooperazione, caratteristica e necessaria non solo tra le varie autorità degli Stati membri ma anche, nei limiti, con altre istituzioni come soprattutto la Commissione (si veda *infra*, Capitolo III).

[144] A. GIURGIU, T. A. LARSEN, Roles and Powers of National Data Protection Authorities, in *European Data Protection Law Review* (EDPL), vol. 2, n. 3, 2016, p. 351.
[145] Corte di giustizia, C-645/19, *Facebook Ireland Limited*, 15 giugno 2021.

Questi aspetti incidono, poi, anche sull'effettività dell'intervento delle autorità, che si è detto essere elemento irrinunciabile per il funzionamento del sistema di protezione dei dati, richiesto sempre dalla giurisprudenza, e che trova ancora nella cooperazione un importante riscontro (ma la cui concreta realizzazione, nell'esercizio dei poteri e dei compiti anche in vista degli interventi di riforma, deve ancora essere analizzata). A completare il quadro, esplicativo del legame suddetto, interviene quindi il requisito della responsabilità, che senz'altro, come si è visto, riguarda i compiti e i poteri delle autorità, ma che richiama anche in particolare l'aspetto a noi caro del controllo *sulle* autorità, ossia sul loro operato e sulle loro decisioni. In esso, ancora di più, emerge l'essenza della *EU rule of law* e quindi il legame tra questa e la protezione dei dati si fa evidente.

Riprendendo, ancora una volta, l'analisi di Hijmans, risulta infatti che, oltre alle accezioni di responsabilità che già riferite, «*accountability of DPAs as independent authorities means in the first place that they should be accountable for their acts before a court, under the rule of law*»[146]. A ciò si dedica, effettivamente, il Capo VIII del GDPR, rubricato "*mezzi di ricorso, responsabilità e sanzioni*", in particolare nella previsione dell'articolo 78 al "*Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo*" [147], molto più articolato rispetto alla scarna previsione dell'articolo 28 paragrafo 3, comma 2 della Direttiva madre (completato, se si vuole, dall'articolo 22 della stessa), rispetto alla quale emerse un'insofferenza chiaramente palesata sin dalla Proposta di regolamento: «*An important change from the DPD is that the GDPR Proposal harmonised data protection enforcement in the EU*»[148]. Il GDPR pare quindi enfatizzare sia la possibilità di ricorso giurisdizionale per le autorità (articolo 58, par. 5) che la possibilità di ricorrere avverso una decisione delle autorità (articolo 58, par. 4 e articolo 78)[149].

---

[146] H. HIJMANS, *The European Union as Guardian of Internet Privacy*, p. 330, sottolineato aggiunto.

[147] GDPR, Articolo 78 – *Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo*

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.
2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77.
3. Le azioni nei confronti dell'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.
4. Qualora siano promosse azioni avverso una decisione di un'autorità di controllo che era stata preceduta da un parere o da una decisione del comitato nell'ambito del meccanismo di coerenza, l'autorità di controllo trasmette tale parere o decisione all'autorità giurisdizionale.

[148] C. KUNER, L.A. BYGRAVE, C. DOCKSEY, Background and Evolution, cit., p. 39.

[149] GDPR, Articolo 58 – *Poteri*

4. L'esercizio da parte di un'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione e degli Stati membri conformemente alla Carta.
5. Ogni Stato membro dispone per legge che la sua autorità di controllo abbia il potere di intentare un'azione o di agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso.

Questo aspetto, invero, fu oggetto di attenzione da parte della Corte di giustizia proprio nel celebre caso c.d. *Schrems I* (ancorché ancora basato sulle norme della direttiva madre), relativo a questioni di trasferimento dei dati verso Paesi terzi. Il caso coinvolgeva essenzialmente il problema di una decisione di rigetto dell'autorità di controllo rispetto a un reclamo sollevato dall'interessato relativo al trasferimento dei propri dati personali verso un Paese terzo di cui poneva in dubbio la sicurezza, rigetto motivato dall'esistenza di una decisione di adeguatezza della Commissione che si esprimeva invece positivamente rispetto alla trasferibilità di dati verso quel Paese terzo (gli USA).

Ebbene, alla vigilia del GDPR, la Corte, dopo aver ripreso la suddetta giurisprudenza per definire i poteri e compiti delle autorità di controllo (v. parr. 40-43 sentenza), e averne riconosciuto la "*competenza a verificare se un trasferimento di dati personali dal proprio Stato membro verso un paese terzo rispetti i requisiti fissati dalla direttiva 95/46*" (par. 47 sentenza) ebbe modo di chiarire che: «*Nel caso in cui detta autorità pervenga alla conclusione che gli elementi addotti a sostegno di una siffatta domanda sono privi di fondamento e, per questo motivo, la respinga, la persona che ha proposto detta domanda deve avere accesso, come si evince dall'articolo 28, paragrafo 3, secondo comma, della direttiva 95/46, in combinato con l'articolo 47 della Carta, ai mezzi di ricorso giurisdizionali che le consentono di contestare una siffatta decisione impugnandola dinanzi ai giudici nazionali. Alla luce della giurisprudenza citata ai punti 61 e 62 della presente sentenza, tali giudici devono sospendere la decisione e investire la Corte di un procedimento pregiudiziale per accertamento di validità, allorché essi ritengono che uno o più motivi di invalidità formulati dalle parti o, eventualmente, sollevati d'ufficio siano fondati Nell'ipotesi contraria, in cui detta autorità reputi fondate le censure sollevate dalla persona che l'ha investita di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali, questa*

Articolo 78 – *Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo*
1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.
Queste ultime considerazioni relative ai risvolti del GDPR sulle autorità di controllo, in termini di maggiore "europeizzazione" della posizione già ibrida delle stesse, trovano conforto nelle valutazioni di A. GIURGIU, T. A. LARSEN, Roles and Powers of National Data Protection Authorities, *cit*.: «*already under Directive 95/46/EC, DPAs have a hybrid position in between national law and EU law. Under the new Regulation, they become even more 'European' and thus more trapped between their own national rules and the EU law. This becomes even clearer when DPAs have to implement EDPB decisions. They are liable before national courts for decisions they are not sovereign in taking*», p. 352.
2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77.
3. Le azioni nei confronti dell'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.
4. Qualora siano promosse azioni avverso una decisione di un'autorità di controllo che era stata preceduta da un parere o da una decisione del comitato nell'ambito del meccanismo di coerenza, l'autorità di controllo trasmette tale parere o decisione all'autorità giurisdizionale.

stessa autorità, ai sensi dell'articolo 28, paragrafo 3, primo comma, terzo trattino, della direttiva 95/46, in combinato, segnatamente, con l'articolo 8, paragrafo 3, della Carta, deve poter promuovere azioni giudiziarie. A tal riguardo, incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione»[150].

Tutto ciò: da un lato, in qualche modo, ribadirebbe i limiti della collaborazione con la Commissione europea (che non deve essere, infatti, cieca abnegazione, ma critica considerazione, in linea con la *ratio* dei compiti e poteri attribuiti alle autorità); dall'altro, soprattutto, confermerebbe l'adagio, ribadito anche in questa pronuncia, secondo cui «*l'Unione è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali*»[151], e tale controllo di conformità viene effettuato, in ultima analisi, appunto dalla Corte di giustizia. Siffatte considerazioni risultano ancora più pregnanti laddove si assuma che «*Full judicial accountability of expert bodies – and of DPAs in particular – can be seen as a means to compensate for the loss of democratic control*»[152]. E infatti, un simile sistema giurisdizionale di controllo sulle autorità rivela la sua indispensabilità proprio nella constatazione del fatto che, a sua volta e come si diceva, la stessa previsione di autorità indipendenti per la protezione dei dati costituisce una peculiarità proprio in termini di definizione del sistema di ricorsi effettivi.

La questione può essere più facilmente compresa se si considera l'intervento delle autorità nell'ambito – più delicato rispetto a quello previsto da Direttiva 95/46 e GDPR – della cooperazione giudiziaria penale (ex Direttiva 2008/977/GAI, nuova Direttiva 2016/680). De Hert e Sajfert ci aiutano con riflessioni al riguardo, che pare utile condividere: «*Some praise the data protection supervisory authorities as the fundamental rights defenders in the information society. These unique organisations played a pivotal role and their presence has become indispensable also in the area of criminal justice.* (…) *the supervisory authorities can act as a proxy for the data subject, which is a fundamental shift away from the traditional legal system, in which the activities of public authorities should be scrutinised only by judges. For example, where a police authority refuses to allow a data subject access to his or her personal data, the supervisory authority can access his or*

[150] Corte di giustizia, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, sentenza del 6 ottobre 2015, punti 64-65.
[151] Ibidem, punto 60.
[152] H. HIJMANS, *The European Union as Guardian of Internet Privacy*, cit., p. 331.

her data stored in police databases and ensure that personal data is correct and processed lawfully. In that regard, it is interesting to have a brief look at Article 13 of the European Convention of Human Rights and the right to an effective remedy (…). In comparison, the above-mentioned Article 8(3) of the Charter of Fundamental Rights and the system of supervisory authorities create a more sophisticated system, whereby the existing complementary right to an effective remedy is further complemented (and not replaced) by watchdogs of administrative nature»[153]. Dunque, secondo gli autori, il sistema predisposto per la protezione dei dati, con la previsione del controllo effettuato *dalle* autorità indipendenti, rappresenterebbe un apparato più sofisticato di rimedi effettivi, anche analizzandolo in parallelo con le previsioni dell'articolo 13 CEDU.

Ebbene, proprio assumendo queste considerazioni, risulta a maggior ragione più pregnante, e più esplicativo dell'essenza della *EU rule of law*, il controllo giurisdizionale effettivo che viene garantito – ormai indubbiamente – sia *tramite* che *sulle* autorità indipendenti tanto, direttamente, dai giudici nazionali (che poi, come si suole ripetere, sono i "giudici comuni" dell'Unione) quanto, indirettamente, dal sindacato (sia esso pregiudiziale o nell'ambito di una paventata infrazione) "ultimo" della Corte di giustizia. E ciò riconduce alle previsioni – parallele a quelle dell'articolo 13 CEDU[154], ma più "sofisticate" proprio se calate nell'ottica dello specifico sistema di protezione dei dati – dell'articolo 47 della Carta: «*Under the rule of law, the procedures before the authorities and the possibilities for judicial review of the acts of the authorities must respect the rights to an effective remedy and fair trial. The requirement of a complete system of judicial protection follows from the right to an effective remedy and to a fair trial under Article 47 Charter*»[155]. L'insieme di queste considerazioni consentirebbe di riconoscere, quindi, che, come palesato dalla Corte nel caso *Schrems I*[156], l'*effettiva* tutela di un diritto sostanziale passa inevitabilmente dalla sua tutela procedurale.

---

[153] P. DE HERT. J. SAJFERT, The Role of the Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data, *cit*., p. 247.

[154] Per un'analisi a A. DI STEFANO, *Convenzione europea dei diritti dell'uomo e principio di sussidiarietà – contributo ad una lettura sistematica degli articoli 13 e 35*, Catania, 2009. Invero, proprio commentando le dette previsioni CEDU, l'autrice metteva in risalto "la problematica effettività dei ricorsi interni quale condizione dell'efficacia dei ricorsi internazionali", p. 26 (cfr. più in generale, su effettività delle tutele interne, pp. 41-142, nonché nell'ambito della costruzione prospettata dalla CEDU, pp. 143-298), a testimonianza del fatto che quel sistema di rimedi poneva inevitabilmente le medesime (classiche) problematiche, che però – calate nel sistema di protezione dei dati a livello sovranazionale, che si connota per il suo specifico apparato istituzionale e per la previsione di rimedi di carattere sia amministrativo che giurisdizionale – assumono attraverso la previsione delle autorità indipendenti tale carattere più "sofisticato":

[155] H. HIJMANS, *The European Union as Guardian of Internet Privacy*, p.331.

[156] *Schrems I*, punti 94-95, sul contenuto essenziale dei due diritti: quello, *ex* articolo 7 Carta, al rispetto della vita privata e quello, *ex* articolo 47 Carta, alla tutela giurisdizionale effettiva. Su questo si dirà più approfonditamente, per ora basti solo riferire il rilievo di Hofmann sulla constatazione da parte della Corte dell'essenza di tali due diritti (quello sostanziale e quello procedurale): "*This double violation of the very essence of the right, which is the first in the caselaw of the Court of Justice, helps to understand what does it mean to have the essence of a right and on the other hand,*

In ciò riposerebbe un aspetto imprescindibile della *EU rule of law*, e la previsione delle autorità indipendenti (nella duplice prospettiva di controllori e controllate) ne è emblematicamente rivelatrice.

Pertanto, alla luce di quanto esposto, si ritiene di poter considerare dimostrato in linee teoriche come il sistema istituzionale di protezione dei dati, attraverso la figura nodale delle autorità indipendenti, articolate tra i vari Stati membri, costituisca una paradigmatica espressione della *EU rule of law*. Sulla base di tali considerazioni, occorrerà esaminare se in pratica, e alla luce dei più recenti sviluppi, ciò trovi o meno concreta conferma.

3. Il ruolo della Commissione europea

Caratteristiche generali del ruolo della Commissione

Passiamo ora ad esaminare il ruolo della Commissione nello specifico contesto della protezione dei dati personali nell'Unione europea. Tra gli svariati profili rispetto ai quali la Commissione assume rilievo, è d'obbligo un previo cenno alla sua collocazione nel più ampio contesto istituzionale dell'Unione europea. Per poterne efficacemente delineare il ruolo nel settore della protezione dei dati occorre infatti individuare le caratteristiche basilari della funzione di tale istituzione nell'ordinamento sovranazionale, ancorché limitandosi al minimo indispensabile ai nostri fini.

Com'è noto, l'articolo 17 TUE dedica ben otto paragrafi alla Commissione, il primo dei quali prevede: "*La Commissione promuove l'interesse generale dell'Unione e adotta le iniziative appropriate a tal fine. Vigila sull'applicazione dei trattati e delle misure adottate dalle istituzioni in virtù dei trattati. Vigila sull'applicazione del diritto dell'Unione sotto il controllo della Corte di giustizia dell'Unione europea. Dà esecuzione al bilancio e gestisce i programmi. Esercita funzioni di coordinamento, di esecuzione e di gestione, alle condizioni stabilite dai trattati. Assicura la rappresentanza esterna dell'Unione, fatta eccezione per la politica estera e di sicurezza comune e per gli altri casi previsti dai trattati. Avvia il processo di programmazione annuale e pluriennale dell'Unione per giungere ad accordi interistituzionali*". Inoltre, il paragrafo 2 attribuisce alla Commissione il monopolio (salve diverse disposizioni dei Trattati) dell'iniziativa legislativa,

clearly drew lines as to how far can a EU institution go in the area of limitation of fundamental rights", cfr. Interview on www.blogdroiteuropeen.com , 2017.

mentre il paragrafo 3 ne stabilisce l'esercizio delle responsabilità in *piena indipendenza*[157]. La promozione dell'interesse generale costituisce quindi «*the proprium of the Commission's institutional mission, considered in itself and, above all, in its relations with the other institutions*»[158].

Dai primi tre paragrafi emerge dunque la missione principale della Commissione, istituzione individuata come massimamente emblematica dell'integrazione sovranazionale e così espressiva del metodo comunitario, mentre il potere di iniziativa esprimerebbe proprio la rappresentanza dell'interesse generale dell'Unione e, così, sarebbe essenziale anche per il mantenimento dell'equilibrio istituzionale[159]. Peraltro, se la previsione della promozione dell'interesse generale dell'Unione può far emergere "il ruolo politico della Commissione", dalla lettura combinata con le disposizioni successive, deriverebbe, però, come il suo ruolo sia "prevalentemente tecnico" ancorché "politicamente connotato"[160]. L'articolo 17 prevede, inoltre, al paragrafo 8, che "*La*

---

[157] Articolo 17 TUE
2. Un atto legislativo dell'Unione può essere adottato solo su proposta della Commissione, salvo che i trattati non dispongano diversamente. Gli atri atti sono adottati su proposta della Commissione se i trattati lo prevedono.
3 Il mandato della Commissione è di cinque anni.
I membri della Commissione sono scelti in base alla loro competenza generale e al loro impegno europeo e tra personalità che offrono tutte le garanzie di indipendenza.
La Commissione esercita le sue responsabilità in piena indipendenza. Fatto salvo l'articolo 18, paragrafo 2, i membri della Commissione non sollecitano né accettano istruzioni da alcun governo, istituzione, organo o organismo. Essi si astengono da ogni atto incompatibile con le loro funzioni o con l'esecuzione dei loro compiti.

[158] E. GIANFRANCESCO, Article 17 [The European Commission], in in H.-J. BLANKE, S. MANGIAMELI (Eds), *The Treaty on European Union (TEU) – A Commentary*, Springer, 2013, p. 684. Ivi l'autore specifica: «*While the other institutions can base their ultimate legitimation on notions that are for the most part stable and defined, such as the representation of the MS (for the European Council: Art. 15.2 TEU; → Art. 15 para 33; for the Council: Art. 16.2 TEU; → Art. 16 para 32), the democratic principle (for the EP: Art. 14.2 TEU; → Art. 14 para 16) or the guarantee of the rule of law (this is the case of the CJEU: Art. 19.1 TEU; → Art. 19 para 14) for the Commission the path is different: it is the Commission itself that identifies, at least at a first level, the general interest of the Union and pursues it in permitted forms according to the Treaties. In this sense, it can be defined as "supranational instance par excellence" and "integrative process engine"*».

[159] Cfr. Y. DEVUYST, The European Union's Institutional Balance after the Treaty of Lisbon: Community Method and Democratic Deficit Reassessed, 39(2) *Georgetown Journal of International Law*, 2008, part. pp. 262-265.
Sul principio dell'equilibrio istituzionale, e sul ruolo della Commissione al riguardo, si segnala in particolare J.P.JACQUÉ, The Principle of constitutional balance, in *Common Market Law Review*, 41, 2004, interessante in particolare laddove richiama gli albori del principio nella giurisprudenza comunitaria (il riferimento è al caso Meroni 9/56) individuando il principio in discorso come sostituto a livello sovranazionale del principio di separazione dei poteri e commentando: « *In the absence of a separation of powers, the principle of institutional balance made it possible to guarantee to undertakings that a modification of the institutional balance would not call into question the decision-making process envisaged the treaties and the accompanying guarantees provided by the treaties. However, this protective aspect of the principle seems to have been gradually lost as other means of protection appeared, including the guarantee of the respect of fundamental rights*», p. 384. Per le evoluzioni e implicazioni del principio dopo Lisbona, *ex multis*, T. CHRISTIANSEN, The European Union after the Lisbon Treaty: An Elusive 'Institutional Balance'?, in A. BIONDI, P.EECKHOUT (Eds), *EU Law after Lisbon*, Oxford, 2012. Si veda inoltre *supra*, Capitolo I.

[160] Così si esprime E. CANNIZZARO nel descrivere la Commissione, partendo proprio dall'indipendenza rispetto agli Stati membri e ai loro interessi: «In questo senso, si può ammettere che il ruolo della Commissione sia di carattere prevalentemente tecnico. Essa ha infatti il compito di realizzare l'interesse dell'Unione come esso emerge dai Trattati istitutivi. Vero è, peraltro, che la realizzazione dei Trattati non è un compito meramente tecnico ma è, a propria volta, politicamente connotato», cfr. *Il Diritto dell'integrazione europea – L'ordinamento dell'Unione*, Terza edizione, Giappichelli, 2020, p. 70 e su "ruolo politico" p. 69.

Commissione è responsabile collettivamente dinanzi al Parlamento europeo. Il Parlamento europeo può votare una mozione di censura della Commissione secondo le modalità di cui all'articolo 234 del trattato sul funzionamento dell'Unione europea". Tale mozione consentirebbe al Parlamento il controllo politico sull'operato della Commissione, anche se si tende a considerarla «un'arma di dissuasione più per la sua semplice previsione che per la sua effettiva possibilità di utilizzazione»[161].

Senza poter indugiare sulle implicazioni di dette previsioni rispetto alla struttura istituzionale, giuridica e politica dell'Unione, da esse è comunque possibile derivare quattro aspetti/caratteristiche di rilievo ai nostri fini per sindacare l'atteggiamento della Commissione nell'ambito della protezione dei dati personali: il potere di iniziativa legislativa; l'indipendenza; il potere di controllo; la rappresentanza esterna dell'Unione.

Si tratta, chiaramente, di aspetti correlati: il potere di iniziativa legislativa, per esempio «è conferito alla Commissione in ragione delle caratteristiche di indipendenza di tale istituzione, al fine di garantire che la proposta prospetti una composizione dei vari interessi che sia conforme all'interesse generale dell'Unione»[162], ancorché tale accostamento non sia scevro da perplessità[163]. Il potere di controllo, poi, è emblematico della generale considerazione della Commissione quale "guardiana dei Trattati", mentre alla detenzione dell'interesse generale dell'Unione si lega anche la rappresentanza esterna (tranne che nel settore PESC e negli altri espressamente previsti) per garantire la coerenza dell'azione dell'Unione (articolo 21, paragrafo 3, comma 2, TUE, vedi *infra*, Capitolo III).

Il potere di iniziativa legislativa, in generale

Partendo, dunque, dal *potere di iniziativa legislativa*, si è già detto che esso è legato all'indipendenza che caratterizza la Commissione e risponde alla missione generale ad essa

[161] Così G. STROZZI, R. MASTROIANNI, *Diritto dell'Unione europea – parte istituzionale*, Ottava edizione, Giappichelli, 2020, p. 103, che confermano questa considerazione, nonostante riconoscano che «Indubbiamente diverso appare il peso di questo strumento nelle mutate condizioni attualmente previste che associano il Parlamento alla nomina del Presidente e all'approvazione dei membri della Commissione, chiamandolo così ad esprimere, in sostanza, un voto di fiducia.», ibidem.

[162] G.GAJA, A. ADINOLFI, *Introduzione al diritto dell'Unione europea*, Quarta edizione, Laterza, 2020, p. 35.

[163] Cfr. N. ROJAS-HUTINEL, *La séparation du pouvoir dans l'Union européenne*, mare&martin, 2017, p. 260: «*dans le cadre de l'initiative législative, mission requérant l'exercice d'un pouvoir d'essence politique, il apparait que l'indépendance dont la Commission est c ensée bénéficier n'est pas effective, de sorte que l'émergence d'un pouvoir politique autonome, pourtant nécessaire, semble compromise. L'exercice du pouvoir de la Commission est alors influencé et peu autonome* ».

conferita. È bene sottolineare quanto questo potere sia centrale, in generale, poiché «*The Commission has significant agenda-setting power through its right to propose legislation*»[164]. Il potere di iniziativa rappresenta, infatti, la possibilità per la Commissione di decidere quali questioni assumono un rilievo tale da essere sottoposte alla procedura legislativa e, dunque, in senso ampio, si lega alla definizione dell'agenda della Commissione: «*The power to establish which issues are the subject of decisional procedures of the Union takes on a natural political importance, and the reservation of this power of selection to the Commission has launched it well beyond the boundaries of administration. This is an essential power of agenda setting which the Commission has used in its relations with the Council and the EP*»[165]. Tutto ciò, com'è noto, si iscrive nella più ampia strategia politica dell'Unione, elaborata insieme dalle istituzioni politiche, e i cui orientamenti sono definiti dal Consiglio europeo. La pagina dedicata alla strategia, poi, specifica: "Anche il presidente della Commissione determina le priorità politiche per il proprio mandato. Ogni cinque anni, all'inizio di un nuovo mandato, il presidente della Commissione indica i settori prioritari su cui ci si concentrerà in tale periodo. La scelta dei settori scaturisce dall'agenda strategica del Consiglio e dalle discussioni con i gruppi politici del Parlamento europeo"[166]. Dunque, il presidente della Commissione predispone all'inizio del suo mandato la priorità per il quinquennio, mentre ogni anno la Commissione presenta il programma di lavoro, durante il c.d. ciclo di pianificazione e programmazione strategica (dove presenta anche i piani per le attività future e le relazioni per quelle passate), in cui espone un piano d'azione annuale per prospettare come realizzare con azioni concrete le priorità politiche[167].

Questo essendo lo sfondo in cui contestualizzare il potere di iniziativa legislativa, con specifico riguardo alla proposta va detto (sempre facendo riferimento a siti istituzionali) che è ora previsto il programma c.d. *legiferare meglio*, disponibile alla pagina dedicata del sito della Commissione, che "riguarda l'elaborazione di politiche basate su elementi concreti, l'elaborazione e la valutazione trasparente delle politiche e delle normative dell'UE, tenendo conto delle opinioni e dell'impatto su coloro che ne saranno interessati e concentrandosi sui risultati nei settori in cui ciò è più

[164] A. BRADFORD, *The Brussels Effect – How the European Union Rules the Word*, Oxford University Press, 2020, p. 8.
[165] E. GIANFRANCESCO, Article 17, *cit*., p. 700.
[166] Commissione europea, pagina web dedicata alla Definizione delle priorità – *Strategia politica complessiva*, disponibile qui: https://ec.europa.eu/info/strategy/priorities-and-goals/how-priorities-are-set_it .
[167] Sul programma di lavoro, dalla pagina web della Commissione ad esso dedicata risulta: "*Il programma di lavoro indica come la Commissione intende tradurre in pratica le priorità politiche definite dal suo presidente. Il programma si colloca in una prospettiva pluriennale per consentire alle parti interessate e alle altre istituzioni dell'UE di pianificare la loro collaborazione con la Commissione*", cfr. https://ec.europa.eu/info/publications/european-commission-work-programme_it , in cui sono disponibili i documenti principali relativi al programma di lavoro per ciascun anno, aggiornati al 2021. Si veda anche: https://ec.europa.eu/info/strategy/priorities-and-goals/how-priorities-are-set_it#howstrategybecomesreality .

importante[168]. La pianificazione e la proposta di atti legislativi seguono, dunque, il suddetto programma di lavoro. Particolare importanza assumono, rispetto alla proposta, sia la c.d. *valutazione di impatt*o, che viene effettuata dunque nella fase preparatoria antecedente alla proposta[169], che la c.d. *previsione strategica*, volta ad orientare gli sviluppi futuri delle politiche anche attraverso l'elaborazione di nuove iniziative[170]. È stato quindi previsto, dall'attuale Commissione, un pacchetto di "*strumenti per legiferare meglio*" che consta di principi generali, previsioni su come effettuare la suddetta valutazione di impatto, spiegazioni su attuazione, recepimento e preparazione delle proposte, oltre a indicare come monitorare gli interventi ed effettuare i correlati controlli di adeguatezza[171].

Da quanto precede si evince, dunque, che il potere di iniziativa in senso lato non si limita alla sola proposta ma comincia ben prima e accompagna la procedura legislativa durante tutto il suo *iter*[172], come peraltro confermato dalle previsioni dei trattati. Questi ultimi, infatti, definiscono la procedura legislativa ordinaria prevedendo, ai sensi dell'articolo 289 TFUE, l'adozione congiunta di un atto normativo da parte di Parlamento europeo e Consiglio "*su proposta della Commissione*", come peraltro ribadito dall'articolo 294, paragrafo 2, TFUE. L'attribuzione espressa di un "monopolio", salvo specifici casi, della proposta legislativa in capo alla Commissione, senza la quale dunque la procedura non può avere inizio, enfatizza l'importanza del ruolo di tale istituzione e, quindi, della sua intera attività ad esso correlata[173]. Ebbene, tale "monopolio" appare in un certo senso rafforzato dalla previsione per cui la Commissione può modificare la propria proposta in tutte le fasi delle procedure legislative (articolo 293 TFUE); nondimeno, esso potrebbe risultare "attenuato" da quelle previsioni che consentono ad altre istituzioni politiche di sollecitare la Commissione ad esercitare il proprio potere, possibilità che, per quanto non ponga su di essa un obbligo di intervenire,

---

[168] Cfr. https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how_it .

[169] Dalla pagina web della Commissione dedicata alle valutazioni di impatto si legge: "*Le valutazioni d'impatto determinano se è necessaria un'azione dell'UE ed esaminano i possibili impatti delle soluzioni disponibili. Sono eseguite durante la fase preparatoria, prima che la Commissione formuli una proposta di nuova legislazione. Forniscono gli elementi per elaborare e sostenere il processo decisionale*". Per ulteriori informazioni su tali valutazioni, v. https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/impact-assessments_it .

[170] Per approfondimenti sulla c.d. previsione strategica, v. https://ec.europa.eu/info/strategy/strategic-planning/strategic-foresight_it .

[171] La pagina web dedicata al pacchetto "legiferare meglio", che comprende tutti gli "strumenti" previsti, è disponibile al seguente link: https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_it .

[172] Nel commento all'articolo 17, infatti, E. GIANFRANCESCO, *cit*., ribadisce al riguardo: «*The Commission's power of initiative can be divided into three elements: the power of initiative in a strict sense, or the exclusive authority to start, with its own act of proposal, the legislative procedure or other decisional procedures of the Union (…); the power to amend and modify the ongoing proposals of the deliberative procedure at any time (…); the power to withdraw the proposal, with the consequent interruption of the procedure*», p. 700.

[173] Cfr. *ex multis* E. CANNIZZARO, *Il Diritto dell'integrazione europea, cit*., p. 70; l'A. ricorda inoltre come la proposta sia al contempo «il punto terminale di un processo complesso di negoziato che intercorre con una ampia serie di attori politici, istituzionali e sociali, e rappresenta, al tempo stesso, il punto iniziale della procedura legislativa», p. 86.

sicuramente le impone di motivare un eventuale rifiuto (articolo 225 TFUE, per il Parlamento; articolo 241 TFUE, per il Consiglio). Invero, da tali ultimi riferimenti sembra piuttosto spiccare come imprescindibile la collaborazione tra le istituzioni, sollecitata sin dalla primordiale definizione delle strategie politiche e confermata da un fondamentale passaggio, sul quale i trattati tacciono, ossia il c.d. *trilogo*, che vede le tre istituzioni politiche incontrarsi per il raggiungimento di un quanto più rapido accordo nell'ambito della procedura legislativa ordinaria. Tale incontro assume particolare rilievo proprio perché testimonierebbe che, «*Despite the different responsibilities of the three institutions, the emphasis in practice is on compromise and dialogue (…). This justifies speaking about one legislator (…). The input of the three institutions, respecting the institutional balance, gives democratic legitimacy to the EU legislator's mandate*»[174]. Dunque, ferma l'importanza della Commissione (soprattutto ai fini della nostra analisi), risulta chiara la centralità della collaborazione tra Parlamento, Consiglio e Commissione nelle dinamiche della politica di regolamentazione europea.

Queste, per punti essenziali, le caratteristiche del potere di iniziativa della Commissione (e l'importanza, come si evince dalla citazione, del suo sfociare nella "unica voce" del legislatore europeo), da cui deriverebbe quindi che tale potere, rivelatore al contempo dell'interesse generale dell'Unione e dell'equilibrio istituzionale, costituisce in effetti un importante elemento della *EU rule of law*. Da qui, la nostra attenzione si rivolge allo specifico settore della protezione dei dati personali, apprezzabile testimonianza dei suddetti passaggi.

Il potere di iniziativa legislativa nel settore della protezione dei dati personali

Si è detto che l'articolo 16 TFUE è base giuridica della competenza dell'Unione a legiferare in materia; esso richiama espressamente al paragrafo 2 la procedura legislativa ordinaria per l'adozione delle rispettive norme e, quindi, inevitabilmente, implica il potere di iniziativa della Commissione in materia. Qualche breve richiamo agli interventi più rilevanti potrà consentire di comprendere la centralità del ruolo della Commissione in tal senso, per consentire, poi, valutazioni sugli ultimissimi sviluppi nella prassi dell'attuale Commissione in materia, ancora in divenire.

Si consideri, per esempio, proprio il primo strumento emblematico nel campo della protezione dei dati personali a livello sovranazionale, ossia la direttiva madre, che rivela la centralità della fase preparatoria sin dagli albori. L'adozione della direttiva 95/46/CE, infatti, è stata il frutto di un processo che solo nel 1990 è sfociato nella proposta della Commissione, e a seguito della quale, tra

[174] H. HIJMANS, *The European Union as Guardian of Internet Privacy*, cit., p. 239.

letture ed emendamenti vari, trascorsero cinque anni[175]. Nondimeno, come si è detto (*supra*, Parte II), l'interesse delle istituzioni politiche, in particolare del Parlamento e della Commissione, cominciò ben prima: può ricondursi infatti addirittura al 1973 la prima Comunicazione della Commissione legata al tema, "*Community Policy on Data Processing*"[176], attraverso cui si cominciava a riconoscere la privacy dei cittadini come una questione di "rilevanza costituzionale" e così a stimolare discussioni anche informali con gli Stati membri per una necessaria armonizzazione delle legislazioni in materia[177].

Facendo poi un salto verso l'intervento legislativo che ha sostituito la direttiva madre, ossia il GDPR, è noto che esso si iscrive in un ben più ampio e complesso processo di riforma (incluso nel pacchetto del 2016, comprendente anche le due direttive 680 e 681, la prima, si è detto, in sostituzione della direttiva 2008/977/GAI) attraverso il quale «*The Commission has undertaken the herculean task to amend the whole EU data protection edifice*»[178]. Con riguardo specifico al GDPR, persino uno dei più autorevoli commentari ad esso dedicati illustra lo sfondo della proposta della Commissione partendo dalla prima relazione dell'istituzione, del 2003, sull'attuazione della direttiva madre[179]. Il richiamo, invero, veniva ivi previsto per dimostrare che allora, pur conscia delle difficoltà di attuazione, la Commissione preferì optare per una non revisione della direttiva. Com'è noto, però, le cose cambiarono dopo il Trattato di Lisbona, seguito infatti dalla famosa Comunicazione del 2010 titolata "*Un approccio globale alla protezione dei dati personali nell'Unione europea*" in cui la Commissione ammetteva che, pur mantenendo saldi e vigenti i principi della direttiva, quest'ultima non poteva più far fronte alle sfide della globalizzazione e dello sviluppo tecnologico[180]. Tale Comunicazione arrivò, come si evince anche dal testo, a seguito di

[175] Per una chiara esposizione di tutti i passaggi che scandirono il periodo dalla proposta della Commissione all'adozione della direttiva, si rinvia alla scheda dedicata relativa al documento, disponibile qui: https://eur-lex.europa.eu/legal-content/IT/HIS/?uri=CELEX%3A31995L0046 .

[176]. Communication of the Commission to the Council, *Community policy on data processing*, SEC (73) 4300 final, 21 November 1973.

[177] Così ci ricorda G. GONZÁLEZ FUSTER, *The emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014, p.117, alla quale si rinvia per un'illustrazione approfondita delle dinamiche che, dagli anni Settanta, hanno caratterizzato il ruolo della Commissione (e non solo) nel periodo sino alla proposta di direttiva, ibidem, pp. 112-124.

[178] P. DE HERT, V. PAPAKONSTANTINOU, The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals, in *Computer Law and Security Review* (28), 2012, p. 130.

[179] Il riferimento è al recente Commentario di C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2020, p. 3.
Quanto alla Prima Relazione della Commissione, il riferimento è a Commission of the European Communities, REPORT FROM THE COMMISSION *First report on the implementation of the Data Protection Directive* (95/46/EC), COM(2003) 265 final, 15.05.2003, disponibile qui: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF .

[180] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, COM(2010) 609 definitivo, Bruxelles, 4.11.2010, in cui si legge in apertura: «La direttiva del 1995 è una pietra miliare nella storia della protezione dei dati personali nell'Unione europea. Essa sancisce due antiche ambizioni ugualmente importanti del

consultazioni, specie in relazione alla tutela dei dati personali rispetto alla riforma della normativa sulle comunicazioni elettroniche (il riferimento è alla direttiva 2009/136/CE che modificava la direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche). Inoltre, e soprattutto, essa fu seguita dalle reazioni dei maggiori esponenti coinvolti: il parere del Garante europeo della protezione dei dati, nel gennaio 2011[181]; la Lettera da parte del Gruppo di Lavoro Articolo 29, sempre nel gennaio 2011[182]; le Conclusioni del Consiglio dell'Unione europea, nel febbraio 2011[183]; il Documento di Lavoro del Parlamento europeo, nel marzo 2011[184]. Ebbene, ci ricordano gli autori, questi documenti di reazione, insieme con la Comunicazione della Commissione, costituirono proprio lo sfondo teoretico e istituzionale che portò alla proposta di Regolamento[185].

Peraltro, a riempire gli interventi che connotano lo sfondo in cui si sviluppa il diritto alla protezione dei dati personali nell'Unione europea, è sempre del 2010, come si è detto (v. *supra*, Parte II) la Comunicazione della Commissione "*EUROPA 2020 Una strategia per una crescita intelligente, sostenibile e inclusiva*" improntata verso una "trasformazione" dell'economia per permettere all'Unione di uscire dalla crisi ed essere al passo coi tempi, assumendo rilievo a livello globale. In questa prospettiva, quindi, veniva prevista, tra le iniziative faro volte a realizzare gli obiettivi della Commissione, *Un'agenda europea del digitale* "per accelerare la diffusione dell'internet ad alta velocità e sfruttare i vantaggi di un *mercato unico del digitale* per famiglie e imprese" e che prevedeva proprio, a livello dell'Unione, l'operatività della Commissione per "creare un quadro

processo d'integrazione europea: la tutela dei diritti e delle libertà fondamentali delle persone, quindi anche del diritto fondamentale alla protezione dei dati, e la realizzazione del mercato interno, ossia, nello specifico, la libera circolazione dei dati personali. A distanza di quindici anni questo duplice obiettivo ha mantenuto la sua validità e i principi che hanno trovato espressione nella direttiva restano saldi. Eppure, la rapidità dell'evoluzione tecnologica e la globalizzazione hanno mutato profondamente il mondo in cui viviamo, ponendo nuove sfide alla protezione dei dati personali».

[181] Parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni — «Un approccio globale alla protezione dei dati personali nell'Unione europea», (2011/C 181/01), https://edps.europa.eu/sites/default/files/publication/11-01-14_personal_data_protection_it.pdf .

[182] Letter from the Article 29 Working Party addressed to Vice-President Reding regarding the Article 29 WP's reaction to the Commission Communication "*A comprehensive approach to personal data protection in the EU*", Brussels, 14.01.2011, D(2011) https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_01_14_letter_artwp_vp_reding_commission_communication_approach_dp_en.pdf

[183] Council conclusions on the Communication from the Commission to the European Parliament and the Council - A comprehensive approach on personal data protection in the European Union – 3071st JUSTICE and HOME AFFAIRS Council meeting, Brussels, 24 and 25 February 2011, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf .

[184] Parlamento europeo – *Commissione per le libertà civili, la giustizia e gli affari interni*, Documento di Lavoro 1 su un approccio globale alla protezione dei dati personali nell'Unione europea, 15.03.2011,

[185] P. DE HERT, V. PAPAKONSTANTINOU, The proposed data protection Regulation, *cit.*, p. 132.

giuridico stabile tale da incentivare gli investimenti in un'infrastruttura aperta e competitiva per l'internet ad alta velocità e nei servizi collegati"[186].

Dopo questo iniziale richiamo, come si è detto, il Mercato Unico Digitale divenne oggetto di una specifica strategia della Commissione, come si evince dalla Comunicazione del 2015 ad esso dedicata, stabilendo: "Il *mercato unico digitale* è un mercato in cui è garantita la libera circolazione delle merci, delle persone, dei servizi e dei capitali e in cui, quale che sia la loro cittadinanza o nazionalità o il luogo di residenza, persone e imprese non incontrano ostacoli all'accesso e all'esercizio delle attività online in condizioni di concorrenza leale e potendo contare su un *livello elevato di protezione dei consumatori e dei dati personali*. La realizzazione del mercato unico digitale consentirà all'Europa di mantenersi *tra i leader mondiali dell'economia digitale*, sostenendo la crescita delle imprese europee su scala mondiale"[187]. La Comunicazione faceva, poi, riferimento anche al GDPR, stabilendo: "Il regolamento generale sulla protezione dei dati rafforzerà la fiducia nei servizi digitali, perché dovrebbe tutelare le persone fisiche con riguardo al trattamento dei dati personali da parte di qualsiasi impresa che offra servizi sul mercato europeo"[188].

In tale contesto, dunque, l'importanza del GDPR contribuisce a confermare che «Il substrato giuridico, oltre al dato economico, è l'altra variabile fondamentale del mercato digitale per assicurare tale sviluppo e minimizzare le asimmetrie regolamentari disincentivanti»[189]. Proprio sposando questa prospettiva, la Comunicazione del 2015 assume rilievo ai nostri fini soprattutto per i suoi tre pilastri: "migliorare l'accesso online ai beni e servizi in tutta Europa per i consumatori e le imprese"; "creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi"; "massimizzare il potenziale di crescita dell'economia digitale". In ciascuno di essi, infatti, la Commissione metteva in risalto la necessità di una regolamentazione armonizzata tra Stati membri alla base della costruzione del mercato unico digitale. Così, per esempio, quanto al primo pilastro, prospettava "una *regolamentazione* del commercio elettronico transfrontaliero degna della fiducia di consumatori e imprese"[190]; quanto al secondo, richiedeva "idoneità delle *norme* nel settore delle telecomunicazioni" nonché "Idoneità del *quadro normativo* per piattaforme e intermediari" e

[186] Commissione europea, EUROPA 2020 – *Una strategia per una crescita intelligente, sostenibile e inclusiva*, COM/2010/2020 def., Buxelles, 3.3.2010.
[187] COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI – *Strategia per il mercato unico digitale in Europa* {SWD(2015) 100 final}, Bruxelles, 6.5.2015.
Si veda anche la pagina dedicata a "*Shaping the Digital Single Market*", disponibile qui: https://ec.europa.eu/digital-single-market/en/shaping-digital-single-market .
[188] Comunicazione SWD(2015) 100 final, cit., p. 14.
[189] E. TOSI, Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo codice privacy, in E. TOSI (a cura di), Privacy Digitale – Riservatezza e protezione dei dati personali tra GDPR e nuovo codice privacy, Giuffrè Francis Lefebvre, 2019, p. 14.
[190] Comunicazione SWD(2015) 100 final, cit., p. 4, enfasi aggiunta.

"strategie e norme in materia di cibersicurezza."[191]. Dal terzo pilastro, poi, risultava che la Commissione avesse già chiaro che "Nel giro di meno di un decennio la maggior parte dell'attività economica dipenderà da ecosistemi digitali che integreranno infrastrutture digitali, hardware e software, applicazioni e dati. Perché l'UE possa restare competitiva, mantenere una base industriale solida e *gestire la transizione verso un'economia industriale e di servizio intelligente, sarà necessaria la digitalizzazione di tutti i settori*. (…) L'UE deve dotarsi di una serie di misure che permettano alle industrie europee di mantenersi all'avanguardia nello sviluppo e sfruttamento delle TIC, nell'automazione e nelle tecnologie di produzione trasformazione sostenibili per poter rispondere alle esigenze dei mercati del futuro. L'economia digitale può anche rendere più inclusiva la società"[192].

Nell'analisi volta a "*costruire un'economia dei dati*", la Commissione teneva presente che "A causa della frammentazione del mercato, le nuvole informatiche, i megadati, la scienza induttiva (data-driven) e l'internet delle cose [elementi centrali per la competitività dell'UE] non raggiungono una scala sufficiente per liberare in Europa tutte le loro potenzialità. *Per trarre tutti i benefici possibili dalle tecnologie digitali e dei dati dovremo eliminare tutta una serie di ostacoli tecnici e normativi*"[193]. Tutti questi aspetti, elementi della più generale azione politica della Commissione, sono poi volti a tradursi, con l'indispensabile contributo di attori istituzionali e non[194], in proposte legislative volte a realizzare quei propositi; ciò si evince sin dalla tabella di marcia di cui all'allegato alla Comunicazione che, per esempio (tra gli altri) comprendeva anche la revisione della direttiva sulle comunicazioni elettroniche, sfociata nella proposta di Regolamento *e-Privacy* del 2017[195]. Pertanto, dalla precedente Commissione sarebbero state presentate 30 proposte legislative sul mercato unico digitale e, alla fine del mandato, ben 28 sarebbero state concordate dai colegislatori[196]. Senza possibilità di approfondimenti, vanno almeno richiamati nell'ambito di questa strategia interventi attualmente di massimo rilievo, quali: il regolamento sulla libera

[191] Ibidem, p. 14, enfasi aggiunta, dove peraltro continua: "Ai servizi di comunicazioni elettroniche si applicano norme specifiche (direttiva relativa alla vita privata e alle comunicazioni elettroniche14), che potranno dover essere riesaminate una volta stabilite le norme generali dell'UE sulla protezione dei dati, in particolare perché gli articoli della vigente direttiva si applicano per la maggior parte solo ai prestatori di servizi di comunicazione elettronica tradizionali, vale a dire alle società di telecomunicazioni "classiche"; in genere restano quindi esclusi dall'ambito d'applicazione i prestatori di servizi della società dell'informazione che si servono di internet per fornire servizi di comunicazione".
[192] Ibidem, p. 15, enfasi aggiunta.
[193] Ibidem, p. 15, enfasi aggiunta.
[194] Si veda, *ex multis*, l'imponente intervento del Parlamento europeo al riguardo, comprensivo anche degli sviluppi seguiti alla pandemia di COVID-19, nella pagina dedicata a "*ubiquità del Mercato unico digitale*", disponibile qui: https://www.europarl.europa.eu/factsheets/it/sheet/43/ubiquita-del-mercato-unico-digitale .
[195] Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM/2017/010 final - 2017/03 (COD).
[196] Così si evince alla pagina dedicata: https://ec.europa.eu/digital-single-market/en/shaping-digital-single-market .

circolazione dei dati non personali[197]; il regolamento sulla cibersicurezza[198]; la direttiva sui dati aperti[199].

In perfetta continuità con queste previsioni, ed in considerazione dell'evolversi delle tecnologie, l'attuale Commissione ha poi fatto del Mercato unico digitale anche una priorità nell'Agenda 2019-2024. In particolare, quest'ultima prevede sei priorità, tra le quali spicca ai nostri fini "*Un'Europa pronta per il digitale*". A rendere chiare le intenzioni della Commissione, pare utile riportare quanto si legge nella pagina dedicata: «*La tecnologia digitale sta cambiando la vita delle persone. La strategia digitale dell'UE mira a fare sì che tale trasformazione vada a beneficio dei cittadini e delle imprese, contribuendo nel contempo a raggiungere l'obiettivo di un'Europa neutra dal punto di vista climatico entro il 2050. La Commissione è decisa a fare di questo decennio il "decennio digitale" europeo. L'Europa deve ora rafforzare la propria sovranità digitale e fissare norme, anziché seguire quelle di altri paesi, incentrandosi chiaramente sui dati, la tecnologia e le infrastrutture*»[200].

È interessante notare, da queste poche battute, da un lato l'insistenza della Commissione, già palesata nel 2015, sulla necessità di regolamentazione; dall'altro, e finalmente, l'espresso riferimento alla tanto predicata "sovranità digitale dell'Unione europea", che invero parrebbe così legata al *potere regolatorio* dell'Unione nella dimensione digitale, dunque alla capacità di "fissare norme", richiamando così anche il suddetto *Brussels effect*. Orbene, la predetta priorità si articola in due punti: decennio digitale europeo; plasmare il futuro digitale dell'Europa.

Quest'ultimo, già emerso tramite l'apposita Comunicazione del 19 febbraio 2020 "*Plasmare il futuro digitale dell'Europea*"[201], dovrebbe riguardare l'intervento della Commissione verso una trasformazione digitale funzionale per tutti, con un approccio basato su tre pilastri: tecnologia al

[197] Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, PE/53/2018/REV/1, GU L 303 del 28.11.2018.
[198] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), PE/86/2018/REV/1, GU L 151 del 7.6.2019.
[199] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico PE/28/2019/REV/1, GU L 172 del 26.6.2019.
[200] Dalla pagina della Commissione dedicata a "*Un'Europa pronta per l'era digitale*", disponibile qui: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_it
[201] COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, Plasmare il futuro digitale dell'Europa, COM(2020) 67 final, 19 febbraio 2020.

servizio delle persone; economia digitale equa e competitiva; società aperta, democratica e sostenibile[202].

Ebbene, nell'ambito della priorità in questione sono state prospettate diverse azioni, tra le quali vanno annoverate (senza potersi soffermare sull'azione sulla cibersicurezza o quella sull'intelligenza artificiale, che è sfociata peraltro nella proposta di regolamento della Commissione del 21 aprile 2021) ai nostri più limitati fini: le due proposte di regolamento, del 15 dicembre 2020, rispettivamente, sui servizi digitali[203] e sui mercati digitali[204], e la Strategia europea in materia di dati[205]. Le prime due recenti proposte di regolamento sono state da subito considerate come espressive di "una riforma ambiziosa dello spazio digitale"[206]. Quanto alla Strategia in materia di dati, prospettata nella Comunicazione del febbraio 2020, essa è volta essenzialmente a riconoscere l'importanza dei dati al punto da porli a fondamento di economia e società europee: "*L'UE può divenire un modello di riferimento per una società che, grazie ai dati, dispone di strumenti per adottare decisioni migliori, a livello sia di imprese sia di settore pubblico. Per concretizzare tale ambizione, l'UE può fare affidamento sia su un quadro giuridico solido, in termini di protezione dei dati, diritti fondamentali, sicurezza e cibersicurezza, sia sul suo mercato interno, caratterizzato da imprese competitive di tutte le dimensioni e da una base industriale diversificata. Se vuole conquistarsi un ruolo guida nell'economia dei dati, l'UE deve agire subito e affrontare in maniera concertata questioni che vanno dalla connettività all'elaborazione e alla conservazione dei dati, dalla potenza di calcolo alla cibersicurezza. Dovrà inoltre migliorare le proprie strutture di*

[202] Dalla pagina della Commissione dedicata a "*Plasmare il futuro digitale dell'Europa*", disponibile qui: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_it .

[203]Dalla pagina della Commissione dedicata https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_it .

European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on a Single Market For Digital Services (*Digital Services Act*) and amending Directive 2000/31/EC, Brussels, 15.12.2020

COM(2020) 825 final, 2020/0361 (COD), Brussels, 15.12.2020, https://ec.europa.eu/info/sites/info/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf .

[204] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (*Digital Markets Act*), COM(2020) 842 final

2020/0374 (COD) Brussels, 15.12.2020, https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf .

[205] Commissione europea, *Strategia europea in materia di dati*, febbraio 2020:

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_it

[206] Così dalla pagina dedicata del sito della Rappresentanza in Italia della Commissione europea, a cui si rinvia per approfondimenti:

https://ec.europa.eu/italy/news/20201215_la_commisisone_propone_nuove_norme_per_le_pattaforme_digitali_it . Per un recente commento su entrambe le proposte si segnala G.M. RUOTOLO, Digital Services Act e Digital Markets Act tra responsabilità dei fornitori e rischi di ne bis in idem, in *SIDIblog*, 29 marzo 2021 (disponibile qui: http://www.sidiblog.org/2021/03/29/digital-services-act-e-digital-markets-act-tra-responsabilita-dei-fornitori-e-rischi-di-bis-in-idem/). Inoltre, dello stesso A., si veda *Scritti di diritto internazionale ed europeo dei dati*, Cacucci editore, 2021, pp. 262-264.

governance per la gestione dei dati e ampliare i propri pool di dati di qualità disponibili per l'utilizzo e il riutilizzo"[207].

Ebbene, in questo contesto veniva avanzata nel novembre 2020 la proposta di c.d. *Data Governance Act*, un Regolamento relativo alla governance europea dei dati[208], quale prima misura di attuazione della suddetta Strategia, volta a facilitare la condivisione di dati tra vari settori e Stati membri.

Inoltre, quanto alle previsioni sul decennio digitale europeo, si tratta di ancor più recenti elaborazioni: risale infatti al 9 marzo 2021 la presentazione da parte della Commissione di prospettive per la trasformazione dell'Europa entro il 2030, per una visione decennale che si svilupperebbe intorno a quattro punti cardine: competenze; infrastrutture digitali; trasformazione digitale delle imprese; digitalizzazione dei servizi pubblici[209]. Da qui, infatti, la denominazione della relativa Comunicazione della Commissione *Bussola per il digitale 2030: il modello europeo per il decennio digitale*", in cui si trovano chiaramente gli attuali intenti: "*perseguire politiche per il digitale che conferiscano ai cittadini e alle imprese l'autonomia e la responsabilità necessarie per conseguire un futuro digitale antropocentrico, sostenibile e più prospero. L'Europa dovrà sfruttare i suoi punti di forza: un mercato unico aperto e competitivo, norme rigorose ancorate ai valori europei, un ruolo da protagonista nel commercio internazionale equo e regolamentato, una solida base industriale, cittadini altamente qualificati e una società civile solida. Al tempo stesso, deve valutare attentamente e gestire eventuali debolezze strategiche, vulnerabilità e dipendenze ad alto rischio che possono ostacolare il conseguimento delle sue ambizioni, come pure accelerare gli investimenti correlati*"[210].

Da questi passaggi emerge chiara l'insistenza attuale sull'aspetto ulteriore che coinvolge la sovranità digitale, e sul quale non abbiamo ancora posto l'accento, anche perché è parso carente nell'operato dell'Unione sino a qualche tempo fa, ma che si palesa ora soprattutto in tali ultimi interventi della nuova Commissione: quello relativo alla necessità che l'Unione, accanto al già ben sviluppato potere regolatorio, realizzi anche un'*autonomia strategica* nella dimensione digitale, specie rispetto ad aziende straniere quanto a servizi e infrastrutture digitali di cui sarebbe risultata

[207] COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Una strategia europea per i dati*, COM/2020/66 final, Bruxelles, 19.02.2020, 1. Introduzione.

[208] Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo alla governance europea dei dati (*Atto sulla governance dei dati*) COM/2020/767 final.

[209] Per approfondimenti si veda la pagina della Commissione dedicata a "*Decennio digitale europeo: obiettivi digitali per il 2030*", disponibile qui: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_it .

[210] COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM(2021) 118 final, 9 marzo 2021, sottolineato aggiunto.

particolarmente sprovvista. Avremo modo di argomentare questi aspetti (*infra*, Capitolo III, Parte IV), ma qui basta rilevare come dalle recenti iniziative la Commissione parrebbe particolarmente orientata in tal senso, volta a promuovere peraltro, come avremo modo di enfatizzare, un modello europeo caratterizzato dal c.d. *approccio antropocentrico*, che farebbe dunque dei valori fondanti dell'Unione, e della tutela dei diritti individuali nella dimensione digitale, il punto nodale anche di tali iniziative.

Che tutto questo abbia un forte legame con l'affermazione della *EU Rule of Law*, rappresentandone in qualche modo una delle molteplici sfaccettature, data dall'atteggiarsi della Commissione rispetto al settore digitale, è reso ancor più palese proprio dalla stessa Agenda dell'attuale Commissione.

Questa, infatti, accanto alla suddetta priorità di un'Europa digitale, ne prevede altre cinque: *Green Deal* europeo; un'economia al servizio delle persone; un'Europa più forte nel mondo; un nuovo slancio per la democrazia europea; *promoting our European way of life*. Orbene, per quanto tutte, in qualche modo, costituiscano espressione, più o meno spiccata, della *EU rule of law*, è l'ultima in particolare che pare esserne schiettamente indicativa, prospettando che: "L'Europa deve tutelare lo Stato di diritto per difendere la giustizia e i valori fondamentali dell'UE"[211]. Ciò basta a rilevare come l'agenda dell'attuale Commissione abbia un'impronta, almeno nelle intenzioni, chiaramente volta a rinsaldare, nelle diverse dimensioni e nei vari e correlati settori, la *EU rule of law*.

Concludendo l'analisi teorica sul potere di iniziativa legislativa della Commissione in tale specifico settore, emerge chiaramente come tale intervento sia espressione dell'orientamento pro-integrazione della Commissione e quindi, proprio per questo, sia particolarmente emblematico di uno dei più classici e indispensabili elementi del "funzionamento" della *EU rule of law*. Si tratterebbe, peraltro, anche di un aspetto del suddetto *Brussels effect*: «*The Brussels effect also strengthens the Commission's bureaucratic interests by enhancing the impact of its regulatory activities. Regulators generally have the incentive to generate more regulation rather than less because their success is measured by how much of their agenda is accomplished. Among the EU institutions, the Commission, in particular, is widely portrayed as a "competence maximizer", constantly looking to expand its powers and increase its influence over policy making. And when the Commission seeks to expand its competencies, it tends to do so via regulation*»[212]. Ciò, infatti, pare abbastanza riscontrabile nel settore della protezione dei dati personali.

[211] Dalla pagina della Commissione sulle priorità 2019-2024: https://ec.europa.eu/info/strategy/priorities-2019-2024_it.
[212] A. BRADFORD, *The Brussels Effect*, *cit*., p. 12, dove chiariva: «(…) *To a large extent, the Commission's tendency to govern through regulation is a result of the EU's small budget. (…) Thus, the only way for the Commission to expand its influence without extensive financial resources is to engage in regulatory activity, as regulations do not depend on the tax revenues available to the Community institutions*».

L'indipendenza, in generale

Passando al carattere di *indipendenza,* occorre brevemente esaminarne le peculiarità rispetto all'istituzione di riferimento. Esso, riconosciuto in generale alla Commissione, con evidenza accomuna quest'ultima alle autorità di controllo per la protezione dei dati.

Com'è noto l'indipendenza della Commissione rispetto ai governi degli Stati membri costituisce una garanzia per il corretto svolgimento delle sue funzioni legate alla realizzazione dell'interesse generale dell'Unione e pertanto appare una caratteristica congenita alla stessa previsione di tale istituzione, difatti prevista sin dagli albori e completata dall'incompatibilità per i commissari di altre attività concomitanti[213]. Le esperienze che hanno accompagnato l'evoluzione del ruolo della Commissione hanno mostrato talvolta la debolezza delle previsioni sull'indipendenza, minacciata non solo da influenze pubbliche ma anche private: «*the problem of the guarantee of independence cannot be resolved on the basis of mere provisions included in institutional treaties and that perhaps, rather than interference coming from the governments of the MS, the greatest dangers for the Commission come from non-public subjects. It is probably in light of such experiences that it was decided to include the provision of the necessary guarantee of independence in the TEU itself besides the general competence of the Commissioners*»[214]. Anche queste considerazioni hanno contribuito alla previsione di maggiori garanzie al riguardo, quali quelle risultanti, specie con il Trattato di Lisbona, dalla combinazione delle previsioni degli articoli 17, paragrafo 3 TUE e 245 e 247 TFUE.

Queste ultime norme, infatti, pongono l'accento sull'indipendenza dei singoli membri della Commissione, prevedendo interventi della Corte di giustizia in caso di violazione di detta indipendenza (articolo 245 TFUE) con la possibilità anche che la stessa Corte dichiari le dimissioni del singolo membro, su istanza del Consiglio o della Commissione (articolo 247 TFUE). Peraltro, oltre a tale responsabilità individuale rispetto al dovere di indipendenza incombente su ogni singolo commissario, è prevista anche (come si è accennato *ex* articolo 17, paragrafo 8 TUE, e specie in virtù del rafforzamento del ruolo del Parlamento e dei rapporti di quest'ultimo con la Commissione), una responsabilità collettiva dell'istituzione che potrebbe portare alle dimissioni congiunte di tutti i membri, che esprimerebbe il controllo politico del Parlamento sull'intera

[213] Cfr. E. GIANFRANCESCO, Article 17, *cit.*, pp. 709-710, che specifica: «*Only in this way would it have been able to permit within the body the majority vote principle, otherwise destined to be sucked into the logic of intergovernmental and interstate relations, with unforeseeable results in a college in which the margin in the origin of the components of the various MS has never been more than one*».
[214] Ibidem, p. 710.

istituzione (articolo 234 TFUE). Tale strumento, in realtà, lungi dall'essere «fisiologico nel rapporto fra Parlamento e Commissione (…) costituisce, semmai, un potere di "ultima istanza", da utilizzare in casi eccezionali»[215]. Se, dunque, è tendenzialmente corretto affermare che "il Parlamento non ha il potere di censurare l'operato dei singoli commissari"[216], assume però rilievo quanto previsto dal c.d. *accordo quadro sulle relazioni tra il Parlamento europeo e la Commissione europea* del 2010 in cui, alla sezione dedicata alla "responsabilità politica", è previsto che :"Qualora il Parlamento chieda al presidente della Commissione di ritirare la fiducia a un singolo membro della Commissione, il presidente prende seriamente in considerazione la possibilità di chiedere a tale membro di rassegnare le dimissioni, in conformità dell'articolo 17, paragrafo 6, TUE. Il presidente chiede le dimissioni di tale membro ovvero illustra al Parlamento il motivo del suo rifiuto di farlo nel corso della tornata successiva"[217].

Dunque, aldilà della più o meno diretta rilevanza sull'indipendenza della Commissione e dei suoi membri, queste considerazioni ci interessano qui anche perché contribuiscono a porre in rilievo le peculiarità in cui si manifesta la *EU rule of law*: «*In any case, the idea is confirmed of an institutional system characterised by a co-penetration and interweaving of powers, rather than the separation of the same*»[218]. E ciò emergerebbe anche dal complesso processo di formazione della Commissione, a cui partecipano sia gli Stati membri che le istituzioni politiche sovranazionali, cosa che ne connoterebbe la "disomogeneità politica" quale «tratto tipico (…) che la differenzia in maniera decisiva dagli esecutivi degli Stati membri»[219]. Come chiarisce Cannizzaro, tale disomogeneità si lega e si giustifica con le finalità proprie del processo di integrazione europea, alla luce delle quali essa va considerata e dunque, chiaramente, conferma la missione di promozione dell'interesse generale attribuita tipicamente alla Commissione: «Se alla sua formazione contribuiscono pressocché tutti gli attori politici dell'Unione, la Commissione si configura quindi come una Istituzione politicamente indipendente e sottoposta unicamente ai vincoli derivanti dai Trattati»[220].

---

[215] E. CANNIZZARO, *Il diritto dell'integrazione europea, cit.*, p. 74.
[216] G.GAJA, A. ADINOLFI, *op. cit.*, p. 44.
[217] Accordo quadro sulle relazioni tra il Parlamento europeo e la Commissione europea, OJ L 304, 20.11.2010, Sezione II, punto 4, disponibile qui: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32010Q1120%2801%29 .
[218] E. GIANFRANCESCO, Article 17, *cit.*, p. 723.
[219] E. CANNIZZARO, *Il diritto dell'integrazione, cit.*, p. 74.
[220] Ibidem, p. 43, dove l'autore continua: «Il prezzo da pagare per tale indipendenza è quello generalmente indicato con il termine "tecnocrazia". Esso esprime il disagio nei confronti di una Istituzione che svolge bensì funzioni politiche ma che appaia politicamente irresponsabile è infatti sempre più difficile qualificare le attività di attuazione dei Trattati istitutivi come attività di carattere tecnico, in particolare, alla luce dello sviluppo delle competenze attribuite all'Unione e del carattere discrezionale di molte di esse. D'altro lato, l'esistenza di una Istituzione preposta unicamente alla realizzazione del progetto politico che si rispecchia nei Trattati presenta l'indubbio vantaggio di sottrarre, per lo meno in parte, tale progetto al negoziato».

L'indipendenza nel settore della protezione dei dati personali

Ebbene, come si diceva, il carattere di indipendenza accomuna la Commissione alle autorità di controllo per la protezione dei dati. E proprio nel settore della protezione dei dati, infatti, tale elemento comune è emerso dall'analisi della giurisprudenza della Corte di giustizia.

In particolare, rispetto al caso *Schrems I* (cui si è già fatto cenno *supra*, e che si tratterà meglio nel prosieguo, Parte IV) qualcuno, tra gli innumerevoli commentatori, ha messo in evidenza come uno degli aspetti fondamentali della pronuncia consistesse proprio nella emersa "concorrenza" tra istituzioni indipendenti, ossia autorità di controllo e Commissione: «*what is at stake is institutional competition within the European Union where the two players – the Commission and the national supervisory authorities – in the field are both independent institutions responsible for the protection of European individuals and their privacy. There were two possible options: one was to subordinate the national player to the supranational one, so as to ensure consistency and uniformity in supervision of international data transfers from Europe; the other option was to disconnect one from the other, so as to expand the venues through which scrutiny of international data transfers may be obtained. The latter was the option chosen by the Court. In contrast with a traditional bias towards centralization, this judgment gives rise to an institutional configuration empowering national supervisory authorities. It reflects a form of institutional trust shifting*»[221].

In quel caso, infatti, la questione riguardava il trasferimento dei dati verso Paesi terzi e, come si è detto, la Corte ebbe modo di chiarire la necessità che le autorità di controllo effettuassero un'autonoma valutazione dei reclami presentati dagli interessati per garantire a questi ultimi un'effettiva tutela, senza arrestarsi alla mera constatazione dell'esistenza di una decisione di adeguatezza della Commissione sul Paese terzo in questione, ma piuttosto, in caso di dubbi sulla conformità di quest'ultima con le previsioni dei Trattati, potendo intervenire per sollecitare un rinvio pregiudiziale di validità alla Corte di giustizia. Nello stesso commento, gli autori sottolineavano come da quella pronuncia derivasse una sorta di "mutamento" nella fiducia istituzionale, con un ridimensionamento del ruolo della Commissione e un potenziamento – per quanto ambiguo – dell'intervento delle autorità di controllo nella gestione del trasferimento dei dati dall'Unione europea verso Paesi terzi; in aggiunta, gli autori ravvisavano anche un aumento della responsabilità al riguardo in capo ad altre istituzioni indipendenti, ossia quelle giudiziarie: i

[221] L.AZOULAI, M. VAN DER SLUIS, Institutionalizing personal data protection in times of global institutional distrust: *Schrems*, in *Common Market Law Review*, 53, 2016, p. 1356.

tribunali nazionali e la Corte di giustizia[222]. Sorvolando per ora su questo ultimo aspetto, rileva qui la rimodulazione del modo di intendere l'intervento delle due figure istituzionali indipendenti, non giudiziarie, nella gestione di un aspetto particolarmente delicato per la protezione dei dati personali, ossia il trasferimento al di fuori dell'Unione europea, nonché l'attenzione sul rapporto tra di esse.

Risulta particolarmente interessante e condivisibile, pertanto, la valutazione degli autori sul carattere di indipendenza delle autorità e, quindi, della Commissione. Questi, facendo un valido parallelo tra la pronuncia in questione e quella relativa al caso *Commissione c. Germania*, rilevante – come si è visto – per l'indipendenza delle autorità di controllo, notavano: «*In* Commission v. Germany, *the Court observed that the purpose of the independence was "to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim". In Schrems, this extends to independence from EU institutions and in particular the one presented as the most trustable one for national authorities and the most protective one for individuals, the European Commission*»[223]. E proprio queste considerazioni, che sono state oggetto privilegiato della seconda pronuncia su caso c.d. *Schrems II* anche in considerazione del rinnovato assetto predisposto dal GDPR, conducono inevitabilmente a valutazioni che implicano l'ulteriore elemento caratteristico della Commissione, e che, ancora una volta, accomuna quest'ultima alle autorità indipendenti: il potere di controllo.

Il potere di controllo, nelle sue varie accezioni

Il *potere di controllo/vigilanza* della Commissione emerge dalle inequivocabili previsioni dell'articolo 17 TFUE e ne consacra il ruolo di "guardiana dei Trattati".

Anche rispetto alla Commissione, come per le autorità nazionali indipendenti, è possibile ravvisare un controllo sia in senso "attivo" che "passivo". Anzitutto va precisato che con potere di controllo previsto dalla norma primaria si fa generalmente riferimento alla vigilanza sul corretto adempimento degli obblighi derivanti dal diritto dell'Unione in capo agli Stati membri. In tal senso, dunque, riconducibile alla prima predetta accezione di controllo, un fondamentale strumento attribuito alla Commissione per esercitare la necessaria vigilanza è la procedura di infrazione che può sfociare in un ricorso alla Corte per inadempimento dello Stato interessato (v. articoli 258-260 TFUE).

[222] Ibidem, p. 1356.
[223] Ibidem, p. 1358.

Nello specifico settore della protezione dei dati personali ciò è avvenuto particolarmente, come si è detto, rispetto alle disposizioni sull'indipendenza delle autorità garanti nazionali, che, come confermato dalla Corte di giustizia, venivano mal interpretate da alcuni Stati membri. Peraltro, interventi di tal genere della Corte di giustizia esprimono, in qualche modo, anche il controllo "passivo" sull'operato della Commissione (in tali casi, con esito a quest'ultima favorevole) rispetto alla vigilanza nella corretta applicazione delle disposizioni relative alla tutela dei dati da parte degli Stati membri.

Ma, tra i molteplici aspetti in cui può declinarsi tale vigilanza, ci interessa particolarmente soffermarci sul controllo che la Commissione è chiamata a effettuare (prima, *ex* articolo 25 Direttiva 95/46/CE; ora, *ex* articolo 45 GDPR) rispetto al livello di adeguatezza che Paesi terzi o organizzazioni internazionali devono soddisfare per consentire il trasferimento di dati personali dall'Unione europea. Considerazioni sul merito della valutazione della Commissione riguardano principalmente aspetti di rappresentanza esterna e/o di coerenza tra azione interna ed esterna, e verranno dunque affrontate successivamente. Qui valga, invece, puntualizzare la portata di tale valutazione, espressa tramite la c.d. *decisione di adeguatezza*, con riguardo al rapporto tra la Commissione e l'apparato istituzionale previsto (soprattutto) dal nuovo sistema di protezione dei dati, ossia le autorità nazionali, da un lato, e il Comitato europeo per la protezione dei dati (EDPB) dall'altro. Come si diceva, l'intervento della Commissione rispetto al trasferimento dei dati personali fuori dall'Unione europea è stato rimodulato dalla Corte di giustizia, in particolare nell'ambito della saga *Schrems*. Mentre la prima pronuncia del 2015 si basava sulle disposizioni della direttiva madre, l'ultima del 2020 prende in considerazione le innovazioni introdotte dal GDPR, ma entrambe presentano tra gli aspetti determinanti la rimodulazione del rapporto tra intervento (e controllo) della Commissione e delle autorità.

Senza poter approfondire adesso i dettagli delle pronunce né le peculiarità del trasferimento dei dati verso l'esterno, basti qui dire che nel caso *Schrems I* la Corte veniva interrogata, tra le altre cose, sulla validità della decisione 2000/520/CE della Commissione relativa all'adeguatezza della tutela offerta dai principi di c.d. approdo sicuro (secondo l'accordo c.d. *Safe Harbor*) rispetto, essenzialmente, al sistema degli Stati Uniti. In quell'occasione, come abbiamo detto, la "mera" esistenza di una tale decisione di adeguatezza indusse l'autorità di controllo competente, ossia il Data Protection Commissioner irlandese, a rigettare la trattazione di un reclamo proposto dal signor Schrems che poneva in dubbio la compatibilità del trasferimento dei dati dall'Unione europea verso gli Stati Uniti operato da Facebook Ireland, in considerazione delle allora recenti e ben note

rivelazioni di Edward Snowden rispetto alle attività dei servizi di intelligence della National Security Agency (NSA) di quel Paese.

È utile rimarcare che quella decisione di adeguatezza venne assunta sulla base delle previsioni della Direttiva madre, la quale dedicava il Capo IV al trasferimento dei dati verso Paesi terzi. In particolare, lo ricordiamo, l'articolo 25 stabiliva: «2. L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, *le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate*. (…) 6. La Commissione *può constatare*, secondo la procedura di cui all'articolo 31, paragrafo 2, *che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo*, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, *ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona*. Gli Stati membri adottano *le misure necessarie per conformarsi alla decisione della Commissione*»[224].

Orbene, la questione posta alla Corte richiedeva, in sostanza, in che misura l'esistenza di una decisione di adeguatezza della Commissione potesse "impedire" all'autorità nazionale di controllo di esaminare un reclamo riguardante il trasferimento di dati personali verso il Paese terzo coinvolto. In ciò, quindi, emerge chiaro il rapporto tra controllo ("attivo") operato dalla Commissione e controllo ("attivo") operato dall'autorità nazionale, quest'ultima, nel caso di specie, realizzando un'autocensura del proprio intervento in vista di quello già svolto dalla Commissione. La questione, insomma, riguardava l'esistenza e/o le modalità di una sorta di relazione "gerarchica" tra intervento delle autorità e intervento della Commissione. E proprio su questo la Corte ha realizzato la suddetta "rimodulazione", essenzialmente chiarendo la portata delle disposizioni e dello spirito della direttiva, in conformità con le previsioni della Carte dei diritti fondamentali: «*Poiché le autorità nazionali di controllo sono incaricate, ai sensi dell'articolo 8, paragrafo 3, della Carta e dell'articolo 28 della direttiva 95/46, di sorvegliare il rispetto delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, ciascuna di esse è quindi*

[224] Direttiva95/46/CE,, Articolo25, parr. 2 e 6.

investita della competenza a verificare se un trasferimento di dati personali dal proprio Stato membro verso un paese terzo rispetti i requisiti fissati dalla direttiva 95/46»[225].

Così esordendo, la Corte riconosceva l'importanza dei trasferimenti di dati verso Paesi terzi per gli scambi internazionali, puntualizzando che ai sensi dell'articolo 25, paragrafo 1, "siffatti trasferimenti possano avere luogo soltanto se tali paesi terzi garantiscono un livello di protezione adeguato", e contrariamente essere vietati. In vista di dette finalità, dunque, sarebbero posti della direttiva degli obblighi in capo agli Stati e alla Commissione, entrambi chiamati a valutare l'adeguatezza dello Stato di destinazione dei dati. La Corte precisava poi che la Commissione può adottare una decisione di adeguatezza, *ex* articolo 25, paragrafo 6, alla quale gli Stati membri devono conformarsi: «*Ai sensi dell'articolo 288, quarto comma, TFUE, essa ha un carattere vincolante per tutti gli Stati membri destinatari e si impone pertanto a tutti i loro organi (...). Pertanto, fintantoché la decisione della Commissione non sia stata dichiarata invalida dalla Corte, gli Stati membri e i loro organi, fra i quali figurano le loro autorità di controllo indipendenti, non possono certo adottare misure contrarie a tale decisione, come atti intesi a constatare con effetto vincolante che il paese terzo interessato da detta decisione non garantisce un livello di protezione adeguato* (…). *Tuttavia, una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, come la decisione 2000/520, non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo di investire le autorità nazionali di controllo di una domanda, ai sensi dell'articolo 28, paragrafo 4, di tale direttiva, relativa alla protezione dei loro diritti e delle loro libertà con riguardo al trattamento di tali dati (...). Né l'articolo 8, paragrafo 3, della Carta né l'articolo 28 della direttiva 95/46 escludono dall'ambito di competenza delle autorità nazionali di controllo il controllo dei trasferimenti di dati personali verso paesi terzi che sono stati oggetto di una decisione della Commissione in forza dell'articolo 25, paragrafo 6, di tale direttiva*»[226]. La Corte ha quindi ritenuto espressamente contraria allo spirito della direttiva, e al sistema da essa predisposto, l'ipotesi che una decisione di adeguatezza della Commissione impedisca all'autorità di controllo di esercitare il proprio potere e dunque apprestare la necessaria tutela ai richiedenti, verificando in piena indipendenza il rispetto dei requisiti previsti per il trasferimento verso l'esterno.

Pertanto, la Corte concludeva che: «*l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, quale la decisione 2000/520, con la quale la Commissione constata che*

[225] Corte di giustizia, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, 6 ottobre 2015, p. 47,enfasi aggiunta.
[226] Ibidem, punti 51-54, sottolineato aggiunto.

un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, esamini la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato»[227]. Questi passaggi, che si commenteranno nel prosieguo anche rispetto a vari altri aspetti, fanno emergere chiaramente come, in sostanza, l'esercizio dei rispettivi poteri di controllo da parte della Commissione e delle autorità nazionali nel settore della protezione dei dati personali (e al fine di garantire adeguata tutela ai titolari dei dati, pur considerando le esigenze degli scambi internazionali) realizzi inevitabilmente una sorta di "capovolgimento" tale per cui il controllo esercitato dalle autorità si manifesta, in qualche modo, anche come possibile controllo indiretto in capo all'operato della Commissione.

In questo senso, non pare errato parlare di un qualche controllo "passivo" che la Commissione subirebbe proprio nell'esercitare il suo controllo "attivo" estrinsecantesi nella decisione di adeguatezza. Per quanto, ovviamente, ciò sarebbe solo potenziale e indiretto da parte delle autorità nazionali, posto che il controllo unico sulla legittimità dell'operato delle istituzioni spetta, come la pronuncia suddetta ha ribadito anche in questo settore, sempre e in ultima analisi alla Corte di giustizia, quale massima espressione della *EU rule of law*[228].

Nondimeno, è interessante poter ravvisare la logica sottesa al sistema, che il ragionamento della Corte ha fatto emergere più chiaramente, di un meccanismo concatenato di interventi e controlli che si implicano e si "vigilano" a vicenda, e che dunque proprio in questo equilibrio (perlomeno,

---

[227] Ibidem, p. 66, enfasi aggiunta.
Prima, il riferimento è ai punti 56-58.Inoltre, al punto 63 si puntualizzava: «Alla luce di tali considerazioni, qualora una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo che è stato oggetto di una decisione della Commissione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, investa un'autorità nazionale di controllo di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di tali dati e contesti, in occasione di tale domanda, come nel procedimento principale, la compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona, *incombe a tale autorità esaminare detta domanda con tutta la diligenza richiesta*».

[228] Cfr. ibidem, punti 60-61: «(…) occorre richiamare la giurisprudenza costante della Corte secondo la quale *l'Unione è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali* (v., in tal senso, sentenze Commissione e a./Kadi, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 66; Inuit Tapiriit Kanatami e a./Parlamento e Consiglio, C-583/11 P, EU:C:2013:625, punto 91, nonché Telefónica/Commissione, C-274/12 P, EU:C:2013:852, punto 56). *Le decisioni della Commissione adottate in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 non possono pertanto sfuggire ad un siffatto controllo*. Ciò premesso, *la Corte è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione*, quale una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, della direttiva 95/46; la natura esclusiva di tale competenza ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione (v. sentenze Melki e Abdeli, C-188/10 e C-189/10, EU:C:2010:363, punto 54, nonché CIVAD, C-533/10, EU:C:2012:347, punto 40).», enfasi aggiunta.

prospettato), testimoniano il peculiare atteggiarsi dei principi della *EU rule of law* nel settore della protezione dei dati personali.

Seguendo questo ordine di considerazioni, la sentenza *Schrems II* fornisce poi un ulteriore supporto nel perfezionare le dinamiche di tale meccanismo, in vista delle innovazioni apportate al sistema dal GDPR. Ci riferiamo alla già accennata istituzione del Comitato europeo per la protezione dei dati (EDPB) che, previsto per la prima volta dall'articolo 68 del GDPR, concorre a incrementare il meccanismo di controlli e così, in qualche modo, forse anche ad incentivare ciò che alcuni autori avevano già considerato in *Schrems I* come «*the Court's apparent distrust towards the Commission*»[229].

Pur rinviando al prosieguo valutazioni sul ruolo effettivo dell'EDPB (e del predecessore WP29), va brevemente detto, intanto, che già prima della pronuncia *Schrems I* il Gruppo di Lavoro Articolo 29 aveva emesso un documento relativo all'applicazione dell'articolo 25 (e 26) della direttiva madre[230], poi sistemato proprio alla luce di quella pronuncia, mentre successivamente nell'ottobre 2016 è intervenuto con un parere su emendamenti a proposte della Commissione relativi ai poteri delle autorità garanti rispetto alle clausole contrattuali tipo e alle decisioni di adeguatezza, proprio in coerenza con le conclusioni della Corte in *Schrems I*. Già questi documenti, consistendo in sostanza nella definizione di direttive su come meglio impostare l'intervento delle istituzioni coinvolte rispetto alla protezione dei dati personali, in un certo senso implicavano una qualche vigilanza/raccomandazione del Gruppo di Lavoro Articolo 29 nei confronti della Commissione. Ebbene, accogliendo questa prospettiva, ciò pare ancor più vero rispetto all'operato dell'EDPB, in particolar modo dopo la pronuncia *Schrems II*.

Si avrà modo di commentare questa pronuncia, soprattutto rispetto a questioni non legate alla decisione di adeguatezza (che risultano di fatto le più rilevanti), ma qui valga ricordare che, com'è noto, la sua immediata risonanza (a livello mediatico, ancor più che scientifico) ha riguardato proprio la *seconda* decisione di adeguatezza della Commissione rispetto al trasferimento dei dati verso gli Stati Uniti, che ha dato nuovamente occasione alla Corte di sanzionare la *validità* della valutazione effettuata dalla Commissione, così ponendone in forte dubbio l'operato e avallando quell'orientamento di "*distrust*" che si era già percepito rispetto alla prima pronuncia. Qui manteniamo, però, l'attenzione sulla "rimodulazione" che, in qualche modo, ha subito il controllo (attivo) della Commissione sull'adeguatezza dei Paesi terzi e, quindi, sulla rimodulazione del

[229] L.AZOULAI, M. VAN DER SLUIS, op. cit., p. 1359.
[230] Gruppo di Lavoro Articolo 29, Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva95/46/CE del 24 ottobre 1995, Adottato il 25 novembre 2005, WP114.

controllo (passivo) al quale la stessa istituzione risulta sottoposta da parte dell'EDPB soprattutto dopo *Schrems II*.

Quanto al primo aspetto, all'indomani della pronuncia qualche autore ha acutamente rilevato come essa rappresentasse, rispetto alle valutazioni di adeguatezza *ex* articolo 45 GDPR, una sorta di passaggio da un controllo "centralizzato" attribuito dalla previsione regolamentare alla Commissione, a un controllo "decentralizzato" che si frammenterebbe tra diversi attori coinvolti, soprattutto potenziando la privatizzazione: «*Schrems II might have profound implications for the system of assessing whether a third country, to which data are transferred, ensures an adequate level of protection. Till now this assessment was done in a centralized way, by the Commission. Without questioning the Commission's powers in this respect, Schrems II operates a huge turn towards a "privatization" and decentralization of such assessments. Taking into consideration, nonetheless, the risks of fragmentation resulting from such an approach, the CJEU proposes a "re-centralization" with an extremely powerful role henceforward for the EDPB*»[231]. Si avrà modo di analizzare le implicazioni appena accennate, qui basti notare che proprio questo ultimo rilievo sulla "ri-centralizzazione" conduce verso il secondo aspetto suddetto, relativo al controllo effettuato dal Comitato europeo.

Com'è noto, ben prima della sentenza *Schrems II* il Comitato aveva emesso linee guida sulla valutazione di adeguatezza, così come pareri rispetto alle decisioni assunte dalla Commissione. Tuttavia, è stato proprio a partire da quella pronuncia che il Comitato europeo è parso diventare il "Grande valutatore dell'adeguatezza giuridica globale", come lo ha inteso Christakis, la cui brillante analisi ci consentirà di spiegare questo aspetto. L'autore parte dal punto 147 della sentenza, che stabilisce: «*Per quanto riguarda la circostanza, menzionata dal Commissario, che trasferimenti di dati personali verso siffatto paese terzo potrebbero eventualmente essere oggetto di decisioni divergenti delle autorità di controllo in Stati membri diversi, occorre aggiungere che, come risulta dall'articolo 55, paragrafo 1, e dall'articolo 57, paragrafo 1, lettera a), del RGPD, il compito di vigilare sul rispetto di tale regolamento è affidato, in linea di principio, a ciascuna autorità di controllo nel territorio dello Stato membro cui essa appartiene. Inoltre, al fine di evitare decisioni divergenti, l'articolo 64, paragrafo 2, di tale regolamento prevede la possibilità, per l'autorità di controllo che ritenga che i trasferimenti di dati verso un paese terzo debbano, in generale, essere vietati, di adire il Comitato europeo per la protezione dei dati (EDPB), il quale può, in applicazione dell'articolo 65, paragrafo 1, lettera c), dello stesso regolamento, adottare una decisione vincolante, in particolare quando un'autorità di controllo non si conforma al parere*

[231] T. CHRISTAKIS, After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe, *European Law Blog*, 21 July 2020.

emesso»[232]. Questo punto, invero, richiama aspetti di coerenza che verranno trattati tra poco, ma esso assume rilievo in parte anche quanto al richiamo al ruolo del Comitato europeo. L'autore, infatti, notava al riguardo: «*Entrusting national DPAs with the task to issue "adequacy decisions", after such complex and difficult assessments of foreign countries laws, presents the risk of fragmentation and divergent views on these issues. In para. 147 of Schrems II the Court proposed a solution by saying that if supervisory authorities disagree about transfers, the EDPB is assigned to resolve such disputes. The Court thus goes back to the need for centralization but the organ entrusted with this mission is not the Commission anymore, but the EDPB. The constitutional significance of this development is evident: the EDPB becomes the all-mighty assessor of global legal adequacy. But if a centralized assessment of adequacy is, in my opinion, a real necessity, the intervention of the EDPB does not come without problems*»[233]. Tralasciando per ora le interessanti valutazioni sulle problematiche sollevate dal ravvisato orientamento della Corte e dal rinnovato intervento del Comitato europeo, qui basti notare che tale analisi fa emergere la considerazione del Comitato europeo come, in qualche modo, *principale* controllore delle valutazioni di adeguatezza. E questo, ovviamente, con delle ripercussioni anche sulla vigilanza effettuata al riguardo dalla Commissione.

Ciò pare, infatti, confermato dagli interventi del Comitato proprio a seguito dell'ultima pronuncia, ossia le famose Raccomandazioni n. 1 e 2 del 10 novembre 2020, che hanno in poco tempo suscitato parecchio scalpore. Anche di esse si approfondirà l'analisi (*infra*, Capitolo II, Parte IV); qui si vuole solo fare cenno, in particolare, alle *Raccomandazioni n. 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza* che, in sostanza, approfondiscono le "quattro garanzie essenziali europee" che spiegherebbero i requisiti giuridici per giustificare le limitazioni ai diritti alla protezione dei dati e alla vita privata per esigenze di trasferimento dei dati fuori dall'Unione.

Tali raccomandazioni, che aggiornano quelle predisposte dal Gruppo di Lavoro Articolo29 dopo *Schrems I* e si basano sulla giurisprudenza della Corte di giustizia (e EDU), hanno l'intento di "*fornire elementi utili a valutare se misure di sorveglianza che consentono l'accesso ai dati personali da parte delle autorità pubbliche di un paese terzo, siano esse agenzie di sicurezza nazionale o autorità incaricate dell'applicazione della legge, possano configurare un'ingerenza giustificabile o meno*" [234]. Nondimeno (e tralasciando valutazioni e critiche rispetto al merito delle

[232] Corte di giustizia, C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems*, 16 luglio 2020, p. 147.
[233] T. CHRISTAKIS, After Schrems II : Uncertainties, *cit*.
[234] Comitato europeo per la protezione dei dati, Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza, Adottate il 10 novembre 2020, punto 7, ma si vedano punti 1-12.

stesse, che si faranno nel prosieguo), esse rappresentano in qualche modo l'emblema di ciò che abbiamo inteso come "rimodulazione" nell'esercizio del controllo da parte della Commissione (e nel rinnovato ruolo riconosciuto alle autorità nazionali e, ancor di più, al Comitato europeo). Al punto 52, infatti, si legge: "Nel valutare l'adeguatezza del livello di protezione, ai sensi dell'articolo 45 del RGPD, *la Commissione dovrà valutare se le garanzie essenziali europee siano soddisfatte* nel quadro degli elementi da considerare per garantire che la legislazione del paese terzo nel suo insieme offra un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE"[235]. Proprio rispetto a questo punto, lo stesso autore qualche mese dopo commentava: «*Paragraph 52 of the "EEG Recommendations" is a "warning shot" that the European Commission cannot afford to ignore: the message is that future adequacy decisions should ensure that the requirements found in the "EEG Recommendations" are met in the foreign country. The Commission now has an updated "user's manual" for adequacy decisions that should be taken into consideration*»[236]. Ciò significa, evidentemente, che se la Commissione deve conformare le proprie decisioni di adeguatezza alle garanzie individuate dall'EDPB, è proprio questi in ultima analisi a realizzare, per quanto indirettamente, un controllo sull'operato della Commissione, dettandone i criteri per il suo operato. Controllo, peraltro, che si aggiunge, come si vedrà, alla prassi di formulazione del Parere dell'EDPB sulla proposta di decisione di adeguatezza della Commissione. Sino a che punto ciò sia funzionale, ovvero implichi complicazioni, rispetto al sistema di protezione dei dati, sarà oggetto di valutazioni successive. Qui riteniamo di poter concludere che, anche alla luce degli ultimi sviluppi, ciò che emerge in teoria è un sistema di protezione dei dati in cui il potere di vigilanza della Commissione, quale "guardiana dei Trattati" ha subito delle smussature e degli adattamenti, che però, soprattutto seguendo il percorso argomentativo della Corte nelle pronunce della saga *Schrems*, parrebbero, almeno in linea teorica, cercare di adattarsi alle peculiarità in cui si estrinseca la *EU rule of law*.

La rappresentanza esterna

Per concludere, il riferimento alle decisioni di adeguatezza cui è tenuta la Commissione coinvolge anche, in qualche misura, l'ultimo aspetto caratteristico dell'istituzione che abbiamo indicato tra

[235] Ibidem, punto 52, enfasi aggiunta.
[236] T. CHRISTAKIS, "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1), in *European Law Blog*, 13 November 2020, in cui l'autore provocatoriamente continua: «*Going even further, a devil's advocate might argue that the "EEG Recommendations" could be a valuable tool in the hands of activists, as a means of challenging the validity of existing adequacy decisions through action at the CJEU. Do the twelve States or entities that have until now benefited from adequacy decisions all meet these EEG requirements? Does Israeli or Japanese surveillance law, for instance, really meet the EEG requirements? And what should the consequences be if they do not?*».

quelli rilevanti nel settore della protezione dei dati personali (specie dal punto di vista a noi più caro, ossia il trasferimento dei dati verso l'esterno): la *rappresentanza esterna dell'Unione*.

Come prevede l'articolo 17, par. 1, TUE, la Commissione rappresenta l'Unione in ambito internazionale, tranne che nel settore PESC e negli altri espressamente previsti dai Trattati. Com'è noto, tale aspetto è stato fortemente ridimensionato a seguito della preminenza riconosciuta dal Trattato di Lisbona all'Alto Rappresentante per gli affari esteri e la politica di sicurezza (articolo 18 TUE), introdotto (con diversa denominazione e differenti peculiarità) dal Trattato di Amsterdam e che comunque da Lisbona è divenuto anche membro e vicepresidente della Commissione, occupandosi appunto delle relazioni esterne.

Senza divagare sul ruolo, pur centrale, dell'Alto Rappresentante, qui va detto che per quanto il carattere di rappresentanza esterna in capo alla Commissione abbia subito dei mutamenti nel corso dell'evolversi del processo di integrazione europea, esso comunque mantiene rilievo, così come previsto dalle disposizioni dei Trattati, poiché in qualche modo costituisce immutabilmente «*the extent of the history of European integration and an insuppressible demand for functionality of the relations of the Union with the external world*»[237]. Ciò trova conferma principalmente nella conclusione di accordi internazionali in materia di politica commerciale comune (articolo 207 TFUE), ma anche, e conseguentemente, negli interventi rispetto alle politiche di allargamento e di cooperazione allo sviluppo o nelle procedure per la conclusione degli accordi di associazione, nonché più in generale (e anche nell'ambito di quegli interventi) rispetto alla promozione dei valori dell'Unione nell'azione esterna.

Ebbene, da queste brevi considerazioni è possibile rintracciare più di un punto di contatto con il settore della protezione dei dati personali, che presterebbe il fianco all'esplicazione del ruolo della Commissione rispetto alla dimensione esterna della *EU Rule of Law*. Senza per ora addentrarci nelle interessanti considerazioni legate alla "esternalizzazione" della normativa europea, che avviene inevitabilmente per il tramite dell'intervento della Commissione e che trova massima espressione nella protezione dei dati (e, in particolare, del GDPR), basti qui dire che (un po' con le stesse logiche che hanno condotto la politica commerciale comune, a partire dalle esigenze del mercato interno) indirettamente il *Brussels effect* «*offers an important foreign policy instrument, compensating the Commission for the lack of power it otherwise has in external affairs. (…) In Brussels Effect, the Commission has a powerful tool to shape global markets and the international*

[237] E. GIANFRANCESCO, Article 17 [The European Commission], in in H.-J. BLANKE, S. MANGIAMELI (Eds), *The Treaty on European Union (TEU) – A Commentary*, Springer, 2013, p. 695.

regulatory environment, without the need to secure unanimity in the Council»[238]. Questa estensione del "*European regulatory state*" fuori dall'Unione, per quanto indiretta e, come abbiamo detto, almeno agli inizi non completamente volontaria, nella misura in cui avviene chiama la Commissione ad agire nel rispetto dei valori che connotano anche l'azione esterna dell'Unione, tanto più che essa la rappresenta e così se ne fa prima promotrice.

Nel settore della protezione dei dati personali la Commissione sembra sempre più consapevole e convinta di voler insistere in questa direzione, nonostante (e in considerazione de) le perplessità emerse dalla giurisprudenza che la coinvolge. Si consideri, per esempio la suddetta *Com2010 su EUROPA 2020*, in cui, in coerenza con gli interventi di Lisbona, si leggeva: *"L'UE conferisce un valore aggiunto sulla scena mondiale. L'UE influirà sulle decisioni politiche mondiali solo se agirà all'unisono. Il potenziamento della nostra rappresentanza esterna dovrà andare di pari passo con un maggiore coordinamento interno*". A maggior ragione ciò risulta dalle priorità dell'attuale Commissione, in una lettura combinata degli obiettivi quali '*un'Europa pronta per l'era digitale*', '*un'Europa più forte nel mondo*' e '*Promoting our European way of life*'.

Ma espressione di rappresentanza esterna, nonché di promozione dei valori identitari dell'Unione, sembra ravvisabile anche nell'espletamento della suddetta valutazione di adeguatezza *ex* articolo 45 GDPR al fine di consentire il trasferimento dei dati personali verso Paesi terzi e organizzazioni internazionali, considerando gli elementi indicati dalla norma (tra cui lo stato di diritto e il rispetto dei diritti umani e delle libertà fondamentali, e la pertinente legislazione nello Stato interessato) e seguendo le garanzie essenziali europee indicate di recente dall'EDPB. Ciò, ovviamente, pur tenendo a mente quanto si è visto emergere dalla saga *Schrems*; in particolare, laddove sono sorte perplessità, emerse rispetto alla prima pronuncia ma ampiamente confermate dalla seconda, proprio quanto al ruolo di "custode dello Stato di diritto" riconosciuto generalmente alla Commissione: «*In this instance, the Commission is regarded by the Court as a political body and not as technical body responsible for the oversight of Union law. Had the Court trusted the Commission in sticking to its traditional role as a guardian of the rule of law, the Court might have invalidated its adequacy decision whilst keeping the national authorities fully subordinate to the Commission. Instead, it decided to rely on supervisory authorities as trustees in the field of data protection. This trust appears mainly to derive from a theoretical analysis of the position of these national supervisory authorities (independence combined with significant powers), rather than from any empirical observations of their actual capacities*.» [239].

[238] A. BRADFORD, op. cit., p. 17.
[239] L.AZOULAI, M. VAN DER SLUIS, *Institutionalizing personal data protection, cit.*, p. 1359.

Queste considerazioni, anche laddove richiamano le relazioni tra intervento della Commissione e quello delle autorità nazionali (nonché, dell'EDPB) implicano inevitabilmente valutazioni sulla coerenza tra azione interna ed esterna dell'Unione, conducendo pertanto all'analisi di tale principio sia in generale che con specifico riguardo alla protezione dei dati personali, così consentendo poi di chiudere questa Parte dedicata all'esposizione teorica degli aspetti che intercettano le peculiarità del sistema di valori dell'Unione, e in particolare il funzionamento della *EU rule of law*, rispetto al settore digitale e, in particolare, alla protezione dei dati dei dati personali.

CAPITOLO III

LA COERENZA TRA AZIONE INTERNA ED ESTERNA DELL'UNIONE QUANTO AL RISPETTO *DELLA EU RULE OF LAW* NELLA PROTEZIONE DEI DATI PERSONALI

1. Il principio generale di coerenza nell'azione dell'Unione

Passiamo ora ad esporre, per linee teoriche e con qualche basilare riferimento alla giurisprudenza che sarà funzionale a successive valutazioni pratiche, perché assume rilievo per il nostro lavoro il concetto di "coerenza" nell'azione dell'Unione europea. In particolare, esso rileva ai nostri fini sotto una duplice accezione: come principio generale, ricavabile dall'articolo 21 TUE, che dovrebbe orientare con uniformità l'operato dell'Unione, sia nella sua dimensione interna che esterna, con particolare riguardo alla conformità ai valori su cui essa si fonda e, in questo senso, anche rispetto al settore della protezione dei dati personali; come specifico elemento di meccanismo di gestione delle relazioni tra istituzioni coinvolte nella protezione dei dati personali, in particolare le autorità nazionali e il Comitato europeo, secondo quanto previsto dal GDPR.

Quanto alla prima accezione, il principio di coerenza tra azione interna ed esterna può ritenersi sancito dall'articolo 21, par. 3, TUE che prevede: "*Nell'elaborazione e attuazione dell'azione esterna nei vari settori compresi nel presente titolo e nella parte quinta del trattato sul funzionamento dell'Unione europea e delle altre politiche nei loro aspetti esterni, l'Unione rispetta i principi e persegue gli obiettivi di cui ai paragrafi 1 e 2. L'Unione assicura la coerenza tra i vari settori dell'azione esterna e tra questi e le altre politiche. Il Consiglio e la Commissione, assistiti dall'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, garantiscono tale coerenza e cooperano a questo fine*". Peraltro, i richiamati paragrafi 1 e 2 precisano che "*L'azione dell'Unione sulla scena internazionale si fonda sui principi che ne hanno informato la creazione, lo sviluppo e l'allargamento e che essa si prefigge di promuovere nel resto del mondo: democrazia, Stato di diritto, universalità e indivisibilità dei diritti dell'uomo e delle libertà fondamentali, rispetto della dignità umana, principi di uguaglianza e di solidarietà e rispetto dei principi della Carta delle Nazioni Unite e del diritto internazionale*", aggiungendo che l'Unione si adopera per assicurare un elevato livello di cooperazione nelle relazioni internazionali anche al fine di salvaguardare i suoi valori.

Per quanto non possa dirsi definibile con incontrovertibile chiarezza, tale principio presenta delle caratteristiche ben precise, tra tutte la vocazione verso un modello coordinato di azione dell'Unione, sia tra le sue istituzioni che tra queste e gli Stati membri, che sia orientato verso obiettivi uniformi e concordati e che si prospettino in maniera inequivoca anche come politiche esterne[240]. La necessità di coerenza sistematica coinvolge l'intera architettura dell'Unione in ogni suo aspetto della dimensione interna, così rispetto all'apparato istituzionale (come si evince dall'articolo 13 TUE) e nella richiesta di leale cooperazione agli Stati membri (articolo 4, paragrafo 3 TUE). Inoltre, la prospettata coerenza nell'ambito dell'azione esterna (e di questa con le altre politiche) si estrinseca a sua volta sia orizzontalmente che verticalmente: «*The obligation to strive for the coherence of all the Union's external action applies horizontally as well as vertically, which means that all the actors at the EU level shall strive to coordinate their actions in such a way as to achieve a consistent and coherent policy (horizontally), as well as that the Union and its MS should try to coordinate in the interest of a coherent policy outcome (vertically)*»[241]. Peraltro, la coerenza nell'azione esterna parrebbe essere diventata quasi una "ossessione", che deriverebbe dalle potenzialità percepite dall'Unione rispetto al suo intervento come attore internazionale: *«' Coherence ' is a fixation with the policy and legal outcomes that the EU should produce in its external action in order to be effective as an international actor*»[242].

Orbene, tralasciando la disamina degli strumenti attraverso i quali tale coerenza dovrebbe attuarsi (che incidono essenzialmente, ma non esclusivamente, sul sistema di attribuzione delle competenze), e sorvolando anche sugli obblighi più o meno definiti che incombono sulle tre istituzioni chiamate dall'articolo 21 TUE a garantire tale coerenza (ossia: Commissione, Consiglio e Alto Rappresentante)[243], ciò che qui ci interessa è valutare il principio di coerenza in termini di rispetto e promozione dei valori propri dell'Unione, in particolare in ciò che ne impernia la struttura oltre che l'azione, ossia la *EU Rule of Law*. Risalta, quindi, anzitutto la combinazione delle disposizioni degli articoli 2 e 3 TUE con l'articolo 21 TUE, laddove il primo, com'è noto, enuclea i valori su cui l'Unione si fonda, come comuni agli Stati membri, e il secondo, in particolare al

[240] Cfr. S. OETER, Article 21 TEU [The Principles and Objectives of the Union's External Action], in H.-J. BLANKE, S. MANGIAMELI (Eds), *The Treaty on European Union (TEU) – A Commentary*, Berlin - Heidelberg - New York, 2013, pp. 868-869. Ivi l'autore continua: «*Institutional arrangements and common objectives do not always achieve the desired result of policy coherence.158 "Consistency" (or "coherence") as a legal concept thus must mean more, must also imply a core of substantial obligations requiring that the institutions strive for consistency and coherence*».
[241] S. OETER, *op. cit*., p. 869.
[242] M. ESTRADA CAÑAMARES, Building Coherent EU Responses': Coherence as a Structural Principle in EU External Relations, in C. CREMONA (ed.), *Structural Principles in EU External Relations Law*, Hart Publishing, 2018, p. 244, che usa il termine "ossessione" e continua: «*There are two fundamental reasons behind the permanent quest for coherence in EU external relations. The first is the complex legal space in which the Union' s external action is to be developed (we may call this 'the internal factor'). The second is the fact that the Union considers ensuring coherence a conditio sine qua non to its effectiveness on the international panorama ('the external factor')*», pp. 244-245.
[243] Per cui si rinvia sempre a S. OETER, *op. cit*., p. 870 ss.

paragrafo 5, prevede che "*nelle relazioni con il resto del mondo l'Unione afferma e promuove i suoi valori e interessi, contribuendo alla protezione dei suoi cittadini*".

Si è già detto delle ambiguità rispetto al riferimento ai valori negli articoli 2 e 3 TUE che sono ripresi dall'articolo 21 TUE come principi (come anche nel Preambolo della Carta dei diritti fondamentali) [244]; qui richiamiamo Cremona perché ci ricorda che detti valori assumono nella dimensione esterna una triplice rilevanza: nell'espressione dell'identità dell'Unione; nella loro promozione verso l'esterno; nella prospettiva di contributo alla "costruzione" di valori, anche influenzando la produzione di nuove norme a livello internazionale[245]. In tali tre accezioni, il ruolo dei valori nell'azione esterna viene riconosciuto dall'autrice «*both as characteristic of the Union's identity, and as the key to achieving specific Union objectives, especially security and stability within Europe and its neighbourhood*»[246]. Ebbene, proprio in considerazione di tale proiezione esterna, e dunque nell'ottica della suddetta coerenza tra azione interna ed esterna, un fondamentale passaggio ai nostri fini riguarda proprio la considerazione della *EU Rule of Law* in tale prospettiva: «*The transformation of the principle of "rule of law" from a criterion of homogeneity. to a fundamental value of the Union is a logical step insofar as the EU constitutes a "legal community" for which the respect of "rule of law" is of the utmost importance. Without rule of law at the MS level, the EU as a "legal community" could not function properly; but the Union cannot expect its members to respect the principles of "rule of law" without itself being based upon the same principles*»[247].

Questa citazione ci consente proprio di far emergere chiaramente il punto nevralgico, ossia la necessità di coerenza, che risulta abbastanza chiara in teoria ma spesso opinabile in pratica, tra tre aspetti: la pretesa di rispetto della *Rule of Law* da parte degli Stati membri, nonché l'esigenza di conformità alla *Rule of Law* da parte dei Paesi terzi che con l'Unione vogliano consolidare

[244] M. CREMONA, *Values in EU Foreign Policy*, in E. SCISO, R. BARATTA, C. MORVIDUCCI (a cura di), *I valori dell'Unione europea e l'azione esterna*, Torino, 2017, p. 8: «*Does this matter? A value may be defined as something which has intrinsic worth, which is esteemed for its own sake. Values can be seen as part of the cultural patrimony or common heritage of Europe, and thus creative of a sense of belonging. A principle is defined as a fundamental truth, a fundamental motive or reason for action, in particular one that is consciously recognised and followed. Perhaps the shift from values in Article 2 TEU to principles in Article 21 TEU signifies the shift from defining the Union's identity to setting out its policies and the actions. More specifically, the reference to "principles" in Article 21 is significant in terms of the potential of the provision in the hands of the Court of Justice. Principles, as we have seen from the Court's case law on general principles of law, are at least potentially justiciable, as well as offering a degree of flexibility and a recognition that different competing principles may need to be reconciled when engaging in concrete actions. In fact, both terms have been used within the EU in multiple senses: as a foundation for Union identity, as a basis for policy, as guiding practice or implementation of policy, and as a goal or objective for action*».

[245] Ibidem, p. 6, laddove l'autrice espone le tre prospettive: "*values and identity; promoting values; building values*", che poi esamina nel corso di tutto il Capitolo, pp. 7-32.

[246] Ibidem, p. 4.

[247] S. OETER, Article 21 TEU [The Principles and Objectives of the Union's External Action], in H.-J. BLANKE, S. MANGIAMELI (Eds), *The Treaty on European Union (TEU) – A Commentary*, Springer, 2013, pp. 845-846.

relazioni, da un lato; e, dall'altro, l'imprescindibilità di una effettiva declinazione di *Rule of Law* che l'Unione deve garantire in quanto tale, come presupposto per poter avanzare quelle pretese, e che abbiamo deciso (cfr. *supra*, Capitolo IV, Parte I) di riferire come *EU Rule of Law* dotata di proprie peculiarità. Il circuito triangolare delle relazioni tra questi tre aspetti auto-implicantisi dovrebbe emergere con maggiore chiarezza, quanto al settore della protezione dei dati personali, soprattutto dall'analisi pratica (*infra*, Parte IV). Nondimeno, qualche spunto di comprensione può derivare sin dalle seguenti considerazioni.

Il primo aspetto, in linea molto generale, richiama il fatto che le istituzioni dell'Unione, in particolare la Commissione e la Corte di giustizia, sono state ultimamente molto coinvolte dai recenti episodi di crisi dello Stato di diritto all'interno di diversi Stati membri, soprattutto riguardanti minacce all'indipendenza della magistratura e dunque alla garanzia di tutela giurisdizionale effettiva[248], con implicazioni anche relative all'applicabilità dello strumento della condizionalità rispetto ai fondi europei[249]; tali situazioni hanno portato ultimamente la Commissione, tra le altre cose, anche a perfezionare il monitoraggio della situazione all'interno degli Stati membri attraverso la già riferita *Relazione sullo Stato di Diritto 2020*, che non si limita a valutazioni strettamente legate al sistema giudiziario, ma tocca (tra i c.d. quattro pilastri) anche il quadro anticorruzione, il pluralismo dei media, nonché questioni istituzionali legate al sistema di bilanciamento dei poteri[250].

In coerenza con tali preoccupazioni rispetto alle situazioni interne agli Stati membri, l'Unione si preoccupa, ancorché con una differente gradualità, di valutare la conformità ai principi della *Rule of Law* da parte di soggetti "esterni" che con essa presentino punti di contatto: così è nell'ambito delle politiche di allargamento, dove ciò è richiesto da uno dei c.d. criteri di Copenaghen per poter aderire all'Unione europea; così nella conclusione di accordi internazionali (anche, ma non solo, attraverso la previsione della clausola sui diritti umani) da parte dell'Unione; così è nel settore PESC quanto all'adozione di misure restrittive da parte dell'Unione (in particolare, dal Consiglio), specie quando queste hanno un'incidenza diretta sui diritti fondamentali dei destinatari, come nel caso delle misure antiterrorismo[251], nonché in maniera ancor più evidente per quelle assunte per

[248] Si veda, ex multis, C. CINNIRELLA, "You cannot beat something with nothing": ossia la strategia della Corte di giustizia per tutelare l´indipendenza dei giudici nazionali (e lo Stato di diritto) nello spazio giuridico europeo, in *Il Diritto dell'Unione europea*, n. 2/2020, pp.

[249] Per cui si rinvia, *ex multis*, a M. FISICARO, Rule of Law Conditionality in EU Funds: the Value of Money in the Crisis of European Values, in *European Papers*, Vol. 4, 2019, No 3, pp. 695-722.

[250] Commissione europea Relazione sullo Stato di diritto 2020, disponibile qui:https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2020-rule-law-report_it .

[251] Rispetto alle quali sia consentito un riferimento a G. LO TAURO, Diritti fondamentali e misure antiterrorismo nell'Unione europea: intervalli melodici tra Consiglio e Corte di giustizia, cit., pp. 151-182.

consolidare e sostenere lo stato di diritto[252]. Rispetto a queste ultime, in particolare, il principio di coerenza è stato richiamato in maniera a noi funzionale: «Se nell'ambito dell'Unione si esige che quest'ultima rispetti lo stato di diritto, allo stesso modo, il principio di coerenza tra l'azione interna ed esterna dell'Unione impone che essa presti la sua assistenza alle autorità politiche degli Stati terzi, al fine di realizzare gli obiettivi della PESC, solo a condizione che sia rispettata la *rule of law* nei paesi interessati. È vero che nell'Unione il rispetto dell'indipendenza dei giudici nazionali è funzionale al buon funzionamento della cooperazione giudiziaria; così non è per le misure restrittive nell'ambito della PESC. Tuttavia, poiché le misure restrittive individuali limitano i diritti fondamentali, occorre che l'Unione sia certa che i giudici del Paese cui viene prestata assistenza siano indipendenti e agiscano liberi da interferenze politiche; in caso contrario, la credibilità dell'Unione, quando essa critica gli attacchi all'indipedenza dei giudici sul piano interno, risulterebbe pregiudicata»[253].

Queste considerazioni ci conducono così, chiaramente, a riconoscere che le pretese – sia dirette agli Stati membri che, pur rimodulate, verso gli Stati terzi – sono avanzate dall'Unione europea essenzialmente nella misura in cui *essa stessa* "rispetti lo stato di diritto", e dunque, o meglio, a conferma delle peculiarità della *EU rule of Law*, che pertanto impone la necessaria coerenza di quell'azione, da manifestarsi tanto nella sua dimensione interna (orizzontale e verticale) che esterna.

Orbene, la declinazione di una tale prospettiva teorica nello specifico settore della protezione dei dati personali trova la sua rispondenza nella giurisprudenza della Corte di giustizia, che molto spesso ha dato piena affermazione di questi assunti teorici cercando di plasmare sempre di più il processo di integrazione verso la persistente realizzazione di un'*Unione di diritto*.

Qualche cenno ad alcuni casi cardinali, specie della giurisprudenza meno recente, ci consentirà di individuare elementi (in senso affermativo o negativo) di coerenza, sia interna che esterna, emergenti nel settore della protezione dei dati personali e, così, di porre le basi per le valutazioni della prossima Parte sulle implicazioni pratiche quanto ai recenti sviluppi. Un buon punto di partenza, in tale prospettiva di analisi sulla coerenza, pare il richiamo a *Digital Rights Ireland* e *Schrems I*, ma anche al parere 1/15, che consentono di toccare gli aspetti sopra esposti, almeno con riguardo alla coerenza pretesa dalle istituzioni dell'Unione (e dunque, interna orizzontale ed esterna).

[252] Per una panoramica delle misure, anche assunte a tal fine, e per gli obiettivi specifici, tra cui anche la violazione di diritti umani, si rinvia alla pagina dedicata ai diversi tipi di sanzioni: https://www.consilium.europa.eu/it/policies/sanctions/different-types/

[253] S. POLI, L'evoluzione del controllo giurisdizionale sugli atti PESC intesi a consolidare la rule of law: il caso delle misure restrittive sullo sviamento di fondi pubblici, in *Il Diritto dell'Unione europea*, n. 2/2019, pp. 303-304.

La celeberrima e fortunata pronuncia sul caso *Digital Rights Ireland* rappresenta infatti, a nostro parere, un chiaro esempio di coerenza interna dell'azione dell'Unione. Com'è noto, si trattava di un rinvio pregiudiziale con cui la Corte veniva interrogata sulla validità della Direttiva 2006/24/CE, c.d. *data retention*, sulla conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica, rispetto agli articoli 7,8 e 11 della Carta dei diritti fondamentali. Ebbene, la Corte ha innanzitutto constatato l'esistenza di un'ingerenza nei diritti fondamentali di cui agli articoli 7 e 8 derivante dalle previsioni della direttiva[254]; quindi, per esaminare la giustificabilità di tali ingerenze, ha effettuato il necessario test di proporzionalità, ritenendo che il legislatore dell'Unione avesse «ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta»[255].

Dunque, quello che ci preme qui sottolineare in termini di rilievo rispetto alla coerenza dell'azione dell'Unione è che la Corte, invalidando la direttiva *data retention*, attraverso l'applicazione del test di proporzionalità sull'operato delle istituzioni dell'Unione, ha ribadito che le istituzioni dell'Unione sono in prima battuta chiamate al rispetto dei diritti previsti dalla Carta nell'esercizio delle loro funzioni, cosa che costituisce espressione della *EU Rule of Law* sia di per sé che in termini di controllo garantito in tal senso dalla Corte di giustizia.

Questa pronuncia, riguardando il delicato settore della *data retention*, viene di solito posta a fondamento di quel filone giurisprudenziale relativo specificamente all'ambito delle comunicazioni elettroniche, ossia coinvolgente la c.d. *direttiva e-privacy*, che propone essenzialmente il problema della possibilità per gli Stati membri, prevista da quella normativa, di imporre agli operatori privati

[254] Corte di giustizia, C-293/12, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a*. (di seguito: *DRI*), 8 aprile 2014: «Imponendo la conservazione dei dati elencati all'articolo 5, paragrafo 1, della direttiva 2006/24 e permettendo l'accesso delle autorità nazionali competenti a questi ultimi, la suddetta direttiva (…) deroga al regime di tutela del diritto al rispetto della vita privata, istituito dalle direttive 95/46 e 2002/58, con riferimento al trattamento dei dati personali nel settore delle comunicazioni elettroniche, in quanto le suddette direttive hanno previsto la riservatezza delle comunicazioni e dei dati relativi al traffico nonché l'obbligo di cancellare o di rendere anonimi i dati stessi quando non siano più necessari alla trasmissione di una comunicazione, a meno che non siano necessari per la fatturazione e solo fintanto che tale necessità perduri. (…) l'obbligo, imposto dagli articoli 3 e 6 della direttiva 2006/24 ai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione elettronica, di conservare per un certo periodo dati relativi alla vita privata di una persona e alle sue comunicazioni, come quelli previsti dall'articolo 5 della suddetta direttiva, costituisce di per sé un'ingerenza nei diritti garantiti dall'articolo 7 della Carta. Inoltre, l'accesso delle autorità nazionali competenti ai dati costituisce un'ingerenza supplementare in tale diritto fondamentale (…). Pertanto, anche gli articoli 4 e 8 della direttiva 2006/24, i quali prevedono regole relative all'accesso delle autorità nazionali competenti ai dati, sono costitutivi di un'ingerenza nei diritti garantiti dall'articolo 7 della Carta. Parimenti, la direttiva 2006/24 è costitutiva di un'ingerenza nel diritto fondamentale alla protezione dei dati personali garantito dall'articolo 8 della Carta, poiché prevede un trattamento dei dati personali. È giocoforza constatare che l'ingerenza che la direttiva 2006/24 comporta nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta si rivela essere (…) di vasta portata e va considerata particolarmente grave. Inoltre, il fatto che la conservazione dei dati e l'utilizzo ulteriore degli stessi siano effettuati senza che l'abbonato o l'utente registrato ne siano informati può ingenerare nelle persone interessate, come rilevato dall'avvocato generale ai paragrafi 52 e 72 delle sue conclusioni, la sensazione che la loro vita privata sia oggetto di costante sorveglianza»; pp. 32 e 34-37.

[255] Ibidem, p. 68. Per le valutazioni su proporzionalità, v. pp. 46-67.

un obbligo di conservazione dei dati relativi alle comunicazioni elettroniche per motivi di sicurezza. A partire dai famosi casi *Tele2 Sverige* e *Watson* sino ai più recenti *Privacy International* e *La Quadrature du Net* dell'ottobre 2020, per continuare ancora con il recentissimo rinvio pregiudiziale estone *H.K. v Prokuratuur* deciso lo scorso marzo 2021[256], la questione ha, sì, sempre riguardato la direttiva *e-privacy*, ma ogni volta in termini di rinvio pregiudiziale di interpretazione che si risolveva, in sostanza, nella constatazione che una normativa di uno Stato membro non fosse conforme alle disposizioni sovranazionali, specie lette alla luce della Carta dei diritti fondamentali. Ciò significa che in tutti questi, pur rilevanti, casi, ai quali si dedicherà ampia analisi (*infra*, Capitolo I, Parte IV), la coerenza si declina più in termini di "primo aspetto" (tra i tre che abbiamo esposto, dunque assimilabile a quelli relativi a episodi di crisi dello Stato di diritto negli ordinamenti di alcuni Stati membri), ossia di pretesa verso gli Stati membri di rispetto delle disposizioni sovranazionali, in linea con i diritti fondamentali, e dunque, nel caso specifico della previsione di sistemi di sicurezza particolarmente invasivi, anche di rispetto (in senso lato) dei principi dello Stato di diritto. E ciò assumerà rilievo, come emergerà dall'analisi pratica del principio di coerenza, nella valutazione della idoneità di sistemi di sorveglianza di diversi Stati membri rispetto alle previsioni del diritto sovranazionale.

Ebbene, rispetto a queste, la pronuncia *DRI* si distingue proprio perché, pur trattando sempre di *data retention*, rappresenta un monito (tra i primi) della Corte alle istituzioni dell'Unione, più che agli Stati membri, circa la necessità di rispettare i diritti sanciti dalla Carta, nonché dunque (indirettamente) i valori fondanti dell'Unione nell'esercizio delle loro funzioni (e dunque tocca ancor più direttamente l'essenza della *EU rule of law*).

Proprio queste considerazioni ci conducono poi a richiamare un esempio di coerenza nell'azione esterna, guardando alla già introdotta saga *Schrems*. Come si diceva, infatti, e tralasciando ancora altri aspetti, l'analisi del ruolo della Commissione nel settore della protezione dei dati, nella misura in cui si estrinseca come espressione della *EU rule of law*, richiama inevitabilmente questioni di coerenza dell'azione esterna: il riferimento è alla valutazione di adeguatezza che la Commissione, in particolare, ma (già chiaramente da *Schrems I* ma soprattutto con gli sviluppi di *Schrems II*) anche le autorità garanti (e finanche gli operatori privati), è chiamata ad effettuare per consentire un lecito trasferimento dei dati personali verso Paesi terzi ai sensi, ora, del GDPR. Ebbene, da quella giurisprudenza emerge chiaramente come la Corte, nell'esercitare il suo controllo tipicamente espressivo della *EU Rule of Law* sull'operato della Commissione, redarguisca per ben due volte

[256] Per cui si veda, *ex multis*, il recente commento a caldo di G. Formici, L'incerto futuro della data retention nell'Unione europea: osservazioni a partire dalla sentenza H.K. v Prokuratuur, in *SIDIblog*, 27 aprile 2021.

l'istituzione affinché, in coerenza con la configurazione di una "Unione di diritto"[257], garantisca, rispetto alla protezione prevista nell'ordinamento dell'Unione (dalla direttiva, prima, dal GDPR, poi, e comunque sempre dalla Carta dei diritti fondamentali) "*la continuità del livello elevato di tale protezione in caso di trasferimento di dati personali verso un paese terzo*"[258].

La necessità di una tale "continuità" del livello di tutela garantito nell'Unione è stata ribadita dalle recenti raccomandazioni dell'EDPB: "Nella recente sentenza C-311/18 (Schrems II) la Corte di giustizia dell'Unione europea (CGUE) ricorda che la protezione concessa ai dati personali nello Spazio economico europeo (SEE) *deve transitare con i dati ovunque essi siano trasferiti*. Il trasferimento di dati personali verso paesi terzi non può essere un mezzo per minare o indebolire la protezione che viene garantita nel SEE. La Corte afferma ciò chiarendo inoltre che il livello di protezione nei paesi terzi non deve necessariamente essere identico a quello garantito all'interno del SEE, ma *sostanzialmente equivalente*"[259]. Rinviando alla disamina del Capitolo successivo quanto al significato di "adeguatezza" o "sostanziale equivalenza", questo rilievo sulla necessaria continuità della tutela apprestata in Europa oltre "gli spazi" risulta particolarmente emblematico dell'atteggiarsi del principio di coerenza nel settore dei dati personali. A conferma di ciò può valere anche, in qualche modo, il rilievo fatto da qualcuno per cui proprio i casi richiamati rappresentano esempi di "*strategic litigation*", ossia «*litigation with a clear focus on law and policy reform in support of the right to privacy and data protection*»[260], e dunque come ulteriore appello – che deriverebbe sia da interventi privati che dalle istituzioni – verso una coerenza generale nella delicata tutela dei dati personali.

Un altro esempio di coerenza nell'azione esterna in tale settore, poi, deriva dal noto parere 1/15 con cui la Corte di giustizia ha interrotto l'accordo PNR con il Canada (sul trasferimento dei dati relativi al codice di prenotazione), rispetto al quale la Commissione aveva avviato i negoziati, seguiti dalla decisione di conclusione del Consiglio, che contestualmente ne chiedeva parere al Parlamento. Proprio il Parlamento ritenne di interpellare la Corte, la quale emise appunto parere negativo, sollecitando la modifica del testo perché ritenuto incompatibile con gli articoli 7 e 8 della Carta[261].

Ebbene, questi riferimenti, laddove ci consentono di delineare la rappresentazione teorica del generale principio di coerenza nel settore della protezione dei dati personali, specie prendendo in

[257] Corte di giustizia, *Schrems I*, cit., p. 60.
[258] Corte di giustizia, *Schrems I*, cit., p. 72; *Schrems II*, cit., p. 93.
[259] EDPB, Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, Adottate il 10 novembre 2020, p. 3, enfasi aggiunta.
[260] M. BRKAN, The Court of Justice of the EU, privacy and data protection, *cit.*, p. 25, ma si veda più ampiamente pp. 26-30.
[261] Corte di giustizia, Parere 1/15, 26 luglio 2017.

considerazione interventi della Corte di giustizia fortemente orientati in questa direzione, stimolano però anche qualche perplessità e dunque degli interrogativi circa l'effettiva possibilità di riscontrare (o continuare a riscontrare) una tale coerenza anche alla luce di recenti sviluppi. In particolare, quanto detto ha dimostrato l'espressione di una coerenza interna, che la Corte esige da parte delle istituzioni dell'Unione quando invalida una direttiva per incompatibilità con le previsioni di tutela (DRI); inoltre, ha dimostrato l'espressione di coerenza esterna, laddove, sempre rivolgendosi essenzialmente alle istituzioni, la Corte ribadisce l'importanza di un operato conforme anche quando esse agiscono verso l'esterno (e dunque: saga Schrems, per decisioni di adeguatezza su USA della Commissione; parere 1/15 per accordo PNR col Canada). Ma resta ancora da comprendere, e sarà oggetto di analisi nel prosieguo, come si atteggia effettivamente tale coerenza in situazioni rispetto alle quali l'interpretazione della normativa sovranazionale operata dalla Corte di giustizia risulta ostare a disposizioni normative nazionali, specie rispetto a sistemi di sorveglianza (per motivi di sicurezza), come testimoniato dalla sopra accennata casistica sulle comunicazioni elettroniche. In casi del genere (come anche, per esempio, nelle questioni che riguardano le implicazioni della Brexit sulla tutela dei dati personali e sui "nuovi" rapporti tra Regno Unito e Unione anche in tale settore), sino a che punto può considerarsi operante il principio di coerenza tra azione interna ed esterna quando da un lato si esige che Stati terzi prevedano garanzie "sufficientemente adeguate" di tutela dei dati che però, in maniera comprovata, non sono apprestate a livello nazionale dagli Stati membri? Può ravvisarsi una coerenza interna (in senso verticale) tra le previsioni sovranazionali e gli ordinamenti domestici?

Lasciamo qui aperto questo interrogativo, che ci consente così di chiudere la disamina teorica sul principio generale di coerenza tra azione interna ed esterna e costituisce, così, lo spunto di partenza per l'analisi pratica che si svolgerà nella Parte IV.

2. Il meccanismo di coerenza tra le autorità di controllo (e la Commissione)

Prima di chiudere questa densa parte di argomentazione teorica relativa all'estrinsecarsi dei principi della *EU Rule of Law* nel settore della protezione dei dati personali, un breve richiamo, come detto, va fatto all'altro aspetto specifico di coerenza che rileva in tale settore: il meccanismo di coerenza previsto dalla Sezione 2 del Capo VII del GPDR (articoli 63-67).

È noto che l'adozione del GDPR fosse chiaramente volta a "assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno" (cfr. Considerando 13 GDPR) e che dunque la necessità di coerenza in tale settore in tutta l'Unione fosse alla base dell'intero impianto di rinnovazione della disciplina. In maniera ancora più specifica, specie in virtù della rilevanza riconosciuta alle autorità nazionali di controllo e all'istituzione del Comitato europeo per la protezione dei dati, tale necessità trova compimento nelle previsioni del GPDR sul c.d. meccanismo di coerenza volto, assieme alle previsioni sulla cooperazione, a regolare le relazioni tra i diversi soggetti suddetti per un effettivo funzionamento del sistema di protezione dei dati in tutta l'Unione.

L'istituzione del meccanismo di coerenza, importante innovazione apportata dal GDPR, risponderebbe, secondo le previsioni dei Considerando, alla "cooperazione tra le autorità di controllo, al fine di assicurare un'applicazione coerente del presente regolamento in tutta l'Unione. Tale meccanismo dovrebbe applicarsi in particolare quando un'autorità di controllo intenda adottare una misura intesa a produrre effetti giuridici con riguardo ad attività di trattamento che incidono in modo sostanziale su un numero significativo di interessati in vari Stati membri. È opportuno che il meccanismo si attivi anche quando un'autorità di controllo interessata o la Commissione chiede che tale questione sia trattata nell'ambito del meccanismo di coerenza. Tale meccanismo non dovrebbe pregiudicare le misure che la Commissione può adottare nell'esercizio dei suoi poteri a norma dei trattati. In applicazione del meccanismo di coerenza il comitato dovrebbe emettere un parere entro un termine determinato, se i suoi membri lo decidono a maggioranza o se a richiederlo è un'autorità di controllo interessata o la Commissione. Il comitato dovrebbe altresì avere il potere di adottare decisioni giuridicamente vincolanti qualora insorgano controversie tra autorità di controllo. A tal fine, dovrebbe adottare, in linea di principio a maggioranza dei due terzi dei suoi membri, decisioni giuridicamente vincolanti in casi chiaramente determinati in cui vi siano pareri divergenti tra le autorità di controllo segnatamente nell'ambito del meccanismo di cooperazione tra l'autorità di controllo capofila e le autorità di controllo interessate sul merito del caso, in particolare sulla sussistenza di una violazione del presente regolamento"[262].

Queste previsioni assumono particolare rilievo, specie alla luce delle considerazioni sopra esposte circa la "rimodulazione" dell'intervento della Commissione e il rapporto tra questa e le autorità indipendenti, nonché il rapporto/controllo rispetto al Comitato europeo. Come si diceva, della coerenza si occupa la Sezione 2 del Capo dedicato, più in generale, a cooperazione e coerenza tra autorità nazionali, Comitato europeo e Commissione, e l'articolo 63, specificamente rubricato

[262] GDPR, Considerando 135 e 135.

"meccanismo di coerenza", lo descrive stabilendo infatti che "Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione". Gli articoli successivi prevedono poi: la previsione di un parere da parte del Comitato qualora un'autorità voglia adottare determinate misure (articolo 64); la composizione di controversie da parte del Comitato (articolo 65, rispetto a cui si segnala il primo esempio nella decisione 1/2020 adottata dall'EDPB il 9 novembre 2020)[263]; la procedura d'urgenza in casi eccezionali (articolo 66); le modalità, definite dalla Commissione, per lo scambio di informazioni tra autorità e tra queste e Comitato europeo (articolo 67). Nell'ambito dello stesso Capo, viene definito il meccanismo di cooperazione (articoli 60-62) che, insieme con quello di coerenza, come si è detto (*supra*, par. 2.1.), si realizza, rispetto ad ogni singolo caso, attraverso la distribuzione tra autorità di controllo capofila e altre autorità di controllo interessate (v. articoli 56 ss, nonché 60 GDPR).

Orbene, e senza addentrarci in approfondite analisi circa il funzionamento di tali meccanismi, due rilievi sorgono rispetto a tale tipo di prospettata coerenza.

Il primo è che, da una prospettiva squisitamente teorica, la previsione del meccanismo di coerenza costituisce, tra le innovazioni del GPDR, la più alta testimonianza dell'intenzione di realizzare un'armonizzazione quanto più compiuta rispetto agli interventi delle autorità garanti e dunque, in sostanza, tra il livello nazionale e quello sovranazionale, che viene così inteso quale unico sistema di gestione della protezione dei dati. In tal senso, dunque, esso rappresenta anche espressione del più generale principio di coerenza, come declinato nello specifico settore dalla *data protection*, e ciò appare comunque in linea anche con il "rimodulato" intervento della Commissione e con il rilievo riconosciuto al Comitato europeo, a completamento di un sistema che, con queste caratteristiche, potrebbe a ragione considerarsi rispondente alle peculiarità della *EU rule of law*.

Il secondo rilievo, tuttavia, riguarda l'effettività del funzionamento di simili previsioni. Il riferimento è alle difficoltà che si riscontrano, in pratica, proprio in considerazione di tali previsioni, quando per esempio la predisposizione di un'autorità capofila potrebbe rendere le cose più complicate invece che semplificarle e ottimizzarle, specie su questioni relative al trasferimento dei dati verso Paesi terzi. Il riferimento, in questo senso, è non solo e ancora una volta al caso *Schrems II* e, in particolare, ai suoi ulteriori sviluppi, ma anche, in particolare, al caso *Facebook* su cui si è espressa la Corte lo scorso giugno 2021 affrontando proprio le perplessità derivanti dal

[263] EDPB, Decisione 01/2020 relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente Twitter International Company ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD – Adottata il 9 novembre 2020, cfr. https://edpb.europa.eu/system/files/2021-04/edpb_bindingdecision01_2020_it.pdf .

funzionamento del meccanismo di sportello unico, cui si è fatto cenno e che si avrà modo di commentare (*infra*, Parte IV).

Con queste suggestioni sulle possibili incongruenze nella pratica rispetto alle prospettate previsioni teoriche, chiudiamo la trattazione di questa Parte e ci accingiamo finalmente all'analisi pratica sui punti di contatto tra *EU rule of Law* e protezione dei dati personali.

PARTE IV

Tutto probabilmente
segue
alla trasformazione delle coordinate
in cui si svolge da sempre
la nostra vita, personale e sociale:
il tempo e lo spazio.

R. Bin, Lo Stato di Diritto

PARTE IV

SOMMARIO: I. Il ruolo della Corte di giustizia nella protezione dei dati personali, tra tecnica decisionale e politica giurisprudenziale. – 1. Cenni introduttivi sul contributo della Corte di giustizia. – 2. Sull'ambito di applicazione della disciplina di protezione dei dati personali. – 2.1. Materiale. – 2.2. Territoriale. – 3. I casi su sicurezza nazionale degli Stati membri e (limiti alla) protezione dei dati personali. – II. Sul trasferimento di dati verso l'esterno. – 1. I riscontri pratici delle premesse teoriche. – 2. La cooperazione internazionale in materia di protezione dei dati personali. – 3. Lo strumentario per il trasferimento dei dati verso l'esterno: l'influenza unilaterale dell'Unione. – 4. Le decisioni di adeguatezza della Commissione. – 5. Sulle garanzie adeguate…e sulle deroghe. – III. Alcune riflessioni sui principi di protezione equivalente e coerenza nella protezione dei dati personali dell'Unione europea. – 1. Livello di protezione adeguato significa sostanzialmente equivalente? – 2. Cooperazione e coerenza tra le autorità di controllo, in pratica. – IV. *EU rule of Law* e protezione dei dati personali *in fieri*: Prospettive della sovranità digitale di un ordinamento autonomo. – 1. Sovranità e legittimazione. – 2. Tre aspetti da chiarire. – 3. La sovranità digitale come sfida dell'Unione europea.

CAPITOLO I

IL RUOLO DELLA CORTE DI GIUSTIZIA

NELLA PROTEZIONE DEI DATI PERSONALI,

TRA POLITICA GIURISPRUDENZIALE E TECNICA DECISIONALE

1. Cenni introduttivi sul contributo della Corte di giustizia

L'analisi sin qui condotta, ancorché prevalentemente teorica, rivelerebbe già la tendenza del processo di integrazione europea *verso una sovranità digitale*, in cui sarebbero coinvolte tutte le istituzioni che più o meno direttamente si iscrivono nel sistema di protezione dei dati personali. I loro interventi, dunque, concorrendo nel medesimo disegno politico, solo valutati insieme possono mostrare (o smentire) l'effettività pratica di quanto asserito in teoria.

Pur consapevoli della necessità di tale approccio onnicomprensivo, l'analisi che segue darà tuttavia particolare attenzione alla giurisprudenza della Corte di giustizia: sia perché ciò agevolerà la stessa comprensione degli altri interventi istituzionali; sia per la preminenza che l'istituzione giudiziaria

assume nell'affermazione della *EU Rule of Law*, tanto nel garantire il controllo sulle altre istituzioni sovranazionali, quanto nel ribadire le garanzie apprestate dal sistema europeo, sia generale che, di riflesso, specifico di protezione dei dati personali.

Peraltro, la risonanza dell'intervento della Corte in materia – completato dai necessari confronti con quello di Strasburgo – si avverte non solo sull'operato delle altre istituzioni, ma anche rispetto agli Stati membri nonché ai Paesi terzi e alle organizzazioni internazionali, come anche sui rilevanti soggetti privati che operano nel settore. Per questo, oltre l'analisi delle tecniche decisionali, vorremmo rintracciare le logiche di politica giurisprudenziale, al fine di mostrare in che misura e con quale impatto sia ravvisabile nell'operato della Corte di giustizia la tendenza verso la sovranità digitale dell'Unione europea. Al riguardo, possiamo anticipare che una recente e molto puntuale analisi della casistica lussemburghese in materia di *data protection* concludeva come segue: «*The current trends in case law of the Court reveal a Court committed to ensuring a wide scope of EU data protection law which is strict on the key principles and provisions of this law*»[1].

Forti delle precedenti esposizioni relative anche alla giurisprudenza sull'evoluzione della protezione dei dati come diritto fondamentale (Capitolo IV, Parte II), sulla rilevanza delle autorità di controllo e della Commissione per il sistema preposto (Capitolo II, Parte III) e sulla coerenza tra azione interna ed esterna per come prospettata teoricamente (Capitolo III, Parte III), è proprio dalle pronunce sull'ambito di applicazione della normativa dedicata che vogliamo cominciare l'analisi della casistica di Lussemburgo. Queste, oltre a rivelare finalmente la portata pratica di alcune riflessioni esposte in precedenza, costituiranno indispensabile premessa per l'analisi della più rilevante casistica sui sistemi di sorveglianza propri degli Stati membri e sul rapporto con la più specifica normativa sovranazionale in tema di comunicazioni elettroniche. A sua volta, tale ulteriore analisi sarà funzionale anche alla comprensione delle necessarie valutazioni richieste per il trasferimento di dati personali verso Paesi terzi. La disamina di tutti questi elementi ci consentirà, poi, di testare l'effettività del principio di coerenza dell'azione dell'Unione, sia nella dimensione interna che in rapporto a quella esterna.

Dunque, l'esame che immediatamente segue, relativo ai casi sull'ambito di applicazione della disciplina, ha una funzione strumentale, rispettivamente: alla comprensione dello spazio di manovra riservato agli Stati membri con riguardo ai sistemi di sicurezza nazionale (quanto all'ambito di applicazione materiale); alle dinamiche relative al trasferimento dei dati personali oltre i confini territoriali dell'Unione europea (quanto all'ambito di applicazione territoriale).

[1] C. DOCKSEY, H. HIJMANS, The Court of Justice as a Key Player in Privacy and Data protection: an Overview of the Recent Trends in Case Law at the Start of a New Era of Data Protection Law, in *European Data Protection Law Review*, n. 3/2019, p. 316.

2. Sull'ambito di applicazione della disciplina di protezione dei dati personali

2.1. *Materiale*

Com'è noto, l'ambito di applicazione materiale della disciplina sovranazionale sulla protezione dei dati personali viene definito oggi dall'articolo 2 GDPR[2], con una formula che riprende sostanzialmente quanto era previsto dall'articolo 3 della Direttiva madre, tenendo conto delle modifiche intercorse a livello di diritto primario. In tal senso, infatti, oltre a quelli di carattere esclusivamente personale o domestico (cfr. articolo 2, par. 2, lett. c, la cui individuazione non è però così scontata, come si evince dalla casistica dedicata, v. *infra*), sono esclusi dall'ambito di applicazione del GDPR anche i trattamenti effettuati "dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE" (cfr. articolo 2, par. 2 lett. b), così riprendendo la struttura a pilastri vigente ai tempi della Direttiva madre e comunque in conformità con le previsioni dei Trattati ai già analizzati articoli 16, par. 2, comma 2, TFUE e 39 TUE[3].

Viene ripresa altresì, e in maniera più argomentata, l'esclusione dei trattamenti "effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali (…)" (cfr. articolo 2, par. 2 lett. d), che, come si è detto, sono

[2] Articolo 2 – *Ambito di applicazione materiale*
1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.
2. Il presente regolamento non si applica ai trattamenti di dati personali:
a) effettuati per attività che e non rientrano nell'ambito di applicazione del diritto dell'Unione;
b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;
c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; (C18)
d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.
3. Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il regolamento (CE) n. 45/2001. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98.
4. Il presente regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.

[3] H. KRANENBORG, Article 2. Material Scope, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2020, pp. 64 e 70.

disciplinati dalla Direttiva 2016/680[4]. Quest'ultima, infatti, contiene una previsione contigua sull'ambito di applicazione (articolo 2, par. 2) ed esclude altresì i trattamenti effettuati in attività che fuoriescono dall'ambito di applicazione del diritto dell'Unione nonché quelli effettuati dalle istituzioni, organi e organismi dell'Unione (articolo 2, par. 3). Ma, come qualcuno ha notato, poiché l'ambito di applicazione specifico di tale Direttiva dipende essenzialmente dalle nozioni di "autorità competente" (definita all'articolo 3, par. 7) e di "reati" (non specificamente definita dalla Direttiva, se non per il riferimento del Considerando 13)[5], ne deriverebbe che «*to a certain extent, the precise delimitation between GDPR and LED depends on the law of the Member States. As follows from the recital 18 of the GDPR (and recital 11 LED) a single public authority can be subject to both the GDPR and the LED depending on the purposes of its activities*»[6].

Peraltro, è importante precisare che quanto a questo aspetto le previsioni in seno al Consiglio d'Europa differiscono. Infatti, com'è noto, la Convenzione 108 sin dagli albori (e con conferma nel Protocollo emendativo, cd. Convenzione 108+, articolo 3), riguarda tutti i trattamenti dei dati personali sia nel settore pubblico che privato, e dunque anche quello di polizia e giustizia penale. Nuovo, rispetto alla disposizione precedente, è invece il riferimento del paragrafo 3 ai trattamenti effettuati/ da istituzioni, organi e organismi dell'Unione, disciplinati da apposito regolamento (che, come si è detto, consiste ora nel c.d. EUDPR, ossia Regolamento 2018/1725).

Infine, non rientrano nel campo di applicazione del GDPR i trattamenti effettuati rispetto ad attività che fuoriescono dall'ambito di applicazione del diritto dell'Unione (art. 2, par. 2, lett. a). Questa ultima ipotesi di esclusione, esposta per prima dalla norma, è quella riferita – come precisa il Considerando 16 del GDPR – ad attività quali quelle "riguardanti la sicurezza nazionale", che tratteremo nel prosieguo (*infra*, par. 3). Anche rispetto a questi casi vi sarebbe difformità in Consiglio d'Europa, poiché l'art. 8 CEDU comprende anche le attività relative alla sicurezza nazionale che, come si vedrà, costituiscono un'importante porzione della giurisprudenza di Strasburgo.

È interessante notare come, con una formulazione molto più asciutta, la Direttiva madre raggruppava essenzialmente in due categorie (nei due "trattini" del par. 2 dell'articolo 3) i

[4] Ibidem: «*The DPD being an internal market instrument excluded it from its scope the area covered by the former second and third pillar of the Union. The new legal basis in principle allowed the Union to adopt a single set of rules potentially applying to the processing of personal data by competent authorities fir criminal investigation and also to the Union institutions and bodies. However, the European Commission, on the basis of Article 16 TFEU, decided to still propose a general regulation on data protection and a specific directive on data protection in the law enforcement sector*», p. 63, v. anche p. 70.

[5] Direttiva95/46/CE, Considerando 13.

[6] H. KRANENBORG, Article 2, *cit*., p. 70. Nello stesso senso, v. anche G. RUGANI, La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della Direttiva (UE) 2016/680: frammentazione ed incertezza applicative, in *Freedom, Security & Justice: European Legal Studies*, 2019, n. 1, p. 88.

trattamenti *esclusi* dal suo ambito di applicazione, che riportiamo di seguito perché costituiscono il punto di partenza della giurisprudenza dedicata della Corte di giustizia: "2. *Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali: – effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale; – effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico*". Dunque, nel "primo trattino" erano comprese tutte le ipotesi di attività *non* rientranti nella sfera di incidenza del diritto sovranazionale (dunque, insieme quelle del secondo e del terzo pilastro), e nel "secondo trattino" quelle riconducibili ad attività squisitamente *personali*. Con questo contesto di riferimento esporremo gli interventi giurisprudenziali.

Ebbene, si è già detto delle prime pronunce con cui la Corte è intervenuta a definire la portata dell'ambito di applicazione materiale della protezione dei dati personali, rispetto a questioni sollevate nella vigenza della direttiva madre (cfr. *supra*, Capitolo IV, Parte II). Ci riferiamo ai casi *ÖRF*, *Linqvist* e *Satamedia*, dai quali, oltre ai profili di rilievo già discussi, emergeva chiara la tendenza della Corte a fornire sin da subito un'interpretazione *ampia* dell'ambito di applicazione materiale della normativa sovranazionale sulla protezione dei dati personali.

In particolare, rispetto ai primi due casi, contrariamente all'illustrato approccio restrittivo dell'AG Tizzano, abbiamo visto che la Corte argomentò nel senso di un'ampia interpretazione dell'ambito di applicazione materiale della direttiva, tale dunque da ricomprendere sia i trattamenti di dati relativi ai redditi di dipendenti pubblici, come nel primo caso, che quelli effettuati nell'ambito di attività di tipo religioso o di volontariato, come nel secondo caso. La Corte stabiliva che tali tipi di trattamenti non rientrassero (come veniva proposto dalle rispettive parti) in nessuna delle due categorie di esclusione contemplate dalla normativa (art. 3, par. 2, direttiva) e che dunque la direttiva si applicasse ai trattamenti di dati coinvolti nelle cause principali[7]. Qualche anno dopo, nel caso *Satamedia*, la Corte tornava ad interpretare l'ambito di applicazione e confermava il suo approccio estensivo, ritenendo compresi nella normativa i trattamenti, effettuati da società private, di dati sul

[7] Corte di giustizia, cause riunite C-465/00, C-138/01 e C-139/01, *Rechnungshof c. Österreichischer Rundfunk e a. e Christa Neukomm e Joseph Lauermann c. Österreichischer Rundfunk*, sentenza del 20 maggio 2003, punti 45-47; causa C-101/01, *Bodil Lindqvist c. Åklagarkammaren i Jönköping*, sentenza del 6 novembre 2003, punti 42-48.

reddito ancorché estratti da documenti pubblici delle autorità tributarie e già pubblicati nei media, non operando neanche in questi casi le suddette esclusioni[8].

Tra le prime pronunce in materia, invero, è possibile rinvenire un caso, interessante sotto diversi profili, in cui la Corte effettivamente riconobbe sussistente un'ipotesi di *esclusione* dall'ambito di applicazione della direttiva madre. Si tratta della sentenza sui ricorsi di annullamento proposti dal Parlamento europeo avverso la decisione del Consiglio di conclusione dell'accordo PNR con gli Stati Uniti, nonché avverso la correlativa decisione di adeguatezza della Commissione. Il caso, apripista dei c.d. casi PNR (ossia riguardanti i c.d. *Passenger Name Records*, i dati relativi al codice di prenotazione acquisiti dai vettori aerei), verrà chiaramente ripreso con gli altri trattando di trasferimento dei dati verso Paesi terzi. Per quel che qui interessa, la questione sull'ambito di applicazione si pose con riguardo alla decisione di adeguatezza della Commissione: il Parlamento riteneva che essa fosse stata adottata in violazione dell'articolo 3, n. 2, primo trattino, della direttiva madre, che, come abbiamo visto, ne escludeva l'applicazione per le attività non rientranti nell'ambito del diritto comunitario, ritenendo che il trattamento dei dati PNR dopo il trasferimento, avvenuto in virtù della decisione di adeguatezza, verrebbe effettuato dalle autorità statunitensi per attività proprie dello Stato. La Commissione riteneva invece il trattamento dei dati PNR effettuato dai vettori aerei, operatori privati, all'interno del territorio comunitario e volto al trasferimento verso il Paese terzo.

Ebbene, la Corte, anche interpretando un Considerando della stessa decisione della Commissione che chiamava a fondamento del trasferimento dei dati PNR una legge degli Stati Uniti, riconobbe che esso effettivamente aveva ad oggetto la pubblica sicurezza e le attività dello Stato in materia di diritto penale. Pertanto, ancorché i dati PNR fossero raccolti da operatori privati per fini commerciali e da questi trasferiti verso Paesi terzi, un tale trasferimento rientrava in un ambito istituito dai poteri pubblici e relativo alla pubblica sicurezza, ponendo quindi la decisione della Commissione *al di fuori* dell'applicazione della direttiva madre (e comportandone, così, l'annullamento proprio per violazione dell'art. 3, n. 2, primo trattino)[9]. Riprenderemo valutazioni su pubblica sicurezza come ipotesi di esclusione della normativa quando esamineremo i casi relativi ai sistemi di sorveglianza nazionale degli Stati membri (*infra*, par. 3).

Ritornando, invece, alle ipotesi di esclusione di cui al "secondo trattino", ossia di trattamenti per finalità puramente personali o domestiche, dopo il caso *Linqvist* la Corte è tornata a precisare la

[8] Corte di giustizia, causa C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy e Satamedia Oy*, sentenza del 16 dicembre 2008, punti 38-49.
[9] Corte di giustizia, cause riunite C-317/04 e C-318/04, *Parlamento europeo c. Consiglio*, sentenza del 30 maggio 2006, punti 54-61.

portata della non scontata previsione, con il caso *Ryneš*. Si trattava di un rinvio pregiudiziale con cui il giudice ceco chiedeva proprio l'interpretazione di quella disposizione rispetto all'ipotesi del caso principale relativa all'utilizzo, da parte del signor *Ryneš*, di un sistema di videocamera installato nella sua abitazione che filmava continuamente, con immagazzinamento su disco duro, non solo la propria abitazione ma anche la strada pubblica e l'ingresso dell'abitazione di fronte. Ebbene la Corte, ribadendo il suo orientamento secondo cui deroghe e limiti alla tutela dei dati personali devono avvenire entro "*lo stresso necessario*", confermava che la deroga di cui all'articolo 3, par. 2, secondo trattino andasse intesa in senso restrittivo e chiariva dunque, nel caso di specie, che il sistema di videocamera «*che sorveglia parimenti lo spazio pubblico, non costituisce un trattamento dei dati effettuato per l'esercizio di attività a carattere esclusivamente personale o domestico, ai sensi di tale disposizione*»[10]. A tal riguardo è, quindi, stato notato: «*It follows from both* Lindquist *and* Rynes *that the exclusion of purely personal or household activities must be interpreted as covering only activities that are carried out in the context of the private or family life of individuals. In that connection, an activity cannot be regarded as being purely personal or domestic where its purpose is to make the data collected accessible to an unrestricted number of people or where that activity extends, even partially, to a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner*»[11].

Sulla stessa scia, quindi, più di recente (ancorché sempre con riguardo alle disposizioni della Direttiva e non del GDPR), nel caso relativo ai *Testimoni di Geova* finlandesi, con riguardo al trattamento dei dati da questi raccolti nell'ambito della loro attività di predicazione porta a porta, la Corte, pur interpretando l'articolo 3 della direttiva alla luce dell'articolo 10 della Carta dei diritti fondamentali (sulla libertà religiosa), ha confermato l'approccio *restrittivo* quanto alle esclusioni ivi previste e dunque quello *estensivo* dell'ambito di applicazione della normativa sulla protezione dei dati, che coprirebbe anche tali trattamenti: «*anche se l'attività di predicazione porta a porta dei membri di una comunità religiosa è tutelata dall'articolo 10, paragrafo 1, della Carta, in quanto espressione della fede del o dei predicatori, tale circostanza non ha l'effetto di conferire alla suddetta attività un carattere esclusivamente personale o domestico ai sensi dell'articolo 3, paragrafo 2, secondo trattino, della direttiva 95/46*»[12].

[10] Corte di giustizia, C-212/13, *František Ryneš c. Úřad pro ochranu osobních údajů*, sentenza del 11 dicembre 2014, punto 35, ma si vedano in generale i punti 26-35.
[11] H. KRANENBORG, Article 2, *cit.*, p. 68.
[12] Corte di giustizia, C-25/17, *Jehovan todistajat*, sentenza del 10 luglio 2018, punto 49, ma v. punti 34-51.
Per un commento della sentenza si indica S. LINDROOS-HOVINHEIMO, Who controls our data? The legal reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojavaltuutettu v Jehovan todistajat*, in *Information & Communications Technology Law*, Vol. 28, 2/2019, laddove, leggendo le due pronunce insieme, confermava l'approccio estensivo della Corte mantenuto anche dopo l'entrata in vigore del GDPR e, pur

Tale interpretazione restrittiva delle esclusioni di cui all'articolo 3 è stata poi ribadita (con particolare riguardo al "primo trattino") nel caso *Puškár*, sul trattamento di dati fiscali, in cui al riguardo la Corte stabiliva che: «*si evince dalla decisione di rinvio che i dati di cui trattasi sono raccolti e utilizzati ai fini della riscossione delle imposte e della lotta alla frode fiscale. Fatte salve le verifiche che devono essere compiute a tal riguardo dal giudice del rinvio, non risulta tuttavia che il trattamento di tali dati abbia ad oggetto la pubblica sicurezza, la difesa o la sicurezza dello Stato. Inoltre, anche se non appare escluso che tali dati possano essere utilizzati nell'ambito dell'azione penale esercitabile, in caso di violazione in materia tributaria, contro talune persone i cui nomi figurano nell'elenco controverso, i dati di cui al procedimento principale non risultano essere stati raccolti con lo scopo specifico di esercitare tale azione penale o nell'ambito di attività dello Stato in materia di diritto penale*»[13].Così la Corte riconosceva l'applicazione della direttiva anche a tali trattamenti. Peraltro, nel caso *Manni*, relativo a dati inseriti nel registro delle imprese che il signor Manni aveva chiesto alla Camera di Commercio di cancellare, la Corte intendeva come trattamento dei dati ai sensi della direttiva anche la trascrizione e conservazione di quelle informazioni nel registro per eventuale comunicazione a terzi, su richiesta, riconoscendo anche l'autorità incaricata della tenuta del registro come *responsabile* di quel trattamento[14]. Inoltre, una nozione ampia di "trattamento" si ravvisa anche nella Convenzione 108+, che all'articolo 2 ricomprende, tra le altre, anche la conservazione dei dati.

Ancora, a conferma di tale tendenza ad *ampliare* l'ambito di applicazione della normativa sulla protezione dei dati personali, vanno richiamati i casi (ancorché non riferiti all'articolo 3 della direttiva, bensì all'articolo 2) *Breyer* e *Nowak*. Entrambi riguardavano un rinvio pregiudiziale di interpretazione per chiarire la nozione di "dati personali": il primo sulla conservazione e registrazione dell'indirizzo IP del signor Brayer da parte delle autorità tedesche nei casi in cui lo stesso aveva consultato i siti internet dei servizi federali tedeschi; il secondo sulla possibilità del signor Nowak di accedere alla copia di una prova d'esame da lui svolta, negatagli dall'autorità garante irlandese che non considerava le informazioni ivi contenute come dati personali. Ebbene, in quest'ultimo caso i giudici affermavano: "*Come ha già constatato la Corte, l'ambito di applicazione della direttiva 95/46 è molto ampio e i dati personali a cui si riferisce sono vari (…). Infatti, l'uso dell'espressione «qualsiasi informazione» nell'ambito della definizione della nozione*

riconoscendo l'importanza dell'intervento definitorio, lamentava la mancanza di un più approfondito bilanciamento, sia con diritti fondamentali ulteriori rispetto alla protezione dei dati personali, sia rispetto all'altro obiettivo della normativa dedicata, ossia la libera circolazione dei dati.

[13] Corte di giustizia, C-73/16, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky*, sentenza del 27 dicembre 2017, punti 39-40.

[14] Corte di giustizia, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, sentenza del 9 marzo 2017, punti 35-36.

di «dati personali», di cui all'articolo 2, lettera a), della direttiva 95/46 riflette l'obiettivo del legislatore dell'Unione di attribuire un'accezione estesa a tale nozione, che non è limitata alle informazioni sensibili o di ordine privato, ma comprende potenzialmente ogni tipo di informazioni, tanto oggettive quanto soggettive, sotto forma di pareri o di valutazioni, a condizione che esse siano «concernenti» la persona interessata"[15], concludendo così per l'applicazione della direttiva poiché le risposte fornite da un candidato in sede d'esame costituiscono dati personali.

Peraltro, è stato rilevato da alcuni studiosi che nel caso di specie la Corte si sia chiaramente riferita, pur senza richiamarlo espressamente, al parere del Gruppo di Lavoro Articolo 29 "sul concetto di dati personali" applicando i "tre test" ivi suggeriti per determinare *quando* un'informazione sia "concernente una persona fisica"[16]: «*The CJEU applied the three tests developed in the opinion on the meaning of 'relates to' in the definition of personal data. These tests are alternative, not cumulative, and in fact they were all met in this case: the* content *of the exam script, which reflects the candidate's knowledge, and the handwriting sample can also provide information on a data subject; the* purpose, *which is to evaluate the candidate professionally, and the* effect, *which is access to a profession or a post*»[17].

Con la stessa tendenza, nel caso *Breyer* la Corte chiarì che «*un indirizzo IP dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone*»[18]. Questo caso, peraltro, è stato ritenuto rilevante al fine di evidenziare la tendenza della Corte verso la "anonimizzazione" e "pseudonimizzazione", che avrebbe dunque ispirato le correlate previsioni del

[15] Corte di giustizia, causa C-434/16, *Peter Nowak c. Data Protection Commissioner*, sentenza del 20 dicembre 2017, punti 33-34, enfasi aggiunta.
[16] ARTICOLO 29 GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI, Parere 4/2007 sul concetto di dati personali, adottato il 20 giugno 2007, 01248/07/IT WP 136, p. 10: «si potrebbe affermare che, per stabilire se i dati "concernono" una persona, dovrebbe ricorrere un elemento di "contenuto" OPPURE di "finalità" OPPURE di "risultato"».
[17] C. DOCKSEY, H. HIJMANS, The Court of Justice as a Key Player in Privacy and Data protection, *cit*., p. 303. Peraltro, gli autori aggiungevano sulla sentenza: «Nowak *may be seen as a partial correction to an eariler ruling in 2014 in* YS and Others*, where the legal analysis of an application for a residence permit contained in an administrative document preparatory to the decision was not considered to be part of the personal data of the applicant*».
[18] Corte di giustizia, causa C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland*, sentenza del 19 ottobre 2016, p. 49.

GDPR (in particolare, la definizione della seconda prevista all'articolo 4, n. 5, nonché la distinzione tra le due nel Considerando 26)[19].

A tal riguardo, va detto che, quanto all'anonimizzazione, è bene tenere in considerazione il parere 5/2014 del Gruppo Articolo 29 a ciò dedicato, che, ribadendo che essa punta alla perdita di identificazione in modo *irreversibile*, esamina le diverse tecniche possibili ma ne riconosce anche i limiti, richiedendo una più appropriata valutazione caso per caso[20]. Ai dati resi anonimi non si applicherà, ovviamente, la normativa sui dati personali. Quanto, poi, alla pseudonimizzazione, essa, ancorché non espressamente contemplata nella Convenzione 108+, viene riferita nella Relazione esplicativa, che distingue l'uso dello pseudonimo dall'anonimizzazione.

Dunque, dall'esposizione di questi casi, ancorché tutti riferiti alle disposizioni della direttiva madre, è possibile evincere il tendenziale orientamento della Corte verso un'interpretazione *estesa* dell'ambito di applicazione materiale quanto ai trattamenti di dati personali – come anche della nozione di "dato personale" – e quindi, in sostanza, della tutela apprestata dal diritto dell'Unione, riducendo allo "stretto necessario" le ipotesi di esclusione. Ciò sarà ancora più interessante da analizzare con riguardo ai casi in cui l'esclusione riguardi attività che si collocano al di fuori del diritto dell'Unione (art. 2, par. 2, primo trattino, Direttiva; art. 3, par. 2, lett. a, GDPR), da leggere peraltro anche in combinazione con le limitazioni espressamente consentite agli Stati membri, rispetto agli obblighi e ai diritti previsti dalla normativa, per specifiche ragioni (art. 13 Direttiva; art. 23 GDPR). Prima di analizzare queste complesse situazioni e le loro più generali implicazioni, in termini di *EU Rule of Law* e anche di effettività del principio di coerenza tra azione interna ed esterna, passiamo ad analizzare l'approccio della Corte rispetto al profilo *territoriale* dell'ambito di applicazione della protezione dei dati personali.

2.2. *Territoriale*

Premesse

[19] Così rilevano, infatti, C. DOCKSEY, H. HIJMANS, The Court of Justice as a Key Player in Privacy and Data protection, *cit*., p. 303. Il riferimento è al punto 46 della sentenza *Breyer*, che viene dagli autori così commentato: «*This is an important clarification of what may be accepted as 'anonymised' data, which falls outside the scope of the GDPR*».
Il GDPR espressamente incentiva la pseudonimizzazione sin dai Considerando 28 e 29.

[20] Gruppo di Lavoro Articolo 29, Parere n. 5/2014 Parere 05/2014 - WP 216, sulle tecniche di anonimizzazione, adottato il 10 aprile 2014.

La questione della portata extraterritoriale della normativa europea sulla protezione dei dati personali assume particolarissimo rilievo nel discorso che vuole verificare la tendenza verso una sovranità digitale dell'Unione europea. Assumendo come punto di partenza le prospettive teoriche cui si è fatto cenno (cfr. *supra*, Capitolo I, Parte III), si procederà quindi ad analizzare gli interventi della Corte di giustizia che hanno seguito e stimolato, a loro volta, le iniziative del legislatore sovranazionale.

Abbiamo visto che l'ambito di applicazione è definito ora dall'articolo 3 del GDPR, che abbiamo detto avere il proposito di far risaltare il GDPR a livello internazionale e che dunque in qualche modo esprime l'esigenza della riforma «*to expand the scope of application of the EU's data protection law. Such an expansion was argued to ensure a 'level playing-field' between businesses based in the EU and businesses based outside the EU, but doing business on the European market*»[21]. In questo senso

Peraltro, commentando le disposizioni dell'articolo 3, Svantesson utilmente suggerisce di leggerle alla luce dell'*Amicus brief* della Commissione europea sul caso *Microsoft Warrant* per cogliere meglio gli aspetti essenziali ai fini della loro migliore applicazione. In particolare, viene segnalata una parte, che è utile qui riportare (in forma più estesa) in quanto si ritiene estremamente importante non solo, effettivamente, rispetto a valutazioni sull'ambito di applicazione territoriale, ma anche per avallare i discorsi che si faranno nel prosieguo sul trasferimento di dati verso Paesi terzi: «*In the European Union's view, from the perspective of public international law, when a public authority requires a company established in its own jurisdiction to produce electronic data stored on a server in a foreign jurisdiction, the principles of territoriality and comity under public international law are engaged, and the interests and laws of that foreign jurisdiction must be taken into account. Any domestic law that creates cross-border obligations—whether enacted by the United States, the European Union, or another state—should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity. The European Union's foundational treaties and case law enshrine the principles of "mutual regard to the spheres of jurisdiction" of sovereign states and of the need to interpret and apply EU legislation in a manner that is consistent with international law*»[22].

[21] D.J.B. SVANTESSON, Article 3. Territorial scope, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020, p. 76.

[22] Amicus Brief of the European Commission on behalf of the EU as *Amicus Curiae* in support of neither party in *United States v Microsoft Corporation*, US 584 (2018), 7 December 2017, pp. 6-7, in cui continuava, in fine, per indicando i seguenti casi: «*See TEU arts. 3(5), 21(1); Case 52/69*, Geigy v. Commission, 11, ECLI:EU:C:1972:73; *Case C-366/10*, Air Transport Ass'n of America v. Sec'y of State for Energy and Climate Change, ¶ 123, ECLI:EU:C:2011:864».

Già da queste poche righe emergono interessanti spunti legati al principio di coerenza tra l'azione interna ed esterna e, più in generale, dei valori e principi che guidano l'azione esterna dell'Unione. Sul rapporto tra queste asserzioni della Commissione e l'articolo 3 del GDPR, Svantesson proponeva valutazioni che si condividono: «*this proclamation draws attention to the fact that a provision such as Article 3 is designed, not only to maximise the implementation of the policy goals pursued in the GDPR, but also to ensure the harmonious coexistence between different legal systems*»[23]. Ciò pare testimoniare l'estensione territoriale del diritto dell'Unione proposta dalla Scott (*supra*, Parte III), come caratterizzata da un "orientamento internazionale", che troverebbe quindi conferma nelle intenzioni della Commissione esposte alla Suprema Corte statunitense, e che sarà utile, pertanto, tenere a mente anche nell'analisi della giurisprudenza.

Ebbene, il c.d. *destination approach* prospettato dall'articolo 3 GDPR, e ancor più quello specifico aspetto di assoluta novità individuato nella c.d. *jurisdiction based on targeting* (cfr. *supra*, Parte III)[24], costituisce un cambiamento fondamentale rispetto al precedente assetto «*based mainly on the principle of territoriality and origin approach*»[25]. Questo era invero ravvisabile nell'articolo 4 della Direttiva madre[26], oggetto principale delle pronunce interpretative più rilevanti quanto alla portata (extra)territoriale della *data protection* europea la cui presentazione è quindi imprescindibile per comprenderne la sostituzione con l'articolo 3 GDPR.

In particolare, le Linee-guida dell'EDPB n. 3/2018 dedicate all'articolo 3 GDPR iniziano proprio chiarendo la fondamentale differenza tra la norma precedente e quella successiva: «mentre il principale obiettivo dell'articolo 4 della direttiva era definire quale diritto nazionale di uno Stato

[23] D.J.B. SVANTESSON, Article 3, *cit*., p. 77.
[24] In particolare, per questi termini e queste analisi v. P. DE HERT-M. CZERNIAWSKI, Expanding the European data protection scope beyond territory, *cit*., pp. 230, 231, 232 e 238.
[25] Ibidem, p. 230.
[26] Articolo 4
Diritto nazionale applicabile
1. Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali:
a) effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile;
b) il cui responsabile non è stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico;
c) il cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea.
2. Nella fattispecie di cui al paragrafo 1, lettera c), il responsabile del trattamento deve designare un rappresentante stabilito nel territorio di detto Stato membro, fatte salve le azioni che potrebbero essere promosse contro lo stesso responsabile del trattamento.

membro fosse applicabile, l'articolo 3 del RGPD definisce l'ambito di applicazione territoriale di un atto normativo direttamente applicabile»[27].

Vanno inoltre richiamate le disposizioni affini della Convenzione 108+ che, definendo l'ambito di applicazione al suddetto articolo 3, indicano che ogni parte dovrà applicarne le disposizioni "*to data processing subject to its jurisdiction*"[28]. Questa scelta costituisce un'innovazione rispetto al precedente riferimento dell'articolo 1 della Convenzione 108 al "territorio di ciascuna parte", producendo un ampliamento dell'ambito di applicazione della Convenzione, particolarmente significativo con riguardo ai discorsi relativi a spinte ed influenze reciproche se si pensa, come alcuni autori hanno notato, che i lavori di modernizzazione iniziarono molto prima delle rivoluzionarie sentenze della Corte di giustizia al riguardo[29] (che quindi, probabilmente, ne furono influenzate), che esamineremo a breve. Peraltro, viene notato che, in virtù del fatto che la normativa sulla protezione dei dati personali è essenzialmente basata sulla tutela dei diritti fondamentali, da un lato essa coinvolge l'ambito di operatività degli strumenti internazionali apprestati a tale tutela (quali l'articolo 13 CEDU) e, dall'altro, «*the fact that the application of the GDPR will impact the human rights of non-EU individuals is of great significance; it means that in assessing the human rights implications of the GDPR account must be taken of human rights law beyond Europe's human rights law*»[30].

Orbene, i casi che assumono rilievo con riguardo all'articolo 4 della Direttiva, e dunque alla portata dell'ambito di applicazione territoriale, non sono numerosi come quelli relativi alla portata materiale, ma hanno avuto un impatto dirompente, specie per le modifiche introdotte nel Regolamento rispetto alle previsioni della Direttiva. Si tratta fondamentalmente di: *Google Spain*, il già analizzato *Weltimmo, VKI c. Amazon* e *Wirtschaftsakademie*.

Google Spain

[27] EDPB, Linee-guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3), Versione 2.1 – 12 novembre 2019, p. 4.
[28] Convenzione n. 108 del 1981, cit.,disponibile qui: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
[29] . P. DE HERT, M. CZERNIAWSKI, Expanding the European data protection scope beyond territory, *cit*., p. 232, dove peraltro commentavano il nuovo approccio in questi termini: «*Such an approach allows for, and may indirectly encourage Convention 108's parties, to expand territorial scope of their national data protection laws beyond their territory*», denotando invero la mancanza di chiarimenti sul concetto di "giurisdizione" e richiamando come plausibile soluzione l'approccio della Corte di Strasburgo nell'interpretare estensivamente l'ambito di applicazione della CEDU oltre il territorio.
[30] D.J.B. SVANTESSON, Article 3, *cit*., p. 78.

Nel caso *Google Spain* la Corte veniva interpellata attraverso un rinvio pregiudiziale spagnolo nell'ambito di un giudizio tra le società Google Spain SL e Google Inc. e, dall'altro lato, l'*Agencia Española de Protección de Datos* (AEPD) e il signor Gonzalez, rispetto a un reclamo proposto da quest'ultimo all'AEPD per il fatto che, introducendo il suo nome e cognome nel motore di ricerca Google, risultavano link di pagine di un quotidiano concernenti l'annuncio di vendita all'asta di immobili dello stesso, relativa a un pignoramento risalente alla fine degli anni Novanta. Il signor Gonzalez richiedeva quindi che il quotidiano sopprimesse o modificasse quelle informazioni e che le società Google oscurassero o sopprimessero quei dati risalenti e ormai privi di riscontro nei suoi confronti. L'AEPD rigettava il reclamo quanto alla richiesta avverso il quotidiano e lo accoglieva rispetto alle società Google, che presentavano quindi dei ricorsi avverso la decisione dell'AEPD. Ebbene, il giudice spagnolo, trattando il ricorso, rilevava perplessità sugli obblighi incombenti ai gestori di motori di ricerca rispetto alla protezione dei dati di interessati con informazioni pubblicate su siti web, nonché localizzate e indicizzate e così ivi disponibili per un tempo indefinito. Per comprendere ciò, egli chiedeva alla Corte anzitutto lumi sull'ambito materiale e territoriale di applicazione della Direttiva, oltre, poi a delucidazioni sulla portata dei diritti derivanti agli interessati dalla stessa. Rispetto a queste ultime è emerso dalla giurisprudenza il celebre c.d. *diritto all'oblio*, che è stato poi codificato nell'articolo 17 del Regolamento e, più in generale, ha assunto particolare rilevanza a livello internazionale. Ai nostri fini, però, è fondamentale il chiarimento relativo *all'ambito territoriale* di applicazione della Direttiva.

Partendo dal Considerando 19 di quest'ultima, che prevedeva che "lo stabilimento nel territorio di uno Stato membro implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile" e che la forma giuridica non fosse rilevante al riguardo, la Corte interpretava l'articolo 4 stabilendo che: "(…) *l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 non esige che il trattamento di dati personali in questione venga effettuato «dallo» stesso stabilimento interessato, bensì soltanto che venga effettuato «nel contesto delle attività» di quest'ultimo*. (…) *Tenuto conto di tale obiettivo della direttiva 95/46 e del tenore letterale del suo articolo 4, paragrafo 1, lettera a), occorre affermare che il trattamento di dati personali realizzato per le esigenze di servizio di un motore di ricerca come Google Search, il quale venga gestito da un'impresa con sede in uno Stato terzo ma avente uno stabilimento in uno Stato membro, viene effettuato «nel contesto delle attività» di tale stabilimento qualora quest'ultimo sia destinato a garantire, in tale Stato membro, la promozione e la vendita degli spazi pubblicitari proposti dal suddetto motore di ricerca, che servono a rendere redditizio il servizio offerto da quest'ultimo*"[31]. In tal modo, la Corte ha esteso

[31] Corte di giustizia, C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, sentenza del 13 maggio 2014, punti 52 e 55. La Corte risolveva quindi questa questione come

per la prima volta la portata territoriale della Direttiva ben *oltre* il territorio dell'Unione, secondo quella che è stata intesa come componente esterna dell'ambito di applicazione della *data protection*[32], essenzialmente ponendo l'accento sul fatto che il trattamento, ancorché operato all'estero (nella specie, in California), rientrasse "nel contesto delle attività" dello stabilimento spagnolo. E questo è stato ritenuto il modo più lineare per assicurare una protezione effettiva[33].

Definita così la nozione di trattamento effettuato *nel contesto* delle attività di uno stabilimento in uno Stato membro, la necessità di ulteriori precisazioni quanto al diritto applicabile al trattamento dei dati e alla nozione di stabilimento è sorta nel caso *Weltimmo*.

Weltimmo

Abbiamo già avuto modo di analizzarlo con riguardo al ruolo delle autorità nazionali di controllo, mostrando che si trattava di una società registrata in Slovacchia ed operante in Ungheria (cfr. *supra* Capitolo II, Parte III). Ebbene, oltre ad assumere rilievo quanto all'individuazione dell'autorità di controllo competente, il caso risalta qui nella misura in cui coinvolgeva anche l'articolo 4, par. 1, lett. a) della Direttiva, questa volta nella sua "componente interna"[34], rispetto a cui l'AG Cruz Villálon spiegava: "*L'articolo 4, paragrafo 1, lettera a), svolge quindi una duplice funzione. Da un lato, consente l'applicazione del diritto dell'Unione attraverso il diritto di uno dei suoi Stati membri quando il trattamento dei dati abbia luogo esclusivamente «nel contesto» delle attività di uno stabilimento situato nel loro territorio, e ciò anche se il trattamento dei dati «in senso proprio» viene effettuato in un terzo Stato (come accadeva nella causa Google Spain e Google (7)). Dall'altro, detta disposizione opera come norma che determina la legge applicabile tra Stati membri (che è la questione ora in esame). In quest'ultima situazione, l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 è la disposizione che determina la legge applicabile in quanto norma di conflitto tra le leggi dei diversi Stati membri*"[35].

---

segue: «occorre rispondere alla prima questione, lettera a), dichiarando che l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 deve essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione suddetta, qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro», p. 60.

[32] C. DOCKSEY, H. HIJMANS, The Court of Justice as a Key Player in Privacy and Data protection, *cit*., p. 305 ss.

[33] Ibidem, p. 306: «*This is probably the most straightforward way of ensuring effective protection; giving a wide interpretation to the application of EU law to non-EU controllers with establishments in the EU avoids the application of more difficult concepts – also in term of enforcement – in order to attribute responsibilities to non-EU entities*».

[34] Ibidem.

[35] Conclusioni AG P. Cruz Villálon, C-230/14, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, presentate il 25 giugno 2015, punto 23.

Pertanto, anche sulla base di varie considerazioni dell'AG, la Corte confermava «(…) *una concezione flessibile della nozione di stabilimento, che si discosta dall'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata*. *Infatti, per determinare se una società, responsabile di un trattamento dei dati, dispone di uno stabilimento, ai sensi della direttiva, 95/46, in uno Stato membro diverso dallo Stato membro o dal paese terzo in cui è registrata, occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle prestazioni di servizi in questione. Ciò vale soprattutto per imprese che offrono servizi esclusivamente tramite Internet.* »[36]. Peraltro, in questo caso la Corte forniva la nozione di "stabilimento", affermando che "*(...) occorre considerare che la nozione di «stabilimento», ai sensi della direttiva 95/46, si estende a qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile"*[37], con una formulazione che verrà sempre richiamata successivamente. Dunque, la Corte ribadiva così l'ampiezza dell'ambito di applicazione territoriale prospettata in *Google Spain*, confermata quindi tanto nella componente interna che esterna. Peraltro, in entrambi i casi è stato riscontrato l'approccio interpretativo *teleologico* della Corte di giustizia, specie laddove prospettava la necessità di garantire una tutela efficace dei diritti fondamentali[38].

VKI c. Amazon

Nel successivo caso *VKI c. Amazon*, relativo a clausole abusive nei contratti stipulati con consumatori, per l'aspetto che qui interessa, il giudice del rinvio chiedeva lumi sull'interpretazione della stessa norma, nel senso di intendere il trattamento effettuato da un'impresa di commercio elettronico come regolato dal diritto dello Stato membro verso cui quella dirige le proprie attività. Ebbene, la Corte chiariva che: «*sebbene il fatto che l'impresa responsabile del trattamento dei dati non possieda né filiali né succursali in uno Stato membro non escluda che essa possa ivi possedere uno stabilimento ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva 95/46, un tale stabilimento non può esistere per il semplice fatto che ivi sia accessibile il sito Internet dell'impresa in questione. Occorre piuttosto valutare, come già rilevato dalla Corte, sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività nello Stato membro interessato (v., in tal*

[36] Corte di giustizia, C-230/14, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, presentate il 1 ottobre 2015, punti 29.
[37] Ibidem, punto 31.
[38] P. DE HERT-M. CZERNIAWSKI, Expanding the European data protection scope beyond territory, *cit.*: «*By applying this method legal provisions are not necessarily read literally but are understood in the light of the purpose, values, legal, social, and economic goals these provisions aim to achieve*», p. 234.

senso, sentenza del 1° ottobre 2015, Weltimmo, C-230/14, EU:C:2015:639, punto 29)»[39]. Dunque, una nozione di stabilimento ampia, ma non illimitata, per cui non è sufficiente che il sito dell'impresa sia accessibile nell'Unione, ma dovrà valutarsi in concreto se il trattamento avviene nel contesto delle attività dello stabilimento[40]. In questo senso, è stato notato che, pur confermando l'interpretazione data nelle precedenti pronunce, «*Amazon does not expand but by revisiting Weltimmo (at least by way of clarification) narrows down the scope of each national law to establishments that are certainly more than just the operation directed at a specific Member State via a generally accessible website*»[41].

Wirtschaftsakademie

L'approccio ampio è stato poi mantenuto, quanto alla componente interna, nel caso *Wirtschaftsakademie*, concernente una controversia tra tale società, specializzata in formazione, e l'autorità garante tedesca che chiedeva con un provvedimento di disattivare una *fanpage* dal social network Facebook. In tal caso la Corte ribadiva l'interpretazione estensiva del "contesto dell'attività di uno stabilimento" già proposta nelle precedenti pronunce, ai fini di una tutela efficace e completa dei diritti fondamentali, ribadendo che la scelta del diritto nazionale applicabile ai trattamenti di dati personali dipendesse dall'articolo 4, par. 1, lett. a)[42]. Pertanto, quanto a questo aspetto, la Corte deduceva nel caso di specie: « *dato che, da un lato, un social network, come Facebook, trae una parte considerevole delle sue entrate segnatamente dalla pubblicità diffusa sulle pagine web che gli utenti creano e a cui essi accedono e, dall'altro, che la filiale di Facebook ubicata in Germania è destinata a garantire, in tale Stato membro, la promozione e la vendita di spazi pubblicitari che servono a rendere redditizi i servizi offerti da Facebook, le attività di tale filiale devono essere ritenute inscindibilmente connesse al trattamento di dati personali del procedimento principale, di cui la Facebook Inc. è il responsabile assieme alla Facebook Ireland. Di conseguenza, un siffatto*

[39] Corte di giustizia, C-191/15, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, sentenza del 28 luglio 2016, punto 76.
[40] EDBP, Linee-guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3), cit., p. 7.
[41] M. D. COLE, Weltimmo Reloaded: CJEU Further Clarifies the Concept of Establishment, in *European Data Protection Law Review*, n. 3/2016, p. 379.
[42] Corte di giustizia, C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, sentenza del 5 giugno 2018, punti 56 e 51: «*La questione relativa a quale diritto nazionale si applichi ai trattamenti dei dati personali è disciplinata dall'articolo 4 della direttiva 95/46. Ai sensi del paragrafo 1, lettera a), di tale articolo ciascuno Stato membro applica le disposizioni nazionali che esso adotta per l'attuazione della presente direttiva al trattamento di dati personali effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio di tale Stato membro. Detta disposizione precisa che, qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile*», p. 51.

trattamento deve essere considerato come effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento, ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 (v., in tal senso, sentenza del 13 maggio 2014, Google Spain e Google, C-131/12, EU:C:2014:317, punti 55 e 56). Ne consegue che, poiché, ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva 95/46, il diritto tedesco era applicabile al trattamento dei dati personali di cui al procedimento principale, l'autorità di controllo tedesca era competente, conformemente all'articolo 28, paragrafo 1, di tale direttiva, ad applicare a detto trattamento la normativa tedesca»[43].

Così, dunque, veniva individuato il diritto tedesco come quello applicabile, confermando la tendenza della Corte (inaugurata con *Google Spain*) ad interpretare l'articolo 4 della Direttiva in maniera ampia per consentire una quanto più efficace tutela dei diritti fondamentali nel caso di trattamento di dati personali. È stato però notato al riguardo che, proprio perché queste pronunce erano riferite esclusivamente alla Direttiva, che non prevedeva i meccanismi di garanzia ora introdotti dal GDPR, l'orientamento della Corte fosse particolarmente volto ad assicurare la più elevata ed efficace tutela degli interessati: «*It should be noted that the CJEU decided* Wirtschaftsakademie *and* Weltimmo *in the context of Directive 95/46, where there was no one-stop shop or consistency mechanism, and the Court's broad approach to the concept of controller and territorial scope was intended to ensure the highest and most effective protection of data subjects. Now the GDP has specifically introduced the one-stop shop and the consistency mechanism as a means of increasing the level of effective protection. So the CJEU can be expected to take this legislative intention into account and to be wary of undermining the effective application of these mechanisms, especially if the effectiveness of protection of individuals is reduced thereby*»[44].

Ebbene, questo orientamento giurisprudenziale teso ad ampliare la portata territoriale della normativa sulla protezione dei dati personali ha influenzato in maniera preponderante il legislatore sovranazionale, come testimoniato dalle disposizioni dell'articolo 3 del GDPR: «*the GDPR*

[43] Ibidem, punti 60-61. La Corte quindi concludeva su questo aspetto come segue: «*Tenuto conto di quanto precede, si deve rispondere alla terza e alla quarta questione dichiarando che gli articoli 4 e 28 della direttiva 95/46 devono essere interpretati nel senso che, qualora un'impresa stabilita al di fuori dell'Unione disponga di varie filiali in diversi Stati membri, l'autorità di controllo di uno Stato membro è autorizzata a esercitare i poteri che le conferisce l'articolo 28, paragrafo 3, di tale direttiva nei confronti di una filiale di detta impresa situata nel territorio di tale Stato membro anche se, in base alla ripartizione delle funzioni all'interno del gruppo, da un lato, tale filiale è competente solamente per la vendita di spazi pubblicitari e per altre attività di marketing sul territorio di detto Stato membro e, dall'altro, la responsabilità esclusiva per la raccolta e per il trattamento dei dati personali grava, per l'intero territorio dell'Unione, su una filiale situata in un altro Stato membro*», p. 64.

[44] C. DOCKSEY, H. HIJMANS, The Court of Justice as a Key Player in Privacy and Data protection, *cit*., p. 307.

continued the trend, first made explicit in Google Spain, of expanding the territorial scope of EU data protection law to have effects beyond the borders of the EU»[45].

Tuttavia, se è vero che *Google Spain* inaugurava questo approccio estensivo, è anche vero che in quella pronuncia la Corte lasciava alcuni nervi scoperti. Tre punti, in particolare, sono stati individuati come irrisolti, tutti rilevanti ai nostri fini: «*Rule of Law and Transparency of the procedure; since the actual application and decision on the application is practically left to Google or the Search Engine Operator (SEO). Rights of the parties affected; since the publisher of the content is not being heard in the process. Territorial scope of application*»[46]. I primi due possono ricondursi alle riflessioni più generali che verranno fatte anche nel prosieguo.

Occorre qui sul terzo focalizzare l'attenzione: la Corte, infatti non precisava l'effettiva portata geografica della deindicizzazione, lasciando aperti dei dubbi che poco dopo mobilitavano diverse parti a rintracciare possibili soluzioni. In particolare, il Gruppo di Lavoro Articolo 29 stabiliva nelle sue Linee Guida sull'attuazione della sentenza: «*(…) limitare la deindicizzazione ai domini UE per il fatto che gli utenti tendono ad accedere ai motori di ricerca a partire dai rispettivi domini nazionali non è da ritenersi sufficiente a garantire adeguatamente i diritti degli interessati nel senso precisato dalla sentenza. Ciò significa, in sostanza, che la deindicizzazione deve operare in ogni caso su tutti i domini pertinenti, compreso .com*»[47]. Gli stessi dubbi venivano affrontati anche, dall'altro lato, dall'*Advisory Council* di Google che al riguardo si pronunciava così: «*The Council supports effective measures to protect the rights of data subjects. Given concerns of proportionality and practical effectiveness, it concludes that removal from nationally directed versions of Google's search services within the EU is the appropriate means to implement the Ruling at this stage*»[48].

Ebbene, la questione si (ri)propose apertamente alla Corte di giustizia con il celebre caso *Google c. CNIL*, che rappresenta la più diretta prosecuzione di *Google Spain* e che assume quindi fondamentale rilievo quanto alla componente esterna dell'ambito di applicazione territoriale. Anche in tal caso, invero, il giudice di rinvio interrogava la Corte sull'interpretazione della Direttiva.

[45] J. QUINN, *Google v CNIL*: Circumscribing the Extraterritorial Eff ect of EU Data Protection Law, in F. FABBRINI, E. CELESTE, J. QUINN (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford, 2020, p. 52.
[46] O. J. GSTREIN, The Judgment That Will Be Forgotten. How the ECJ Missed an Opportunity in Google vs CNIL (C-507/17), in *Verfassunsblog*, 25 settembre 2019.
[47] Gruppo di Lavoro Articolo 29, Linee Guida sull'attuazione della sentenza della Corte di giustizia dell'Unione europea nel caso C-131/12 "Google Spain e Inc. contro Agencia Espanola de la Proteccion de datos (AEPD) e Mario Costeja Gonzalez", WP 225, adottate il 26 novembre 2014, p. 2.
[48] The Advisory Council to Google on the Right to be Forgotten, 6 February 2015, p. 20, disponibile qui: https://static.googleusercontent.com/media/ archive.google.com/it//advisorycouncil/ advisement/advisory-report.pdf.

Tuttavia, poiché quest'ultima, nel periodo tra la domanda pregiudiziale e la pronuncia, venne abrogata dal Regolamento, la Corte esaminò le questioni alla luce di entrambe le normative[49].

Google c. CNIL

Si trattava di un rinvio pregiudiziale scaturito nell'ambito di una controversia tra Google LLC, succeduta alla Google Inc., e l'autorità garante francese che aveva irrogato una sanzione nei confronti della prima per aver rifiutato, accogliendo parzialmente una domanda di deindicizzazione, di applicarla su tutte le estensioni del nome di dominio del suo motore di ricerca. La faccenda riguardava, insomma, la portata territoriale del diritto all'oblio.

La questione dall'ambito territoriale della normativa sulla protezione dei dati (in particolare, del vigente GDPR) ancora una volta implicava la portata della tutela da apprestare agli interessati: riconoscere un ambito di applicazione esteso a tutti i nomi di dominio (dunque, in sostanza, globalmente), per garantire la più effettiva tutela del diritto all'oblio ed evitare il rischio che venisse aggirata. Seguendo l'approccio "pragmatico" suggerito dall'AG Szpunar[50], con la sua pronuncia la Corte ha definito i confini geografici del diritto all'oblio da essa stessa elaborato, escludendone (almeno, in linea generale) la globalità e limitandone quindi la portata territoriale alle sole versioni del motore di ricerca corrispondenti a tutti gli Stati membri.

Si riportano i punti salienti del ragionamento seguito dalla Corte: «*(...) l'obiettivo della direttiva e del regolamento suddetti è quello di garantire un elevato livello di protezione dei dati personali in tutta l'Unione. È vero che una deindicizzazione effettuata su tutte le versioni di un motore di ricerca è idonea a soddisfare pienamente tale obiettivo. (...) Occorre, tuttavia, sottolineare che molti Stati terzi non riconoscono il diritto alla deindicizzazione o comunque adottano un approccio diverso per tale diritto. Inoltre, il diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità (...). A ciò si aggiunge che l'equilibrio tra il diritto al rispetto della vita privata e alla protezione dei dati personali, da un lato, e la libertà di informazione degli utenti di Internet, dall'altro, può variare notevolmente nel mondo. (...) pur se il*

[49] Corte di giustizia, C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, sentenza del 24 settembre 2019, punti 40-41.

[50] Così veniva definito da DOCKSEY, H. HIJMANS, The Court of Justice as a Key Player in Privacy and Data protection, *cit*., p. 306: «*Advocate General Szpunar has proposed a pragmatic solution: de-referencing should have effect within the EU, not across the whole world, but the search engine operator should use geoblocking techniques to prevent persons in the EU from using technology to circumvent the de-referencing. This pragmatic solution is also based on a practical consideration: if the EU were to require worldwide de-referencing, other – less democratic – jurisdictions could require the same, possibly leading to censorship on the internet*».

legislatore dell'Unione, nell'articolo 17, paragrafo 3, lettera a), del regolamento 2016/679, ha effettuato un bilanciamento tra tale diritto e tale libertà per quanto concerne l'Unione […], si deve necessariamente constatare che, d'altro lato, esso non ha, allo stato attuale, proceduto a tale bilanciamento per quanto riguarda la portata di una deindicizzazione al di fuori dell'Unione. In particolare, dal tenore letterale delle disposizioni dell'articolo 12, lettera b), e dell'articolo 14, primo comma, lettera a), della direttiva 95/46 o dell'articolo 17 del regolamento 2016/679 non risulta affatto che il legislatore dell'Unione abbia scelto (…) di attribuire ai diritti sanciti da tali disposizioni una portata che vada oltre il territorio degli Stati membri e che abbia inteso imporre a un operatore che, come Google, rientra nell'ambito di applicazione della direttiva o del regolamento suddetti, un obbligo di deindicizzazione riguardante anche le versioni nazionali del suo motore di ricerca che non corrispondono agli Stati membri. Inoltre (…) si deve necessariamente rilevare che il diritto dell'Unione non prevede attualmente strumenti e meccanismi di cooperazione siffatti per quanto riguarda la portata di una deindicizzazione al di fuori dell'Unione. Ne consegue che, allo stato attuale, non sussiste, per il gestore di un motore di ricerca che accoglie una richiesta di deindicizzazione presentata dall'interessato, eventualmente, a seguito di un'ingiunzione di un'autorità di controllo o di un'autorità giudiziaria di uno Stato membro, un obbligo, derivante dal diritto dell'Unione, di effettuare tale deindicizzazione su tutte le versioni del suo motore»[51]. La Corte aggiungeva poi: «*È compito, inoltre, del gestore del motore di ricerca adottare, se necessario, misure sufficientemente efficaci per garantire una tutela effettiva dei diritti fondamentali della persona interessata. Tali misure devono soddisfare tutte le esigenze giuridiche e avere l'effetto di impedire agli utenti di Internet negli Stati membri di avere accesso ai link in questione a partire da una ricerca effettuata sulla base del nome di tale persona o, perlomeno, di scoraggiare seriamente tali utenti (…)*»[52]. Sarebbe, insomma, il riferimento al meccanismo, indicato anche dall'AG Szpunar, di c.d. blocco geografico[53].

[51] Corte di giustizia, C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, sentenza del 24 settembre 2019, punti 54-55 e 59-65, sottolineato aggiunto.

:[52] Ibidem, punto 70, sottolineato aggiunto.

[53] Conclusioni AG M. Szpunar, C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, depositate il 10 gennaio 2019, punto 78: "*Pertanto, propongo di rispondere alla seconda e alla terza questione pregiudiziale dichiarando che il gestore di un motore di ricerca è tenuto a sopprimere i link controversi che appaiono in esito a una ricerca effettuata, a partire dal nome del richiedente, da un luogo situato all'interno dell'Unione europea. In tale contesto, detto gestore è tenuto ad adottare tutte le misure a sua disposizione per garantire una cancellazione efficace e completa. Ciò include, in particolare, la tecnica detta del «blocco geografico» da un indirizzo IP che si ritiene localizzato in uno degli Stati membri assoggettato alla direttiva 95/46, e ciò indipendentemente dal nome di dominio utilizzato dall'utente di Internet che effettua la ricerca*".

Invero, qualche commentatore faceva notare, a pochi mesi dalla pronuncia, che tale "blocco geografico" fosse effettivamente utile a garantire la deindicizzazione «nonostante il regolamento UE 2018/302 – che ne ha vietato l'impiego finalizzato a impedire l'accesso a tutte le versioni nazionali di siti Internet a prescindere dalla collocazione geografica dell'IP in un determinato Stato membro, dalla nazionalità, dal luogo di residenza o stabilimento degli utenti – ne abbia recentemente ridimensionato l'utilizzabilità», cfr. E. ROSSI, Forget me…or not? La Corte di giustizia torna

Infine, la Corte puntualmente precisava: «*Occorre infine sottolineare che il diritto dell'Unione, pur se – come rilevato al punto 64 della presente sentenza – non impone, allo stato attuale, che la deindicizzazione accolta verta su tutte le versioni del motore di ricerca in questione, neppure lo vieta. Pertanto, un'autorità di controllo o un'autorità giudiziaria di uno Stato membro resta competente ad effettuare, conformemente agli standard nazionali di protezione dei diritti fondamentali (...), un bilanciamento tra, da un lato, il diritto della persona interessata alla tutela della sua vita privata e alla protezione dei suoi dati personali e, dall'altro, il diritto alla libertà d'informazione e, al termine di tale bilanciamento, richiedere, se del caso, al gestore di tale motore di ricerca di effettuare una deindicizzazione su tutte le versioni di suddetto motore*»[54].

Ebbene, da questi estratti emerge l'essenza dello stato dell'arte sulla portata territoriale della protezione dei dati personali e, quindi, sul ruolo della Corte di giustizia nel manovrare gli snodi del processo di integrazione europea verso una sovranità digitale. Andiamo con ordine.

Com'è evidente, la prima impressione è quella di un ridimensionamento della portata territoriale, e dunque quasi di un *revirement* rispetto all'orientamento che aveva caratterizzato la giurisprudenza audace a partire da *Google Spain*, intesa generalmente (ossia, non solo con riguardo all'ambito territoriale) "dato-centrica"[55], laddove la Corte si mostrava (non senza suscitare critiche) particolarmente sensibile alla tutela dei dati personali come diritto fondamentale spesse volte prevalente nel bilanciamento con altri. Intesa in questo senso, la pronuncia è stata oggetto di forti attacchi, sotto diversi aspetti, tra cui per esempio la definizione della portata sostanziale del diritto all'oblio o il bilanciamento con il diritto di accesso alle informazioni[56]. Ma, in particolare ai nostri fini, tali attacchi hanno riguardato l'estensione territoriale, con commenti anche di autorità nazionali di controllo, quale quella italiana che rilevava come "la barriera territoriale appare sempre più

sul diritto di farsi dimenticare. Prima lettura di due recenti pronunce sul «diritto all'oblio», in *SIDIBlog*, 25 novembre 2019.

[54] Ibidem, punto 72, sottolineato aggiunto.

[55] Così la definisce O. POLLICINO, L' "autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale, in *federalismi.it*, n. 19/2019, p. 6.

[56] O. J. GSTREIN, The Judgment That Will Be Forgotten – How the ECJ Missed an Opportunity in Google vs CNIL (C-507/17), in *Verfassungsblog*, 25 September 2019, laddove, per esempio, quanto a questo preciso aspetto notava: «*Completely missing the point and denying its mandate in Article 19 paragraph 1 sentence 2 TEU as well as the existence of a fully harmonized data protection law in the EU in 2019, the ECJ does not even attempt to define what 'necessity' and 'proportionality' mean for the RTBF as entailed in the GDPR, recapping the (obvious) need for balancing. Again, it remains unclear how delisting is in detail enshrined in the GDPR* (…)». Inoltre, con riguardo al punto 70 della sentenza (relativo ai doveri del motore di ricerca, v. *supra*), l'autore commentava condivisibilmente: «*Hence, the problematic aspects threatening the rule of law and democratic control of digital space are neither resolved, nor addressed by this judgment, which is worrying since the digital domain is already heavily influenced by the forces of 'surveillance capitalism'*».

anacronistica"[57], oltre che ovviamente in dottrina: «*The Court does not only open the door to fragmentation in European data protection law but also fails to further develop the protection of individual rights in the digital age*»[58].

Eppure, a fronte delle perplessità che la sentenza parrebbe mantenere aperte, un chiarimento rispetto alla portata territoriale sarebbe invero ravvisabile: «*What* Google v CNIL does *make clear is that the general rule is that a standard dereferencing request is limited to the EU domains of the search engine, plus necessary additional techniques such as geoblocking. A global dereferencing is still* possible *but only as an exception where the relevant EU authority believes that the threat to the data subject' s rights to privacy outweighs concerns for access to information*»[59]. Quest'ultimo passaggio (che si riferisce al punto 72 della sentenza, v. *supra*) ha suscitato maggiori perplessità, per l'indeterminatezza del margine lasciato aperto, prestandosi a interpretazioni e commenti di tendenze contrapposte e variegate: da chi lo ha considerato "eccessivo"[60], a chi auspicava ulteriori interventi della Corte per chiarire le incertezze al riguardo[61] o a chi, sulla stessa scia, ribadiva che la grande domanda lasciata aperta fosse proprio "*what set of facts are necessary for the CJEU to make a global dereferencing order"*[62]; da chi lamentava addirittura l'attribuzione alle autorità di controllo e giudiziarie nazionali di discrezionalità sulla portata della deidicizzazione, come una scelta "contro lo spirito del GDPR" poiché in contrasto con i risultati di armonizzazione in materia di *data protection*[63], a chi, da un'altra (e interessante) prospettiva, invece ravvisava in ciò un orientamento a favore dei poteri pubblici rispetto a quelli privati, particolarmente incidenti nel settore[64].

---

[57] Diritto all'oblio: Antonello Soro, Garante privacy, su sentenza Google della Corte di Giustizia Ue, 24/09/2019, disponibile qui: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9145764 . Si veda anche: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9147231 .

[58] Ibidem.

[59] J. QUINN, *Google v CNIL*: Circumscribing the Extraterritorial Effect of EU Data Protection Law, in F. FABBRINI, E. CELESTE, J. QUINN (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford, 2020, p. 57.

[60] Così E. ROSSI, Forget me…or not?, *cit.*: «Ai titolari del trattamento che devono stabilire quando accogliere le richieste di deindicizzazione degli interessati, così come alle autorità nazionali di controllo che devono stabilire se ordinare o meno ai titolari la deindicizzazione, sembra, insomma, essere stato lasciato, anche nella scelta concreta delle misure tecniche da adottare, un eccessivo margine di discrezionalità nelle valutazioni sul bilanciamento delle esigenze in gioco e, conseguentemente, sulla congruità della deindicizzazione.».

[61] Cfr. M. SAMONTE, Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law, in *European Law Blog*, 29 October 2019, laddove a caldo rilevava proprio incertezze quanto alle condizioni in presenza delle quali le autorità di controllo potrebbero estendere la portata territoriale della deindicizzazione su tutte le versioni del motore di ricerca.

[62] J. QUINN, *Google v CNIL*: Circumscribing the Extraterritorial Effect of EU Data Protection Law, *cit.*, p. 62, che continuava, concludendo: «*If a data protection authority encounters a set of facts upon which it views the threat to a data subject ' s privacy rights as suffi ciently serious to request a search engine to dereference the information globally, many of these arguments will need to be revisited*».

[63] Così O. J. GSTREIN, The Judgment That Will Be Forgotten, *cit.*, laddove, proprio con riguardo a quel punto della pronuncia, affermava: «*(…) paragraph 72 is a sin against the spirit of European integration since it denies much which has been achieved in the harmonization of the EU data protection framework over the past decades. Rendering its own preceding elaborations practically meaningless, the ECJ states that national authorities might 'in the light of national*

Invero, molti di questi (e non solo) commentatori hanno affrontato le loro analisi attraverso il (potrebbe dirsi, inevitabile) parallelo con un altro caso su cui la Corte si era pronunciata qualche giorno dopo, ossia il noto *Eva Glawischnig-Piesczek c. Facebook*. Il caso riguardava, invero, tutt'altra normativa, in particolare la c.d. direttiva *e-commerce* (n. 2000/31/CE), e tutt'altro contesto, trattandosi della rimozione di contenuti *illeciti* dal social network *Facebook*. L'aspetto che avvicina il caso a *Google c. CNIL* sta nella *portata territoriale* di tale, pur diverso, obbligo di rimozione.

Invero, e anche al fine di comprendere meglio le analisi comparatistiche svolte al riguardo, ci pare non di poco conto riconoscere rilievo al fatto che, mentre la composizione collegiale della Corte (oltre che, quindi, il giudice relatore) era diversa nei due casi, entrambi sono trattati dallo stesso Avvocato Generale Szpunar. Questo è, a nostro avviso, l'elemento che più di altri può aiutare a risolvere le pur interessanti criticità che sono state riscontrate nel raffronto tra le due decisioni.

Il confronto con il caso Eva Glawischnig-Piesczek c. Facebook

Il rinvio pregiudiziale sorse nell'ambito di una controversia tra la signora Glawischnig-Piesczek, deputata austriaca, e *Facebook Ireland*, quanto alla pretesa della prima di rimuovere dal social network contenuti diffamatori e lesivi che un utente aveva rivolto nei suoi confronti. A fronte di una mancata rimozione dei contenuti da parte di Facebook, la ricorrente otteneva un'ordinanza cautelare a seguito della quale Facebook disabilitava l'accesso in Austria ai contenuti contestati. In appello l'ordinanza veniva confermata quanto alle affermazioni identiche, mentre si ponevano peculiarità quanto alle affermazioni equivalenti. Entrambe le parti ricorrevano in cassazione, dove il rinvio pregiudiziale venne sollevato per vari motivi, tra cui, ai nostri fini, capire se l'obbligo di rimozione dovesse valere a livello mondiale o solo nello Stato membro di riferimento. La Corte, quindi, stabiliva: «*la direttiva 2000/31 non prevede a tal riguardo alcuna limitazione, segnatamente*

standards of protection of fundamental rights' require SEOs to carry out universal delisting' (!). This is completely against the spirit of the GDPR, giving back the power of regulation to member states. In light of this statement one wonders how the judges would explain to data subjects across the EU that they might have a right to delist information universally in one country (e.g. France), 'glocally' in another (e.g. Germany), and only nationally in the third (e.g. the United Kingdom or what will be left of it). It is also unclear whether there will be the possibility for 'forum shopping' for European data subjects, picking and choosing the kind of delisting that they prefer themselves. With this looming threat of fragmentation, one might argue that even SEOs like Google cannot be content with the outcome of the proceedings».

[64] Così O. POLLICINO, L' "autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete, *cit.*, laddove, commentando la sentenza assieme ad un'altra (che si vedrà) rilevava: «(…)il voler evitare da parte del giudice di Lussemburgo che, anche con riferimento al regime legato alla regolazione dei contenuti in rete, sia commesso quel peccato originario già noto in relazione alla protezione dati – e solo in parte ridotto, dal punto di vista territoriale, dalla delimitazione europea dei confini operata dalla sentenza *Google v. CNIL* prima ricordata - di attribuzione di un potere discrezione a un operatore privato in caso di bilanciamento o comunque di scelte che hanno a che fare con la protezione dei diritti fondamentali», p. 9.

territoriale, alla portata dei provvedimenti che gli Stati membri hanno diritto di adottare conformemente alla direttiva in parola. Di conseguenza (...) la direttiva 2000/31 non osta a che detti provvedimenti ingiuntivi producano effetti a livello mondiale. Tuttavia (...) stante la dimensione mondiale dei servizi elettronici, il legislatore dell'Unione ha ritenuto necessario garantire la coerenza delle norme dell'Unione in tale ambito con le norme applicabili a livello internazionale. Spetta agli Stati membri garantire che i provvedimenti da essi adottati e che producono effetti a livello mondiale tengano debitamente conto di queste ultime norme»[65].

Ebbene, da questi passaggi si evince chiaramente perché questa pronuncia, ancorché successiva alla *Google c. CNIL*, rispetto a quest'ultima sia stata considerata più in linea con la precedente giurisprudenza estensiva *Google Spain*[66], specie nell'ampliare l'obbligo di rimozione "al di là di quanto stabilito dalla direttiva 2000/31 sul commercio elettronico"[67]. Invero, pur ben consci della necessità di cautela nell'accostare questioni che in realtà differiscono sia per contesto normativo di riferimento (direttiva 95/46 e GDPR, in un caso; direttiva e-commerce, nell'altro) che per portata materiale della questione (informazioni obsolete e risalenti, nel caso di deindicizzazione; contenuti illeciti in quanto dichiaratamente offensivi e diffamatori, nel caso della rimozione dal social network), ossia per elementi che già di per sé giustificherebbero divergenza di valutazioni e, dunque, di direzione delle decisioni, alcuni trovavano comunque interessanti punti di contatto per commentare questa pronuncia insieme con *Google CNIL* e, almeno a primo impatto, trovare singolare la divergenza di orientamenti, quindi avanzare valutazioni di coerenza o incoerenza nell'orientamento della Corte.

I due casi sono apparsi affini nella misura in cui entrambi tirano in ballo la portata territoriale degli obblighi di rimozione o deindicizzazione (o, per altro verso, dei limiti all'accesso di materiale su internet). Combinandone i contenuti, dalla lettura collata delle pronunce vi è chi ha dedotto: «*In the future, when considering the possibility for a global dereferencing order, the relevant content may need to be close to that in* Eva Glawischnig-Piesczek v Facebook. *In other words, after* Google v CNIL *, any content that may warrant a global dereferencing order is likely to be much more serious that standard set out in* Google Spain *of ' inadequate, irrelevant or no longer relevant, or excessive ' and instead may need to be highly damaging to the person ' s reputation in a global context*»[68]. Inoltre, è stata enfatizzata anche la rilevanza riconosciuta alle autorità di controllo e

[65] Corte di giustizia, C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, sentenza del 3 ottobre 2019, punti 49-52.
[66] Così, per esempio, J. QUINN, *Google v CNIL*, cit., p. 58.
[67] M. CASTELLANETA, *Corte Ue e obblighi di rimozione di contenuti illeciti dal web – EU Court ruling on Facebook duty to take down illegal content*, in www.marinacastellaneta.it, 15 ottobre 2019.
[68] J. QUINN, *Google v CNIL*, cit., p. 59.

giurisdizionali degli Stati membri (che pure qualcuno ha criticato, quale motivo di frammentazione in contrasto con l'armonizzazione che dovrebbe guidare il sistema di protezione dei dati)[69], affidando loro, in entrambi i casi, l'ultima decisione sull'opportunità di estendere la portata globale dei rispettivi obblighi (rimozione o deindicizzazione)[70].

A nostro parere, come si anticipava, una lucida spiegazione del rapporto tra i due casi e le questioni che essi sollevano parrebbe in realtà potersi rintracciare a monte, ossia senza bisogno di *scomodare* le due pronunce della Corte e così evitando di attribuirle incoerenza o anche solo apparente "schizofrenia giudiziale"[71]: basti guardare alle Conclusioni dell'AG Spzunar. Questi, avendo trattato entrambi i casi, esponeva chiaramente (e veniva poi, pertanto – forse non altrettanto chiaramente – seguito da entrambe le sezioni chiamate a decidere ciascun caso) come segue: «*La situazione di cui al procedimento principale è diversa, a priori, da quella che costituiva il punto di partenza della mia analisi relativa alla portata territoriale di una cancellazione dei risultati di un motore di ricerca nella causa Google (...). Tale causa riguarda la direttiva 95/46/CE, la quale armonizza, a livello dell'Unione, talune norme sostanziali relative alla protezione dei dati. È segnatamente il fatto che le norme in tale materia sono armonizzate che mi ha indotto a concludere che un prestatore doveva essere tenuto a cancellare i risultati visualizzati a seguito di una ricerca effettuata non soltanto a partire da un solo Stato membro ma a partire da un luogo all'interno dell'Unione. Tuttavia, nelle mie conclusioni presentate in tale causa, non escludevo che possano sussistere casi in cui l'interesse dell'Unione esige un'applicazione delle disposizioni di tale direttiva al di fuori del territorio dell'Unione. Pertanto, per quanto riguarda le violazioni risultanti da atti diffamatori, l'imposizione in uno Stato membro di un obbligo consistente nel rimuovere talune informazioni a livello mondiale, per tutti gli utenti di una piattaforma elettronica, a causa dell'illiceità di tali informazioni accertata in forza di una legge applicabile, avrebbe come conseguenza che l'accertamento del loro carattere illecito esplichi effetti in altri Stati (...). Tuttavia, non è escluso che, secondo le leggi designate come applicabili in forza delle norme nazionali di conflitto di tali Stati, tale informazione potrebbe essere considerata lecita. (...) il giudice del rinvio non invoca strumenti giuridici del diritto dell'Unione pertinenti in tale materia. Esso invoca unicamente la direttiva 2000/31. Orbene, risulta dall'articolo 1, paragrafo 5, lettera b), di tale direttiva che quest'ultima non si applica alle questioni relative ai servizi della società dell'informazione oggetto delle direttive relative alla tutela dei dati personali. Infine, se è possibile*

[69] Come già esposto, il riferimento è ancora a O. J. GSTREIN, The Judgment That Will Be Forgotten, *cit*.
[70] O. POLLICINO, L' "autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete, *cit*.,…
[71] Ibidem, p. 4. L'autore si esprime in tal senso anche laddove introduce: «Le risposte della Corte di giustizia potrebbero sembrare, a prima lettura, contraddittorie, quasi rivelatrici di una schizofrenica natura della sua giurisprudenza, visto il limitato lasso di tempo che separa le due decisioni», p. 3.

ricavare dal regolamento n. 1215/2012 insegnamenti in relazione agli effetti prodotti dalle ingiunzioni negli Stati membri, così non è per quanto riguarda quelli prodotti al di fuori dell'Unione. Infatti, tale regolamento non esige che un'ingiunzione emessa dal giudice di uno Stato membro esplichi effetti anche in Stati terzi (...). Per siffatti motivi, tanto la questione degli effetti extraterritoriali di un'ingiunzione che impone un obbligo di rimozione quanto quella della portata territoriale di un simile obbligo dovrebbero essere oggetto di un'analisi effettuata alla luce non del diritto dell'Unione ma, segnatamente, del diritto internazionale pubblico e privato non armonizzato a livello dell'Unione. Infatti, non c'è nulla che evidenzi che la situazione oggetto del procedimento principale possa rientrare nella sfera di applicazione del diritto dell'Unione e, pertanto, delle norme di diritto internazionale che possono incidere sull'interpretazione del diritto dell'Unione. Di conseguenza, per quanto riguarda la portata territoriale di un obbligo di rimozione imposto ad un host provider nell'ambito di un'ingiunzione, si deve ritenere che quest'ultimo non sia disciplinato né dall'articolo 15, paragrafo 1, della direttiva 2000/31 né da nessun altra disposizione di siffatta direttiva e, pertanto, che tale disposizione non osti a che un host provider sia costretto a rimuovere informazioni diffuse a mezzo di una piattaforma di rete sociale a livello mondiale. Inoltre, detta portata territoriale non è neanche disciplinata dal diritto dell'Unione, nella misura in cui, nella specie, il ricorso della ricorrente non è fondato sul medesimo»[72]. Quindi, l'AG si prodigava in osservazioni supplementari quanto alla rimozione a livello globale, concludendo che: «(…) *risulta dalle considerazioni che precedono che il giudice di uno Stato membro può, in teoria, statuire sulla rimozione di informazioni diffuse a mezzo Internet a livello mondiale. Tuttavia, a causa delle differenze esistenti fra le leggi nazionali, da un lato, e la tutela della vita privata e dei diritti della personalità da esse prevista, dall'altro, e al fine di rispettare i diritti fondamentali ampiamente diffusi, un siffatto giudice deve adottare piuttosto un atteggiamento di autolimitazione. Di conseguenza, nel rispetto della cortesia internazionale (...) tale giudice dovrebbe limitare, per quanto possibile, gli effetti extraterritoriali delle sue ingiunzioni in materia di pregiudizio alla vita privata e ai diritti della personalità. L'attuazione di un obbligo di rimozione non dovrebbe eccedere quanto necessario ad assicurare la protezione della persona lesa (...). Per riprendere una riflessione formulata nel contesto di situazioni che rientrano nel diritto dell'Unione: la protezione della vita privata e dei diritti della personalità non deve necessariamente essere assicurata in maniera assoluta, ma deve essere ponderata con la protezione di altri diritti fondamentali. Occorre*

[72] Conclusioni AG M. Szpunar, C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, depositate il 4 giugno 2019, punti 79-80 e 90-93, sottolineato aggiunto.

pertanto evitare misure esorbitanti, le quali trascurerebbero il compito di assicurare un giusto equilibrio fra i diversi diritti fondamentali»[73].

Dunque, l'AG escludeva del tutto che nel secondo caso, avente altro contesto normativo e altri contenuti di riferimento rispetto a *Google c CNIL*, la questione della portata territoriale della rimozione rientrasse nel diritto dell'Unione. Pertanto, e alla luce di simili premesse, risulta più chiaro comprendere che la Corte abbia affermato in tal caso che la direttiva *e-commerce* non pone limitazioni territoriali alla portata dei provvedimenti degli Stati membri, che possono anche produrre effetti estesi, ma che, stante la dimensione globale dei servizi elettronici, il legislatore sovranazionale abbia voluto garantire coerenza delle norme dell'Unione in materia con quelle internazionali, così interpretando la norma contestata nel senso che il giudice dello Stato membro può «*ordinare a un prestatore di servizi di hosting di rimuovere le informazioni oggetto dell'ingiunzione o di bloccare l'accesso alle medesime a livello mondiale, nell'ambito del diritto internazionale pertinente*»[74]. Nessuna incoerenza, a nostro avviso, e neppure necessità di rintracciare affannosamente punti di contatto tra le due pronunce per giustificare un'agognata continuità, al punto da spingersi inevitabilmente a considerazioni di politica giurisprudenziale talvolta artificiose.

Così, tornando a *Google*, dal raffronto Quinn poneva l'accento su bilanciamento e proporzionalità anche ai fini della portata territoriale: «*At every step of the evolution of the right to dereferencing, the CJEU emphasised that the right to erasure/right to be forgotten is not absolute and that there is a need for a balancing of rights and proportionality*. *The judgment in* Google v CNIL *demonstrates this commitment to the principles of balancing and proportionality (…). The significance of* Google v CNIL *is that it limits what had previously been interpreted as an expansionary vision of dereferencing: in its ruling, the CJEU clarified that the right to be forgotten is limited to within the geographical boundaries of the EU in line with the balancing of rights and proportionality*»[75]. Ancora, per esempio, Rossi riteneva le due pronunce molto coerenti tra loro poiché in entrambe la Corte avrebbe «incentrato il proprio convincimento sul tenore letterale delle disposizioni del diritto dell'Unione»[76]. Di respiro più ampio, poi, Pollicino ravvisava il *trait d'union* tra le due pronunce soprattutto nell'intento della Corte – di politica giurisprudenziale, appunto – di valorizzare in entrambi i casi l'impegno delle autorità di controllo e giurisdizionali nazionali, per supportarne

[73] Ibidem, punti 100 e 102, sottolineato aggiunto. Poi l'AG chiudeva queste riflessioni concludendo al punto 103: «Fatta salve le suesposte osservazioni supplementari, mantengo, in relazione alla portata territoriale di un obbligo di rimozione, la posizione sostenuta al paragrafo 93 delle presenti conclusioni».
[74] Corte di giustizia, C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, cit., dispositivo. Il riferimento è anche ai punti 49-52.
[75] J. QUINN, *Google v CNIL*, cit., pp. 60 e 62.
[76] E. ROSSI, *op. cit*.

l'intervento in quanto espressione di potere pubblico a fronte del paventato pericolo di arbìtri (o, a detta dell'autore, "funzioni para-costituzionali") sempre più verosimili causati dall'incremento dei poteri privati che, di fatto, predominano nella dimensione digitale: «si è parlato di potere, ed in particolare di nuovi poteri privati che, in ambito digitale, competono con i classici poteri pubblici. Occorre quindi chiedersi, a questo proposito: quale è il momento in cui alcune forme di iniziativa economica, specialmente in ambito digitale, si trasformano tecnicamente in potere. E, conseguentemente: quale strumentario offre oggi il diritto costituzionale per reagire a tale trasformazione? Tali quesiti conclusivi (…) toccano una premessa fondamentale, del diritto pubblico, quella per cui l'unico potere legittimo è quello pubblico»[77]. Questa condivisibile prospettiva, che analizza dunque le attribuzioni alle autorità nazionali in termini di rapporto tra poteri pubblici (da rafforzare) e privati (da limitare) si oppone a quella che invece in esse vedrebbe una (ri)frammentazione, di cui si è già ampiamente detto.

In questi ultimi termini, nondimeno, è interessante riferire le valutazioni di Miglio che, ancorché precedenti a entrambe le sentenze in commento, nella misura in cui commentavano la portata territoriale del diritto all'oblio e, più in generale, della normativa sulla protezione dei dati personali, riprendevano i primi risultati della Bradford, proponendo interessanti riflessioni ai nostri fini. A suo dire, l'evolversi dell'effetto Bruxelles potrebbe anche provocare una tendenza alla frammentazione geografica di internet: «*Interestingly, although both global and territorially selective delisting might contribute to increase fragmentation, they point to two very different models of fragmentation. In the territorially selective model, geographic filtering allows global businesses to offer online services across a number of jurisdictions and permits the coexistence of a plurality of divergent local laws each in its own territorial sphere. By contrast, if regulatory divergences remain and different jurisdictions advance claims for the global application of conflicting local laws, businesses may prove unable to comply with all regulatory regimes and the threat of sanctions may ultimately undermine their ability to offer their services across multiple jurisdictions*»[78].

[77] O. POLLICINO, L' "autunno caldo" della Corte di giustizia, *cit*., pp. 11-12, nonché più in generale da p. 9. Nello stesso senso, oltre le critiche di "approccio anacronistico e conservatore" rispetto al diritto all'oblio in Google c. CNIL, A. CORRERA, La tutela dei dati personali e la portata territoriale dell'obbligo di deindicizzazione dei contenuti online, in *rivista.eurojus.it*, n. 3/2020, p. 49: «(…) in disparte i profili di criticità evidenziati, la circostanza che la Corte abbia salvato il potere dei garanti nazionali di emettere ordini di rimozione dei links contestati con effetti extra-UE, consente di affermare che le statuizioni previste nel caso Facebook sulla natura globale dell'ordine di rimozione non costituiscono una contraddizione con quanto rilevato in riferimento al caso *Google 2 judgement*».

[78] A. MIGLIO, Enforcing the Right to Be Forgotten Beyond EU Borders, in E. CARPANELLI and N. LAZZERINI (eds), *Use and Misuse of New Technologies – Contemporary Challenges in International and European Law*, Springer, 2019, p. 324.

Ebbene, per quanto si ritiene che ognuna di queste prospettive possa considerarsi tendenzialmente condivisibile, il rapporto tra le due recenti pronunce pare a noi molto più logicamente spiegabile in un'ottica di sovranità digitale. Invero, nel suo commento Pollicino affermava pure che «*Sembra proprio che ci sia la volontà di esercitare una sovranità europea digitale alla base del processo in corso ad opera di giudici di Lussemburgo di europeizzazione di Internet, la cui natura transnazionale di portata globale non sembra supportare il successo, con riferimento, appunto, alla effettività della tutela apprestata, di tentativi, seppure comprensibili e financo lodevoli negli intenti, di radicale regionalizzazione della protezione. Regionalizzazione, quest'ultima, che rischia di trasformarsi, peraltro, come si diceva, in una segmentazione e perfino balcanizzazione dei meccanismi di protezione*»[79]. Si concorda con la prima parte, non invece con l'ultima, di tale assunto. Soprattutto, essenzialmente, perché non si concorda con la visione di sovranità digitale come intesa a costruire una «*fortezza continentale, inespugnabile internamente in materia di protezione dei dati personali, ma che rischia di non avere quei ponti levatoi che consentano un'effettività extraterritoriale*»[80].

A nostro avviso, le due pronunce, lette o meno insieme, sono entrambe squisitamente espressive della tendenza della Corte *verso la sovranità digitale dell'Unione europea*, proprio nella misura in cui vengono affrontate dalla Corte per quello che sono: i giudici risolvono quesiti *diversi* in maniera *diversa*, usando forse (come hanno notato alcuni) la stessa tecnica decisionale (di interpretazione letterale della normativa e/o di attenzione alla proporzionalità), e sicuramente condotti dallo stesso orientamento che, lungi dal creare una "fortezza continentale", pare chiaramente tenere conto (come si evince dalle pronunce e anche dalle osservazioni dell'AG) delle dinamiche che potrebbero intaccare e/o provocare reazioni di Stati terzi, che non necessariamente condividono il medesimo sistema valoriale dell'Unione.

La "cautela" di una Corte attenta a delimitare, come regola generale, la portata territoriale della deindicizzazione o di definire ciò che (non) rientra nel diritto dell'Unione, quanto alla rimozione dei contenuti illeciti da Facebook, ben lungi dall'essere un controsenso o un passo indietro rispetto a *Google Spain*, ovvero ancora quasi una preoccupazione rispetto all'incontrastata emersione dei poteri privati, sembrerebbe a nostro avviso la più elevata conferma della (auto)identificazione dell'Unione come primo regolatore della dimensione digitale. Nella misura in cui, cioè, la Corte riconosce e, così *regola* la posizione dei vari operatori della dimensione digitale, tanto del motore di ricerca quanto (più o meno indirettamente) degli Stati terzi, tanto del prestatore di servizi di hosting quanto delle autorità degli Stati membri, ecco che essa si erige a mantenere e muovere le redini per

[79] O. POLLICINO, L' "autunno caldo" della Corte di giustizia, *cit.*, p. 11.
[80] Ibidem.

direzionare il processo di integrazione europea verso una sovranità digitale. Fuori da idealizzazioni, si tratta pragmaticamente di una (sempre maggiore, se la si lega alla giurisprudenza pregressa) assunzione di consapevolezza che nella misura in cui le *regole del gioco* vengono stabilite dall'Unione europea spetta ai suoi giudici (che vanno così intesi in senso lato, dunque assolutamente comprensivi anche dei giudici comuni degli Stati membri) definire la portata di quelle norme che hanno evidentemente un impatto a misura di digitale. Pertanto, così intese, anche le determinazioni rispetto ai *poteri privati*, piuttosto che essere lette come reazioni a possibili preoccupazioni (nel caso su Facebook) ovvero come quasi intimorimenti (nel caso Google), vanno visti, ancora una volta, come l'intento di *ordinare* una dimensione nella quale quegli attori sono evidentemente di rilievo e che, come tali, devono essere anche presi in considerazione dalla Corte/Unione. Ciò avviene da parte della Corte talvolta in un senso che può apparire loro più favorevole, talaltra in senso opposto, ma sempre risolvendo il caso specifico con le sue peculiarità e secondo le questioni che presenta, ancorché operando nella più ampia propensione verso la sovranità digitale. Così, l'orientamento risulta perfettamente *coerente* con gli intenti sopra esposti della Commissione. Che poi questo intento *ordinatorio* non soddisfi pienamente le aspettative e lasci aperte diverse perplessità, non cambia tali premesse, anzi. Le perplessità lasciate aperte saranno senz'altro nuovi spunti per ulteriori interventi di definizione, come paventato tra i commenti a *Google c. CNIL*[81].

Dunque, è questo il modo in cui proponiamo di leggere le pronunce della Corte che incidono sulla portata territoriale della protezione dei dati personali e in questo senso ci aspettiamo nuove e più definite pronunce che certo l'articolo 3 GDPR già richiederebbe. Questi rilievi, peraltro, ci aiuteranno a condurre l'analisi sul trasferimento di dati verso Paesi terzi, prima di affrontare la quale è ancora indispensabile esporre un altro settore nel quale l'intervento della Corte è particolarmente eloquente e rispetto al quale pare fondamentale anche il confronto con decisioni della Corte di Strasburgo.

Si tratta, come si accennava, del settore che particolarmente incide sul nucleo dei principi che strutturano la *rule of law*, sia a livello di ordinamenti domestici che anche sovranazionale, poiché riguarda la delicatissima questione dei limiti al potere pubblico: ci riferiamo alla casistica relativa ai sistemi di sorveglianza degli Stati membri e al rapporto con la rispettiva tutela dei dati personali dei cittadini, dalla quale massimamente emerge la misura del ruolo delle Corti europee, e in particolare della Corte di giustizia, nel bilanciare gli interessi in gioco e, dunque, dirigere, in un senso o nell'altro, il processo di integrazione europea nella dimensione digitale. In breve: si tratta di una

[81] Così M. SAMONTE, Google v CNIL Case C-507/17, cit., nella parte conclusiva.

verace manifestazione di sovranità digitale. L'analisi che segue sarà, inoltre, come anticipato, funzionale a comprendere e comparare le valutazioni sui sistemi di sorveglianza di Stati terzi per i flussi di dati.

3. I casi su sicurezza nazionale degli Stati membri e (limiti alla) protezione dei dati personali

Premessa

La tensione tra protezione dei dati personali ed esigenze di sicurezza è sicuramente la più rappresentativa del bilanciamento che si propone classicamente nel rapporto tra prerogative del potere pubblico e (limitazioni alle) garanzie individuali.

In tempi recenti (tralasciando l'attuale emergenza pandemica), la tensione ha riguardato soprattutto questioni di terrorismo internazionale, che hanno portato, specie dopo gli eventi dell'11 settembre, alla predisposizione in seno alle Nazioni Unite di un sistema di sanzioni ai sensi del capo VII della Carta ONU. Sistema che, com'è noto, ha fatto sorgere non poche perplessità quanto alla compatibilità con la tutela dei diritti individuali dei soggetti colpiti da quelle sanzioni[82]. Simili questioni hanno coinvolto inevitabilmente anche preoccupazioni relative alla cybersicurezza, per la necessità di far fronte a minacce particolarmente insidiose nei confronti degli Stati rispetto all'uso di internet, che con diversi interventi, in seno alle Nazioni Unite e non solo, si cerca di fronteggiare a livello globale[83].

Guardando, poi, al contesto regionale, è proprio dall'articolo 15 CEDU, contenente la c.d. *clausola di deroga* che consente agli Stati parti di venir meno ad alcuni obblighi convenzionali "in caso di guerra o in caso di altro pericolo pubblico che minacci la vita della nazione", che venne elaborata la c.d. *dottrina del margine di apprezzamento* dalla Corte di Strasburgo, come tecnica interpretativa

[82] Per una ricognizione delle misure e per il loro impatto a livello UE si consenta ancora un rinvio a G. LO TAURO, Diritti fondamentali e misure antiterrorismo nell'Unione europea "Intervalli melodici" tra Consiglio e Corte di giustizia, in *Diritto Pubblico Comparato ed Europeo*, n. 1/2020, p. 151 ss.

[83] Per una ricognizione degli interventi anche più risalenti, a partire dagli anni Novanta, sia a livello internazionale che sovranazionale, si rinvia a D. MARRANI, Cybersicurezza e tutela della riservatezza dei dati personali: le decisioni *Breyer* e *Tele2 Sverige c. Watson* della Corte di giustizia UE, in *Diritto dell'Unione europea*, n. 4/2017, pp. 790-806; nonché, per quelli più recenti, ID., Il coordinamento delle politiche per la cybersecurity dell'UE nello spazio di libertà, sicurezza e giustizia, in *Freedom, Security & Justice: European Legal Studies*, n. 1/2021, pp. 77-99.
Per un'analisi, tra le molteplici, del rapporto tra terrorismo e protezione dei dati, si veda *ex multis* M. NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, Napoli, 2012.

per riconoscere ai singoli Stati dei margini di discrezionalità nell'adozione di misure limitative dei diritti individuali riconosciuti nella CEDU, giustificate proprio da esigenze di pubblica sicurezza[84]. In tal senso, è copiosa la giurisprudenza di Strasburgo (di qualche pronuncia si è già detto, *supra*, Capitolo IV, Parte II, di altre si dirà *infra*) relativa all'interpretazione dell'articolo 8 CEDU e alla compatibilità di sistemi statali di sorveglianza di massa[85]. Con specifico riguardo, poi, alle preoccupazioni cibernetiche, è nota in seno al Consiglio d'Europa la Convenzione di Budapest come espressione dell'impegno rispetto ai rischi della criminalità informatica, e che risponde quindi, a fronteggiare le possibili minacce in rete (l'attenzione al quale è testimoniata dal progetto di secondo protocollo aggiuntivo dello scorso 12 aprile)[86] insieme con altre iniziative, di cui la Convenzione 108 (e il relativo protocollo di modernizzazione) costituisce l'esempio per noi più rilevante[87].

Peraltro, l'evoluzione delle tecnologie e l'indispensabilità di internet nella vita di tutti i giorni hanno portato inevitabilmente a relativizzare la comprensione della dicotomia protezione dati/pubblica sicurezza nel senso di rapporto tra interessi individuali *versus* prerogative pubbliche. In tal senso, è stato notato che la «prospettiva in cui *privacy* o protezione dei dati e sicurezza sono complementari e non alternative esce ulteriormente rafforzata se si guarda alla protezione dei dati come interesse collettivo della società. Se infatti, come il Regolamento afferma esplicitamente, la protezione dei dati è non solo un diritto individuale ma ormai compiutamente un interesse primario della società, lo è proprio perché esso appare strumentale, da un lato, alla garanzia dei diritti e, dall'altro lato, alla tenuta complessiva degli ordinamenti democratici. In questo senso, la protezione dei dati è necessaria sia a garantire la sicurezza declinata come sicurezza dei diritti sia la sicurezza come percezione soggettiva di sicurezza e collante ultimo delle società»[88].

Guardando più specificamente al livello sovranazionale, merita particolare considerazione anche la prospettiva di Fichera, che suggerisce di considerare la sicurezza come meta-valore insito nel cuore

[84] Per la dottrina del margine di apprezzamento si rinvia, *ex multis*, a R. SAPIENZA, Sul margine di apprezzamento statale nel sistema della Convenzione europea dei diritti dell'uomo, in *Rivista di Diritto Internazionale*, LXXIV/ 1991, pp. 573 -614.

[85] Per una ricognizione delle pronunce più rilevanti, si rinvia al facsheet dedicato a "*Mass surveillance*", aggiornato al Maggio 2021, disponibile qui: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf .

[86] Convention on Cybercrime, Budapest, 23November2001: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 .

[87] Ma il riferimento è anche alla Convenzione di Varsavia sulla prevenzione del terrorismo, del 2005 (v. https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/196 9 e alla Convenzione di Lanzarote contro sfruttamento e abusi sessuali su minori, del 2007 (v. https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/201). La Convenzione di Budapest sulla criminalità informatica, del 2001, è disponibile qui: https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/185 .

[88] Così M. OROFINO, Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione, in *Medialaws*, n. 2/2018, p. 104, laddove concludeva quindi che "*privacy* (protezione dei dati personali) è sicurezza", sottolineato aggiunto.

dell'identità costituzionale europea e guiderebbe l'Unione come entità politica, rivelandosi attraverso due fondamentali discorsi del potere: sicurezza in senso stretto, sia interna che esterna, e diritti fondamentali[89].

L'autore poneva l'attenzione sullo "spazio di libertà, sicurezza e giustizia" da intendere «*not so much as a policy area, but as an overarching aspiration of the EU as a whole. It is by examining the self-representation of the EU as a polity, which develops in the direction of an AFSJ, that we may reveal something new, or unexplored, about the European liberal project*»[90]. Proponendo una prospettiva alternativa rispetto alla narrativa classica del processo di integrazione europea, quale mercato interno con un nucleo centrale essenzialmente economico e rispetto al quale solo il progressivo sviluppo dalla comunità economica avrebbe portato all'emersione di diritti fondamentali, prima assenti, e di altri valori condivisi, l'autore valorizzerebbe, invece, che «*right at the core of the EU, security and fundamental rights operate as self-justifying discourses of power, and therefore in terms of empowerment both of the EU citizen and of the EU as a collective entity*»[91]. In questo ordine di considerazioni, l'autore afferma: «*The importance of Europe is expressed not merely by the need to develop shared values and establish procedure to enforce them (or, as some would say, 'integration through law'), but also by the urge to ensure that these values are protected over an extended period of time. Yes, at the same time security as meta-value also inevitably embraces and challenges all other values*»[92].

Ebbene, queste riflessioni si legano inevitabilmente ai discorsi sulla *EU rule of law* e li integrano con la componente della sicurezza, che viene così intesa a corroborare quel sistema di garanzie e che, pertanto, ne giustificherebbe, proprio nell'ottica della compiuta attuazione dei valori dell'Unione, limitazioni e deroghe da parte sia dei singoli Stati membri che dell'Unione. In che termini ed entro quali limiti ciò effettivamente avverrebbe e/o verrebbe consentito dalla Corte di giustizia, specie con riguardo allo specifico settore della protezione dei dati personali, sarà oggetto della seguente analisi.

Sulla base di queste brevi premesse, dunque, si procederà a valutare le peculiarità del rapporto tra protezione dei dati e sicurezza nel processo di integrazione europea, con particolare riguardo alle misure limitative (e/o ai sistemi di sorveglianza) adottate dagli Stati membri, in linea con le previsioni dell'articolo 4, paragrafo 2, TUE[93], per come affrontate dalla giurisprudenza di

[89] M. FICHERA, *The Foundations of the EU as a Polity*, Elgar, 2018, pp. 1-2 e 24.
[90] Ibidem, p. 24.
[91] Ibidem, p. 25.
[92] Ibidem, p. 24.
[93] *Articolo 4 TUE* – 2. L'Unione rispetta l'uguaglianza degli Stati membri davanti ai trattati e la loro identità nazionale insita nella loro struttura fondamentale, politica e costituzionale, compreso il sistema delle autonomie locali e regionali.

Lussemburgo. Ciò verrà fatto procedendo ad un inevitabile confronto con le pronunce di Strasburgo, interessante esempio di contaminazione e confronto tra modelli interpretativi nel delicato settore che tocca prerogative della sovranità nazionale. Inoltre, e soprattutto, ciò sarà finalizzato a consentire successive valutazioni sulla pretesa adeguatezza dei sistemi di Paesi terzi ai fini del trasferimento di dati personali dall'Unione europea e, quindi, a sviluppare riflessioni sulla portata effettiva del prospettato principio di coerenza tra azione interna ed esterna dell'Unione (rispetto ai principi della *EU rule of law*), specie nell'ottica della sua tensione verso la sovranità digitale.

Per procedere all'analisi della casistica rilevante e del relativo ruolo della Corte di giustizia, sarà indispensabile riprendere brevemente la normativa coinvolta (e i connessi interventi istituzionali più rilevanti), oggetto delle interpretazioni dei giudici sovranazionali.

Normativa interessata

Anzitutto, il breve richiamo (per l'esposizione più estesa si veda *supra,* Parte II) degli interventi normativi servirà a fugare pur plausibili dubbi tra provvedimenti assunti a livello sovranazionale per garantire una qualche cooperazione e armonizzazione rispetto ad esigenze di sicurezza condivise tra gli Stati membri (e dunque, esigenze di "sicurezza sovranazionale") e, dall'altro lato, provvedimenti che, a livello sovranazionale, consentono agli Stati membri spazi di discrezionalità domestica per "derogare" alla disciplina comune e adottare misure limitative al fine di salvaguardare giustificate esigenze di sicurezza nazionale. A queste ultime essenzialmente, infatti, sarà dedicata la giurisprudenza a cui faremo riferimento. È bene, nondimeno, offrire una panoramica generale, sia per non confondere gli ambiti di intervento che, anche, per comprendere come i principi emersi da quella giurisprudenza si adattino in generale a qualsiasi provvedimento sovranazionale nel settore.

Alla prima categoria delle due individuate va sicuramente ricondotta, nell'ambito della normativa vigente, la c.d. *direttiva PNR,* ossia relativa ai c.d. dati del codice di prenotazione dei passeggeri aerei, che tanto ha fatto discutere prima della sua adozione (la proposta della Commissione risale addirittura al 2007) e che è finalmente stata adottata, nel contesto della riforma sui dati, il 27 aprile 2016. Dai Considerando 3, 5 e 6 della stessa se ne evincono ragioni e obiettivi: "*Nella comunicazione del 21 settembre 2010 sull'approccio globale al trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) verso paesi terzi la Commissione espone alcuni*

Rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro.

elementi essenziali di una politica dell'Unione in questo ambito (...). Gli obiettivi della presente direttiva sono, tra l'altro, garantire la sicurezza, proteggere la vita e l'incolumità delle persone, nonché creare un quadro normativo per la tutela dei dati PNR per quanto riguarda il loro trattamento da parte delle autorità competenti. L'uso efficace dei dati PNR (...) è necessario per prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi e rafforzare così la sicurezza interna, per raccogliere prove e, se del caso, scoprire complici e smantellare reti criminali"[94]. Peraltro, l'articolo 1 chiarisce l'ambito di applicazione, riferito al trasferimento dei dati PNR dei voli extra-UE da parte dei vettori aerei, nonché al trattamento di tali dati dagli Stati membri e allo scambio tra gli stessi, ai fini suddetti di sicurezza contro reati gravi e terrorismo; l'articolo 2 prevede la facoltà per gli Stati membri di estendere la normativa ai voli intra-UE[95]. Come il lungo e travagliato iter per l'adozione lascia intendere, la direttiva è stata spesso oggetto di ampie critiche e perplessità, solo parzialmente sopite con la sua approvazione, specie quanto alla compatibilità delle sue previsioni con le disposizioni della Carta dei diritti fondamentali e con la giurisprudenza (di cui diremo a breve) che aveva sollevato criticità rispetto a normative affini: «La circostanza per la quale la direttiva PNR permette di armonizzare le disposizioni legislative degli Stati Membri, contrastando tanto la mancanza di uniformità all'interno dell'Unione quanto le lacune dei sistemi di sicurezza nazionale, con beneficio di tutti i Paesi interessati, è un merito incontestato che tuttavia non preserva la stessa da un'eventuale dichiarazione di invalidità, basandosi, quest'ultima, su altri presupposti»[96].

Vanno poi segnalati, nell'ambito di questa prima categoria, i provvedimenti più direttamente espressivi di esigenze sovranazionali di cybersicurezza. Quest'ultima, invero, è stata sempre più

[94] Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, L 119/132, Considerando 3, 5, 6.

[95] Ibidem, Articolo 1 – *Oggetto e ambito di applicazione*

1. La presente direttiva prevede:

a) il trasferimento a cura dei vettori aerei dei dati del codice di prenotazione dei passeggeri (PNR) dei voli extra-UE;

b) il trattamento dei dati di cui alla lettera a), comprese le operazioni di raccolta, uso e conservazione a cura degli Stati membri e il loro scambio tra gli Stati membri.

2. I dati PNR raccolti a norma della presente direttiva possono essere trattati unicamente a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, secondo quanto previsto all'articolo 6, paragrafo 2, lettere a), b) e c).

[96] F. DI MATTEO, La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella direttiva PNR?, in *Diritti Umani e Diritto Internazionale*, n. 1/2017, pp. 234-235, che concludeva affermando «(…) la direttiva PNR non può dirsi, ancor oggi, al riparo da una possibile dichiarazione d'invalidità per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza, alla luce degli articoli 7, 8 della Carta dei diritti fondamentali». Si veda anche in tal senso C. DI FRANCESCO MAESA, Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR). In *Eurojus.it*, 24.05.2016, che, nel criticare la direttiva, proponeva audacemente un regolamento nel settore: «*Considering that Member States turned down the possibility of adopting such unified rules in a regulation, we should consider if the Member States are willing to adopt such a regulation in a field so strictly connected with State sovereignty as criminal law. It can be hoped that the inadequacies of the directives considered herein will make the EU legislator take this step forward*».

oggetto di interventi politici dell'Unione, attraverso la predisposizione da parte della Commissione di diverse *Strategie,* da quella di *sicurezza interna dell'UE* del 2010 sino a quella per *l'Unione della direttivasicurezza* del 2020 e finanche la recentissima *per contrastare la criminalità organizzata* del 2021[97]. Per le medesime esigenze è stata istituita, come si sa, l'ENISA, Agenzia europea di sicurezza delle reti e dell'informazione (con Regolamento n. 460/2004), di recente rafforzata, come diremo a breve. Tra gli atti normativi di rilievo, va segnalata innanzitutto la c.d. *direttiva NIS*, adottata nel 2016 e "recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" che, oltre a richiedere agli Stat di adottare una strategia nazionale per la sicurezza della rete, istituisce un gruppo di cooperazione per agevolare lo scambio di informazioni tra Stati membri, e crea altresì una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (c.d. rete CSIRT)[98]. Ai sensi dell'articolo 2, il trattamento dei dati personali viene effettuato ai sensi della direttiva madre e, per le istituzioni dell'Unione, del rispettivo regolamento. Nonostante sia abbastanza recente, la Commissione ha già proposto, lo scorso 16 dicembre 2020, una nuova direttiva a sostituirla, c.d. *direttiva NIS 2*, puntando essenzialmente ad estendere l'ambito della prima e a potenziare l'assetto sanzionatorio, espressione della già esposta Strategia della Commissione *Plasmare il Futuro dell'Europa*, per rafforzare la cybersicurezza. Un altro importante strumento normativo è il c.d. *Cybersecurity Act*, ossia il Regolamento n. 881/2019 (detto anche regolamento sulla cybersicurezza), che ha potenziato il ruolo dell'ENISA, con lo scopo di "*garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione*"[99].

Passando, invece, alla seconda categoria di atti normativi, che assume maggiore rilievo ai nostri fini perché riguarda le questioni affrontate dalle pronunce che andremo ad analizzare, va ripreso anzitutto il riferimento all'ambito di applicazione materiale della normativa sulla protezione dei dati personali (cfr. *supra*, par. 2.1.) che costituisce il punto di partenza dalle cui deroghe ed eccezioni ricavare i provvedimenti di rilievo.

Come si è detto, sulla scia del "primo trattino" del par. 2, art. 3 della direttiva madre, il GDPR esclude dall'ambito di applicazione i trattamenti di dati personali effettuati dagli Stati membri nell'esercizio delle attività PESC e quelli "*effettuati dalle autorità competenti a fini di prevenzione,*

[97] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS *on the EU Strategy to tackle Organised Crime* 2021-2025, 14 April 2021.
[98] Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi, Articolo 1, par. 2, lett. a), b), c).
[99] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), Articolo 1.

indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse"[100]. Nel solco di questa esclusione, come abbiamo visto, opera la direttiva 2016/680[101], adottata nel pacchetto di riforma insieme con il GDPR, che interviene ad abrogare la precedente decisione quadro (2088/977/GAI), e si dedica a disciplinare il trattamento dei dati personali da parte di autorità competenti ai fini di perseguimento di reati, con tutte le accennate perplessità in termini di precisa definizione dell'ambito di applicazione (rispetto al GDPR), e che dipendono essenzialmente dalla nozione di "autorità competente".

Infatti, è vero, come è stato rilevato, e come appare in linea anche con le previsioni della Dichiarazione 21 allegata al Trattato di Lisbona[102], che mantenere "frammentata" la struttura della normativa sulla protezione dei dati personali risponde all'esigenza di prendere in considerazione i diversi settori di intervento e il diverso ambito e scopo che ciascuno di essi presenta, per cui «*It might be preferable to keep the three horizontal instruments instead of a single, overly general instrument, requiring further specification in a plethora of sectorial legislation, rendering the body of EU data protection legislation unreadable*»[103]; è vero anche, però, che le perplessità prospettate rispetto alla corretta applicazione della direttiva 680 (specie in rapporto alla delimitazione con il GDPR) si aggiungono a uno scenario complesso, che richiede particolare coordinamento nella regolazione del trattamento dei dati nel settore della criminalità: «La disciplina della *data protection* nel settore della cooperazione giudiziaria e di polizia in materia penale risulta dunque contraddistinta da grande frammentazione, la quale rappresenta un fattore problematico in sé: il fatto che esistano ancora norme specifiche sulla protezione dei dati negli strumenti che disciplinano

[100] GDPR, Articolo 2, par. 2, lett. d) e, quanto alle attività PESC, lett. b).

[101] Direttiva n.2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, 27aprile 2016.
Peraltro, tale normativa si applica anche nel contesto della Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo; cfr. Considerando 25 di quest'ultima.

[102] 21. *Dichiarazione relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia*
La conferenza riconosce che potrebbero rivelarsi necessarie, in considerazione della specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, in base all'articolo 16 del trattato sul funzionamento dell'Unione europea.

[103] P. DE HERT. J. SAJFERT, The Role of the Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data, in C. BRIÈRE and A. WEYEMBERGH (Eds), *The Needed Balances in EU Criminal Law: Past, Present and Future*, Oxford, 2018, p. 247.

i sistemi Europol, Eurojust, SIS, Prum, comporta inevitabilmente che, in ultima istanza, il livello di tutela garantito agli individui si riduca»[104].

Così brevemente segnalata la normativa riferita agli Stati che rientra nell'esclusione dall'ambito di applicazione del GDPR, un'altra previsione del Regolamento di particolare rilievo quanto a misure statali è l'articolo 23 dedicato alle "limitazioni", che, riprendendo l'analoga disposizione dell'(ex) articolo 13 della direttiva madre, consente *anche* agli Stati (oltre che all'Unione) di adottare misure legislative per limitare la portata de diritti e obblighi previsti nel GDPR, laddove ciò – con una formula che rievoca sia la CEDU e la Carta dei diritti, che la giurisprudenza di Strasburgo e Lussemburgo – "*rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica*". La norma elenca poi una serie di cause in presenza delle quali ciò è possibile, tra cui sicurezza nazionale e pubblica, difesa e perseguimento di reati, indipendenza della magistratura e controllo connesso all'esercizio di pubblici poteri[105]. Il Considerando 73 precisa, infatti, che "*Tali limitazioni dovrebbero essere conformi alla Carta e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*",

[104] G. RUGANI, La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della Direttiva (UE) 2016/680, cit., p. 90.

[105] GDPR, Articolo 23 – *Limitazioni*

1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:
a) la sicurezza nazionale;
b) la difesa;
c) la sicurezza pubblica;
d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
i) la tutela dell'interessato o dei diritti e delle libertà altrui;
j) l'esecuzione delle azioni civili.
2. In particolare qualsiasi misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, se del caso:
a) le finalità del trattamento o le categorie di trattamento;
b) le categorie di dati personali;
c) la portata delle limitazioni introdotte;
d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;
e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari;
f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;
g) i rischi per i diritti e le libertà degli interessati; e
h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

riprendendo effettivamente le previsioni dell'articolo 52 della Carta e, oltre ai paragrafi 2 degli articoli da 8 a 11 della CEDU. Ciò, peraltro, è in linea con quanto precisato dal GDPR sin dal Considerando 4, per cui "*Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità*"[106].

Particolarmente interessante, poi, il rapporto tra la normativa generale e la c.d. direttiva *e-privacy*, dedicata ai trattamenti di dati nel settore delle comunicazioni elettroniche (e adottata all'indomani dell'attacco terroristico dell'11 settembre), definito da espresse previsioni del GDPR, tra cui anzitutto il Considerando 173 che specifica che il Regolamento debba applicarsi a tutti i trattamenti che non rientrino in obblighi specifici quali quelli della suddetta direttiva, auspicando una modifica della stessa in linea con il primo[107]. Si è detto, al riguardo, della proposta di Regolamento *e-privacy*, che non ha ancora trovato compimento, per cui risulta ancora in vigore la direttiva.

Il rapporto tra i due strumenti normativi viene quindi esplicitato dall'articolo 95 GDPR, che esclude che il Regolamento imponga obblighi supplementari per i trattamenti realizzati nel quadro della fornitura di servizi di comunicazione elettronica, rispetto agli obblighi specifici con lo stesso obiettivo fissati dalla direttiva 2002/58/CE[108]. Dal canto suo, la direttiva, volta ad armonizzare le disposizioni degli Stati membri per garantire un livello equivalente di tutela dei diritti rispetto ai trattamenti di dati personali nel settore delle comunicazioni elettroniche, nonché per assicurare la circolazione dei dati e dei servizi di comunicazione elettronica, espressamente si propone di integrare la normativa generale sulla protezione dei dati personali (il riferimento è all'allora direttiva 95/46) ed esclude la sua applicazione alle attività PESC e di cooperazione giudiziaria, nonché a tutte le attività legate alla sicurezza o ad attività degli Stati in settori che rientrano nel diritto penale[109].

---

[106] GDPR, Considerando 4.

[107] GDPR, Considerando 173: È opportuno che il presente regolamento si applichi a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo, di cui alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio, compresi gli obblighi del titolare del trattamento e i diritti delle persone fisiche. Per chiarire il rapporto tra il presente regolamento e la direttiva 2002/58/CE, è opportuno modificare quest'ultima di conseguenza. Una volta adottato il presente regolamento, la direttiva 2002/58/CE dovrebbe essere riesaminata in particolare per assicurare la coerenza con il presente regolamento.

[108] Articolo 95 – *Rapporto con la direttiva 2002/58/CE*
Il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE

[109] Direttiva 2002/58/CE – Articolo 1 – *Finalità e campo d'applicazione*

Inoltre, sempre in linea con quanto abbiamo esposto rispetto alla normativa generale, l'articolo 15 prevede l'applicazione di alcune disposizioni della direttiva madre, tra cui rilevano ai nostri fini proprio quelle che consentono agli Stati membri di limitare i diritti e gli obblighi stabiliti dalla direttiva *e-privacy* per motivi di sicurezza, difesa e perseguimento di reati, laddove costituiscano misure necessarie e proporzionate in linea con quanto previsto dall'allora articolo 13 della direttiva 95/46/CE (corrispondente all'attuale articolo 23 GDPR): "*A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo*"[110]. In linea con queste previsioni, vale la pena di segnalare, avendo accennato anche a questioni di cybersicurezza, che la Commissione, nell'ambito della già citata strategia *Plasmare il futuro digitale dell'Europa*, ha avanzato lo scorso dicembre 2020 una proposta di Regolamento "relativo a una deroga temporanea talune disposizioni della direttiva 2002/58/CE" ai fini della lotta contro gli abusi sessuali su minori online[111].

Tralasciando quest'ultimo richiamo, il riferimento alle predette disposizioni della direttiva madre, del GDPR e della direttiva *e-privacy* è indispensabile, poiché esse sono centrali nell'analisi della giurisprudenza rilevante ai nostri fini. In tal senso, è doveroso un richiamo alla direttiva c.d. *data retention*, ossia la n. 2006/24/CE (prevista a seguito degli attacchi terroristici di Madrid e Londra, di cui si è già detto quanto alla pronuncia di invalidità della Corte di giustizia, cfr. *supra*, Parte III), che interveniva proprio a modificare la direttiva *e-privacy*. Più precisamente, anzitutto nei vari considerando si prospettava la necessità di un'armonizzazione delle discipline degli Stati membri sulla conservazione dei dati da parte di fornitori di servizi per la prevenzione o il perseguimento di

[110] Articolo 15 – *Applicazione di alcune disposizioni della direttiva 95/46/CE*
1. Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.
2. Le disposizioni del capo III della direttiva 95/46/CE relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa.
3. Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE, svolge i compiti di cui all'articolo 30 della direttiva stessa anche per quanto concerne materie disciplinate dalla presente direttiva, segnatamente la tutela dei diritti e delle libertà fondamentali e degli interessi legittimi nel settore delle comunicazioni elettroniche.
[111] Commissione europea, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE del Parlamento europeo e del Consiglio per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali sui minori online, Bruxelles, 10.09.2020, COM(2020) 568 final, disponibile qui: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0568&from=EN .

reati, poiché la differenziazione tra le varie discipline costituiva un ostacolo al mercato interno delle comunicazioni elettroniche, specificando che la direttiva riguardasse esclusivamente i dati generati o trattati come conseguenza di una comunicazione o di un servizio di comunicazione e non invece il contenuto dell'informazione comunicata[112]. Inoltre, l'articolo11, rubricato "modifica della direttiva 2002/58/CE, prevedeva: "*All'articolo 15 della direttiva 2002/58/CE è inserito il seguente paragrafo: «1 bis. Il paragrafo 1 non si applica ai dati la cui conservazione è specificamente prevista dalla direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione (8), ai fini di cui all'articolo 1, paragrafo 1, di tale direttiva*"[113].

Orbene, affrontando le ragioni che hanno portato alla totale invalidità di tale direttiva *data retention*, torniamo a richiamare il già illustrato caso *Digital Rights Ireland* (di seguito *DRI*) e iniziamo così, finalmente, ad analizzare gli interventi della Corte di giustizia nel delicato settore coinvolgente esigenze di sicurezza nazionale degli Stati membri.

Il caso Digital Rights Ireland

Si è già proposta la causa *DRI*, rinvio pregiudiziale sorto nell'ambito di un caso sulla legittimità di misure legislative e amministrative irlandesi relative alla conservazione di dati di comunicazioni elettroniche, come esempio per illustrare il principio di coerenza interna dell'azione dell'Unione. In quell'occasione, lo si ripete, la Corte invalidava l'intera direttiva utilizzando «la Carta come parametro diretto di legittimità delle limitazioni ai diritti fondamentali previste da un atto dell'UE»[114]. Riconoscendo che l'accesso ai dati consentito dalla direttiva alle autorità nazionali costituisse un'ingerenza "di vasta portata" e "particolarmente grave" nei diritti fondamentali degli interessati sanciti agli articoli 7 e 8 della Carta, la Corte, pur confermando le esigenze di sicurezza per la lotta contro il terrorismo e la criminalità grave anche a livello di Unione (nonché come diritto fondamentale riconosciuto dall'articolo 6 della Carta), si spingeva a verificare la proporzionalità dell'ingerenza e, così, finalmente, concludeva che «*il legislatore dell'Unione ha ecceduto i limiti*

[112] Direttiva , Considerando 4-6 e 12-13, nonché 15.
Per un'analisi della misura e del suo rapporto (*rectius*, incompatibilità) con i diritti fondamentali e la *rule of law*, ben prima della pronuncia di invalidità della Corte, si veda T. KONSTADINIDES, Destroying Democracy on the Ground of Defending It? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem, in *European Law Review*, 36 (5), 2011, pp. 722-736.
[113] Ibidem, articolo 11.
[114] F. BESTAGNO, Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali, in *Il Diritto dell'Unione europea*, n. 1/2015, pp. 25-56.

imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta»[115].

L'importanza della pronuncia è data dal rilievo che la Corte riconosce al puntuale scrutinio di proporzionalità e necessità, per preservare il contenuto essenziale dei diritti, sancendo così indubitabilmente l'indispensabilità di ciò che è stato individuato come "*justification test for limiting rights*"[116] e quindi, così, riconoscendo la preminenza della tutela dei diritti fondamentali a livello sovranazionale (specie in un periodo, quale quello in cui si discuteva dell'accesso dell'Unione alla CEDU per rendere effettive le previsioni dell'articolo 6 TUE, di particolare sensibilità/preoccupazione rispetto a tali scrutini), tanto da arrivare, per la prima volta, a dichiarare una direttiva invalida *in toto*[117] – e non solo rispetto ad alcune disposizioni, come era già avvenuto in precedenza – a ragione della incompatibilità con le previsioni della Carta. Invero, non solo l'importanza di proporzionalità e necessità veniva così messa in luce a livello giurisprudenziale (e da qui in poi, con *Schrems I* e con le ulteriori pronunce di cui diremo a breve); ma essa coinvolgeva nello stesso periodo la sensibilità anche delle altre istituzioni, come si evince dal Parere n. 1/2014 del Gruppo di Lavoro Articolo 29 "*sull'applicazione dei principi di necessità e proporzionalità nell'azione di contrasto*", emesso per orientare l'adozione di misure nello Spazio di libertà, sicurezza e giustizia da parte di autorità nazionali e dell'Unione, che espressamente indicava come i concetti fossero stati sviluppati proprio dalla giurisprudenza EDU. Ciò a corroborare la tendenza degli attori coinvolti in tale sistema verso una coerenza interna, in questo settore, che si mostrava così già chiaramente ispirata dagli orientamenti di Strasburgo[118].

Fondamentale esempio di funzionamento della *EU rule of law*, questa pronuncia costituisce uno delle prime e più alte espressioni, potremmo dire, della *centralità* dei giudici di Lussemburgo nell'evoluzione verso una sovranità digitale dell'Unione europea, nella misura in cui la Corte si erige a ultimo controllore delle garanzie predisposte dal sistema sovranazionale, sindacando la conformità dell'operato delle istituzioni europee e arrivando così a censurarlo (coerenza interna orizzontale).

---

[115] Corte di giustizia, C-293/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a*., 8 aprile 2014, p. 79, nonché i riferimenti precedenti ai punti 37 e 42-45, e ancora, per il ragionamento sulla proporzionalità e necessità, i punti 46-68.

[116] Così S. PEERS, S. PRECHAL, Article 52, in S. PEERS, T. HERVEY, J. KENNER, A. WARD, *The EU Charter of Fundamental Rights - A Commentary*, Hart Publishing, 2014, p. 1480 ss.

[117] Cfr. A. ARENA, La Corte di Giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?, in *Quaderni costituzionali*, n. 3/ 2014, p. 722. Si veda anche G. TIBERI, La Corte di giustizia sulla conservazione dei dati: la protezione dei diritti fondamentali nel "dopo-Lisbona", in *Quaderni costituzionali*, n. 3/ 2014, p. 719.

[118] Gruppo di Lavoro Art. 29, Parere 01/2014 - WP 211, *sull'applicazione dei principi di necessità e proporzionalità nell'azione di contrasto*, adottato il 27 febbraio 2014, disponibile qui in italiano: https://www.privacy.it/archivio/grupripareri201401.html

Le pronunce successive, specie quelle dedicate allo "scrutinio" dei sistemi nazionali di sicurezza (dunque di coerenza interna verticale), rappresentano un altro elemento a conferma di quella centralità e, quindi, una prosecuzione di quella giurisprudenza applicata a misure (non solo sovranazionali, ma anche) statali.

I casi Tele2Sverige e Watson

Le cause riunite *Tele2Sverige e Watson* sono, infatti, una diretta prosecuzione della invalidazione della direttiva *data retention*. In esse la Corte veniva chiamata da due rinvii pregiudiziali, rispettivamente, dei giudici di Svezia e Regno Unito, ad interpretare proprio l'articolo 15 della direttiva *e-privacy* (unica disposizione rimasta, dopo la decisione *DRI*, a consentire eccezioni statali rispetto alla conservazione dei dati nel settore delle comunicazioni elettroniche, alla luce degli articoli 7, 8, e 52 della Carta dei diritti fondamentali) quanto alla compatibilità di normative nazionali sulla conservazione, da parte di sistemi di fornitura di reti e servizi di comunicazione elettronica, dei dati relativi al traffico e all'ubicazione ai fini dell'accesso da parte delle autorità nazionali. Entrambe le questioni, infatti, chiedevano chiarimenti sulla portata delle implicazioni della sentenza *DRI* rispetto ai regimi nazionali fondati sulla direttiva *data retention*, a seguito della suddetta dichiarazione di invalidità. In particolare, nel caso svedese, alcune leggi nazionali prevedevano, in conformità con la direttiva *data retention*, l'accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica da parte delle autorità nazionali per l'accertamento di reati.

A seguito della sentenza *DRI*, la *Tele2 Sverige*, che fornisce servizi di comunicazione elettronica in Svezia, comunicava la cessazione della conservazione dei dati, prevista dalle leggi svedesi, con conseguente soppressione degli stessi, provocando una denuncia da parte della polizia nazionale. L'altra causa vedeva agire i signori Watson, Brice e Lewis dinanzi alla Alta Corte di giustizia (Inghilterra e Galles) avverso l'articolo 1 della legge del 2014 sulla conservazione dei dati e sui poteri di indagine (*Data Retention and Investigatory Powers Act*, di seguito DRIPA), sempre a seguito della pronuncia *DRI*, questionando la compatibilità del previsto regime generale di conservazione dei dati con le disposizioni della Carta (e della CEDU), specie quanto alla poca chiarezza sull'accesso e l'utilizzo dei dati, peraltro non subordinati a un controllo preventivo di un giudice o un'autorità indipendente.

Anzitutto, la Corte verificava se le normative nazionali rientrassero nell'ambito di applicazione del diritto dell'Unione, riconoscendo che esse riguardassero attività degli Stati legate a finalità proprie di questi ultimi, ai sensi dell'articolo 15 della direttiva; ciononostante, "alla luce dell'economia

generale della direttiva 2002/58" e per preservarne il suo "effetto utile", la Corte concludeva che tali normative fossero comprese nell'ambito di applicazione della stessa "*dato che quest'ultima autorizza espressamente gli Stati membri ad adottare le misure in questione unicamente a condizione di rispettare le condizioni da essa previste*"[119]. Su questo aspetto, dunque, anche tramite richiami alla propria giurisprudenza (cfr. in particolare *Promusicae*), la Corte ribadiva il proprio orientamento estensivo nella definizione dell'ambito di applicazione materiale della protezione dei dati personali (anche nel settore delle comunicazioni elettroniche). Al riguardo, è stato notato che «*The rules of interpretation of particularly Articles 7 and 8 could apply more generally – perhaps to PNR data (another form of mass surveillance) - and beyond*»[120].

Quanto, poi, all'interpretazione dell'articolo 15 della direttiva alla luce delle disposizioni della Carta, la Corte, in vista del fatto che esso prevede delle eccezioni al principio di riservatezza delle comunicazioni, confermava la necessità di intenderlo in senso restrittivo, ribadendo di interpretarlo alla luce delle disposizioni della Carta (non solo 7 e 8, ma anche 11) in linea con la propria richiamata giurisprudenza (tra cui *DRI*, *Google Spain* e *Schrems*)[121]. Quindi, passava a sindacare la deroga di cui all'articolo 15 alla luce dell'articolo 52, par. 1 della Carta e del correlato vaglio di proporzionalità e necessarietà delle misure nazionali consentite.

Ciò facendo, nella più genuina applicazione del suddetto "*justification test for limiting rights*", la Corte si atteggiava in tutto e per tutto a giudice dei diritti[122] e, sindacando la discrezionalità delle autorità nazionali rispetto a misure in deroga, inevitabilmente effettuava delle valutazioni che, *mutatis mutandis*, risultano evocative della c.d. *dottrina del margine di apprezzamento* elaborata e costantemente utilizzata dalla Corte di Strasburgo. In effetti, ben due pronunce di quest'ultima venivano espressamente richiamate dalla Corte di Lussemburgo.

---

[119] Corte di giustizia, cause riunite C-203/15 e C-698/15, *Tele2 Sverige* e *Watson e a*., 21 dicembre 2016, p. 73, nonché, più in generale, punti 65-81.

[120] Così L. WOODS, Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber), in *EU law Analysis*, 21 December 2016, in cui continuava: «*It is also worth noting that according to a leaked Commission document, it is proposed to extend the scope of the Privacy and Electronic Communications Directive to other communications service providers not currently regulated by the directive, but who may be subject to some data retention requirements already*».

[121] Ibidem, punti 89-93.

[122] Così confermando l'orientamento sempre più spiccato a seguito di Lisbona (e, dunque, dalla portata vincolante riconosciuta alla Carta), come testimonia la saga *Kadi* in materia di terrorismo, ma anche i casi DRI e Schrems nel più specifico settore dei dati personali, cfr. T. OJANEN, Right-based Review of Electronic Surveillance after *Digital Rights Ireland* and *Schrems* in the European Union, in D. COLE, F. FABBRINI, S. SCHULHOFER (Eds), *Surveillance, Privacy and Trans-Atlantic Relations*, Hart Publishing, 2017: «*Finally, the judgments in* Digital Rights Ireland *and* Schrems *feature as a continuation of such constitutional dynamics that have significantly strengthened the status of fundamental rights within the EU legal order in recent years, as well as transformed the CJEU into a supranational constitutional court that is rapidly becoming a forerunner of rights protection in several areas, including counterterrorism. In particular, the entry into force of the Lisbon Treaty in December 2009, rendering the EU Chapter of Fundamental Rights a legal binding rights catalogue with the same legal values as the founding treaties of the EU, has produced important constitutional dynamics in the use of the CFR by the CJEU*», p. 17.

Intanto, la Corte UE constatava che «*una normativa nazionale come quella in discussione nei procedimenti principali, la quale riguarda in maniera generalizzata tutti gli abbonati ed utenti iscritti e ha ad oggetto tutti i mezzi di comunicazione elettronica nonché l'insieme dei dati relativi al traffico, non prevede alcuna differenziazione, limitazione o eccezione in funzione dell'obiettivo perseguito. Essa concerne in maniera globale l'insieme delle persone che si avvalgono di servizi di comunicazione elettronica, senza che tali persone si trovino, anche solo indirettamente, in una situazione suscettibile di dar luogo ad azioni penali. Essa si applica dunque finanche a persone per le quali non esiste alcun indizio di natura tale da far credere che il loro comportamento possa avere un nesso, sia pur indiretto o remoto, con violazioni penali gravi. Inoltre, essa non prevede alcuna eccezione, di modo che essa si applica anche a persone le cui comunicazioni sono sottoposte, secondo le norme del diritto nazionale, al segreto professionale*»[123]. Quindi, rilevava come siffatte normative travalicassero i "limiti dello stretto necessario", in contrasto con le previsioni dell'articolo 15 letto alla luce della Carta, in virtù del quale, le pur consentite previsioni degli Stati membri, volte alla conservazione mirata dei dati per finalità di "lotta contro la criminalità grave", devono subordinarsi a certe condizioni (quali categorie dei dati, mezzi interessati, persone riguardate e durata) che vanno previste da norme chiare e precise e rispondere a criteri oggettivi[124].

Proprio nel ribadire la necessità di queste previsioni, valutando l'idoneità degli obiettivi volti a giustificare le deroghe nazionali al principio di riservatezza delle comunicazioni elettroniche, la Corte richiamava la pertinente giurisprudenza di Strasburgo, in particolare i famosi casi *Zakharov c. Russia* e *Szabó e Vissy c. Ungheria*, per individuare le condizioni che consentirebbero l'accesso e precisare che quest'ultimo deve essere subordinato a un controllo preventivo di un'autorità giurisdizionale o amministrativa indipendente[125]. Tra gli aspetti particolari che prevedeva a garanzia della tutela dei dati in caso di deroghe giustificate, la Corte stabiliva anche che i fornitori di servizi dovessero "*garantire un livello particolarmente elevato di protezione e di sicurezza mediante misure tecniche e organizzative appropriate. In particolare, la normativa nazionale deve prevedere la conservazione nel territorio dell'Unione nonché la distruzione irreversibile dei dati al termine della durata di conservazione degli stessi*"[126], richiamando – più volte – per analogia la sentenza

[123] Ibidem, p. 105.
[124] Ibidem, pp. 107-112, e si vedano anche i punti 117-118.
Il riferimento è ai casi Corte europea dei diritti umani, ricorso n. 47143/06, *Zakharov c. Russia*, 4 dicembre 2015, p. 260; ricorso n. 37138/14, *Szabó e Vissy c. Ungheria*, 12 gennaio 2016, pp. 77 e 80.
[125] Corte di giustizia, *Tele2 Sverige* e *Watson, cit*., punti 119-120.
[126] Ibidem, p. 122.

DRI, per concludere infine che le normative nazionali esaminate, nelle loro previsioni generalizzate, non fossero compatibili con l'articolo 15 letto alla luce della Carta[127].

Rispetto agli aspetti che peculiarmente la Corte enfatizzava, veniva già notato a caldo che «*Some of these points will be difficult to reconcile with the current regime in the United Kingdom regarding communications data*»[128], rilievo particolarmente interessante perché effettivamente divenuto oggetto di più recenti questioni anche dinanzi ai giudici di Lussemburgo, come vedremo a breve, oltre che per le implicazioni nell'era post-Brexit.

Inoltre, va enfatizzato il richiamo esplicito alle pronunce (e, dunque, all'orientamento interpretativo) della Corte EDU in materia, che rende questa sentenza particolarmente emblematica della suddetta contaminazione dei modelli interpretativi tra giudici europei, quale elemento performativo del processo di integrazione (anche in vista della sovranità digitale dell'Unione) e, in questo caso ancor più specificamente, del suddetto *Strasbourg effect* proposto da Bygrave (*supra*, Capitolo I, Parte III). Contaminazione che, però, come la Corte tiene a precisare, non significa confusione negli ambiti di intervento: laddove il giudice di rinvio britannico chiedeva se l'interpretazione della *DRI* andasse oltre l'articolo 8 CEDU, i giudici lussemburghesi chiarivano che la direttiva *e-privacy* va interpretata (da Lussemburgo) *soltanto* alla luce della Carta[129]. Piuttosto, detta contaminazione potrebbe rappresentare un esempio di coerenza tra le due Corti, specie nel delicato settore della sorveglianza: «*Despite emphasising that the ECHR is not part of EU law, the Court relies on two recent cases from the ECtHR, perhaps seeking to emphasis the consistency in this area between the two courts – or perhaps seeking to put pressure on Strasbourg to hold the line as it faces a number of state surveillance cases on its own docket, many against the UK*»[130]. Ed invero, le pronunce di Strasburgo sul sistema di sicurezza previsto in Regno Unito assumono particolare rilievo per la Corte di giustizia, non solo per la soluzione di casi analoghi riguardanti lo Stato membro e la compatibilità con disposizioni sovranazionali, come vedremo a breve.

Raffronti con la Corte di Strasburgo

[127] Cfr, *ex multis*, G. CAGGIANO, Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione, in *MediaLaws – Rivista di Diritto dei Media*, n. 2/2018, p. 76, laddove sottolinea l'importanza, emersa dalla pronuncia, dell'obbligo di interpretazione conforme alla Carta da parte delle autorità nazionali nell'applicare il diritto dell'Unione.
[128] L. WOODS, Data retention and national law, *cit*. L'autrice commentava, nondimeno: «*More generally, the Court's analysis – by comparison with that of the Advocate General – was less detailed and structured, particularly about the meaning of necessity and proportionality*».
[129] Corte di giustizia, *Tele2 Sverige* e *Watson*, pp. 126-133.
[130] L. WOODS, Data retention and national law, *cit*.

Tra gli interessanti interventi della Corte di Strasburgo nel delicato settore della sorveglianza (in particolare, si ricordino, tra le numerose relative al Regno Unito, le pronunce sui casi *Allan* e *Kennedy*, nonché il già discusso *Klass*)[131], i casi citati dalla Corte di giustizia (*Zakharov* e *Szabo*) meritano attenzione per varie ragioni. Anzitutto, in essi la Corte conferma il proprio orientamento nell'affrontare questioni relative a misure statali di sorveglianza, rispetto alle quali una prova della violazione da parte del ricorrente risulta particolarmente complessa, reiterando così (ben oltre le previsioni dell'articolo 34 CEDU) la propria valutazione "in astratto"[132].

Entrambi i casi coinvolgevano legislazioni nazionali che prevedevano misure di sorveglianza ai fini di contrasto al terrorismo. Il caso russo riguardava l'intercettazione di comunicazioni elettroniche, che i fornitori dei servizi di telefonia avrebbero consentito al Servizio federale di sicurezza senza una preventiva autorizzazione da parte di un'autorità giudiziaria. Nel caso ungherese i ricorrenti lamentavano che la legislazione non fornisse abbastanza garanzie rispetto agli abusi nella sorveglianza, peraltro non autorizzata da un'autorità giurisdizionale. In entrambi i casi, la Corte riconosceva le previsioni nazionali sulla sorveglianza in violazione dell'articolo 8 CEDU.

L'importanza della pronuncia *Zakharov*, anche rispetto a valutazioni della Corte di giustizia, risiede nel fatto che, pur non riguardando uno Stato membro dell'Unione, in essa la Corte di Strasburgo individuava gli standard che una legislazione sulla sorveglianza dovrebbe seguire per garantire una protezione adeguata dei diritti degli interessati, assumendo quindi le sue considerazioni un respiro

[131] Corte europea dei diritti umani, ricorso n. 48539/99, *Allan c. Regno Unito*, 5 novembre 2002, in cui la Corte accertò una violazione dell'articolo 8 CEDU rispetto alla registrazione di conversazioni private di un detenuto per mancanza di leggi che disciplinassero l'uso di dispositivi di registrazione segreta nelle carceri da parte della polizia.
Corte europea dei diritti umani, ricorso n. 26839/05, *Kennedy c. Regno Unito*, 18 agosto 2010, in cui, pur non avendo ravvisato una violazione dell'articolo 8 (né 13, quanto ai rimedi interni) CEDU, la Corte, dopo aver ribadito il suo approccio nella valutazione di misure di sorveglianza segreta adottato in *Klass* e *Malone* (cfr. ,punti 120-123), affermava: «*In order to assess, in a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the Court must have regard to the availability of any remedies at the national level and the risk of secret surveillance measures being applied to him. Where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by this Court*», p. 124.

[132] Così, espressamente (sulla scia di come già fatto, tra gli altri, in *Klass*, p. 33, e in *Kennedy*, p. 124), Corte europea dei diritti umani, *Zakharov*, cit.: *«The Court has consistently held in its case-law that the Convention does not provide for the institution of an* actio popularis *and that its task is not normally to review the relevant law and practice* in abstracto*, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention. (...)Thus, the Court has permitted general challenges to the relevant legislative regime in the sphere of secret surveillance in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them*», pp. 164-165, ma v. anche pp. 169, 171 e 178; *Szabó e Vissy*, cit.: «*As to the applicants' victim status, the Court has consistently held in its case-law that its task is not normally to review the relevant law and practice* in abstracto*, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention (...). However, in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has accepted that, under certain circumstances, an individual may claim to be a victim on account of the mere existence of legislation permitting secret surveillance, even if he cannot point to any concrete measures specifically affecting him*», pp. 32-33.

più ampio del caso specifico[133]. Invero, la Corte riprendeva la propria giurisprudenza in materia di misure di sorveglianza segreta per individuare le "garanzie minime" che dovrebbero essere previste dalla legge per evitare abusi di potere[134]; quindi, valutando se il perseguimento di uno scopo pur legittimo possa dirsi anche "necessario in una società democratica", la Corte affermava: «*when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by national law*»[135].

Sviluppando il ragionamento esposto nel caso russo, la Corte affrontava poi il caso ungherese esigendo in maniera ancor più rigida la predisposizione di "garanzie sufficientemente precise efficaci ed esaurienti" rispetto a sistemi di sorveglianza, pur giustificati da esigenze di pubblica sicurezza, richiamando l'attenzione – particolarmente rilevante ai nostri fini – sulla compatibilità dell'interferenza delle autorità esecutive rispetto ai diritti individuali in termini di rispetto della *rule of law*: «*The Court recalls that the rule of law implies,* inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure. In a field where abuse is*

[133] In tal senso, si veda M. D. COLE, A. VANDENDRIESSCHE, From Digital Rights Ireland and Schrems in Luxembourg to Zakharow and Szabo/Vissy in Strasbourg, in European Data Protection Law Review (EDPL), vol. 2, no. 1, 2016, p. 128: «*With Roman Zakharov v Russia the European Court of Human Rights laid down the standards secret surveillance legislation should live up to for an adequate protection of individual rights compliant with Article 8*».
V. anche M. OROFINO, Diritto alla protezione dei dati personali e sicurezza, *cit*., p. 99, che descriveva le considerazioni della Corte come «un decalogo per ogni sistema di sorveglianza adottato con finalità di antiterrorismo a tutela, quindi, della sicurezza nazionale e della sicurezza pubblica».
[134] Corte europea dei diritti umani, *Zakharov*, cit.: «*In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed*», p. 231.
[135] Ibidem, p. 232, sottolineato aggiunto.

potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge»[136].

Dunque, applicando la dottrina del margine di apprezzamento ed effettuando valutazioni rispondenti alla *rule of law*, la Corte in entrambi casi sindacava i sistemi nazionali di sorveglianza e (ancor più particolarmente per il caso ungherese, poiché riguardava uno Stato membro dell'Unione) ne rilevava l'inidoneità e dunque la violazione dell'articolo 8 CEDU. Nel farlo, peraltro, non solo forniva spunti alla Corte di giustizia – come emerse a partire dalla analizzata pronuncia *Tele2 e Watson* – ma soprattutto da essa traeva a sua volta ispirazione, come testimoniato dall'espresso richiamo in entrambe le sentenze alle considerazioni dedotte da Lussemburgo nel caso *Digital Rights Ireland* (nonché nel caso *Schrems I*, espressamente richiamato solo in *Szabo e Vissy*)[137].

Rispetto a queste interazioni tra le Corti in materia, veniva notato da un lato, con favore, un allineamento degli standard di tutela tra i due sistemi europei (specie a seguito del parere negativo della Corte di giustizia quanto all'adesione dell'Unione alla CEDU); dall'altro, comprensibilmente, il fatto che gli standard minimi così individuati risulterebbero di fatto particolarmente difficili da rispettare per ogni sistema nazionale di sorveglianza degli Stati europei[138].

Ciò presta il fianco alle considerazioni in tema di effettività della *rule of law* all'interno dell'Unione e degli Stati membri, nonché del già richiamato principio di coerenza tra azione interna ed esterna dell'Unione, specie con riguardo alle valutazioni sull'adeguatezza dei sistemi di Paesi terzi destinatari di flussi di dati dall'Unione, che verranno trattate nel prosieguo. Soprattutto, ciò denota una certa "convergenza"[139] tra gli orientamenti delle Corti europee che pare mantenersi, tendenzialmente, anche quando l'evoluzione giurisprudenziale condurrebbe verso nuovi e, in qualche modo, contrapposti atteggiamenti.

---

[136] Corte europea dei diritti umani, *Szabó e Vissy c. Ungheria*, *cit*., p. 77.
Per i riferimenti precedenti nonché le considerazioni conclusive, v. p. 89.
Sul riferimento ai criteri ancor più rigidi richiesti dalla Corte, si considerino le riflessioni di M. D. COLE, A. VANDENDRIESSCHE, From Digital Rights Ireland and Schrems in Luxembourg to Zakharow and Szabo/Vissy in Strasbourg:«*It can be deduced from these criteria that the scope of action of Member States is significantly reduced when it comes to enacting mass surveillance legislation. In Szabo and Vissy v Hungary the Court even hinted that it will hold mass surveillance legislation to even more strict standards of protection of individual rights in the future. The Court therefore indicated the course it will be embarking upon in the future, and that the principles developed in Roman Zakharov v Russia and in Szabo and Vissy vHungarywill be its starting point*», p. 128.
[137] Corte europea dei diritti umani, *Zakharov*, cit., p. 147; *Szabó e Vissy c. Ungheria*, *cit*., p. 15 (*Schrems*, pp. 13 e 15).
[138] Così M. D. COLE, A. VANDENDRIESSCHE, From Digital Rights Ireland and Schrems, cit., p. 129: «*These judgments also demonstrate an aligning of standards between Luxembourg and Strasbourg, irrespective of the current muteness between the two courts on political level after the CJEU handed down its opinion on accession of the EU to the ECHR. (…) The strict minimum standards set by both the CJEU and the ECtHR will be difficult for any European mass surveillance law to live up to, leading De Hert and Cristo bal Bocos to conclude 'the hunting has started'*».
[139] Per usare un termine che tornerà nell'analisi congiunta di BBW e Privacy International, soprattutto, proposta da M. ZALNIERIUTE, A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence, in *EJIL:Talk!*, June 4, 2021.

Il riferimento è ai casi *La Quadrature du Net* e *Privacy International* trattati in Lussemburgo nell'ottobre 2020 che, riguardando non solo/tanto l'accesso ai dati relativi alle comunicazioni da parte delle autorità statali, ma, più ampiamente, la sorveglianza di massa posta in essere dai sistemi di sicurezza nazionali, si legano inevitabilmente alla giurisprudenza di Strasburgo in materia, specie alla recentissima Grande Camera del 25 maggio 2021 sul celeberrimo caso *Big Brother Watch* (di seguito anche BBW), nonché su quello svedese *Centrum för Rättvisa* (di seguito anche CFR). Al primo, particolarmente, faremo riferimento, proprio perché relativo al sistema di sicurezza del Regno Unito e quindi per le implicazioni delle valutazioni della Corte di Strasburgo non solo rispetto alla giurisprudenza di Lussemburgo ma, più in generale, all'atteggiarsi dell'Unione europea rispetto alle previsioni del suo sistema di protezione dei dati a seguito dell'evento Brexit, conducendo così agli accennati discorsi sul funzionamento in pratica del trasferimento dei dati verso Paesi terzi.

Sulla paventata "nuova tendenza" delle Corti europee in materia di sicurezza nazionale

Per analizzare quella che può considerarsi una "nuova tendenza" delle Corti europee rispetto alle prerogative securitarie degli Stati, è necessario anzitutto chiarire la differenza tra sorveglianza mirata e sorveglianza di massa. Alla prima si riferisce, sicuramente, la giurisprudenza sovranazionale appena analizzata: come si è visto, nei casi *DRI* e *Tele2 Sverige e Watson*, la Corte di giustizia, invalidando la direttiva *data retention* e interpretando l'articolo 15 della direttiva *e-privacy*, stabiliva essenzialmente che per essere proporzionata la sorveglianza deve essere "mirata", ossia relativa a specifiche persone in presenza di certi requisiti per i propositi elencati nella norma, nel caso di specie di lotta alla criminalità "grave", la sola che potrebbe giustificare la gravità dell'ingerenza da parte della autorità pubbliche tramite l'accesso ai dati relativi alle comunicazioni elettroniche[140].

- *Corte di giustizia, Ministerio Fiscal*

In particolare, poi, sulla gravità dell'ingerenza e sulla correlazione con il carattere "grave" della criminalità da perseguire, la Corte di giustizia si soffermava nel caso *Ministerio Fiscal*, relativo proprio all'accesso da parte di autorità pubbliche ai dati per l'identificazione dei titolari di carte SIM relative a un telefono cellulare rubato. In tal caso, la Corte ha avuto l'occasione di chiarire, riprendendo e affinando *Tele2 Sverige*, che l'obiettivo di perseguimento di reati che ai sensi dell'articolo 15 della direttiva *e-privacy* consente deroghe al principio di riservatezza delle

[140] Corte di giustizia, *Tele2*, cit., punto 115.

comunicazioni giustificherebbe una grave ingerenza in casi di criminalità grave, ma non escluderebbe un'ingerenza più ridimensionata per gli altri reati: valutando, infatti, le circostanze del caso, la Corte applicava il principio di proporzionalità e deduceva che "*l'ingerenza che un accesso a tali dati comporterebbe può quindi essere giustificata dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di «reati» in generale, di cui all'articolo 15, paragrafo 1, primo periodo, della direttiva 2002/58, senza che sia necessario che tali reati siano qualificati come «gravi»*"[141]. Dunque, pur arrivando in sostanza a un diverso risultato, la Corte confermava qui quanto elaborato in *Tele2Sverige*: «*the facts in* Ministerio Fiscal *are a good example of a specific, targeted request for access to personal data accompanied by necessary safeguards such as priori judicial approval* (…)*. Thus where the interference is not serious, such as the limited identification data in this case, then less serious offences may justify access to personal data. However, applying the same principle as in Tele2, more intrusive access to the content of communications or metadata, which would permit the profiling of individuals, would only be allowed for more serious offences*»[142].

- *Corte di giustizia, Prokuratuur*

Nello stesso filone si iscrive anche la più recente pronuncia del marzo 2021 sul caso estone *Prokuratuur*, che ancora interrogava la Corte sull'interpretazione dell'articolo 15 della direttiva *e-privacy*, tramite un rinvio pregiudiziale sollevato nell'ambito di un procedimento penale a carico di *H.K.* imputato di furto, uso della carta bancaria di terzi e violenza verso partecipanti ad un procedimento giudiziario. Le questioni riguardavano: la possibilità di ammettere come elementi di prova dei processi verbali fondati su dati raccolti da comunicazioni elettroniche, dunque la compatibilità con l'articolo 15 suddetto; la proporzionalità dell'ingerenza, considerando la precedente giurisprudenza al riguardo; la possibilità di considerare il pubblico ministero estone come un'autorità indipendente ai fini del controllo preventivo per l'accesso a tali dati.

Ebbene, nel risolvere le prime questioni, la Corte affinava la propria giurisprudenza, riprendendo *Ministerio Fiscal* per insistere sulla gravità delle forme di criminalità che consentirebbero una grave ingerenza della pubblica autorità[143]. Quindi, faceva frequenti riferimenti alle argomentazioni utilizzate in *La Quadrature du Net* (che analizzeremo a breve) per spiegare come il principio di

[141] Corte di giustizia, C-207/16, *Ministerio Fiscal*, 2 ottobre 2018, p. 63.
Inoltre, il riferimento precedente è ai punti 56-57: "*In conformità al principio di proporzionalità, infatti, una grave ingerenza può essere giustificata, in materia di prevenzione, ricerca, accertamento e perseguimento di un reato, solo da un obiettivo di lotta contro la criminalità che deve essere qualificata come «grave». Al contrario, qualora l'ingerenza che comporta tale accesso non sia grave, detto accesso può essere giustificato da un obiettivo di prevenzione, ricerca, accertamento e perseguimento di un «reato» in generale*". Si veda, meglio, a partire da p. 53.
[142] C. DOCKSEY, H. HIJMANS, The Court of Justice as a Key Player in Privacy and Data protection, *cit.*, p. 312.
[143] Corte di giustizia, C-746/18, *Procedimento penale a carico di H.K (Prokuratuur)*, sentenza del 2 marzo 2021, p. 35.

proporzionalità (secondo consolidata giurisprudenza) impone che le deroghe alla protezione dei dati siano limitate allo stretto necessario, ma soprattutto per ribadire i principi (ivi esplicitati, come vedremo) di *equivalenza* ed *effettività* nel definire che, "allo stato attuale del diritto dell'Unione" (sic!, p. 41), tocca al diritto interno dello Stato membro predisporre regole per l'ammissibilità di prove ottenute tramite la conservazione generalizzata di dati non conforme al diritto dell'Unione: «*in assenza di norme dell'Unione in materia, spetta all'ordinamento giuridico interno di ciascuno Stato membro, in virtù del principio dell'autonomia procedurale, stabilire le regole di procedura applicabili ai ricorsi giurisdizionali destinati a garantire la tutela dei diritti riconosciuti ai singoli dal diritto dell'Unione, a condizione però che le regole suddette non siano meno favorevoli di quelle disciplinanti situazioni analoghe assoggettate al diritto interno (principio di equivalenza) e che non rendano impossibile in pratica o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'Unione (principio di effettività)*»[144].

Sulla base di simili considerazioni, la Corte dunque risolveva le prime due questioni interpretando l'articolo 15 nel senso che la normativa nazionale analizzata, nella misura in cui consentiva l'accesso di autorità pubbliche ai dati relativi al traffico o all'ubicazione, ancorché per finalità di prevenzione e perseguimento di reati, ma «*senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo*», dovesse considerarsi ad esso contraria[145]. Inoltre, interpretando la medesima disposizione alla luce della Carta, la Corte escludeva che il pubblico ministero, incaricato di dirigere il procedimento istruttorio, potesse considerarsi autorità indipendente per autorizzare l'accesso ai dati, non potendo "*dirimere in piena indipendenza una controversia*" rispetto alla quale sarebbe parte nel procedimento penale[146].

[144] Ibidem, p. 42, ma si vedano anche i punti 41 e 43.
[145] Ibidem, p. 45, sottolineato aggiunto.
[146] Ibidem, punti 54-56: «*Dalle considerazioni che precedono risulta che il requisito di indipendenza che l'autorità incaricata di esercitare il controllo preventivo deve soddisfare, ricordato al punto 51 della presente sentenza, impone che tale autorità abbia la qualità di terzo rispetto a quella che chiede l'accesso ai dati, di modo che la prima sia in grado di esercitare tale controllo in modo obiettivo e imparziale al riparo da qualsiasi influenza esterna. In particolare, in ambito penale, il requisito di indipendenza implica, come rilevato in sostanza dall'avvocato generale al paragrafo 126 delle sue conclusioni, che l'autorità incaricata di tale controllo preventivo, da un lato, non sia coinvolta nella conduzione dell'indagine penale di cui trattasi e, dall'altro, abbia una posizione di neutralità nei confronti delle parti del procedimento penale. Ciò non si verifica nel caso di un pubblico ministero che dirige il procedimento di indagine ed esercita, se del caso, l'azione penale. Infatti, il pubblico ministero non ha il compito di dirimere in piena indipendenza una controversia, bensì quello di sottoporla, se del caso, al giudice competente, in quanto parte nel processo che esercita l'azione penale. La circostanza che il pubblico ministero sia tenuto, conformemente alle norme che disciplinano le sue competenze e il suo status, a verificare gli elementi a carico e quelli a discarico, a garantire la*

In questi termini, dunque, tale pronuncia, che ribadiamo riguarda il trattamento di dati nell'ambito di un'indagine penale, parrebbe (ri)confermare l'orientamento "pro-privacy" emerso da *DRI* e confermato con *Tele2* e *Watson* e, in linea teorica, anche *Ministerio Fiscal*, mentre si allontanerebbe, per certi aspetti, dalle ultime pronunce più "morbide" dell'ottobre 2020: «*While the court's first decisions clearly upheld the necessity of protecting privacy, the subsequent decisions specified and relativised the conditions for data retention. This decision, however, prevents softening the requirements even further. Instead, the interpretation of art. 15 regarding access to traffic and location data is restricted to investigating serious crimes (…). However, defining what constitutes a serious crime is still up to the Member States*»[147].

In realtà, riteniamo più correttamente che il punto di contatto tra quest'ultima pronuncia e la giurisprudenza meno recente sia dato proprio dal fatto che essa, come quella giurisprudenza, riguardi situazioni di sorveglianza mirata, ovvero essenzialmente legate alla conservazione di dati per l'accesso da parte delle autorità pubbliche e tendenzialmente nell'ambito di un'indagine penale. Altra cosa, invece, quanto alla sorveglianza di massa legata a esigenze più generali di sicurezza nazionale (e dunque, dell'ambito di intervento dei servizi di *intelligence*), più frequentemente trattata dalla Corte di Strasburgo, che proprio le pronunce di ottobre hanno preso in considerazione, in una prospettiva che, quanto a quegli aspetti, è stata ribadita anche nei richiami ad esse fatti dalla Corte in *Prokuratuur* (cfr, punto 33) e che, dunque, appare (pericolosamente?) in linea, come si accennava, con ultime considerazioni della Grande Camera della Corte EDU.

In buona sostanza, la distinzione tra sorveglianza mirata e di massa implica che la seconda venga effettuata, sì, per esigenze di pubblica sicurezza, ma che siano tali da escludere la necessità di un sospetto rispetto a specifiche persone o circostanze, permettendo un controllo *generalizzato nei confronti di chiunque* (e coinvolgendo, quindi, l'attività dei servizi di sicurezza, e non dell'autorità pubblica rispetto ad attività di rilievo penale): «*The particular problem is that surveillance has historically been considered from the perspective of individual surveillance, where a person may be the subject of surveillance when there are reasonable grounds for suspicion. The very nature of bulk data acquisition and intelligence gathering means that there is no such suspicion*»[148].

- *Corte EDU, Big Brother Watch (2018)*

---

legittimità del procedimento istruttorio e ad agire unicamente in base alla legge ed al suo convincimento non può essere sufficiente per conferirgli lo status di terzo rispetto agli interessi in gioco». Si vedano anche punti 49-53.

[147] S. ROVELLI, Case *Prokuratuur*: Proportionality and the Independence of Authorities in Data Retention, in *European Papers*, Vol. 6, 2021, No. 1, p. 207.

[148] L. WOODS, Big Brother Watch v UK: the ECtHR Grand Chamber rules on mass surveillance, in *EU Law Analysis*, 17 June 2021.

Invero, già nella prima pronuncia del 2018 relativa al caso *BBW*, la Corte EDU richiamava la propria giurisprudenza sulla sorveglianza di massa (in particolare *Weber* e *Liberty*) per confermare la ravvisata compatibilità di simili regimi nazionali con le previsioni della CEDU, ancorché nel rispetto di determinati requisiti e per il perseguimento di uno scopo legittimo, in quanto rientranti nel margine di apprezzamento riconosciuto agli Stati per esigenze di sicurezza nazionale: «*The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security* (…). *Furthermore, in* Weber and Saravia *and* Liberty and Others *the Court accepted that bulk interception regimes did not* per se *fall outside this margin. Although both of these cases are now more than ten years old, given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the Internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation. Nevertheless, as indicated previously, it is evident from the Court's case-law over several decades that all interception regimes (both bulk and targeted) have the potential to be abused, especially where the true breadth of the authorities' discretion to intercept cannot be discerned from the relevant legislation (see, for example,* Roman Zakharov… *and* Szabó and Vissy v. Hungary*…). Therefore, while States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security, the discretion afforded to them in operating an interception regime must necessarily be narrower*», facendo poi riferimento ai sei requisiti minimi elaborati in *Weber* da soddisfare per ridurre il rischio di abusi di potere (tanto nei casi di sorveglianza mirata che di massa)[149].

Il caso, com'è noto, riguardava tre ricorsi presentati da ben 16 ricorrenti a seguito delle rilevazioni di Edward Snowden (come avvenne per la saga *Schrems* in Lussemburgo) relative ai programmi di sorveglianza elettronica operati dai servizi di *intelligence* in USA e Regno Unito, volti a contestare il regime di sorveglianza predisposto nel Regno Unito, essenzialmente per come previsto dal RIPA (*Regulation of Investigatory Powers Act* 2000, per certi aspetti sostituito dal IPA, *Investigatory Powers Act* 2016, non sindacato dalla Corte nel 2018) per mancanza delle necessarie garanzie richieste dagli articoli 8, 10 e 6 CEDU. In particolare, rispetto alle doglianze sull'articolo 8 CEDU, i

[149] Corte europea dei diritti umani, ricorsi n. 58170/13, 62322/14 e 24960/15, *Big Brother Watch and others v. UK*, 13 settembre 2018, pp. 314-315.

ricorrenti ritenevano che le loro comunicazioni elettroniche fossero state intercettate dai servizi segreti britannici, ottenute da questi dopo essere state intercettate da servizi di *intelligence* stranieri, ovvero acquisite dalle autorità britanniche da parte di fornitori di servizi di comunicazione (*Communication Service Providers*, di seguito anche CSPs)[150]. Pertanto, erano tre i regimi sottoposti al vaglio della Corte: il regime previsto dalla sezione 8(4) del RIPA, relativo alla intercettazione generalizzata di comunicazioni da parte dei servizi segreti britannici; il regime di condivisione dei dati con partners di intelligence stranieri (in particolare USA, nell'ambito dei programmi PRISM e Upstream); il regime di cui al Capitolo II del RIPA sull'acquisizione dei dati delle comunicazioni[151].

Senza approfondire la già complessa e articolata pronuncia, che peraltro, oltre a replicare l'applicazione dei sei requisiti stabiliti in *Weber* e altra precedente giurisprudenza in materia, richiamava anche giurisprudenza UE per avvalorare l'analisi condotta sul sistema britannico, basti dire che la Prima Sezione della Corte di Strasburgo concludeva che i regimi di cui alla Sezione 8(4) e del Capitolo II RIPA fossero in violazione dell'articolo 8 CEDU, ma di non riscontrare una violazione quanto alla condivisione di informazioni con i servizi di *intelligence* USA[152].

Come veniva immediatamente rilevato, tale pronuncia, a seconda del punto di vista, poteva essere considerata una conferma della possibilità di consentire la sorveglianza di massa (così ai suddetti punti 314-15) ovvero una riconosciuta insufficienza del regime predisposto dal RIPA e, dunque, nella misura in cui lo riprendeva, delle previsioni del successivo IPA[153]. Nondimeno, a fronte delle variegate critiche alle quali si prestava e alle perplessità che manteneva[154], nel malcontento dei

[150] Ibidem, punti 7-8.
[151] Ibidem, rispettivamente: punti 270 ss.; 389 ss.; 450 ss.
[152] Ibidem, punti 4-6 del dispositivo.
[153] Così, L. WOODS, Analysis of the ECtHR judgment in Big Brother Watch: part 2, in *EU Law Analysis*, 20 September 2018.
[154] Ibidem, per esempio, si condivide il seguente rilievo: «*The Court's response is detailed and considered but -in the end – perhaps overly deferential to a set of institutions which seemed happily unaware of the practices of the security and intelligence services*». Per commenti di tenore critico si veda anche: T. FALCHETTA, Intelligence Sharing and the Right to Privacy after the European Court Judgment in Big Brother Watch v. UK, in *EJIL: Talk!*, September 24, 2018: «*The Court's findings are sorely overdue. Intelligence sharing is one of the most pervasive, and least regulated, surveillance practices in the modern world. Such sharing is facilitated by rapidly changing technology that has allowed for the storage and transfer of vast amounts of data within and between countries*»; J. VERMEULEN, Big brother may continue watching you, in *Strasburgobservers*, October 12, 2018; E. WATT, Much Ado About Mass Surveillance – the ECtHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK, in *Strasbourgobservers*, June 28, 2021, che rispetto alla pronuncia del 2018 poneva in risalto due aspetti: «*The judgment made it clear that in so far as the conducting of bulk interception of foreign communications is concerned, the ECtHR will pursue its earlier approach laid down in Weber and Liberty in that it does not concern itself with their legality vis-à-vis states' obligations under Article 8, but rather with whether the manner of their operation meets the necessary standards. Second, the applicants contended that the requirement of 'reasonable suspicion' introduced in Zakharov should equally be applicable to bulk systems. This claim was rejected as the Court reasoned that 'bulk interception is by definition untargeted and to require "reasonable suspicion" would render the operation of such a scheme impossible' (para 317)*».

ricorrenti, il caso venne deferito alla Grande Camera che si è definitivamente pronunciata lo scorso 25 maggio 2021.

Sicuramente, risultava confermato dalla pronuncia del 2018 che a Strasburgo i regimi di sorveglianza di massa *non* fossero considerati incompatibili con le previsioni della CEDU, nonostante le condizioni mutate dalla pervasività del progresso tecnologico (rispetto alle precedenti pronunce del medesimo tenore). Pertanto, risalta che nell'opinione parzialmente dissenziente i giudici Pardalos ed Eicke rilevassero come l'approccio della Corte di Strasburgo fosse in chiaro contrasto rispetto alla giurisprudenza della Corte di giustizia dell'Unione europea, audacemente garantista – come si è visto *supra* – rispetto all'accesso ai dati delle comunicazioni da parte delle autorità pubbliche[155].

Eppure, è proprio a partire dal periodo successivo alla pronuncia di Strasburgo che sarebbe, invece, possibile ravvisare un approccio differente della Corte di giustizia e, così, una "*dangerous convergence*"[156] tra le due Corti europee in materia.

- *Corte di giustizia, Privacy International e La Quadrature du Net e altri*

Ci riferiamo ai casi decisi il 6 ottobre 2020 dalla Corte di giustizia, *La Quadrature du Net* e *Privacy International*, relativi, ancora una volta, all'interpretazione (prevalentemente) dell'articolo 15 della direttiva *e-privacy* ma implicanti, finalmente, sorveglianza non solo mirata ma anche generalizzata. In entrambi i casi, la Corte ha riconosciuto che la lettura della direttiva *e-privacy* alla luce delle disposizioni della Carta escluderebbe in linea generale la conservazione e generalizzata e indifferenziata di dati relativi al traffico e all'ubicazione. Nondimeno, in *La Quadrature du Net* la Corte sembrerebbe ammettere misure legislative statali che la consentirebbero per esigenze di sicurezza nazionale[157], cosa che denoterebbe un mutamento di approccio in Lussemburgo.

Il caso *Privacy International*, invero, è quello più in linea con l'orientamento della pregressa giurisprudenza.

Si trattava di un rinvio pregiudiziale sollevato nell'ambito di una controversia tra la ONG e i Ministri degli Esteri e dell'Interno nonché i servizi di sicurezza e intelligence del Regno Unito, relativa alla legittimità della normativa che consentiva a quei servizi l'acquisizione e l'utilizzo di dati di comunicazione in massa (c.d. *bulk communications data*) a seguito della pubblicazione nel

[155] JOINT PARTLY DISSENTING AND PARTLY CONCURRING OPINION OF JUDGES PARDALOS AND EICKE, p. 22.
[156] Si riprende così la formulazione utilizzata da M. ZALNIERIUTE, A Dangerous Convergence: The Inevitability of Mass Surveillance, *cit*., ma svariati sono i commenti nello stesso senso, come si vedrà.
[157] M. ZALNIERIUTE, A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union, in *Modern Law Review*, Vol 85(1) 2022 *forthcoming*, [2021] UNSWLRS 34, p. 1.

2015 di un rapporto che spiegava le pratiche effettuate in ottemperanza a quelle previsioni. La normativa contestata era, quindi, il *Telecommunications Act* del 1984 che, come il giudice di rinvio precisava, si distingueva dal regime previsto dal DRIPA e oggetto della pronuncia *Tele2 e Watson*[158] riguardante, lo si ripete, l'accesso ai dati delle comunicazioni da parte delle autorità pubbliche per il perseguimento di reati. Lo stesso giudice del rinvio, poi, richiamando la sentenza *Parlamento c. Consiglio* sul trasferimento dei dati PNR (trattata *supra*), considerava «*che le attività delle società commerciali nell'ambito del trattamento e del trasferimento di dati al fine di tutelare la sicurezza nazionale non sembrano rientrare nell'ambito di applicazione del diritto dell'Unione. Occorrerebbe verificare non se l'attività controversa costituisca un trattamento di dati, ma soltanto se, nella sua sostanza e nei suoi effetti, l'oggetto di tale attività sia quello di supportare una funzione essenziale dello Stato, ai sensi dell'articolo 4, paragrafo 2, TUE, nell'ambito di un quadro stabilito dai pubblici poteri in ordine alla pubblica sicurezza. Nell'ipotesi in cui le misure controverse nel procedimento principale rientrassero tuttavia nell'ambito di applicazione del diritto dell'Unione, il giudice del rinvio ritiene che le prescrizioni di cui ai punti da 119 a 125 della sentenza del 21 dicembre 2016, Tele2 (…), appaiano inadeguate nel contesto della sicurezza nazionale e siano tali da ostacolare la capacità dei servizi di sicurezza e di intelligence di far fronte a talune minacce alla sicurezza nazionale*»[159].

Ebbene, rispondendo alla prima questione sulla possibilità di comprendere la normativa nazionale nell'ambito di applicazione della direttiva *e-privacy* (in particolare, il suo articolo 1 letto alla luce dell'articolo 4, par. 2 TUE), la Corte riteneva la giurisprudenza *Parlamento c. Consiglio* non trasponibile al caso di specie e suggeriva di considerare l'autore del trattamento dei dati per stabilire

[158] Corte di giustizia, C-623/17, *Privacy International*, 6 ottobre 2020, pp. 24-26: «*Secondo detto giudice, il regime controverso nel procedimento principale si distingue da quello risultante dal Data Retention and Investigatory Powers Act 2014 (legge del 2014 sulla conservazione dei dati e sui poteri d'indagine), controverso nella causa che ha dato luogo alla sentenza del 21 dicembre 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970), poiché quest'ultimo regime prevedeva la conservazione dei dati da parte dei fornitori di servizi di comunicazione elettronica e la loro messa a disposizione, nell'interesse della sicurezza nazionale, non soltanto dei servizi di sicurezza e di intelligence, ma anche di altre autorità pubbliche, in relazione alle loro esigenze. Tale sentenza avrebbe peraltro riguardato un'indagine penale e non la sicurezza nazionale. Il giudice del rinvio aggiunge che le banche dati costituite dai servizi di sicurezza e di intelligence formano oggetto di un'elaborazione di massa e automatizzata, non specifica, diretta a rivelare l'esistenza di eventuali minacce ignote. A tal fine, tale giudice afferma che gli aggregati di metadati così costituiti dovrebbero essere il più possibile completi, al fine di poter disporre di un «pagliaio» per trovare l'«ago» che vi si cela. Riguardo all'utilità della raccolta di dati in massa da parte di detti servizi e delle tecniche di consultazione di tali dati, detto giudice fa riferimento in particolare alle conclusioni del rapporto redatto il 19 agosto 2016 dal sig. David Anderson, QC, all'epoca United Kingdom Independent Reviewer of Terrorism Legislation (controllore indipendente del Regno Unito della legislazione relativa al terrorismo), e che si sarebbe fondato, per redigere tale rapporto, su un esame effettuato da un gruppo di specialisti dell'intelligence e sulla testimonianza di agenti dei servizi di sicurezza e di intelligence. Il giudice del rinvio precisa altresì che, secondo la Privacy International, il regime controverso nel procedimento principale è illegittimo alla luce del diritto dell'Unione, mentre i convenuti nel procedimento principale ritengono che l'obbligo di trasmissione dei dati previsto da tale regime, l'accesso a tali dati nonché il loro utilizzo non rientrino nelle competenze dell'Unione, conformemente, in particolare, all'articolo 4, paragrafo 2, TUE, ai sensi del quale la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro*».

[159] Ibidem, pp. 27-28.

se quest'ultimo rientrasse o meno nell'ambito di applicazione del diritto dell'Unione: «*l'insieme dei trattamenti di dati personali effettuati dai fornitori di servizi di comunicazione elettronica rientra nell'ambito di applicazione di detta direttiva, ivi compresi i trattamenti derivanti da obblighi loro imposti dai pubblici poteri, mentre questi ultimi trattamenti potevano, eventualmente, rientrare nell'ambito di applicazione dell'eccezione prevista all'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, tenuto conto della formulazione più ampia di tale disposizione, riguardante l'insieme dei trattamenti, a prescindere dal loro autore, aventi ad oggetto la pubblica sicurezza, la difesa o la sicurezza dello Stato*». Ricordando, poi, che la direttiva è stata abrogata dal GDPR, la Corte chiariva che "*se è vero che detto regolamento precisa, all'articolo 2, paragrafo 2, lettera d), che esso non si applica ai trattamenti effettuati «dalle autorità competenti» a fini, in particolare, di prevenzione e di accertamento di reati, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse, risulta dall'articolo 23, paragrafo 1, lettere d) e h), dello stesso regolamento che i trattamenti di dati personali effettuati a questi stessi fini da privati rientrano nell'ambito di applicazione di quest'ultimo. Ne consegue che l'interpretazione dell'articolo 1, paragrafo 3, dell'articolo 3 e dell'articolo 15, paragrafo 1, della direttiva 2002/58 che precede è coerente con la delimitazione dell'ambito di applicazione del regolamento 2016/679 che tale direttiva completa e precisa. Invece, quando gli Stati membri adottano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche, senza imporre obblighi di trattamento ai fornitori di servizi di tali comunicazioni, la tutela dei dati delle persone interessate rientra non già nell'ambito di applicazione della direttiva 2002/58 ma in quello del solo diritto nazionale, fatta salva l'applicazione della direttiva (UE) 2016/680*"[160].

In tal modo la Corte risolveva la prima questione ritenendo che rientrasse nell'ambito di applicazione del diritto dell'Unione «*una normativa nazionale che consente a un'autorità statale di imporre ai fornitori di servizi di comunicazione elettronica di trasmettere ai servizi di sicurezza e di intelligence dati relativi al traffico e dati relativi all'ubicazione ai fini della salvaguardia della sicurezza nazionale*».

Ciò posto, la Corte affrontava poi la seconda questione, sulla compatibilità dell'articolo 15 della direttiva e-privacy, letto alla luce dell'articolo 4 TUE e della Carta, con una normativa nazionale che consente alla pubblica autorità di imporre ai fornitori di servizi di comunicazione elettronica una trasmissione generalizzata e indifferenziata dei dati di comunicazione ai servizi di *intelligence* per motivi di sicurezza nazionale. Richiamando la propria giurisprudenza ed effettuando il necessario vaglio di proporzionalità, pur tenuto conto delle deroghe previste dalla normativa

[160] Ibidem, pp. 47-48.

sovranazionale e delle possibilità di porre limiti ai diritti per esigenze di sicurezza, la Corte concludeva che «*Dato che la trasmissione dei dati relativi al traffico e dei dati relativi all'ubicazione avviene in maniera generalizzata e indifferenziata, essa riguarda in maniera globale l'insieme delle persone che fanno uso dei sistemi di comunicazione elettronica. Essa si applica quindi anche a persone per le quali non esiste alcun indizio tale da far credere che il loro comportamento possa avere un nesso, ancorché indiretto o remoto, con l'obiettivo di salvaguardia della sicurezza nazionale e, in particolare, senza che sia accertata una correlazione tra i dati di cui è prevista la trasmissione e una minaccia per la sicurezza nazionale (…). Tenuto conto del fatto che la trasmissione di tali dati alle autorità pubbliche equivale (…) ad un accesso, si deve ritenere che una normativa che consente una trasmissione generalizzata e indifferenziata dei dati alle autorità pubbliche implichi un accesso generale. Ne consegue che una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica di procedere alla comunicazione mediante trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence eccede i limiti dello stretto necessario e non può essere considerata giustificata in una società democratica, così come richiesto dall'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce dell'articolo 4, paragrafo 2, TUE nonché degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta*»[161].

Qui, dunque, una chiara conferma dell'approccio "*proprio*" della Corte di giustizia rispetto a questioni di tutela dei dati personali, specie rispetto ad esigenze di sicurezza nazionale, e quindi implicanti i "classici" equilibri tra principi fondanti della *rule of law*. La pronuncia assume rilievo soprattutto se si considera che oggetto di analisi era il regime del Regno Unito, rendendola così ancor più interessante rispetto alle valutazioni di Strasburgo in *BBW*.

In questo senso, la pronuncia è stata quindi considerata una "*easy victory*"[162] per la protezione dei dati e un passo avanti rispetto al filone *Tele2*: «*In the most recent and relevant case to Big Brother Watch – Privacy International (…) the CJEU unequivocally ruled that mass transmission of personal data by commercial operators to UK intelligence agencies is not consistent with EU law. The CJEU thus reiterated its strong position in Tele 2 Sverige, prohibiting bulk transmission and interception of personal data. Yet, because Tele 2 Sverige concerned data retention regimes for the purposes of combatting crime, Privacy International went a step further and imposed the same demands on the intelligence agencies. And if the intelligence agencies are not allowed to demand*

[161] Ibidem, pp. 80-81.
[162] Così la descrive J. SAJFERT, Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy, in *European Law Blog*, 26 October 2020, contrapponendola, invece, a *La Quadrature du Net*, intesa piuttosto come "*a complex victory for the law enforcement community and a major step back in the Court's data retention jurisprudence*".

bulk data transmission from service providers for the purposes of national security, no other agencies are in any other context»[163]. La stessa autrice, peraltro, acutamente rilevava, altrove, l'impatto di questa decisione sulla delimitazione di competenze tra gli Stati membri e l'Unione: «*These rulings suggest that the CJEU has become an important actor in the national security landscape, which has traditionally been outside the scope of the European integration but has increasingly become a ground for political struggle between the EU institutions and Member States*»[164]. Per queste ragioni, risulta invece peculiare la decisione assunta dalla Corte nell'altra pronuncia.

Nelle cause riunite *La Quadrature du Net e altri* la Corte di giustizia veniva interrogata sull'interpretazione dell'articolo 15 della direttiva *e-privacy* (nonché di alcune norme della direttiva *e-commerce*, dichiarata in realtà non applicabile ai casi di specie) rispetto ai regimi di conservazione dei dati di comunicazione previsti in Francia, dopo gli attacchi terroristici a *Charlie Hebdo* e *Bataclan*, e in Belgio, con una legge del 2016, alla luce della Carta e dell'articolo 4 TUE.

In realtà, la pronuncia non parrebbe discostarsi del tutto dalla precedente giurisprudenza, come invece sembrerebbe dalla mole di commenti (in parte anticipati) che in essa vedrebbero un tramutato orientamento della Corte di giustizia di apertura alla conservazione generalizzata dei dati per la salvaguardia di prerogative securitarie. Peraltro, la circostanza che il giudice relatore (T. von Danwitz, notoriamente sensibile all'affermazione delle garanzie individuali a livello sovranazionale) sia sempre lo stesso, non solo di *Privacy International*, ma anche di tutte le pronunce analizzate in materia, potrebbe già di per sé suggerire di guardare con prudenza al deplorato *revirement* della Corte.

Certo è, però, che con tale pronuncia viene aperto uno spiraglio in tal senso, laddove prima pareva netta l'incompatibilità di forme di conservazione generalizzata dai dati con il diritto dell'Unione. In realtà, si tratterebbe piuttosto del fatto che, ancorché confermando le conclusioni precedenti sull'interpretazione dell'articolo 15, in questo caso "*la Corte fornisce precisazioni, in particolare, sulla portata dei poteri che tale direttiva riconosce agli Stati membri in materia di conservazione di tali dati ai fini summenzionati*"[165]. Si tratta, infatti, di precisazioni rispetto a questioni non affrontate sino ad allora nell'interpretazione della controversa norma della direttiva *e-privacy*.

[163] M. ZALNIERIUTE, A Dangerous Convergence: The Inevitability of Mass Surveillance, *cit*.
[164] M. ZALNIERIUTE, A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union, in *Modern Law Review*, Vol 85(1) 2022 *forthcoming*, [2021] UNSWLRS 34, p. 3.
[165] Così si legge dalla relazione di sintesi, disponibile qui: https://curia.europa.eu/juris/document/document.jsf?docid=232121&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=IT&cid=22718350#Footnote5 .

Appare significativo, quindi, il modo in cui la Corte avvia la sua analisi: «*Si deve osservare che l'obiettivo di salvaguardia della sicurezza nazionale, evocato dai giudici del rinvio e dai governi che hanno presentato osservazioni, non è ancora stato specificamente esaminato dalla Corte nelle sentenze che interpretano la direttiva 2002/58. A tal riguardo, si deve anzitutto rilevare che l'articolo 4, paragrafo 2, TUE stabilisce che la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro. Detta competenza corrisponde all'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società e comprende la prevenzione e la repressione di attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese, e in particolare da minacciare direttamente la società, la popolazione o lo Stato in quanto tale, quali in particolare le attività di terrorismo. Orbene, l'importanza dell'obiettivo di salvaguardia della sicurezza nazionale, letto alla luce dell'articolo 4, paragrafo 2, TUE, supera quella degli altri obiettivi di cui all'articolo 15, paragrafo 1, della direttiva 2002/58, in particolare degli obiettivi di lotta alla criminalità in generale, anche grave, e di salvaguardia della sicurezza pubblica. Infatti, minacce come quelle menzionate al punto precedente si distinguono, per la loro natura e la loro particolare gravità, dal rischio generale che si verifichino tensioni o perturbazioni, anche gravi, della pubblica sicurezza. Fatto salvo il rispetto degli altri requisiti previsti all'articolo 52, paragrafo 1, della Carta, l'obiettivo di salvaguardia della sicurezza nazionale è quindi idoneo a giustificare misure che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero giustificare tali altri obiettivi*»[166]. È a partire da simili premesse che va inteso il ragionamento sviluppato nella pronuncia.

In sostanza, la Corte, intanto ribadiva che l'interpretazione dell'articolo 15 alla luce della Carta non consente in linea di principio misure legislative che prevedono a titolo preventivo la conservazione generalizzata e indiscriminata dei dati relativi al traffico e all'ubicazione, mentre non esclude, a certe condizioni, misure di conservazione mirata, così confermando, soprattutto, *Tele2*[167]. Tuttavia, essa introduceva un elemento di novità, specificando i casi nei quali, alla luce delle suddette premesse, l'articolo 15 non escluderebbe neppure misure di conservazione *generalizzata e indifferenziata* di dati relativi al traffico e all'ubicazione, nonché di indirizzi IP e dei correlati dati relativi all'identità civile degli utenti: l'ingerenza particolarmente grave data dalla conservazione generalizzata nonché dall'analisi automatizzata dei dati raccolti «*possono soddisfare il requisito di proporzionalità solo in situazioni nelle quali uno Stato membro si trovi di fronte ad una minaccia*

[166] Corte di giustizia, cause riunite C-511/18, C-512/18, C-520/18, *La Quadrature du Net e altri*, 6 ottobre 2020, pp. 134-136, sottolineato aggiunto.
[167] Ibidem, punti 117-119 e 132, nonché soprattutto 140-144; per la conservazione mirata v. punti 147-151 e 168.

grave per la sicurezza nazionale che risulti reale e attuale o prevedibile, e a condizione che la durata di tale conservazione sia limitata allo stretto necessario»[168].

Nonostante le attenzioni rispetto alla necessità che simile conservazione indiscriminata sia "*soggetta a limitazioni ed accompagnarsi a garanzie rigorose che consentano di proteggere efficacemente i dati personali degli interessati contro il rischio di abusi*", è per queste conclusioni che molti hanno ravvisato un "cambio di paradigma" nell'approccio della Corte di giustizia, probabilmente influenzato dalle conclusioni della Prima Sezione di Strasburgo in *BBW*: «Tele 2 Sverige *did not concern national security, like* Quadrature Du Net *did, so maybe this is why the CJEU had adopted a softer approach, given that national security has traditionally been outside of European integration (…). Could it be that lax proceduralist approach adopted in 2018 in the Chamber rulings in* Big Brother Watch *ruling (very similar decision to Grand Chamber) and* Centrum för Rättvisa *(which found no violation at all!) had influenced the CJEU's softer approach in* Quadrature Du Net*? Either way,* Quadrature Du Net *signals a paradigm shift away from the CJEU's earlier progressive approach against securitisation and mass-surveillance. A further echoing of this approach in* Big Brother Watch *and* Centrum för Rättvisa *by the ECtHR's GC points to a dangerous convergence of the two European courts on the acceptability of the good old "inevitability of securitisation" narrative in context of intelligence collection and sharing*»[169].

Prima di procedere a qualche valutazione in termini di politica giurisprudenziale della Corte di giustizia, questo commento ci fornisce l'occasione per trattare le recenti conclusioni della Grande Camera di Strasburgo a cui si era fatto cenno e che ora possono essere meglio analizzate.

- *Corte EDU, Big Brother Watch (GC, 2021)*

Salvo che per più raffinate e attualizzate considerazioni (specie, per esempio, quanto al più ampio novero di criteri previsti, rispetto ai sei *Weber* utilizzati dalla Prima Sezione, per valutare il margine di apprezzamento consentito al Regno Unito, in linea con gli sviluppi tecnologici cfr. p. 361 e 367),

[168] Ibidem, p. 177. Dello stesso tenore, rispetto specificamente alle misure di conservazione preventiva dei dati di traffico e ubicazione per esigenze di sicurezza nazionale, al punto 137: «*in situazioni come quelle descritte ai punti 135 e 136 della presente sentenza, l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, non osta, in linea di principio, a una misura legislativa che autorizzi le autorità competenti ad imporre ai fornitori di servizi di comunicazione elettronica di procedere alla conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli utenti dei mezzi di comunicazione elettronica per un periodo limitato, se ricorrono circostanze sufficientemente concrete che consentono di ritenere che lo Stato membro interessato affronti una minaccia grave come quella indicata ai punti 135 e 136 della presente sentenza per la sicurezza nazionale che si rivela reale e attuale o prevedibile. Anche se una misura siffatta riguarda, in maniera indifferenziata, tutti gli utenti di mezzi di comunicazione elettronica senza che questi ultimi sembrino, a prima vista, presentare alcun collegamento, ai sensi della giurisprudenza richiamata al punto 133 della presente sentenza, con una minaccia per la sicurezza nazionale di tale Stato membro, si deve tuttavia considerare che l'esistenza di una simile minaccia è idonea, di per sé, a stabilire detto collegamento*».

[169] da M. ZALNIERIUTE, A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence, in *EJIL:Talk!*, June 4, 2021.

la Grande Camera su *BBW* non si è discostata in realtà dalle conclusioni del 2018 quanto alle asserite violazioni dell'articolo 8 CEDU: ha riconosciuto una violazione rispetto ai regimi di cui alla sezione 8(4) e al Capitolo II RIPA, ancora una volta, nessuna violazione rispetto al regime di condivisione di dati con servizi di *intelligence* stranieri. Peraltro, sebbene nel caso CFR la Corte ha ritenuto il regime svedese carente e dunque riscontrato una violazione dell'articolo 8 CEDU, in entrambe le pronunce veniva riconosciuta da Strasburgo la "importanza vitale" delle intercettazioni di massa per la sicurezza nazionale[170]. In questo senso, la Corte sembra in realtà consolidare il proprio (preoccupante) orientamento sulla sorveglianza di massa: «*the ECtHR sowed the seeds of bulk interception of communications in the mid-2000s, which seemed to have 'flown under the radar' of the general public. Big Brother Watch reiterates and elaborates on this policy line, which will most likely be the guiding precedent for the ECtHR when confronted with the pending mass surveillance cases*»[171].

Sicuramente, la pronuncia definitiva in *BBW* ha il merito di chiarire la distinzione tra intercettazioni mirate e intercettazioni di massa (cfr. p. 345 ss.) e, rispetto alle ultime (pur ammissibili) sottolineare la necessità di garanzie fondamentali per ridurre al minimo il rischio di abusi di potere (cfr. p. 350, nonché 348-364). Non mancano, però, elementi di perplessità che hanno sollevato parecchi disappunti, a cominciare dall'opinione parzialmente dissenziente del giudice Pinto de Albuquerque, che sicuramente è stata fonte privilegiata di ispirazione: «*This judgment fundamentally alters the existing balance in Europe between the right to respect for private life and public security interests, in that it admits non-targeted surveillance of the content of electronic communications and related communications data, and even worse, the exchange of data with third countries which do not have comparable protection to that of the Council of Europe States. (...) with the present judgment the Strasbourg Court has just opened the gates for an electronic "Big Brother" in Europe*»[172].

Alcune riflessioni su "pericolose" contaminazioni, tecnica decisionale e politica giurisprudenziale

Tra i molteplici punti critici emersi dalla recente decisione di Strasburgo, molti hanno enfatizzato la tendenziale "deferenza" della Corte rispetto agli Stati parti quanto alle salvaguardie da

[170] Corte europea dei diritti umani (GC), ricorsi n. 58170/13, 62322/14 e 24960/15, *Big Brother Watch e altri*, 25 maggio 2021, p. 424.
Corte europea dei diritti umani (GC), ricorso n. 35252/08, *Centrum for Rattvisa c. Svezia*, 25 maggio 2021, p. 365.
[171] E. WATT, Much Ado About Mass Surveillance – the ECtHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK, *cit*.
[172] PARTLY CONCURRING AND PARTLY DISSENTING OPINION OF JUDGE PINTO DE ALBUQUERQUE, p.59.

predisporre[173]. Ma soprattutto, sempre seguendo interessanti commenti a caldo, sono stati rintracciati, come si anticipava, punti di *convergenza* tra la Grande Camera di Strasburgo e la Corte di Lussemburgo.

In senso positivo, per esempio, è stato rilevato come la prima abbia considerato i metadati non meno sensibili del contenuto, in ciò riprendendo conclusioni della Corte di giustizia[174].

Alcune perplessità, invece, sono state sollevate rispetto alla ravvisata "tendenza", che starebbe diventando comune alle Corti europee (tenendo in considerazione, invero, essenzialmente *La Quadrature du Net*, da un lato, e *BBW*, dall'altro), verso una "*normalizzazione della sorveglianza di massa*" (ancorché l'espressione sia usata dal commentatore rispetto alle sole due decisioni del 25 maggio a Strasburgo), che avverrebbe essenzialmente attraverso una tecnica – in questo senso comune ad entrambe le Corti – per cui, piuttosto che bandirla *in nuce*, ne richiede l'assoggettamento ad una regolamentazione precisa e a garanzie amministrative e giudiziarie: «*The price of that normalization is the subjecting of such surveillance to more rigorous regulation and administrative and judicial safeguards, but without really questioning the substantive merits of these programmes*»[175].

Si tratterebbe, insomma, di ciò che è stato definito "feticismo procedurale", tale per cui i regimi di sorveglianza di massa, consideratane l'inevitabilità per ragioni di sicurezza, sono ritenuti ammissibili purché soddisfino le garanzie richieste: «*Grounded in "procedural fetishism", this convergence signals: not only can governments continue to deploy mass surveillance regimes, they can also share the information with other countries, as long as certain safeguards – even if sometimes (often?) vague – are incorporated (…). The procedural fetishism reinforces what I term the "inevitability of securitisation" narrative, which disregards the effectiveness or proportionality of blanket surveillance regimes, and instead assumes that they are inevitable and necessary for*

[173] M. MILANOVIC, The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa, in *EJIL.Talk!*, May 26, 2021: «*The Court's overall posture is very deferential towards the respondent governments, especially as to the actual functioning of the surveillance programmes in fact*». Si veda anche L. WOODS, Big Brother Watch v UK: the ECtHR Grand Chamber rules on mass surveillance, *cit.*: «*Rather than assess the surveillance by reference to existing standards – for example, the presumption of innocence and the impact of a State carrying out surveillance (which is recognised through the case law on the mere storing of data), the Court abandons these standards as part of its updating in order to fit round state choices. In so doing, it gives some legitimacy to the idea that the State may carry out surveillance on individuals without any grounds related to that person (para 317, 348)*».

[174] Ibidem, la stessa autrice: «*The key positive is that the Court does not think that meta data is less sensitive than content (para 363)…In this, the Court joins the Court of Justice (see eg. Tele2/Watson, para 99)*».

[175] M. MILANOVIC, The Grand Normalization of Mass Surveillance, *cit*. Nello stesso senso, J. SAJFERT, The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?, in European Law Blog, 8 June 2021: «*Rather than banning certain intrusive intelligence or investigatory measures at the outset, the trend is to allow and then burden it with several procedural and technical safeguards. However, in practice these safeguards often become just a bit more paperwork and rubber-stamping*».

ensuring national security»[176]. Nello stesso ordine di idee, sono già stati ipotizzati interessanti possibili influssi derivanti dalla prospettata "accettazione" delle esigenze securitarie da parte di entrambe le Corti europee, che vale la pena qui richiamare perché anticipano spunti su prospettive future della sovranità digitale, quanto al contesto post-pandemico e all'evento Brexit: «*This could have a spill-over effect to other State activities, in the pandemic (or post-pandemic) context. Secondly, in the UK context and its data protection adequacy talks with the European Commission, the Big Brother Watch can only strengthen the UK case. The UK can now argue that its mass surveillance regime is not per se violating the ECHR and that it will, or it already did, bring itself in line with the Strasbourg requirements easily*»[177].

In realtà, se è vero che la sorveglianza di massa non è mai stata completamente bandita a Strasburgo, è anche vero che potrebbe essere quantomeno prematuro ravvisare un totale allineamento a questa tendenza in Lussemburgo sulla sola base della pronuncia *La Quadrature du Net*. Eppure, nonostante la solida pregressa giurisprudenza sia stata confermata pienamente nella pronuncia *Privacy International* dello stesso giorno, la percezione diffusa nei commentatori dal confronto con la Grande Camera in *BBW* pare proprio in termini di ciò che, ancora, è stato descritto come "pericolosa convergenza": «*although the UN human rights apparatus continues to regard mass surveillance as inherently disproportionate, the CJEU, by acquiescing to the possibility of EU states adopting in certain circumstances indiscriminate data retention legislation, has seemingly legitimised such measures and, at least for the time being, aligned itself closer with the ECtHR's approach to mass surveillance*»[178].

Pur ritenendo simili considerazioni assolutamente puntuali e condivisibili, esse potrebbero forse apparire avventate. Non bisogna, infatti, sottovalutare che nella suddetta opinione parzialmente dissenziente sulla pronuncia *BBW* è stato uno stesso giudice di quella Grande Camera a riconoscere una profonda differenza nell'approccio di Lussemburgo e ad elogiarne l'audacia (ancorché, molto probabilmente, non ancora consapevole – come le tempistiche fanno ritenere – delle conclusioni adottate in *La Quadrature du Net*): «*This conclusion is all the more justified in view of the CJEU's peremptory rejection of access on a generalised basis to the content of electronic communications, its manifest reluctance regarding general and indiscriminate retention of traffic and location data and its limitation of exchanges of data with foreign intelligence services which do not ensure a level*

[176] M. ZALNIERIUTE, A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence, *cit*. più in particolare, sul "procedural feticism", v. ID., Procedural Fetishism and Mass Surveillance under the ECHR, in *Verfassungsblog*, 2 June 2021.
[177] J. SAJFERT, The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?, *cit*.
[178] E.WATT, Much Ado, cit.

of protection essentially equivalent to that guaranteed by the Charter of Fundamental Rights. On all these three counts, the Strasbourg Court lags behind the Luxembourg Court, which remains the lighthouse for privacy rights in Europe»[179]. Ciò per dire che, in realtà, se è vero che *La Quadrature du Net* sembrerebbe in qualche modo discostarsi dall'orientamento prevalente della Corte di giustizia, è anche vero che, a nostro avviso, non lo farebbe in modo così incauto e preoccupante come parrebbe emergere dai commenti riportati, ma, anzi, abbastanza in linea con lo stile tendenzialmente assunto in materia, quantomeno in termini di tecnica decisionale.

In quest'ultimo senso, una conferma deriva anche dal modo in cui la Corte ha affrontato le altre questioni sottoposte dalle cause riunite in *La Quadrature du Net*. Alla domanda del giudice del rinvio sulla compatibilità di una normativa nazionale, che impone ai fornitori di servizi di comunicazione online e di hosting la conservazione generalizzata dei dati personali relativi a quei servizi, con le disposizioni della direttiva *e-commerce* letta alla luce della Carta, la Corte precisa l'ambito di applicazione di detta direttiva e arriva ad escluderne l'applicazione al caso di specie, poiché la tutela della riservatezza delle comunicazioni e delle persone fisiche rispetto al trattamento dei dati personali nell'ambito dei servizi della società dell'informazione viene disciplinata, in base ai casi, dalla direttiva *e-privacy* o dal GDPR. Pertanto, soffermandosi su quest'ultimo, interpreta l'articolo 23 (cfr. *supra*), anche in parallelo con l'articolo 15 della direttiva *e-privacy,* e alla luce della Carta, nel senso che «*osta a una normativa nazionale che impone ai fornitori di accesso a servizi di comunicazione al pubblico online e ai fornitori di servizi di hosting la conservazione generalizzata e indifferenziata, in particolare, dei dati personali relativi a tali servizi*»[180]. Inoltre, sull'ultima questione, afferente ai limiti nel tempo degli effetti di una dichiarazione di illegittimità che il giudice di uno Stato membro deve adottare in considerazione dell'incompatibilità della normativa nazionale con il diritto dell'Unione (quella, appunto, relativa alla conservazione generalizzata di dati, in contrasto con l'articolo 15 della direttiva), la Corte anzitutto ribadisce il principio del primato del diritto dell'Unione su quello degli Stati membri, finanche richiamando (oltre alla più recente) la giurisprudenza *Costa*. Quindi, rispetto al problema implicitamente connesso e sollevato da alcune parti, sul "*se il diritto dell'Unione osti all'utilizzo, nell'ambito di un procedimento penale, di informazioni ed elementi di prova che sono stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con tale diritto*", la Corte delineava la prerogative del diritto nazionale rispetto a tale ammissibilità e precisava, così, i principi di effettività ed equivalenza, che verranno quindi ripresi (come si è visto, *supra*) nell'ultima pronuncia *Prokuratuur*.

[179] Judge Pinto de Albuquerque, *cit*., p. 59.
[180] Corte di giustizia, *La Quadrature du Net*, cit., p. 212. Si vedano, più ampiamente, pp. 206-212.

Dopo aver ricordato che spetta agli ordinamenti interni stabilire le modalità processuali dei ricorsi per garantire ai singoli le tutele previste dal diritto dell'Unione, la Corte chiariva: «*Per quanto concerne il principio di equivalenza, spetta al giudice nazionale investito di un procedimento penale fondato su informazioni o elementi di prova ottenuti in violazione dei requisiti risultanti dalla direttiva 2002/58 verificare se il diritto nazionale che disciplina tale procedimento preveda norme meno favorevoli riguardo all'ammissibilità e all'uso di tali informazioni ed elementi di prova rispetto a quelle che disciplinano le informazioni e gli elementi di prova ottenuti in violazione del diritto interno. Quanto al principio di effettività, occorre rilevare che lo scopo delle norme nazionali relative all'ammissibilità e all'uso delle informazioni e degli elementi di prova consiste, in base alle scelte operate dal diritto nazionale, nell'evitare che informazioni ed elementi di prova ottenuti in modo illegittimo rechino indebitamente pregiudizio a una persona sospettata di avere commesso reati. Orbene, tale obiettivo può, secondo il diritto nazionale, essere raggiunto non solo con un divieto di utilizzare tali informazioni ed elementi di prova, ma altresì mediante norme e prassi nazionali che disciplinano la valutazione e la ponderazione delle informazioni e degli elementi di prova, o prendendo in considerazione il loro carattere illegittimo nell'ambito della determinazione della pena*»[181]. Per questa via, la Corte concludeva che l'articolo 15 della direttiva, interpretato alla luce del principio di effettività, impone al giudice nazionale di non tener conto di quelle informazioni se le persone interessante non possono efficacemente prendere posizione su di esse.

Ebbene, anche le conclusioni relative a tali altre questioni (rispetto alla ammissibilità della conservazione generalizzata *tout court*) si ritengono degne di nota nella valutazione circa il possibile *revirement* della Corte di giustizia in tema di affermazione delle garanzie individuali quanto alla protezione dei dati personali e di discordanti prerogative nazionali.

Sicuramente, in termini di *tecnica decisionale* esse conducono non solo ad escludere qualsiasi cambio di paradigma ma addirittura a testimoniare una ancor più raffinata conferma delle garanzie, soprattutto procedurali, riconosciute ai singoli dal diritto dell'Unione e, più in generale, rispetto al sistema nel suo complesso, in piena coerenza con i principi della *EU rule of law*.

Infatti, le riportate ultime battute della Corte convalidano che «l'effettività stessa di un ordinamento giuridico, ivi compreso quello dell'Unione, si determina in gran parte a fronte degli strumenti attraverso i quali si persegue l'osservanza dei suoi precetti da parte dei soggetti cui esso stesso si indirizza. (…) l'ordinamento può dirsi realmente dotato di effettività quando gli Stati membri osservino l'obbligo di approntare gli strumenti processuali necessari a tutelare le sue norme

[181] Ibidem, pp. 224-225. Per i riferimenti precedenti, v. pp. 213-223.

sostanziali, ossia a garantirne la corretta applicazione»[182]. Peraltro, come si è detto, ciò è ulteriormente confermato dall'ultima pronuncia (in vista anche della decisione nel merito, cfr. *supra*) relativa al caso *Prokuratuur* e potrebbe confermarsi ulteriormente nei casi affini attualmente pendenti[183].

Qualche perplessità, invero, permane in termini di *politica giurisprudenziale*, senza negare la pur avvenuta apertura rispetto a possibili situazioni di sorveglianza generalizzata, ancorché eccezionali e ampiamente giustificate, oltre che corredate di tutte le debite garanzie richieste. Pur senza negarla, infatti, e anche alla luce delle ultime considerazioni sulla medesima sentenza, si ritiene di confermare valutazioni volte a (almeno, allo stato dell'arte) ridimensionarne la portata rivoluzionaria e contraddittoria rispetto all'orientamento precedente, considerando piuttosto l'approccio di Lussemburgo ancora lontano da quello assunto da tempo a Strasburgo sul tema. Ciò non tanto per negare in questo caso la, generalmente conclamata, contaminazione tra giudici europei, ma piuttosto per tenere in considerazione proprio la diversa posizione di quei giudici europei, che in questioni molto similari come quelle *de quo* facilmente rischia di essere confusa.

Intendiamo dire che se è vero che le questioni analizzate, nella misura in cui coinvolgono esigenze di sicurezza nazionale e bilanciamento con diritti individuali, si presentano come particolarmente analoghe a Strasburgo e a Lussemburgo, è anche vero che la prospettiva con cui queste vengono affrontate dalle due diverse Corti non può essere la stessa, semplicemente perché ciascuna assolve a compiti differenti (ancorché sempre più affini) e, soprattutto, risponde a entità con obiettivi differenti. È per questo che, quand'anche in termini di *tecnica decisionale* potrebbero ravvisarsi delle analogie tra le due Corti, specie nell'affascinante tentazione di rintracciare la dottrina del margine di apprezzamento elaborata a Strasburgo anche in alcune interpretazioni della Corte di giustizia, è proprio alla prova dell'analisi di *politica giurisprudenziale* che tutte le suddette considerazioni in termini di "pericolosa convergenza" potrebbero risultare non facilmente sostenibili.

La questione starebbe, in definitiva, nel considerare la Corte di giustizia come organo giurisdizionale di un ordinamento il cui funzionamento è imperniato, tra gli altri, sul *principio di*

[182] Così G. VITALE, Il principio di effettività della tutela giurisdizionale nella Carta dei diritti fondamentali, in *Federalismi.it*, 28 febbraio 2018, pp. 24-25. Per una più generale disamina del diritto dei singoli a una tutela giurisdizionale effettiva tra i fondamentali principi di *rule of law* nell'ordinamento dell'Unione, si veda *ex multis* R. MASTROIANNI, L'effettività della tutela giurisdizionale alla prova della Carta dei diritti fondamentali, in *Liber Amicorum*
Antonio Tizzano – De la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne, Giappichelli, 2018, pp. 586-600.
[183] Il riferimento è ai casi: C-793/19, *SpaceNet*; C-794/19 *Telekom Deutschland*; C-817/19 *Ligue des droits humans*; C-140/20 *Commissioner of the Garda Síochána*; C-397/20 *SR.*

attribuzione delle competenze, principio dal quale non può prescindere tutte le volte che è chiamata a dirimere il delicato discrimine rispetto alle prerogative degli Stati membri. Questo è ciò che, a nostro avviso, risalta prevalentemente dalla sentenza tanto temuta e che, però, letta in quest'ottica, risulta totalmente coerente non solo con la giurisprudenza pregressa ma anche successiva (o meglio, la concomitante *Privacy International* e la successiva *Prokuratuur*).

In quest'ottica, si condividono le seguenti riflessioni: «*At the heart of* Privacy International *and* Quadrature Du Net *is the struggle for competence at the intersection of data retention and national security. The EU institutions, including the CJEU, but also the EU Commission, EP, are institutionally inclined to define 'national security' narrowly, strengthening their own role in the area. The Member States, on the other hand, have an institutional interest in keeping the EU institutions out of their national security business. At the same time, the Member States cannot avoid the growing European interdependence in security matters, so the struggle will continue. Yet, while* Privacy International *is an unequivocal assertion of CJEU's authority in the area of national security and a welcome victory for privacy advocates,* Quadrature Du Net *does not oppose indiscriminate data retention in principle and is an ambivalent response by the CJEU in the face of political pressure*»[184]. Occorrerà, senz'altro, attendere le prossime pronunce in materia, ma anche l'impatto di quelle sin qui esaminate sulle proposte legislative in atto e sulla prassi delle altre istituzioni, che verrà affrontato nel prosieguo, concorre a delineare la centralità del ruolo della Corte di giustizia rispetto alle dinamiche di coerenza interna dell'Unione, tra prerogative degli Stati membri e sollecitazioni sovranazionali, quanto a delicate esigenze di sicurezza.

Alla luce di tutto quanto esposto, è possibile finalmente, per un quadro completo di analisi, passare all'esame degli elementi di coerenza esterna che, nel settore di riferimento, si risolvono essenzialmente nella questione del trasferimento dei dati verso Paesi terzi.

[184] M. ZALNIERIUTE, A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union, *cit.*, p. 27.

CAPITOLO II

SUL TRASFERIMENTO DI DATI VERSO L'ESTERNO

1. I riscontri pratici delle premesse teoriche

Questa parte della trattazione ci darà finalmente l'occasione di verificare in pratica le prospettazioni teoriche sin qui analizzate e comprendere le implicazioni dei casi già trattati, tutti elementi che convogliano insieme nell'ottica che indaga la tendenza verso una sovranità digitale dell'Unione europea. Ciascun profilo di analisi sin qui illustrato (in questa Parte, come nelle precedenti) trova infatti nella trattazione che segue una sua soluzione, concorrendo ad avallare la tesi generale che si vuole sostenere e che, tramite quanto stiamo per dire, assume così pienamente giustificazione.

Il trasferimento di dati personali al di fuori del territorio dell'Unione europea, soprattutto nelle sembianze attuali, è infatti massimamente esplicativo dei moti esogeni ed endogeni che sono stati presentati, nonché della loro combinazione nello stato corrente dell'integrazione europea.

Anzitutto, esso chiaramente dimostra il c.d. *effetto Bruxelles*, come capacità di influenzare l'esterno legata alle dinamiche di mercato; ma esso spiega anche il c.d. *regulatory*/*normative power Europe* e concretizza altresì aspetti di extraterritorialità o estensione territoriale del diritto dell'Unione, costituendo in qualche modo il più esemplare caso di "*global reach of the EU law*" inteso in termini di influenza *unilaterale* dell'Unione verso l'esterno, che tende così ad affermarsi come attore globale[185]. In questo senso, è stata anche riconosciuta la forte tendenza della Corte di giustizia (a partire dalla giurisprudenza *DRI*, ma poi soprattutto con *Schrems*, e non solo, come vedremo) ad utilizzare il settore della protezione dei dati personali per affermare i diritti fondamentali dell'Unione nel contesto internazionale[186].

[185] Al riguardo, ci ricorda C. KUNER, The Internet and the Global Reach of EU Law, in in C. CREMONA, J. SCOTT (Eds), *EU law beyond EU border – The Extraterritorial Reach of EU Law*, Oxford University Press, 2019, che «*The global reach of EU law is manifested in different types of actions taken by the EU and its Member States, such as asserting EU values and interests in international organizations and the conclusion of international treaties; influencing the adoption of legislation in third countries; and requiring compliance with EU law with regard to activities carried out by parties in third countries*», p. 113, calando poi l'analisi allo specifico settore della protezione dei dati personali.

[186] C. KUNER, International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR, in *Common Market Law Review*, 55, 2018, p. 858: «*Since then* [*DRI*], *the Court has also used data protection as a vehicle to assert EU fundamental rights in an international context*» o ancora, ibidem: «*These judgments demonstrate that data protection has become a vehicle through which the Court has expanded the reach of the Charter to cover situations involving third countries*».

Inoltre, il trasferimento di dati personali fuori dall'Unione è anche in qualche misura indicativo della cooperazione internazionale che essa pone in atto tramite accordi, bilaterali ma anche multilaterali, che coinvolgono più o meno direttamente questioni di protezione di dati, dunque non in termini di influenza unilaterale ma piuttosto di collaborazione volta, comunque, alla promozione dei propri valori e principi, come previsto dagli articoli 3, par. 5 TUE e 21 TUE. In termini più generali, tale promozione di valori e principi propri dell'Unione tramite la conclusione di accordi internazionali si esplicherebbe, per esempio, nella previsione di clausole sui diritti umani, che costituirebbero infatti «*an identity-creating feature of EU external policy*»[187].

Ancora, il trasferimento dei dati personali verso l'esterno si rivela ambito particolarmente idoneo per testare l'*effettività* del principio di coerenza tra azione esterna e interna dell'Unione (*ex* art. 21, par. 3, c. 2, TUE, cfr. *supra*, Capitolo III, Parte III), in particolare considerando quanto esaminato da ultimo circa l'idoneità di sistemi di sicurezza degli Stati membri e, in parallelo, l'adeguatezza di quelli di Stati terzi al fine di consentire legittimi flussi di dati dall'Unione europea.

Com'è noto, i trasferimenti verso l'esterno vengono ora disciplinati dal GDPR – salvo i casi che non rientrano nel suo ambito di applicazione, per esempio quando si applica la direttiva n. 680/2016, che comunque prevede disposizioni analoghe – al Capo V, costituito dagli articoli 44-50 e rubricato proprio "*Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*".

Un'utile esplicazione della *ratio* che guida la disciplina sul trasferimento dei dati deriva dal Considerando 101 del GDPR, che recita: «*I flussi di dati personali verso e da paesi al di fuori dell'Unione e organizzazioni internazionali sono necessari per l'espansione del commercio internazionale e della cooperazione internazionale. L'aumento di tali flussi ha posto nuove sfide e problemi riguardanti la protezione dei dati personali. È opportuno però che, quando i dati personali sono trasferiti dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso, anche nei casi di trasferimenti successivi dei dati personali dal paese terzo o dall'organizzazione internazionale verso titolari del trattamento e responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale. In ogni caso, i trasferimenti verso paesi terzi e*

[187] Così F. MARTINES, Humans Rights Clauses in EU Agreements, in S. POLI (ed.), *Protecting Human Rights in the European Union's External Relations*, CLEER PAPERS 2016/5, p. 61, che specifica, in senso congeniale alle nostre più generali considerazioni: «*The rationale of the human rights clause, in other words, lies in the self-representation of the EU as a global actor that defines its role and its foreign policy as a human rights and democracy promoter, its foreign relations being guided – according to the EU Treaty – by the same 'principles that have inspired its own creation'*». Ciò, tuttavia, senza misconoscere le criticità che lo strumento presenta nell'attuazione pratica.

organizzazioni internazionali potrebbero essere effettuati soltanto nel pieno rispetto del presente regolamento»[188]. Al riguardo, è stato osservato che il trasferimento dei dati verso l'esterno risponderebbe, in senso opposto, alla logica sottesa alla costruzione di un libero spazio di circolazione dei dati all'interno dell'Unione europea, per incentivare più in generale il funzionamento del mercato unico, seguendo dunque «il binomio "libera circolazione" (all'interno dell'Unione) / "circolazione controllata" (al di là dell'Unione)»[189]. Si tratta, in buona sostanza, della stessa logica che sta alla base della più generale costruzione del mercato interno, a partire da libera circolazione delle merci e unione doganale[190].

La normativa precedente, costituita dalle previsioni della Direttiva madre, dedicava il Capo IV al solo "*Trasferimento di dati personali verso Paesi terzi*", composto di due articoli: il 25, sui principi, e il 26, sulle deroghe. Si avrà modo di analizzare le più rilevanti differenze tra la normativa previgente e quella attuale. Qui basti chiarire che, in entrambi i casi, possono essere distinte due "macroaree" di legittimazione dei trasferimenti di dati al di fuori dell'Unione europea: «una prima ipotesi in cui la legittimazione discende da un'intesa tra istituzioni pubbliche (…); l'altra ipotesi che trova fonte, invece, nell'autonomia privata, seppur integrata dalle prescrizioni legislative»[191]. Daremo conto di entrambe le macroaree, ma diciamo sin da subito che i profili di autonomia privata fuoriescono dai nostri fini e dunque verranno trattati solo marginalmente. Quanto alla legittimazione (più o meno indiretta) da parte di istituzioni pubbliche, in essa riteniamo vadano inquadrati sia i profili di intervento unilaterale dell'Unione che quelli di cooperazione, entrambi, come detto, espressivi del "moto opposto" che abbiamo descritto.

Prima di analizzare i profili pratici dell'influenza unilaterale (nelle varie accezioni in cui è stata esposta *supra*, Capitolo I, Parte III), accenneremo ora agli aspetti essenziali che interessano le

[188] GDPR, Considerando 101, sottolineato aggiunto.

[189] Così G.M. RICCIO, F. PEZZA, Trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali, in E. TOSI (a cura di), *Privacy Digitale – Riservatezza e protezione dei dati tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, 2019, p. 590. In particolare, a p. 588, si specificava: «Uno degli obiettivi dichiarati del Regolamento 2016/679/UE (GDPR) consiste nel facilitare il traffico dei dati personali all'interno dei Paesi membri dell'Unione (…). Proprio la *ratio* di una simile previsione, quindi, ci consente di comprendere, in senso opposto, il divieto (o meglio, le limitazioni) imposte al titolare e al responsabile del trattamento ogniqualvolta il trasferimento dei dati avvenga al di fuori del contesto europeo».

[190] Per la quale si rinvia, *ex multis*, alla generale esposizione di F. BESTAGNO, Libera circolazione delle merci, in A. ARENA, F. BESTAGNO, G. ROSSOLILLO (a cura di), *Mercato unico e libertà di circolazione nell'Unione europea*, Giappichelli, 2020, pp. 1-16.

[191] Così G.M. RICCIO, *Model Contract Clauses* e *Corporate Binding Rules*: valide alternative al *Safe Harbor Agreement*?, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali – Dai "Safe Harbourprinciples" al "Privacy Shield"*, Roma Tre Press, 2016, p. 216, che continuava specificando: «All'interno di questa seconda macroarea occorre poi distinguere l'ipotesi in cui sia lo stesso soggetto interessato a prestare il proprio consenso, in maniera inequivocabile al trasferimento del dato (art. 26, par. 1, lett. a) della direttiva), da quella in cui sia stata la Commissione europea ad approvare gli accordi interni alle imprese (nel caso delle *corporate binding rules*) o, in alternativa, a dettare le clausole da recepire nei contratti di esportazione dei dati personali (nel caso delle *model contract clauses*)». Ancorché riferite alla direttiva e non ancora al GDPR, tali precisazioni possono ritenersi ancora valide per la normativa vigente.

dinamiche delle relazioni esterne dell'Unione, specie laddove incidenti sulla protezione dei dati personali, e quindi dei rapporti tra il diritto internazionale e dell'Unione europea al riguardo, per una più agevole comprensione degli elementi di cooperazione internazionale.

2. La cooperazione internazionale in materia di protezione dei dati personali

Premesse

Riprendendo quanto sostenuto da Schwartz circa l'importanza della cooperazione internazionale come ulteriore fattore che crea un'influenza dell'Unione verso l'esterno nel settore della protezione dei dati personali e che dunque, al pari degli altri interventi unilaterali, rientra in ciò che abbiamo chiamato "moto opposto" (cfr. *supra*, Capitolo I, Parte III), non poco rilievo assumono gli accordi conclusi dall'Unione con Paesi terzi relativi al trasferimento di dati. Intanto, alcune premesse.

Nella Comunicazione della Commissione del 10 gennaio 2017 su "*Scambio e protezione dei dati personali in un mondo globalizzato*", oltre allo strumentario di meccanismi per il trasferimento prospettato dal GDPR (che vedremo), viene illustrata al paragrafo 3.3. la "cooperazione internazionale per la protezione dei dati personali". Essa si esplicherebbe, anzitutto, nella promozione di standard di tutela elevati a livello globale, attraverso la collaborazione e il dialogo con i diversi attori coinvolti a livello internazionale. In tal senso, come abbiamo già detto, la Commissione si impegnava a promuovere l'adesione di Paesi terzi alla Convenzione n. 108 e al relativo protocollo addizionale. Nella stessa ottica, la Commissione prospettava un intervento attivo in consessi multilaterali, specie in seno ad organizzazioni internazionali quali le Nazioni Unite ovvero con organizzazioni regionali come l'APEC (Cooperazione economica Asia-Pacifico). Inoltre, puntava sulla necessità di rafforzare la cooperazione nell'attività di contrasto attraverso collaborazioni e assistenza con le autorità preposte all'applicazione delle norme nei Paesi terzi per garantire un'efficace tutela degli interessati e anche a beneficio degli operatori economici, nonché per il perseguimento di reati che assumono, nel digitale, una portata globale. A quest'ultimo proposito, la Commissione faceva quindi riferimento all'attività di negoziazione come valido

strumento per migliorare la cooperazione nell'attività di contrasto (con specifico riferimento agli USA)[192].

Orbene, è utile chiarire che anche per la comprensione dell'attività negoziale dell'Unione assume preponderante rilievo la separazione delle competenze tra Unione e Stati membri in relazione all'azione esterna della prima. Ancora una volta, quindi, ciò tocca le prerogative della sovranità e la correlata condivisione/cessione tra Unione e Stati membri, che abbiamo trattato per cercare di delineare la posizione dell'ente sovranazionale (cfr. *supra*, Parte I).

La questione, che qui si può solo accennare, diventa chiaramente peculiare nella dimensione digitale, riprendendo quindi anche le considerazioni sull'extraterritorialità dell'intervento dell'Unione (*supra*, Capitolo I, Parte III), e intaccando così inevitabilmente anche la sovranità di Stati terzi, come ci ricorda Hijmans: «*Exercise of EU competence on the internet affects legitimate claims to sovereignty by third countries, and also instruments of international law, be it in the areas of privacy and data protection or in other related areas. This is the external effect of the exercise of internal powers of the European Union*»[193]. Ciò, inevitabilmente, coinvolge non solo la ripartizione di competenze interna all'Unione (i.e. con gli Stati membri) ma anche il rapporto tra il diritto dell'Unione e il diritto internazionale. Infatti, nell'enfatizzare il contesto giuridico pluralista in cui l'Unione eserciterebbe il suo intervento esterno in materia di protezione dei dati personali, Hijmans distingue tre caratteristiche: «*the international competence of the European Union as determined by international law, the internal division of powers within the European Union as determined by EU law, and finally the primacy of international law, albeit subject to limitations*»[194], ovvero quelle limitazioni derivanti proprio dall'autonomia dell'Unione, per come riconosciuta da consolidata giurisprudenza della Corte di giustizia[195]. Queste considerazioni meritano un minimo approfondimento per comprendere meglio la misura della competenza dell'Unione a concludere accordi che coinvolgono la protezione dei dati personali.

La competenza dell'Unione a concludere accordi coinvolgenti la protezione dei dati personali

[192] Cfr. COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO, *Scambio e protezione dei dati personali in un mondo globalizzato*, COM (2017) 7 final, 10 gennaio 2017, part. p. 16, ma più in generale pp. 13-17.
[193] H. HIJMANS, *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU*, (PhD Thesis) University of Amsterdam, 2016, p. 397.
[194] Ibidem, p. 411.
[195] Il riferimento è alle considerazioni emerse dall saga Kadi (in particolare, Kadi I), ma anche al Parere sull'adesione alla CEDU n. 2/2013.

Dal punto di vista del diritto internazionale, l'Unione ha sicuramente soggettività[196], che la rende titolare di prerogative e subordinata agli obblighi da esso derivanti, e invero la sua personalità giuridica è ormai chiaramente sancita dall'articolo 47 TUE. La capacità di concludere accordi internazionali, oltre a potersi dedurre da disposizioni di diritto internazionale[197], è espressamente prevista dall'articolo 216 TFUE che «codifica i casi in cui, in passato, la giurisprudenza della Corte aveva ritenuto esistente un *treaty-making power* dell'Unione»[198]. Orbene, con riguardo allo specifico settore della protezione dei dati personali, il ruolo dell'Unione europea rispetto a quello degli Stati membri nel contesto internazionale assume ulteriore rilievo a seguito del GDPR, come Hijmans chiarisce: «*The logical consequence of this should be that in the international domain, too, the European Union is the principal – if not sole – actor, representing the internal acquis in this area. This role of the European Union – based on EU law – is recognised under international law. The rule is that, due to the very nature of EU law, the European Union in its relations with international organisations has many characteristics of a state*»[199]. Nondimeno, e come chiarito anche dalla Corte nel parere n. 2/13, l'Unione non è del tutto assimilabile a uno Stato nel contesto internazionale[200].

Ciò induce, quindi, a riflettere sulla seconda caratteristica rilevante individuata dall'autore, ossia la ripartizione interna di competenze tra Unione e Stati membri ai fini della definizione delle competenze esterne. Al riguardo, riprendendo le considerazioni dell'AG Kokott, «La questione della portata dei poteri degli organi dell'Unione per quanto riguarda l'azione esterna non riveste solo una rilevante importanza pratica, ma è di natura costituzionale»[201].

---

[196] Cfr. Corte internazionale di giustizia, *Parere sulla riparazione dei danni subiti al servizio delle Nazioni Unite*, 11 aprile 1949, pp. 174-176.

[197] Così denota, per esempio, E. CANNIZZARO, *Diritto Internazionale – Quinta Edizione*, Giappichelli, 2020, trattando della distribuzione del potere tra Unione e Stati quanto alla conclusione di accordi internazionali: «Non è irragionevole ritenere che il diritto internazionale dia rilievo alla ripartizione interna di poteri e finisca con il considerare invalido un accordo concluso da uno degli enti in manifesta violazione di essa. Questa regola si può dedurre, sulla base di un ragionamento di tipo analogico, dalle regole che considerano invalido un trattato stipulato da organi interni privi di competenza a stipulare (art. 46 della Convenzione di Vienna sul diritto dei trattati del 1969 nonché della Convenzione di Vienna sul diritto dei trattati stipulati fra Stati e organizzazioni internazionali o fra organizzazioni internazionale del 1986», p 330.

[198] C. CELLERINO, *Soggettività internazionale e azione esterna dell'Unione europea – fondamento, limiti e funzioni,* Aracne editrice, 2015, p. 61.

[199]H. HIJMANS, *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU*, (PhD Thesis) University of Amsterdam, 2016, p.412.

[200] Corte di giustizia, parere n. 2/13, 18 dicembre 2014, p. 156: «(…) l'Unione, dal punto di vista del diritto internazionale, non può, per sua stessa natura, essere considerata come uno Stato».
Hijmans ricorda, a tal proposito, che (a riprova della reticenza degli Stati membri al riguardo) l'Unione non è parte dell'ONU, del Consiglio d'Europa o dell'OCSE, né può agire dinanzi alla Corte internazionale di giustizia e, più in generale, ha un margine di intervento limitato in seno alle organizzazioni internazionali, cfr. p. 412.

[201] Conclusioni dell'AG J. Kokott, causa C-137/12, *Commissione c. Consiglio* (*Convenzione sui servizi ad accesso condizionato*), presentate il 27 giugno 2013, p. 1. Per un commento più generale sulla sentenza e sulle implicazioni nell'orientamento successivo della giurisprudenza, sia consentito un rinvio a R. MASTROIANNI, G. LO TAURO, Common Commercial Policy or internal market rules as legal basis for the conclusion of international agreements after Lisbon:

E invero, la ripartizione interna delle competenze tra Stati e Unione definisce anche la misura dell'intervento, unilaterale o congiunto, rispettivamente dell'Unione e degli Stati nel contesto internazionale. In tal senso, è imprescindibile la giurisprudenza *AETS*, con la quale la Corte di giustizia, cinquant'anni orsono, ha elaborato la celeberrima c.d. *dottrina dei poteri impliciti*, riconoscendo che «*Onde accertare, in un caso determinato, se la Comunità sia competente a concludere accordi internazionali, si deve prendere in considerazione sia il trattato nel suo complesso, sia le sue singole disposizioni* (…). *Detta competenza non dev'essere in ogni caso espressamente prevista dal trattato (...) ma può desumersi anche da altre disposizioni del trattato e da atti adottati, in forza di queste disposizioni, dalle istituzioni della Comunità. (...) nell'attuare le disposizioni del trattato non è possibile separare il regime dei provvedimenti interni alla Comunità da quello delle relazioni esterne*»[202]. Si creerebbe così, dunque, un "parallelismo" tra le competenze interne e quelle esterne dell'Unione.

Ciò non contrasta, dunque, con il principio di attribuzione delle competenze, sancito ora nell'articolo 5, par. 1 TUE, secondo cui "*l'Unione agisce esclusivamente nei limiti delle competenze che le sono attribuite dagli Stati membri nei trattati per realizzare gli obiettivi da questi stabiliti. Qualsiasi competenza non attribuita all'Unione nei trattati appartiene agli Stati membri*" (cfr. articolo 5, par. 2, TUE e articolo 4, par. 1, TUE). E infatti, nel definire l'ambito di competenza esclusiva, l'articolo 3 TFUE prevede al par. 1 un elenco di ambiti in cui l'Unione gode di tale esclusività di intervento (c.d. competenze esclusive *a priori*) e poi aggiunge al par. 2 che "*l'Unione ha inoltre competenza esclusiva per la conclusione di accordi internazionali allorché tale conclusione è prevista in un atto legislativo dell'Unione o è necessaria per consentirle di esercitare le sue competenze a livello interno o nella misura in cui può incidere su norme comuni o modificarne la portata*". Ebbene, la lettura congiunta dell'articolo 3, par. 2 TFUE e dell'articolo 216 TFUE è stata considerata proprio come la codificazione della giurisprudenza *AETS*[203].

Conditional Access Convention, in G. BUTLER, R. A. WESSEL (Eds), *EU External Relations Law: The cases in context*, Oxford: Hart Publishing, 2021 (*in corso di pubblicazione*), da cui emerge come il caso in commento (C-137/12), nel novero della più ampia giurisprudenza *AETS*, testimoni la tendenza della Corte, sempre più forte negli sviluppi successivi al primo periodo post-Lisbona (ossia, con riguardo, per esempio, al parere 2/15, al parere 3/15 o al caso *Commissione c. Consiglio* sull'Accordo di Lisbona riveduto), verso una "*EU-only action*" nella conclusione di accordi internazionali, volta a ridimensionare la possibilità di accordi misti con gli Stati membri e quindi l'intervento di questi ultimi sulla scena internazionale (e, dunque, volendo, in termini di "sovranità esterna"). Per un approfondimento sull'interessante questione si rinvia, *ex multis*, ai contributi in M CHAMON AND I GOVAERE (Eds), *EU External Relations Post-Lisbon – The Law and Practices of Facultative Mixity*, Leiden–Boston, Brill–Nijoff, 2020.

[202] Corte di giustizia, causa 22/70, *Commissione c. Consiglio (Accordo europeo trasporti su strada)*, 31 marzo 1971, pp. 15-19.

[203] Cfr. C. CELLERINO, *op. cit*., pp. 86 ss., in cui aggiunge che «la c.d. "costituzionalizzazione" delle competenze implicite potrebbe aver creato una base giuridica per l'azione esterna dell'Unione suscettibile di estendere i poteri impliciti al di là di quanto autorizzato da un'applicazione rigorosa della dottrina del "parallelismo"», p. 69.
Si ricorda, qui, l'articolo 216 TFUE:

Dunque, trasponendo la dottrina dei poteri impliciti al settore della protezione dei dati personali, Hijmans rilevava acutamente la connessione tra gli articoli 16 e 216 TFUE, alla luce della quale arrivava ad affermare una competenza esterna esclusiva dell'Unione nella conclusione di accordi internazionali implicanti questioni di protezione dei dati personali: «*The doctrine means that where an internal power to legislate exists there also may be an external power to conclude agreements. This is obviously the case for the area of data protection covered by Article 16 TFEU. Article 16 TFEU, read in connection with Article 216 TFEU, implies that the European Union also has external powers in the area of data protection. Under EU law, it is not fully clear whether the implied powers of the European Union to conclude agreements in the area of data protection qualify as an exclusive or a shared competence. This qualification determines to what extent the Member States are still competent to conclude agreements with third countries on the protection of personal data, or even on other subjects, but with provisions on data protection (...). In any event, in our view, the existence of an exclusive EU competence under Article 16 TFEU must be assumed on the basis of the reasoning that effective protection of the fundamental rights of privacy and data protection on the internet cannot be achieved by internal rules alone. Effective protection requires the widest possible geographical scope of protection, and hence external action. The effectiveness or effet utile of the internal regulation justifies exclusive competence for external action. Arguably, the Member States lost their external competence to conclude agreements with third countries on the protection of personal data, or to include provisions on data protection in agreements concerning different subjects*»[204]. Concordiamo pienamente con tale assunto, che risulta particolarmente corretto nell'ambito coperto dal GDPR, in cui ormai gli Stati non possono che attenersi alle disposizioni di portata generale. Ciò anche se è pur vero che, come Kuner ha acutamente notato, «*EU data protection legislation does not specify the conditions under which international agreements may provide a legal basis to transfer personal data*»[205]. Nondimeno, lo stesso autore rilevava che «*Since the criterion of achieving the objectives of EU law under Article 216(1) tends to be interpreted very broadly, the EU will generally have external competence to conclude international agreements for the transfer of personal data notwithstanding the failure to specify this in legislation*»[206].

---

1. L'Unione può concludere un accordo con uno o più paesi terzi o organizzazioni internazionali qualora i trattati lo prevedano o qualora la conclusione di un accordo sia necessaria per realizzare, nell'ambito delle politiche dell'Unione, uno degli obiettivi fissati dai trattati, o sia prevista in un atto giuridico vincolante dell'Unione, oppure possa incidere su norme comuni o alterarne la portata.
2. Gli accordi conclusi dall'Unione vincolano le istituzioni dell'Unione e gli Stati membri.

[204] H. HIJMANS, *The European Union as Guardian of Internet Privacy, cit*., p. 413, sottolineato aggiunto.
[205] C. KUNER, International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR, *cit*., p. 877.
[206] Ibidem, p. 878.

Infine, quanto alla terza caratteristica rilevante rintracciata da Hijmans, l'autore notava che rispetto alla giurisdizione dell'Unione nell'ambito del diritto internazionale è inevitabile il riferimento alla portata territoriale, che soprattutto (ma non solo) nella dimensione digitale si tradurrebbe inevitabilmente nella già richiamata extraterritorialità, come parrebbe derivare (ancorché con riferimento agli Stati) sin dal celeberrimo caso *Lotus* della Corte permanente di giustizia internazionale[207]. Qui, infatti, l'autore ravvisa una certa "ambizione" dell'Unione ad agire extraterritorialmente, in coerenza con le previsioni degli articoli 3, par. 5 e 21 TUE nella anzidetta promozione dei suoi valori fondanti verso l'esterno, che nella protezione dei dati personali troverebbe massima espressione[208].

Al riguardo Cremona ci ricorda che, nel fare ciò, «*the EU is constrained procedurally by its institutional legal framework and substantively by the need to ensure compliance with its own constitutional principles, including the protection of fundamental rights and the rule of law*», cosa che si traduce, da un lato, nell'ottemperanza a principi "costituzionali" quali quello di attribuzione delle competenze o di equilibrio istituzionale anche rispetto all'azione esterna, e, dall'altro, nel controllo della Corte di giustizia anche in aree in cui l'intervento dell'Unione sarebbe escluso, per garantire comunque tutela ai valori fondanti[209]. Ma la propensione extraterritoriale si inserisce, come abbiamo detto, nell'influenza unilaterale dell'Unione verso l'esterno (che tratteremo meglio a breve).

Ciò che qui vogliamo discutere è, invece, l'intervento dell'Unione di concerto con altri attori nella scena internazionale. Infatti, in quest'ordine di considerazioni Hijmans colloca, anche richiamando autori ai quali ci siamo riferiti nell'esposizione delle varie teorie che caratterizzano ciò che abbiamo chiamato 'moto opposto', le tre strategie attraverso cui l'Unione agirebbe verso l'esterno nella promozione della *data protection*, ossia unilaterale, bilaterale e multilaterale, senza escludere la possibilità di una commistione tra tali diverse strategie[210]. Focalizzandoci su quella bilaterale, è stato notato quanto al settore della protezione dei dati che «*Since the GDPR has comprehensively regulated data protection and rules covering international data transfers in the Union, in practice,*

[207] Permanent Court of International Justice – Twelfth (Ordinary) Session, The Case of the S.S. Lotus, France v. Turkey, Judgment No. 9, 7 September 1927.
[208] H. HIJMANS, *The European Union as Guardian of Internet Privacy, cit*., pp. 418, 424-425.
[209] M. CREMONA, Extending the Reach of EU Law – The EU as an International Legal Actor, in C. CREMONA, J. SCOTT (Eds), *EU law beyond EU border – The Extraterritorial Reach of EU Law*, Oxford University Press, 2019, p. 65, ove infatti continua specificando: «*Even those areas of its external activity which may seem to be least subject to the control of the courts—such as the CFSP—are subject to these legal constitutional constraints*».
[210] H. HIJMANS, *The European Union as Guardian,* cit., p. 427.

Member States have only a limited margin to enter into international agreements governing international data transfers, if at all»[211].

Invero, Hijmnans riconosce interessanti caratteristiche alla strategia bilaterale dell'Unione nel settore. Tra i vantaggi, infatti, l'autore ravviserebbe (pur concentrandosi sulle specifiche relazioni tra UE e USA nel settore) la possibilità di evitare la percezione di "imperialismo normativo" spesso criticamente rilevato in capo all'Unione, incentivando lo sforzo congiunto verso sfide comuni che la protezione dei dati presenta, specie nell'attività di contrasto; inoltre, ciò potrebbe portare il Paese terzo di riferimento ad adottare gli standard dell'Unione, così facilitando il compito di promozione su di essa incombente *ex* articolo 3, par. 5 TUE, ma anche agevolare le imprese che operano in diversi contesti ordinamentali, per condurre in ultima analisi ad una (auspicata) armonizzazione globale delle politiche in materia[212].

Eppure, l'autore non esclude qualche svantaggio. Infatti, un'azione concertata potrebbe non tanto portare all'affermazione degli standard europei ma, al contrario, richiedere di scendere a compromessi con il rischio di un abbassamento di quegli standard per raggiungere un accordo sul necessario scambio di dati tra l'Unione e il Paese terzo di riferimento[213].

Ebbene, a partire da queste basilari premesse, è possibile passare a una breve rassegna degli accordi più rilevanti che coinvolgono l'Unione nel settore della protezione dei dati personali per valutare se e quanto, in pratica, tali benefici e perplessità siano ravvisabili.

Gli accordi conclusi dall'Unione in materia di protezione dei dati personali

Occorre ricordare che, a seguito del Trattato di Lisbona, la procedura per la conclusione di accordi internazionali da parte dell'Unione europea è ora prevista dall'articolo 218 TFUE, che – a proposito dei principi costituzionali di cui si diceva – delinea il ruolo delle istituzioni europee al riguardo.

[211] C. KUNER, Article 44. General principle for transfers, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2020, p. 761.
[212] H. HIJMANS, op. cit., p. 430: «*In the first place, the strategy avoids what may be perceived from the US side as regulatory imperialism by the EU. In the second place, the strategy may have benefits to the benefit of global privacy and data protection. A cooperation between the EU and the US jurisdictions – whether or not by way of formal treaties – would be a means to face common challenges in the area of privacy and data protection in a coordinated manner and to allow both parties to join forces, for instance in the field of enforcement. In the third place, if well negotiated, the strategy might encourage the US to adopt the standards originating from the EU and hence be instrumental to the fulfilment of the EU's task under Articles 3(5) and 21 TEU to uphold and promote its values in the wider world. In the fourth place, the strategy might create a level playing field between companies operating from the US and those operating from the EU and, by doing so, contribute to ensuring the competitive position of EU companies. In the fifth place, if the great powers act in concert, this is a more effective way of policy-making and harmonisation in a global environment than is the case where these powers fail to agree*».
[213] Ibidem, p. 431.

Spetta al Consiglio autorizzare (con una decisione) l'avvio dei negoziati, come anche la conclusione e la firma, oltre a definire le direttive del negoziato e il negoziatore, a seconda della materia. La Commissione o l'Alto Rappresentante (nei casi PESC) presentano raccomandazioni al Consiglio per consentigli di espletare le suddette funzioni. In alcuni casi, elencati dall'articolo, il Consiglio adotta la decisione di conclusione dell'accordo previa approvazione del Parlamento, che si è rivelata particolarmente rilevante nei casi relativi alla nostra materia. Infine, altrettanto rilevante ai nostri fini, l'ultimo paragrafo prevede il coinvolgimento della Corte di giustizia, che può essere richiesta di un parere sulla compatibilità del prospettato accordo con i trattati, rispettivamente, da parte di uno Stato membro o del Parlamento europeo, della Commissione o del Consiglio. Se il parere è negativo, l'accordo non può entrare in vigore a meno di modifiche dello stesso o revisione dei trattati[214].

Orbene, anzitutto è immancabile il riferimento agli accordi sul trasferimento e sull'uso dei dati del codice di prenotazione (*Passenger Name Record* – PNR). Si è già detto della normativa a ciò dedicata a livello sovranazionale, ossia la c.d. *direttiva PNR* n. 2016/681, volta a consentire la cooperazione ed armonizzazione tra Stati membri nel settore, essenzialmente ai fini di contrasto al terrorismo e ad altre forme di criminalità, per salvaguardare la sicurezza interna dell'Unione. Sul fronte esterno, l'Unione cerca di perseguire gli stessi fini tramite la stipula di accordi internazionali, per fronteggiare il terrorismo e i reati gravi di natura transnazionale con Paesi terzi rispetto ai quali condivide valori comuni e per tutelare le rispettive società democratiche[215].

In tal senso, l'Unione aveva già stipulato degli accordi PNR con Australia (2008), Canada (2006) e Stati Uniti (2007)[216], con i quali ultimi invero accordi erano stati già previsti in precedenza. In particolare, va richiamata la sentenza della Corte di giustizia del 2006 sul caso *Parlamento c. Consiglio*, di cui si è già detto, con cui vennero annullate sia la decisione di adeguatezza della Commissione che, soprattutto ai nostri fini, la decisione del Consiglio relativa alla conclusione dell'accordo PNR con gli USA, essenzialmente per lo stesso motivo relativo all'ambito di applicazione, ossia per il fatto che anche quella decisione riguardasse trattamenti che fuoriuscivano dall'ambito di applicazione della direttiva e dunque per mancanza di competenza della (allora)

[214] Cfr. Articolo 218 TFUE.
[215] Per uno sguardo veloce sulla disciplina UE relativa all'uso dei dati PNR, sia sul fronte interno che esterno, si rinvia alla pagina del Consiglio dedicata: https://www.consilium.europa.eu/it/policies/fight-against-terrorism/passenger-name-record/ .
[216] Accordo PNR Stati Uniti del 2007: https://www.garanteprivacy.it/documents/10160/10704/1531335.pdf/a3150f97-1b75-49d4-97f5-e3b85f278498?version=1.1

Comunità a concludere l'accordo[217]. Successivamente, venne stipulato un accordo nell'ottobre 2006 che sarebbe scaduto nel 2007, sostituito quindi da quello menzionato[218].

Ebbene, in considerazione della necessità di incrementare l'attività di contrasto rispetto alle minacce di terrorismo e criminalità internazionale sempre più fitte, nonché in vista del fatto che, a tali fini, diversi Stati sia membri UE (come il Regno Unito) che non (come Corea del Sud , Nuova Zelanda e Giappone) facessero un uso sempre più ordinario dei sistemi PNR, l'esigenza di garantire un livello di tutela dei dati personali adeguato agli standard europei portò la Commissione nel 2010 a fissare dei criteri generali da rispettare per i futuri accordi bilaterali PNR, nella Comunicazione "*sull'approccio globale al trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) verso paesi terzi*"[219]. Di qui la necessità di una rinegoziazione, che portò a nuovi accordi con l'Australia e gli Stati Uniti, entrambi del 2012[220]. Quanto all'accordo con il Canada, invece, è noto che, seguendo la procedura suddetta di cui all'articolo 218 TFUE, il Parlamento europeo avanzò perplessità per cui chiese parere alla Corte di giustizia.

Con il celebre *parere n. 1/15* del 26 luglio 2017 la Corte di giustizia (nella sua Grande Sezione, ancora una volta con T. von Danwitz relatore) ha dichiarato per la prima volta una proposta di accordo incompatibile con le previsioni della Carta (in particolare, gli articoli 7, 8, 21 e 52, par. 1), individuando i necessari interventi per consentirne la compatibilità. Il parere appare per diversi aspetti, ai nostri fini, un chiaro esempio di concreta applicazione del principio di coerenza dell'azione sia interna che esterna dell'Unione (cfr. in teoria *supra*, Capitolo III, Parte III) rispondendo pienamente ai dettami della *EU rule of law*, a cominciare proprio dalla testimoniata "vitalità"[221] della procedura di cui all'articolo 218 TFUE che comproverebbe il funzionamento del principio dell'equilibrio istituzionale nel settore, con il ruolo di rilievo del Parlamento e il coinvolgimento di tutte le istituzioni, sino ad arrivare alla Corte.

---

[217] Corte di giustizia, cause riunite C-317/04 e C-318/04, *Parlamento europeo c. Consiglio*, sentenza del 30 maggio 2006, punti 62-70.

[218] Cfr. https://eur-lex.europa.eu/summary/IT/l33277 .

[219] COMUNICAZIONE DELLA COMMISSIONE sull'approccio globale al trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) verso paesi terzi, Bruxelles, 21.9.2010, COM(2010) 492 definitivo, part. pp. 2-3, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0492:FIN:IT:PDF .

[220] Accordo Australia, GU L 186 del 14.7.2012.
Accordo USA, GU L 215 dell'11.8.2012.
Per entrambi gli accordi, la valutazione congiunta è attualmente in corso, come risulta anche dalla recente Relazione della Commissione sul riesame della direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, COM (2020) 305 final, 24 luglio 2020, pp. 2-3.

[221] Così precisamente connotata da C. KUNER, International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR, *cit.*, p. 881.

Tra gli interessanti aspetti trattati nel parere (incluso quello della base giuridica, che tralasceremo), ci interessa quello relativo alla questione della compatibilità della proposta di accordo con il rispetto dei diritti fondamentali garantiti nell'Unione europea, in particolare con il livello di protezione dei dati personali. La Corte riconobbe effettivamente nella proposta di accordo un'interferenza rispetto a tali diritti e, nell'analizzare se potesse dirsi giustificata, rispettandone il *contenuto essenziale,* e proporzionata entro i limiti dello stretto necessario, effettuò il classico test richiesto dall'articolo 52 della Carta sotto diversi profili[222]. Dall'accurato esame, pur riconoscendo l'importanza degli obiettivi tesi a giustificare le limitazioni dei diritti, ossia esigenze di sicurezza pubblica volte a prevenire e perseguire reati di terrorismo o reati gravi di natura transnazionale, la Corte ravvisò che diverse previsioni dell'accordo proposto eccedessero i limiti dello stretto necessario[223]. In quest'ottica, la continuità con la giurisprudenza pregressa risulta particolarmente rilevante.

Anzitutto, laddove la Corte riprende l'importanza di salvaguardare il *contenuto essenziale* dei diritti rispetto ai quali pur consente limitazioni, se da un lato parrebbe così corroborare la propria giurisprudenza (in particolare *DRI* e *Schrems I*), dall'altro qualcuno ha notato che al contrario ne prenderebbe quasi le distanze, rendendo invero particolarmente complesso comprendere cosa intenda il riferimento all'essenza dei diritti: «*From a constitutional perspective, however, the Court distances itself both from its case law where the benchmark was access to content data, as well as from its case law where the interference with the fundamental right should not call into question the existence of the fundamental right. Rather, it adopts a position that the interference with the essence of the right to privacy is a question of a degree of interference with the fundamental right, given that it takes as a benchmark the limited nature of the acquired and processed data. In that sense, a parallel could perhaps be drawn with Digital Rights Ireland where access to content was also a manifestation of a higher degree of interference. Nevertheless, these divergent findings on essence make it difficult to define how exactly the Court conceptualizes the essence of fundamental rights*»[224].

[222] Corte di giustizia, Parere n. 1/15, *Accordo PNR Canada*, 26 luglio 2017, pp. 121-141 e 148-217.
[223] Ibidem, pp. 181, 203, 211, 215 e 217.
[224] M. BRKAN, The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU's Constitutional Reasoning, in *German Law Journal* 20, no. 6 (2019), p. 878. Dello stesso tenore, C. KUNER, International agreements, data protection, and EU fundamental rights on the international stage, *cit*., p. 875: «*One can argue that the essence of a fundamental right cannot be described in abstract terms and can only be determined based on the circumstances of a particular case. However, the need for clarity and predictability makes it important to develop a normative framework for determining the essence of rights, which the Court has thus far not done for the rights protected by Articles 7 and 8 of the Charter. Its task in this regard is made more difficult by the rapid societal and technological evolution of the conditions under which personal data are processed, and the fact that privacy itself is notoriously difficult to define and has been found to be largely contextual.126 In time the Court will hopefully articulate a conceptual framework for defining the essence of the rights to privacy and data protection*».

Inoltre, quanto ai casi particolari di ammissibilità di un'archiviazione dei dati prolungata, ancorché soggetta a garanzie, da un lato riprende espressamente la pregressa giurisprudenza *Tele2*[225] e dall'altro, a nostro avviso, parrebbe porre le basi per le considerazioni che sono poi state sviluppate da ultimo (e pur considerando le varie critiche già esposte) in *La Quadrature du Net*. In ciò, dunque, si ritiene ravvisabile un elemento di piena continuità (piuttosto che di mutamento) nella giurisprudenza anche attuale, ancorché rimodulata in ragione delle rinnovate circostanze.

Ancora, un riferimento va fatto sin d'ora ai frequenti richiami alla tutela *sostanzialmente equivalente* che dovrebbe essere garantita nel Paese terzo per consentire un legittimo trasferimento di dati dall'Unione. Rinviando per valutazioni più approfondite, va detto che il parere ha il merito di chiarire che tale indispensabile criterio si applica sia quando il trasferimento venga legittimato da una decisione di adeguatezza della Commissione (come chiarito, a partire dalle disposizioni della Direttiva madre , in *Schrems I*) che anche quando avvenga, come nel caso di specie, sulla base di un accordo internazionale: «*un trasferimento di dati personali dall'Unione a un paese terzo può avvenire solo se tale paese assicura un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'Unione. Tale requisito vale anche nel caso della comunicazione dei dati PNR dal Canada verso altri paesi terzi, di cui all'articolo 19 dell'accordo previsto, al fine di evitare che il livello di protezione previsto da tale accordo possa essere eluso da trasferimenti di dati personali verso paesi terzi e di assicurare la continuità del livello di protezione offerto dal diritto dell'Unione (...). In tali circostanze, una siffatta comunicazione richiede l'esistenza o di un accordo tra l'Unione e il paese terzo interessato equivalente a detto accordo, oppure di una decisione della Commissione, ai sensi dell'articolo 25, paragrafo 6, della direttiva 95/46, che accerti che detto paese terzo assicura un livello di protezione adeguato ai sensi del diritto dell'Unione e ricomprenda le autorità verso le quali il trasferimento dei dati PNR è previsto*»[226]. Ciò potrebbe dirsi a buon diritto esplicativo del principio di coerenza nell'azione esterna.

E invero, partendo da questi spunti, Kuner proponeva delle riflessioni particolarmente interessanti quanto alle implicazioni di tale parere sulla *governance* dei diritti fondamentali, che dipenderebbero in ultima analisi dalla prospettiva che si assume. Rilevava l'autore: «*From the point of view of EU law (...) Opinion 1/15 could be viewed as an example of the self-correcting nature of the EU fundamental rights system, with violations by some institutions (in this case the Commission and the Council) corrected later on by others (the Court). However, from the point of view of third countries seeking to enter into international agreements with the EU, the fact that conclusion of the*

[225] Corte di giustizia, parere n. 1/15, *cit*., pp. 207 e 210.
[226] Ibidem, p. 214. Si vedano anche pp. 93e 134.

Draft Agreement was blocked after years of effort and a successful negotiation must seem to be a waste of time and resources, and may make the EU appear to be an unreliable negotiating partner»[227]. Dal primo punto di vista, esso rappresenterebbe invero un'ulteriore conferma del principio di coerenza interna, in perfetta continuità con quanto abbiamo visto avvenire rispetto al caso *DRI* (che infatti descrivevamo emblematico della coerenza interna, cfr. *supra*, Capitolo III, Parte III). Nel censurare l'operato delle istituzioni sovranazionali rispetto all'esigenza di garantire il livello di tutela dei diritti proprio dell'Unione (come, peraltro, avvenuto anche in *Schrems* rispetto all'operato della Commissione), la Corte opererebbe in linea con il ruolo designatole nella delineazione della *EU rule of law*. Tuttavia, non appena ci si allontana da valutazioni speculative e di principio e, soprattutto trattando (come in questo caso) di accordi internazionali – ossia per definizione guidati da scelte politiche e soluzioni di compromesso –, ci si confronta con le esigenze pratiche di negoziazione, ecco che lo stesso principio di coerenza (specie laddove debitamente adempiuto) pare far emergere perplessità che fanno sorgere inevitabilmente domande del tipo: «*how could the Commission and the Council negotiate and approve a text that the Court subsequently found to be so deficient in the protection of fundamental rights? Or did they do the best job possible under the circumstances, given that third countries may not always be willing to accept EU fundamental rights standards?*»[228].

Procedendo in riflessioni di questo tipo, l'autore prospettava quindi i plausibili effetti del parere sulla negoziazione di accordi internazionali da parte dell'Unione europea rispetto alla condivisione di dati, rilevando che lo stretto scrutinio della Corte, se da un lato induce accordi garantisti in termini di tutela dei diritti (e così, li rende base giuridica adeguata per il trasferimento dei dati al pari delle altre previste dal GDPR), dall'altro lato potrebbe comportare una certa reticenza degli Stati terzi nell'intraprendere negoziazioni che possono risolversi in un nulla di fatto dopo lo stretto scrutinio della Corte: «*If not carefully considered, the unilateral assertion of EU fundamental rights on the international stage may lead to less, rather than more, data protection in practice (such as by causing third countries to resort unilaterally to increased data processing or surveillance)*»[229]. Considerazioni di non poco conto e che torneranno utili nell'analisi dell'azione unilaterale dell'Unione e, in particolare, delle decisioni di adeguatezza. Si tratta evidentemente di perplessità legittime e fondante, ma che devono fare i conti con il fatto che è il ruolo stesso della Corte ad imporle, in ultima analisi, di attenersi ai dettami della *EU rule of law* e rendersi di essa massimamente rappresentativa, nel suo richiesto intervento di controllo sull'operato delle altre

[227] C. KUNER, International agreements, data protection, and EU fundamental rights on the international stage, *cit*., pp. 873-874.
[228] Ibidem, p. 874.
[229] Ibidem, pp. 881-882.

istituzioni sovranazionali. E ciò, assolvendo al principio di coerenza, tanto quando le istituzioni agiscono in espressione dell'azione interna che quando lo fanno, rispetto ad attori terzi, nell'azione esterna.

Peraltro, sempre quanto alle possibili implicazioni del parere, qualcuno lo ha considerato possibile parametro non solo per sollevare perplessità sugli altri accordi PNR (suddetti) in vigore, ma anche per ripensare, a livello interno, la discussa direttiva 681/2016[230]. Su quest'ultima, invero, è intervenuta di recente la Commissione con la sua Relazione sul riesame biennale, come previsto dall'articolo 19 della direttiva stessa, precisando espressamente quanto al parere 1/15 "*che le circostanze di fatto e di diritto della direttiva PNR siano diverse da quelle considerate dalla Corte di Giustizia in tale causa*"[231].

Richiamando, infine, l'accennato parallelo tra accordi internazionali di condivisione dei dati e decisioni di adeguatezza della Commissione, sempre Kuner riteneva preferibile la seconda come più consona base giuridica per il trasferimento, per esempio perché consentirebbe un'analisi più approfondita dei sistemi di tutela dei Paesi terzi rispetto a quella realizzabile tramite gli accordi[232]. Avremo modo di sviscerare le caratteristiche delle decisioni di adeguatezza. La riflessione, comunque, assume qui particolare rilievo perché ci consente di passare a trattare gli altri accordi, diversi dai PNR, che coinvolgono il trasferimento di dati personali verso Paesi terzi. E infatti, lo stesso autore evidenziava come in realtà il rapporto giuridico tra accordi internazionali e decisioni di adeguatezza parrebbe alquanto confuso, e a dimostrazione di ciò richiamava *l'Umbrella Agreement*[233].

---

[230] V. NARDONE, The Passenger Name Record Case: Profiling Privacy and Data Protection Issues in Light of CJEU's Opinion 1/15, in E. CARPANELLI, N. LAZZERINI (eds), *Use and Misuse of New Technologies – Contemporary Challenges in International and European Law*, Springer, 2019, pp. 146-147. Così anche E. CARPANELLI, N. LAZZERINI, PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU, in *Air & Space Law*, 42, no. 4&5 (2017), pp. 379-380 e 402. Queste ultime autrici, peraltro, avanzavano interessanti riflessioni circa possibili "effetti collaterali" del parere, tra cui l rischio di «*a DRI or Schrems 'reloaded' scenario, where the Court's review of EU acts in light of the EU Charter was provoked by references to a preliminary ruling raised by national courts*», p. 402.

[231] RELAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO sul riesame della direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, COM(2020) 305 final, 24.7.2020, p. 9.

[232]Cfr. C. KUNER, International agreements, data protection, and EU fundamental rights on the international stage, *cit*., p. 878. In realtà, oltre a «*a more thorough investigation of data protection standards in third countries*», l'autore individuava altre possibili ragioni per preferire le decisioni di adeguatezza agli accordi in materia: «*Changes to the law have also made it easier to adopt adequacy decisions for data sharing; (…) Political factors also favour the use of adequacy decisions*». Nello stesso senso si esprimeva l'autore anche in ID., Article 45. Transfers on the basis of an adequacy decision, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2020, p. 777.

[233] Ibidem, rispetto al quale rilevava possibili confusioni e coì, più in generale, esortava le istituzioni a interventi chiarificatori sul rapporto tra decisioni di adeguatezza e accordi: «*The EU institutions should pay closer attention to the relationship between adequacy decisions and international agreements, in order to avoid confusion between these two legal bases for data transfers*», p. 879.

Il c.d. *Umbrella Agreement* è un accordo stipulato tra UE e USA, dopo sei anni di trattative, che riguarda il trasferimento dei dati personali nell'attività di contrasto, per la prevenzione e il perseguimento di reati (che dunque, sotto il profilo interno, fuoriescono dall'ambito di applicazione del GDPR e sono disciplinati dalla direttiva 680/2016)[234]. Si tratta di un intervento volto ad integrare gli accordi esistenti puntando l'attenzione sulla tutela delle informazioni scambiate. Infatti, come prevede l'articolo 1, l'accordo mira a un livello elevato di tutela delle informazioni scambiate nell'ambito della cooperazione giudiziaria tra UE e USA per prevenzione e perseguimento di reati, compreso il terrorismo; tuttavia, esso "*non costituisce la base giuridica per il trasferimento delle informazioni personali*", rispetto al quale resta sempre necessaria una base giuridica[235]. Inoltre, all'articolo 5 si precisa: "*Il presente accordo integra, senza sostituire, le disposizioni sulla protezione delle informazioni personali contemplate negli accordi internazionali conclusi tra le parti, o tra gli Stati Uniti e gli Stati membri, che disciplinano materie rientranti nel campo di applicazione del presente accordo.*"[236]. Di qui, si comprendono le preoccupazioni sollevate dall'autore rispetto alla confusione che può ingenerarsi nel rapporto tra decisioni di adeguatezza e accordi con un certo Paese terzo. In quest'ordine di considerazioni potrebbero inserirsi anche le riflessioni di Hijmans sugli accordi UE-USA, laddove ravvisava che «*the agreements are exponents of a mix between a unilateral and a bilateral strategy, not of a genuine bilateral strategy*»[237].

Peraltro, è molto interessante in questo senso la questione, a cui qui si può solo fare cenno, del trasferimento dei dati personali rispetto agli accordi sul commercio internazionale[238]. Al riguardo, va segnalato che di recente il Garante europeo per la protezione dei dati si è proprio espresso,

[234] Accordo tra gli Stati Uniti d'America e l'Unione europea sulla protezione delle informazioni personali a fini di prevenzione, indagine, accertamento e perseguimento di reati, GU L 336 del 10.12.2016.
[235] Ibidem, Articolo 1 – *Scopo dell'accordo* (in part. par. 3).
[236] Ibidem, Articolo 5 – *Effetti dell'accordo*, par. 1. Ivi continua: "*il trattamento delle informazioni personali da parte degli Stati Uniti o dell'Unione europea e dei suoi Stati membri in relazione alle materie rientranti nell'ambito di applicazione del presente accordo è considerato conforme alle rispettive legislazioni sulla protezione dei dati che limitano o sottopongono a condizioni i trasferimenti internazionali di informazioni personali, e non è necessaria alcuna ulteriore autorizzazione ai sensi di tali legislazioni*", par. 3.
[237] H. HIJMANS, op. cit., p. 432.
[238] Per cui si rinvia, *ex multis*, a F. VELLI, The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements, in *European Papers*, Vol. 4, 2019, No 3, pp. 881-894.
Quanto allo specifico rilievo della base giuridica dei trasferimenti dei dati nel settore del commercio internazionale, Kuner segnalava la preferenza verso la decisione di adeguatezza: «The Commission has determined that data transfers in the contet of international trade are to be legalised by adequacy decisions rathern then by international agreements, based on a desire to avoid poitical controversy», C. KUNER, Article 45, cit., p. 777.

rispetto alle relazioni commerciali con il Regno Unito, nel senso di una impossibilità di negoziare la protezione dei dati, con il parere 3/2021 sulla conclusione dell'accordo commerciale EU-UK[239].

Per concludere con il riferimento agli accordi che coinvolgono la protezione dei dati, va detto, tornando ai PNR, che nel febbraio 2020 il Consiglio ha adottato una decisione di autorizzazione dell'avvio dei negoziati per un accordo PNR con il Giappone[240]. Inoltre, riprendendo le relazioni con gli USA (rispetto alle quali possono essere utili le note tematiche dei siti istituzionali sui trasferimenti tra i due Paesi)[241], va richiamato il *Terrorist Financing Tracking Programme* (TFTP), relativo ai dati di messaggistica finanziaria nell'ambito del controllo delle transazioni finanziarie dei terroristi, entrato in vigore nel 2010, rispetto al quale è stato notato il rilevante ruolo del Parlamento nelle varie vicende[242], e oggetto di verifica, la cui più aggiornata risale al 2019[243].

Inoltre, un cenno va fatto all'articolo 96 del GDPR, che stabilisce che gli accordi conclusi dagli Stati membri prima dell'entrata in vigore del Regolamento, laddove coinvolgono il trasferimento di dati personali, possono rimanere in vigore se conformi al diritto dell'Unione, anche se si tratta di una previsione soggetta a limitazioni[244].

Infine, trattando brevemente la "strategia multilaterale"[245], mentre la cooperazione al riguardo consisterebbe nella promozione di interventi volti a sensibilizzare gli attori internazionali rispetto

---

[239] EDPS, Opinion n. 3/2021 on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement, 22 February 2021, disponibile qui: https://edps.europa.eu/system/files/2021-02/2021_02_22_opinion_eu_uk_tca_en.pdf .
Per uno sguardo veloce, si indica anche il comunicato stampa: https://edps.europa.eu/press-publications/press-news/press-releases/2021/data-protection-non-negotiable-international_en .

[240] Decisione del Consiglio che autorizza l'avvio di negoziati con il Giappone per un accordo tra l'Unione europea e il Giappone sul trasferimento e sull'uso dei dati del codice di prenotazione (*Passenger Name Record*, PNR) al fine di prevenire e combattere il terrorismo e reati gravi di natura transnazionale, n. 5378/20, 4 febbraio 2020, disponibile qui: https://data.consilium.europa.eu/doc/document/ST-5378-2020-INIT/it/pdf .

[241] Dalla pagina web della Commissione europea *EU-US data transfers*: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_it , nonché quella Rules on international data transfers: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_it .

[242] Per il quale si rinvia, *ex multis*, alle considerazioni di J. SANTOS VARA, Transatlantic counterterrorism cooperation agreements on the transfer of personal data – A test for democratic accountability in the EU, in E. FAHEY, D. CURTIN Eds), *A Transatlantic Community of Law – Legal Perspectives on the Relationship between the EU and US Legal Orders* , 2014, Cambridge University Press, pp. 256-288.

[243] Il riferimento è alla RELAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO *relativa alla verifica congiunta dell'attuazione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi*, COM(2019) 342 final, 22.7.2019, disponibile qui: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=COM:2019:342:FIN&rid=4 .
Si riporta, inoltre, la Decisione del Consiglio di conclusione dell'accordo del 13 luglio 2010: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32010D0412&qid=1625827854511 .

[244] GDPR, Articolo 96 – *Rapporto con accordi precedentemente conclusi*. Il riferimento alle limitazioni è di D. MOORE, Article 96. Relationship with previously concluded Agreements, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU Gkeneral Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2020, p. 104, ma si veda pp. 1302-1306.

[245] Riprendendo Hijmans, p. 434 ss.

alla tutela dei dati, come le proposte di dialogo della Commissione e il suo incoraggiamento rispetto alla Convenzione 108 fanno intendere[246], strumenti rilevanti a livello internazionale (ancorché non vincolanti) sono le note Linee Guida OCSE e anche i principi previsti *nell'APEC Privacy Framework*[247]. Tale strategia rientrerebbe perfettamente nel solco delle previsioni dell'articolo 3, par. 5 TUE, riguardando anche la collaborazione con altre organizzazioni internazionali (in particolare, ONU), ma in realtà i risultati sembrano ben lontani da ciò che ci si potrebbe effettivamente aspettare: «*Given that the uncertainty that currently characterizes the 'EU case' also extends beyond EU borders, the most suitable solution would be the endorsement of a global approach, preferably through the adoption of a legally binding multilateral treaty. Yet, whilst the increasing complexity of the current scenario should ordinarily act as a catalyst for beginning negotiations in this respect, the growing reluctance of States to undertake binding international commitments, and the very specific nature of the subject at hand, suggest that this will hardly be the case*»[248].

Ebbene, alla luce di quanto esposto sui più rilevanti interventi di cooperazione internazionale e richiamando la posizione di Schwartz sul punto, è possibile assumere il significato e l'importanza dell'articolo 50 GDPR, che chiude il Capo V dedicato al trasferimento dei dati verso l'esterno ed è proprio dedicato alla cooperazione internazionale nella protezione dei dati personali[249]. Una simile previsione, che non trova un parallelo nella normativa precedente della Direttiva madre, testimonia infatti la sensibilità rinnovata del legislatore europeo rispetto all'importanza della cooperazione internazionale per incentivare la protezione dei dati personali a livello globale. Ciò, in linea con l'approccio che stiamo proponendo in questo lavoro, pare in qualche misura esplicativo dei due moti che condizionerebbero lo sviluppo del processo di integrazione europea. Infatti, è sicuramente possibile ravvisare delle spinte esterne che hanno apportato sfide al diritto europeo alla protezione dei dati personali e che sono quindi state rilevate sin dalla proposta della Commissione per il

[246] Cose che, come si è detto, si evincono dalla Comunicazione del 2017, cit.

[247] APEC PrivacyFramework, 2015, available here: https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[248] E. CARPANELLI, N. LAZZERINI, PNR: Passenger Name Record, Problems Not Resolved?, *cit*., pp. 401-402.

[249] GDPR, Articolo 50 – *Cooperazione internazionale per la protezione dei dati personali*
In relazione ai paesi terzi e alle organizzazioni internazionali, la Commissione e le autorità di controllo adottano misure appropriate per:
a) sviluppare meccanismi di cooperazione internazionale per facilitare l'applicazione efficace della legislazione sulla protezione dei dati personali;
b) prestare assistenza reciproca a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, in particolare mediante notificazione, deferimento dei reclami, assistenza alle indagini e scambio di informazioni, fatte salve garanzie adeguate per la protezione dei dati personali e gli altri diritti e libertà fondamentali;
c) coinvolgere le parti interessate pertinenti in discussioni e attività dirette a promuovere la cooperazione internazionale nell'applicazione della legislazione sulla protezione dei dati personali;
d) promuovere lo scambio e la documentazione delle legislazioni e prassi in materia di protezione dei dati personali, compresi i conflitti di giurisdizione con paesi terzi

GDPR, trovando così espressione nell'articolo 50: «*data processing has become globalised through the growth of the internet and other electronic communications networks; the reduction of capital controls and the liberalisation of international trade by the foundation of the World Trade Organization ('WTO'); the increasing economic and political power of developing countries outside of Europe and North America*»[250]. Nell'ottica di queste spinte esterne va inteso, dunque, il "moto opposto" che si comprende nella lettura congiunta degli articoli 3 GDPR e delle previsioni (articoli 44-50) del suo Capo V, verso un'estensione della portata del diritto europeo alla protezione dei dati. Ebbene, in questo ordine di idee, la cooperazione internazionale, ancorché non ancora assimilabile agli interventi unilaterali (che illustreremo a breve) quanto a risultati tangibili in termini di influenza dell'Unione verso l'esterno, per le delineate perplessità e difficoltà che essa contiene, è comunque considerata potenzialmente molto utile (se non, per certi aspetti, *più* utile dell'intervento unilaterale) a corroborare l'intervento dell'Unione nel prossimo futuro. In questo senso, l'articolo 50 esorta la Commissione e le autorità di controllo ad adottare le misure appropriate, ribadendo l'importanza delle ultime anche sul piano esterno, che si aggiunge quindi alle altre previsioni che richiedono la cooperazione tra autorità di controllo a livello interno, e si aggiunge anche ai compiti attribuiti all'EDPB rispetto alla cooperazione internazionale (cfr. Articolo 70, par. 1, lett. v) e w), GDPR)[251]. La suddetta Comunicazione della Commissione del 2017 parrebbe in linea con queste previsioni nel promuovere la cooperazione internazionale. Eppure, come abbiamo visto, allo stato attuale l'intervento dell'Unione pare ancora parziale. Sicuramente, previsioni del genere a livello legislativo e di prassi sono già emblematiche dell'attenzione riconosciuta a livello istituzionale, ma in sostanza deve ancora darsi una piena attuazione a tali previsioni. Sicuramente, e come il suddetto recente parere del EDPS dimostra, l'evento Brexit sarà foriero di interessanti occasioni di cooperazione tra l'Unione e il Regno Unito che, più o meno indirettamente coinvolgeranno la protezione dei dati.

Così delineato il quadro di intervento dell'Unione quanto alla cooperazione internazionale per il trasferimento di dati personali, possiamo passare elementi ad un'analisi critica di quello unilaterale.

[250] C. KUNER, Article 50. International cooperation for the protection of personal data, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020, p. 858.

[251] Ibidem, pp. 859-860. Si segnala che l'autore spiega come l'articolo sia ispirato alle Raccomandazioni OCSE e, commentandolo, che può dividersi in due aree, rispettivamente individuabili nelle prime due e ultime due lettere dell'articolo 50: «*namely tasks that are designed to enhance cross-border enforcement of data protection violations, and exortations to the Commission and data protection authorities to cooperate with other actors on the international data protection stage*».

3. Lo strumentario per il trasferimento dei dati verso l'esterno: l'influenza unilaterale dell'Unione

Il GDPR dedica, come abbiamo detto, un'importante parte ai meccanismi per il trasferimento dei dati dall'Unione europea verso l'esterno, che pare abbastanza ricca specie in raffronto alla normativa precedente prevista dalla Direttiva madre (composta di soli due articoli). Ciò, invero, costituisce anche un'importante conseguenza delle conclusioni della Corte di giustizia nel caso *Schrems I*. Pertanto, nel condurre l'analisi che segue, l'intera *saga Schrems* sarà il nostro punto di vista privilegiato, indispensabile per comprendere le cause che l'hanno generata e soprattutto le conseguenze che ha comportato per l'intero impianto sovranazionale di protezione dei dati personali e non solo, con un impatto notevole sia sulle dinamiche interne ed esterne di mercato che, più in generale, sulle scelte politiche e sull'affermazione (ovvero, sulle sfide) del sistema valoriale dell'Unione. Ancora una volta, quindi, pur nel prospettare un'analisi onnicomprensiva delle non poche figure di rilievo nel settore, sicuramente rileverà (potremmo dire, quale *primus inter pares*) il ruolo della Corte di giustizia.

Ad apertura del Capo V, l'articolo 44, che va letto insieme ai Considerando 101 e 102, espone il "*principio generale per il trasferimento*"[252], dal quale si evince, in continuità con la direttiva, che il livello di tutela garantito dalla normativa europea non deve essere pregiudicato dal trasferimento; inoltre, innovando rispetto alla direttiva, esso amplia la portata della normativa poiché estende l'applicazione del Regolamento anche ai trasferimenti alle organizzazioni internazionali, nonché ai c.d. *trasferimenti successivi*, ossia quelli che vengono effettuati dal Paese terzo o l'organizzazione internazionale destinatari di dati dall'Unione europea ad altri Paesi terzi o organizzazioni internazionali. Dunque, è bene ribadirlo, il principio generale che governa la materia dei trasferimenti è, sin dalla direttiva madre, quello della *continuità di tutela dei dati personali*[253].

Va segnalata, inoltre, la questione del rapporto tra le previsioni del Capo V e l'articolo 3 del GDPR. La trattazione del Capo dedicato al trasferimento di dati verso l'esterno richiama, infatti,

[252] GDPR, Articolo 44 – *Principio generale per il trasferimento*
Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

[253] Come ribadito nell'interessante EDPS *Case-Law Digest: transfers of personal data to third countries*, 2021, p. 2, a cui si farà spesso riferimento.

inevitabilmente le esposte considerazioni sull'ambito territoriale del GDPR, nonché le riflessioni teoriche sull'extraterritorialità e/o estensione territoriale del diritto dell'Unione nella dimensione esterna. Infatti, «*the GDPR's rules on trans-border data flows can be viewed as a form of applicable law provision. The interaction between Article 3 and Chapter V can result in situations where the GDPR both applies to a non-EU data controller or processor, and a data transfer mechanism must be used in order to transfer data to such parties (…). However, as things now stand, Article 3 and Chapter V must be applied separately, and compliance with one does not remove the obligation to comply with the other when it is applicable*»[254]. Anche l'EDPB rilevava, invero, la relazione tra tali previsioni del GDPR, nelle suddette Linee-guida n. 3/2018, prospettando la possibilità di orientamenti chiarificatori al riguardo, laddove necessari[255]. Ad ogni modo, se è vero che, come si anticipava, la demarcazione sia tra i diversi gradi possibili di extraterritorialità che tra questa e l'estensione territoriale tendono a svanire quando si tratta di influenza esterna dell'Unione nel settore della protezione dei dati personali, è altrettanto vero però che le disposizioni del Capo V costituiscono un importante esempio di tale applicazione extraterritoriale del diritto dell'Unione[256].

Ciò posto, risulta ben rafforzato lo strumentario che consente ora di trasferire dati all'esterno: oltre alla classica decisione di adeguatezza della Commissione, prevista in maniera più dettagliata (dall'attuale articolo 45, rispetto all'articolo 25 della direttiva), il Regolamento aggiunge all'articolo 46 che in mancanza di tale decisione "*il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi*", riprendendo in maniera più arricchita le previsioni dell'articolo 26 della Direttiva per individuare le c.d. *garanzie adeguate*. Tra queste, vanno da subito segnalate le c.d. *norme vincolanti di impresa* (*binding corporate rules*, di seguito anche BCR) e le c.d. *clausole tipo di potezione* (*standard contractual clauses*, di seguito anche SCC); delle prime, nella misura in cui vengono approvate dall'autorità di controllo nell'ambito del meccanismo di coerenza (cfr. *supra*, Capitolo III, Parte III e *infra*, Capitolo III), si occupa l'articolo 47 del GDPR. Quindi, l'articolo 48 riguarda i trasferimenti non autorizzati dal diritto dell'Unione, richiamando accordi internazionali, mentre l'articolo 49 riguarda le deroghe in specifiche situazioni, che consentirebbero il

[254] C. KUNER, Article 44, *cit*., p. 758.
[255] EDPB, Linee-guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3), *cit*., p. 24.
[256] Cfr. C. KUNER, The Internet and the Global Reach of the EU Law, cit., p. 124, in cui si legge: «*Much of the EU's infuence in data protection occurs through the extraterritorial application of EU law. There are different varieties or degrees of extraterritoriality (…). With regard to EU data protection law, it is less important to categorize the exact form of extraterritoriality used, than to recognize that it exerts its influence in different ways on persons and activities in third countries*».

trasferimento nonostante non ricorrano le condizioni degli articoli 45 e 46. Si è già detto, infine, dell'articolo 50 che chiude il capo V con un riferimento ai casi di cooperazione internazionale per il trasferimento dei dati verso l'esterno. Dunque, il GDPR propone attraverso il Capo V una "*three-tiered structure*" per le basi giuridiche legittimanti i trasferimenti verso l'esterno, con la decisione di adeguatezza a livello più alto, le garanzie adeguate in mezzo e le deroghe al livello più basso[257].

Inoltre, per completezza, va segnalato che, poiché, come abbiamo visto, il GDPR non copre i trattamenti effettuati dalle autorità nazionali competenti per fini penali (*ex* art. 2, par. 2, lett d) dei quali si occupa la direttiva 680/2016, che contiene delle previsioni parallele al GDPR quanto ai trasferimenti di dati verso l'esterno. Infatti, il Capo V della direttiva è rubricato "*Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*" e si compone di cinque articoli (da 35 a 40) corrispondenti a quelli del GDPR ma specifici dell'ambito di applicazione della direttiva. Senza poterne approfondire i commenti, basti dire che la differenza principale con la normativa prevista dal GPDR è data dal fatto che, trattandosi di una direttiva, nei casi di trasferimenti di dati rientranti nel suo ambito di applicazione toccherà agli Stati membri implementarne le previsioni: «*the LED requires implementation in the Member States and compliance with requirements of national law. the LED is generally more liberal about allowing data transfers and contains bses for them that do not appear in the GDPR*»[258].

Prima di analizzare gli strumenti più rilevanti che costituiscono la base giuridica dei trasferimenti, con particolare attenzione alle previsioni degli articoli 45, 46 e 49 del GDPR anche tramite l'analisi della prassi e della giurisprudenza correlate, procediamo a dare conto delle due suddette innovazioni presentate dal GDPR per l'intera disciplina, ossia il riferimento esplicito alle organizzazioni internazionali come possibili destinatarie del trasferimento, e l'ampliamento della normativa ai trasferimenti successivi. Per farlo, cerchiamo di capire anzitutto cosa si intende per "trasferimento di dati personali" verso l'esterno, al fine di comprendere in quali casi si applichi la disciplina appena esposta. In generale, segnaliamo che un'interessante guida alla comprensione delle disposizioni del Capo V è data ora dal *EDPS case-law digest: transfers of personal data to third countries* del giugno 2021, realizzato, appunto, dal Garante europeo per chiarire la struttura dell'analisi realizzata dalla Corte di giustizia rispetto alla complessa materia del trasferimento dei dati personali all'esterno, al quale faremo spesso riferimento.

Come i commentatori sogliono evidenziare, una definizione di trasferimento non è espressamente prevista dal GDPR, non potendosi essa ravvisare nel riferimento dell'articolo 4, p. 23, lett. a) e b),

[257] C. KUNER, Article 45. Transfers on the basis of an adequacy decision, *cit.*, p. 774.
[258] C. KUNER, Article 44, *cit*. p. 766.

GDPR, poiché il "trasferimento transfrontaliero" ivi previsto riguarda situazioni coinvolgenti più Stati membri, dunque non di circolazione all'esterno dell'Unione europea. E invero, così rilevava la Corte nel primo caso che sollevò una questione di trasferimento di dati, ossia il già trattato caso *Lindqvist*, in cui espressamente riconosceva che la direttiva non prevedesse in nessuna disposizione la nozione di trasferimento verso uno Stato terzo. La questione sollevata in quel caso, come si ricorderà, riguardava la possibilità di ravvisare un "trasferimento verso Paesi terzi" nel caso di caricamento in una pagina Internet di dati personali da parte di una persona residente in uno Stato membro, per il fatto che i dati divenissero accessibili anche da soggetti che si trovavano in Stati terzi. Si trattava, dunque, di «stabilire se la nozione di "trasferimento" dovesse ricomprendere o meno il puro transito dei dati»[259]. La Corte, a seguito di analisi al riguardo, concludeva che "*operazioni come quelle effettuate dalla sig.ra Lindqvist non costituiscono di per sé un «trasferimento verso un paese terzo di dati». Non è quindi necessario accertare se una persona di un paese terzo abbia avuto accesso alla pagina Internet di cui trattasi o se il server di tale fornitore si trovi fisicamente in un paese terzo. (…) non si configura un «trasferimento verso un paese terzo di dati» ai sensi dell'art. 25 della direttiva 95/46 allorché una persona che si trova in uno Stato membro inserisce in una pagina Internet - caricata presso il suo fornitore di servizi di ospitalità («web hosting provider»), stabilito nello Stato stesso o in un altro Stato membro - dati personali, rendendoli così accessibili a chiunque si colleghi ad Internet, compresi coloro che si trovano in paesi terzi*"[260].

A partire, dunque, da ciò che i trasferimenti *non* sono, questa conclusione della Corte ha rappresentato per parecchio tempo, e anzi potrebbe dirsi ancora ora[261], il solo riferimento definitorio a livello sovranazionale, nonostante il sollecito avanzato dall'EDPS alla Commissione per individuare una nozione più puntuale in sede di proposta di GDPR[262]. Gli interventi giurisprudenziali successivi, come ci ricorda Kuner, hanno infatti corroborato questo orientamento insistendo sulla necessità di garantire un adeguato livello di tutela alla luce della Carta: «*The* Schrems *judgment demonstrates that the CJEU views the concept of an international data transfer in terms of requiring a high level of protection based on EU standards with regard to personal data*

[259] G.M. RICCIO, F. PEZZA, Trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali, *cit*., p. 593.
[260] Corte di giustizia, causa C-101/01, *Bodil Lindqvist c. Åklagarkammaren i Jönköping*, 6 novembre 2003, pp. 70-71. Prima, sulla mancanza di definizioni nella direttiva, p. 56.
[261] G.M. RICCIO, F. PEZZA, *op. cit*., che rilevano come si tratti «di una nozione la cui esatta demarcazione appare tuttora controversa e che, senz'altro risulta ancor più difficoltosa alla luce dell'avvento di tecnologie sempre più avanzate», p. 593. Al riguardo, dopo aver ripensato al caso *Linqvist* alla luce dei casi *Schrems* e del parere 1/15, Kuner a sua volta riteneva: «*if the CJEU were faced today with a case involving facts similar to those in Linqvist, it would likely be reluctant to find that the GDPR does not apply to placing personal data on an internet site*», cfr. C. KUNER, Article 44, *cit*., p. 763.
[262] Opinion EDPS on data protection reform package, 7 March 2012, https://edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf .

that are sent or made accessible across national borders, rather than based on a set definition. The Grand Chamber of the Court then affirmed the Schrems *rationale in* Opinion 1/15»[263]. Dunque, si potrebbe concludere al riguardo che, nella continua assenza di una precisa definizione, come riconosce anche l'EDPS, è necessaria ancora una valutazione caso per caso per individuare le situazioni in presenza delle quali può ritenersi avvenire un trasferimento[264].

Passiamo quindi a sindacare brevemente i due punti di novità che abbiamo presentato.

Cominciando coi "trasferimenti successivi", va detto che anche in tal caso il GDPR manca di una definizione precisa, limitandosi (all'articolo 44 e al Considerando 101) ad indicare che essi riguardano trasferimenti da Paesi terzi o organizzazioni internazionali destinatari di dati personali dall'Unione europea verso ulteriori Paesi terzi o organizzazioni internazionali. La stessa scarna indicazione si rinviene nelle nuove *clausole contrattuali tipo* individuate come garanzie adeguate dalla Commissione nella sua recente decisione di esecuzione del 4 giugno 2021[265]. Come nota Kuner, i trasferimenti successivi sono in realtà molto frequenti e possono chiaramente portare al rischio di aggirare il principio della continuità dell'adeguato livello di tutela dei dati trasferiti dall'Unione europea: «*The reasons for requiring a high level of protection for onward transfers under the GDPR can be explained in light of concerns that arose under the EU-US Safe Harbor system invalidated by the CJEU in* Schrems*, in which data transferred first to the US could then be easily on to other third countries*»[266]. In tal senso, l'autore segnalava l'importanza dei *criteri di riferimento per l'adeguatezza* adottati dal Gruppo di Lavoro Articolo 29, in cui si prospettavano restrizioni ai trasferimenti successivi[267]. E infatti, nel suddetto parere 1/15 la Corte di giustizia espressamente ribadiva la necessità di evitare il rischio che il livello di protezione garantito dall'Unione e preteso dai destinatari dei dati venisse raggirato con trasferimenti successivi: «*un*

[263] C. KUNER, Article 44, *cit*., p. 763.
[264] EDPS *Case-Law Digest, cit.*, p. 31: «*a case-by-case assessment is necessary, which takes into consideration the intentions of the legislature (purpose and structure of the transfers provisions), as well as the consequences of the qualification of the data processing as transfer to third countries*».
[265] Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, C/2021/3972.
[266] C. KUNER, Article 44, *cit*., p. 763.
[267] Gruppo di Lavoro Articolo 29*, Criteri di riferimento per l'adeguatezza* – Adottati il 28 novembre 2017, Versione emendata e adottata il 6 febbraio 2018, WP 254 rev.01, scaricabili da qui: https://ec.europa.eu/newsroom/article29/items/614108 .
9) *Restrizioni ai trasferimenti successivi*
Ulteriori trasferimenti dei dati personali da parte del destinatario del primo trasferimento dovrebbero essere consentiti soltanto quando anche il secondo destinatario (ossia il destinatario del trasferimento successivo) è soggetto a norme (comprese le norme contrattuali) che assicurano un livello di protezione adeguato e prevedono il rispetto delle istruzioni pertinenti durante il trattamento dei dati per conto del titolare del trattamento. Il livello di tutela delle persone fisiche i cui dati sono trasferiti non deve essere compromesso dal trasferimento successivo. Spetta al primo destinatario dei dati trasferiti dall'UE assicurare che siano previste garanzie adeguate per i trasferimenti successivi dei dati in mancanza di una decisione di adeguatezza. Tali trasferimenti successivi di dati dovrebbero essere possibili soltanto per finalità determinate e limitate e purché sussista una base giuridica per il trattamento.

trasferimento di dati personali dall'Unione a un paese terzo può avvenire solo se tale paese assicura un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'Unione. Tale requisito vale anche nel caso della comunicazione dei dati PNR dal Canada verso altri paesi terzi, di cui all'articolo 19 dell'accordo previsto, al fine di evitare che il livello di protezione previsto da tale accordo possa essere eluso da trasferimenti di dati personali verso paesi terzi e di assicurare la continuità del livello di protezione offerto dal diritto dell'Unione»[268].

Passando, poi, al nuovo riferimento alle organizzazioni internazionali tra i possibili destinatari di trasferimenti di dati dall'Unione europea, una definizione di queste può rintracciarsi invece nell'articolo 4, par. 1, n. 23) del GDPR[269]. La questione del rapporto tra GDPR e organizzazioni internazionali riguarda essenzialmente l'applicabilità del primo alle seconde, e/o la prevalenza di previsioni di diritto internazionale. Kuner si è occupato dell'impatto del GDPR per i trattamenti di dati effettuati dalle organizzazioni internazionali, rilevando che nonostante il Regolamento contenga diverse disposizioni che si riferiscono alle OI, esso effettivamente non chiarisce se si applica alle stesse o meno[270]. In particolare, l'autore rilevava a favore della posizione per cui il GDPR non dovrebbe applicarsi alle OI la constatazione che tutte le volte in cui queste sono menzionate, vengono accostate agli Stati terzi, ai cui trattamenti il GDPR ovviamente non si applica. Inoltre, in questa prospettiva, mancherebbero dei riferimenti espliciti a obbligazioni poste dal GDPR in capo a OI, salvo quella appunto dell'articolo 44 ossia in caso di trasferimenti di dati dall'Unione europea[271]. Nondimeno, alla luce di un'analisi comprendente anche privilegi e immunità di cui le OI potrebbero godere in virtù del diritto internazionale, l'autore concludeva che «*it seems that IOs may potentially fall under both the material scope and the territorial scope of the GDPR*»[272]. Invero, la questione rimane controversa per la tensione che mantiene tra diritto sovranazionale, in vigore negli Stati membri UE che partecipano a quelle OI, ed internazionale, con privilegi e immunità che riconosce queste ultime: «*In enacting the GDPR, the EU legislator failed to clarify its application to IOs, which creates legal uncertainty for IOs, the individuals whose*

[268] Corte di giustizia, Parere n. 1/15, *Accordo PNR Canada*, cit., p. 214, sottolineato aggiunto.
Al riguardo, cfr. EDPS *Case-Law Digest, cit*., p. 54.
[269] GDPR, Articolo 4 – *Definizioni*
26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.
Si rinvia al commento di L. TOSONI, L.A. BYGRAVE, Article 4. Definitions, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2020, p. 101 ss.
[270] C. KUNER, The GDPR and International Organisations, *AJIL Unbound*, 114, 2020, p. 15.
[271] C. KUNER, International Organizations and the EU General Data Protection Regulation, University of Cambridge Faculty of Law Research Paper No. 20/2018, pp. 12-13.
[272] Ibidem p. 16, ma si veda da p. 14 ss.

personal data they process, and regulators who are charged with enforcing data protection law»[273]. Se è vero che l'impatto globale del GDPR ha portato (come anche molti Stati terzi) diverse organizzazioni internazionali a conformarvi il proprio sistema di protezione dei dati[274], è anche vero che permangono perplessità al riguardo, come quelle sollevate di recente dinanzi la Corte di giustizia proprio rispetto al trattamento operato da Interpol rispetto a dati trasferiti ai sensi della direttiva 2016/680[275]. La questione dell'applicazione del GDPR può comunque esaurirsi con il seguente riferimento: «*The Commission has taken the view informally that the GDPR does not directly apply to international organisations, but that they must comply with the GDPR's data transfer rules when they receive personal data from the EU*»[276]. Dunque, e per quel che interessa ai nostri fini, sicuramente i trasferimenti di dati dall'Unione europea verranno coperti dalla normativa sovranazionale (in senso lato, comprensiva della direttiva), a seconda dei diversi meccanismi consentiti, come per gli Stati terzi, che passeremo ora ad analizzare.

Sulle questioni che potrebbero sorgere con riguardo al concetto di "Paesi terzi" rispetto al peculiare caso del Regno Unito (prima Stato membro, poi terzo), esse verranno eventualmente trattate nella parte dedicata alle conseguenze della Brexit per la protezione dei dati personali.

4. Le Decisioni di adeguatezza della Commissione

[273] C. KUNER, The GDPR and International Organisations, *cit*., p. 19, in cui l'autore continuava criticamente: «*The European Commission should also confirm publicly its informal position that the GDPR does not apply to IOs (aside from its rules on data transfers from the EU) and indicate the legal reasoning that underlies it*».

[274] Ibidem, pp. 15-16: «*Data protection laws can provide "rules of the road" for the processing of personal data that are derived from regional and international human rights standards, and can also help to build trust with the individuals and organizations to whom IOs are accountable. For these reasons, a number of IOs have already adopted their own internal data protection rules, including the International Organization for Migration, the International Committee of the Red Cross (ICRC), the UN High Commissioner for Refugees, the International Criminal Police Organization (INTERPOL), and the World Food Programme, among others. In December 2018, the United Nations also approved a set of personal data protection and privacy principles for processing personal data by or on behalf of UN organizations*».

[275] Come fa notare C KUNER, Article 44, cit. p. 764, il riferimento è ad un rinvio pregiudiziale tedesco in cui si dubitava dell'adeguato livello di protezione dei dati nel caso di trasferimento a Interpol secondo le previsioni della direttiva, su cui la Corte si è pronunciata lo scorso maggio 2021. Cfr. Corte di giustizia, C-505/19, *WS c. Bundesrepublik Deutschland*, 12 maggio 2021, in part. p. 37: «*Il giudice del rinvio indica che la Commissione e gli Stati membri non sembrano essersi avvalsi, per quanto riguarda l'Interpol, della possibilità, offerta dall'articolo 40 della direttiva 2016/680, di adottare norme sulla cooperazione internazionale nel settore della protezione dei dati personali in relazione ai paesi terzi e alle organizzazioni internazionali. Inoltre, gli articoli 36 e 37 di questa direttiva sarebbero riferibili unicamente ai trasferimenti di dati personali all'Interpol, e non al trasferimento di tali dati dall'Interpol agli Stati membri. Secondo il giudice del rinvio, detta direttiva contiene quindi una lacuna normativa che dovrebbe essere colmata. Il fatto che l'Interpol proceda al trasferimento verso gli Stati membri di dati personali contenuti nei suoi avvisi rossi, nonostante l'applicabilità del principio del ne bis in idem ai fatti oggetto di tali avvisi, e non assicuri che tali dati siano cancellati senza indugio quando il trattamento di tali dati è illecito solleverebbe seri dubbi in merito all'affidabilità, in materia di protezione dei dati personali, di tale organizzazion*e».

[276] C. KUNER, Article 44, cit., p. 764.

Previsioni normative

L'articolo 25 della Direttiva madre, dedicato ai principi per il trasferimento di dati verso Paesi terzi, prevedeva al par. 6 che la Commissione adottasse decisioni (seguendo la procedura dell'art. 31) con cui constatare che un Paese terzo garantiva un livello di protezione adeguato. In sede di riforma, mentre, come si è visto, le disposizioni di principio sono contenute nell'articolo 44, la decisione di adeguatezza viene trattata, in maniera molto più approfondita, dall'articolo 45 GDPR.

Seguendo le previsioni che abbiamo illustrato, dalla riforma emerge un ampio strumentario per legittimare il trasferimento di dati personali dall'Unione europea, con la previsione, come si è anticipato, della decisione di adeguatezza della Commissione quale base giuridica principale e preferenziale, in mancanza della quale vale il riferimento alle garanzie adeguate e solo da ultimo è prevista la possibilità di deroghe (secondo ciò che Kuner ha individuato come struttura a tre livelli).

Quanto all'ambito di applicazione del GDPR, l'attuale articolo 45 si compone di ben nove paragrafi, dedicati al ruolo della Commissione prima e dopo l'adozione della decisione, che specificano anche le modalità di valutazione dell'adeguatezza, contenendo una dettagliata lista di condizioni, nonché la necessità di un riesame periodico (almeno quattro anni) e la possibilità di revoca, modifica o sospensione della decisione[277].

Come si prospettava, i trasferimenti di dati effettuati dalle autorità per il perseguimento di reati vengono, invece, disciplinati dalla direttiva 2016/680, che, parallelamente al GDPR, pure dedica l'articolo 36 alla decisione di adeguatezza della Commissione.

Le decisioni di adeguatezza trovano il loro fondamento nell'articolo 288, c. 4, TFUE e, come prevede l'articolo 45 GDPR, vengono adottate secondo la procedura indicata dall'articolo 93 GDPR, che rinvia alle previsioni del Regolamento n. 182/2011.

Sul significato di adeguatezza

La prima questione che si pone trattando queste decisioni è, chiaramente, cosa si intenda per "adeguatezza" del livello di protezione garantito dal Paese terzo o dall'organizzazione

[277] GDPR, Articolo 45 – *Trasferimento sulla base di una decisione di adeguatezza*
1. Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono *un livello di protezione adeguato*. In tal caso il trasferimento non necessita di autorizzazioni specifiche. (…)

internazionale destinatari di dati. Ebbene, a seguito delle previsioni della direttiva madre, il Gruppo di Lavoro Articolo 29 intervenne nel 1998 con un documento di lavoro con cui, trattando dell'applicazione degli articoli 25 e 26, affrontava il tema della tutela adeguata. Va ricordato che l'articolo 25 (con una struttura diversa rispetto all'attuale articolo 45 GDPR) richiedeva che il Paese terzo destinatario garantisse un "livello di protezione adeguato" rispetto al quale disponevano e interagivano gli Stati membri e la Commissione, con la possibilità di adottare misure nel caso di constatazione di non adeguatezza (cfr. art. 25, parr. 1-4)[278]. Ebbene, nel sindacare in cosa consistesse la "tutela adeguata", il Gruppo di Lavoro A29 prospettava intanto un approccio che è in linea con l'analisi pratica che vogliamo qui condurre, stabilendo una cosa tanto scontata quanto utile, dopo aver constatato una continuità tra le previsioni della direttiva e quelle della Convenzione 108 come anche degli orientamenti OCSE e ONU in materia, ossia che "*Tali norme, tuttavia, contribuiscono alla tutela dell'individuo solo se sono osservate nella pratica. È pertanto necessario considerare non soltanto il contenuto delle norme applicabili ai dati personali trasferiti verso un paese terzo, ma anche i meccanismi posti in essere per garantirne l'efficacia*"[279]. Pertanto, in quest'ottica il Gruppo di lavoro ribadiva che il significato di "tutela adeguata" si componesse di "*due elementi essenziali: il contenuto delle norme applicabili e gli strumenti per assicurarne un'efficace applicazione*", prospettando quindi una lista di condizioni minime per valutare detta adeguatezza[280]. Ebbene, la previsione di una lista di requisiti necessari per sindacare l'adeguatezza

[278] Direttiva 95/46, Articolo 25 – *Principi*
1. *Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva*. 2. *L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate*. 3. *Gli Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2.* 4. Qualora la Commissione constati, secondo la procedura dell'articolo 31, paragrafo 2, che un paese terzo non garantisce *un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione.* 5. *La Commissione avvia, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione di cui al paragrafo 4.* 6. *La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona. Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.*

[279] Gruppo di Lavoro A29, Documento di lavoro – *Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati*, Approvato il 24 luglio 1998, WP12, p. 5, disponibile qui: https://www.garanteprivacy.it/documents/10160/10704/COMMISSIONE+EUROPEA+-+Trasferimenti+di+dati+personali+verso+Paesi+terzi.pdf/05447447-7f9b-4571-8da7-50d029a5f62c?version=1.1 .

[280] Ibidem, in cui continuava: "*dovrebbe essere possibile individuare un nucleo di principi di 'contenuto' e di prescrizioni di 'procedura/applicazione', la cui osservanza potrebbe essere considerata una condizione minima di adeguatezza della tutela. Si tratterebbe di una lista di riferimento duttile: eventualmente da integrare in alcuni casi, da ridimensionare quanto alle prescrizioni di altri. Il grado di rischio insito nel trasferimento per la persona interessata sarà un elemento importante ai fini della determinazione delle prescrizioni esatte di un caso particolare. Pur con*

del sistema destinatario del trasferimento di dati dall'Unione europea viene ora, in qualche modo, evocata dall'articolo 45 GDPR, che al paragrafo 2 individua tre gruppi di elementi, di portata più generale rispetto alle condizioni di tutela precitate, che la Commissione deve prendere in considerazione nel suo scrutinio sul sistema esterno, sintetizzabili come segue: il primo riguarda lo stato di diritto, in tutti i suoi elementi peculiari; quindi, l'effettiva sussistenza di autorità di controllo indipendenti in quel sistema; infine, gli impegni internazionali assunti da Paese terzo o organizzazione internazionale destinatari[281]. Sul punto, va notato il parallelo con la previsione dell'articolo 36 della direttiva 2016/680, che ripropone essenzialmente gli stessi elementi con riguardo allo specifico ambito di applicazione. In questo specifico settore, tuttavia, Kuner notava che «[it] *may be difficult for foreign law enforcement authorities to meet since independent data protection authorities are a specific feature of EU data protection law that is not replicated in all other systems*»[282]. In realtà, l'espressa previsione normativa in tali nuovi articoli degli elementi che la Commissione deve tenere in considerazione nella sua valutazione ai fini dell'adozione delle decisioni di adeguatezza, di cui pure si sentiva l'urgenza sin da subito (come palesato dal documento del Gruppo di Lavoro A29), è stata grandemente stimolata dalla sentenza della Corte di giustizia sul caso *Schrems I*[283].

Il caso Schrems I

Abbiamo avuto modo di esporre il caso *Schrems I* quando abbiamo analizzato il ruolo delle autorità di controllo nella trattazione di reclami relativi a decisioni di adeguatezza della Commissione (cfr. *supra*, par. 2, Capitolo III). I fatti sono, dunque, noti. Ebbene, quella pronuncia risulta particolarmente rilevante rispetto alle decisioni di adeguatezza della Commissione e sicuramente

---

questa limitazione, la compilazione di una lista di condizioni minime costituisce un utile punto di partenza per qualsiasi analisi". pp. 5-6, per le condizioni v. sino a p. 8.

[281] GDPR, Articolo 45 – *Trasferimento sulla base di una decisione di adeguatezza*

2. Nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione in particolare i seguenti elementi:

a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento;

b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e

c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali.

[282] C. KUNER, Article 45, *cit.*, p. 792.

[283] Ibidem, p. 788.

costituisce un punto di riferimento al riguardo. Infatti, è vero che essa non è stata la prima in cui la Corte ha annullato una tale decisione, posto che ciò avvenne già – come abbiamo detto – nella pronuncia del 2006 sul caso *Parlamento c. Consiglio* relativo al trasferimento dei dati PNR, ma in tale caso la Corte annullò l'allora decisione di adeguatezza della Commissione sugli USA (come anche la decisione del Consiglio di concludere un accordo in materia) perché fuoriusciva dall'ambito di applicazione della direttiva[284], dunque senza sindacarne il merito. Pertanto, possiamo dire a buon diritto che la pronuncia sul caso *Schrems I* rappresenta la prima al riguardo, da cui l'impatto che ne è derivato.

Per la prima volta, infatti, un cittadino dell'Unione, a seguito delle rilevazioni di Snowden sugli scandali della NSA degli Stati Uniti (che possiamo senz'altro considerare di fatto tra le "spinte esterne" che ultimamente modellano lo sviluppo del processo di integrazione europea), poneva in dubbio, nell'ambito di quello che può dirsi per definizione un esempio di *strategic litigation*[285], la valutazione sull'adeguatezza del sistema statunitense ritenuta dalla Commissione con la decisione 2000/520, tramite cui la Commissione approvava i principi del regime c.d. *Safe Harbor* ("approdo sicuro")[286], contestandone dunque la validità. Invero, va detto che proprio a seguito di quelle rilevazioni sul sistema di sicurezza statunitense la Commissione europea (dopo ben 13 anni dall'approvazione della decisione) palesò in due Comunicazioni del 2013 delle perplessità sugli scambi di dati UE-USA[287], rintracciando già vari punti deboli del regime di approdo sicuro[288].

Ebbene, la Corte, trovandosi ad analizzare le disposizioni della direttiva madre, anzitutto constatava che «*né l'articolo 25, paragrafo 2, della direttiva 95/46 né nessun'altra disposizione della medesima contengono una definizione della nozione di livello di protezione adeguato*»[289], quindi proponeva una lettura del paragrafo 6 (secondo cui la Commissione poteva constatare che un Paese terzo garantisse un livello adeguato di tutela) condotta alla luce della Carta: «*l'articolo 25,*

[284] Corte di giustizia, cause riunite C-317/04 e C-318/04, *Parlamento europeo c. Consiglio*, 30 maggio 2006, pp. 54-59.
[285] Cfr. M. BRKAN, The Court of Justice of the EU, privacy and data protection: Judge-made law as a leitmotif in fundamental rights protection, in M. BRKAN-E. PSYCHOGIOPOULOU (Eds), *Courts, privacy and data protection in the digital environment*, Elgar, 2017, p. 25 ss.
[286] Per un'esposizione dei lavori che portarono a tali principi nonché un'analisi degli stessi, si rinvia *ex multis* a S. SICA, V. D'ANTONIO, Verso il *Privacy Shield*: il tramonto dei *Safe Harbour Privacy Principles*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali – Dai "Safe Harbourprinciples" al "Privacy Shield"*, Roma Tre Press, 2016, pp. 137-167.
[287] COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite, COM(2013) 847 final, 27.11.2013, disponibile qui: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52013DC0847&from=EN .
[288] COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO – *Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, COM(2013) 846 final, 27.11.2013, part. pp. 7-9, disponibile qui: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0846:FIN:IT:PDF .
[289] Corte di giustizia, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, sentenza del 6 ottobre 2015, p. 71 (di seguito: *Schrems I*).

paragrafo 6, della direttiva 95/46 attua l'obbligo esplicito di protezione dei dati personali previsto all'articolo 8, paragrafo 1, della Carta e mira ad assicurare, come rilevato dall'avvocato generale al paragrafo 139 delle sue conclusioni, la continuità del livello elevato di tale protezione in caso di trasferimento di dati personali verso un paese terzo»[290]. Da qui, la Corte definiva per la prima volta i termini dell'adeguatezza richiesta al Paese terzo: "*È vero che il termine «adeguato» figurante all'articolo 25, paragrafo 6, della direttiva 95/46 implica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione. Tuttavia, come rilevato dall'avvocato generale al paragrafo 141 delle sue conclusioni, l'espressione «livello di protezione adeguato» deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46, letta alla luce della Carta. Infatti, in assenza di un siffatto requisito, l'obiettivo menzionato al punto precedente della presente sentenza sarebbe disatteso. Inoltre, il livello elevato di protezione garantito dalla direttiva 95/46, letta alla luce della Carta, potrebbe essere facilmente eluso da trasferimenti di dati personali dall'Unione verso paesi terzi ai fini del loro trattamento in tali paesi (...). In tali condizioni, in sede di esame del livello di protezione offerto da un paese terzo, la Commissione è tenuta a valutare il contenuto delle norme applicabili in tale paese risultanti dalla legislazione nazionale o dagli impegni internazionali di quest'ultimo, nonché la prassi intesa ad assicurare il rispetto di tali norme; al riguardo, tale istituzione deve prendere in considerazione, in conformità all'articolo 25, paragrafo 2, della direttiva 95/46, tutte le circostanze relative ad un trasferimento di dati personali verso un paese terzo*"[291]. Da qui rileva subito non solo che la Corte abbia sicuramente in qualche modo seguito le suddette indicazioni del Gruppo di Lavoro, ma soprattutto che essa abbia finalmente definito il significato di "adeguatezza" che, per quanto possa ancora suonare vago per certi versi, da allora è indiscutibilmente e generalmente inteso come "essenziale equivalenza".

Ma la questione si fa ancor più interessante laddove la Corte si addentra, finalmente, nel merito della decisione sindacata. Qui vengono in ausilio tutte le esposizioni e valutazioni che abbiamo prospettato nella previa trattazione. Ma vengono anche in ausilio, oltre ai commenti di autorevole dottrina (solo in minima parte riferibili, rispetto alla sterminata mole dedicata), le considerazioni del Professor H. Hoffman, difensore *pro bono* del signor Schrems in tutte le cause che lo hanno visto dinanzi alla Corte di giustizia, che ci ha gentilmente concesso una conversazione, impreziosendo

[290] Ibidem, p. 72.
[291] Ibidem, punti 73 e 75.

questo lavoro di una *field-research* particolarmente illuminante per la comprensione di alcuni passaggi chiave della giurisprudenza in oggetto (intesa, in senso complessivo, sull'intera saga). Ed è qui, soprattutto, che la pronuncia della Corte (che, ancora una volta – vale la pena precisarlo –, ha avuto come relatore T. von Danwitz) assume portentoso rilievo, con un impatto "costituzionale" che va ben oltre il settore della protezione dei dati personali e abbraccia l'intero ordinamento dell'Unione e, così, connota l'orientamento che il processo di integrazione europea ha cercato da allora (2015, ancor più palesemente, ma già da *DRI* e *Google Spain* dell'anno prima) di mantenere e tendenzialmente incrementare sino ad oggi (al netto *revirements* paventati dalle ultime pronunce sui sistemi di sicurezza nazionale, degli Stati membri, di cui si è detto *supra*, spec. *La Quarature du Net*).

La Corte apriva la propria analisi insistendo sulla necessità, dato che la situazione di un Paese considerato "adeguato" può ben evolversi nel tempo, di tenere conto delle circostanze sopravvenute dopo l'adozione della decisione e dunque chiariva che, anche in considerazione dell'importanza riconosciuta alla protezione dei dati personali e al suo impatto, il potere discrezionale della Commissione dovesse considerarsi ridotto e che essa stessa avrebbe proceduto a un *controllo stretto* dei requisiti della direttiva. Seguiva, così, un esame da cui la Corte riconosceva che sebbene un sistema di autocertificazione, come quello previsto dai principi di approdo sicuro (*Safe Harbor*), non sarebbe in quanto tale in contrasto con le previsioni della direttiva, potrebbero presentarsi dubbi quanto alla sua affidabilità, rispetto alla previsione di meccanismi efficaci per l'accertamento e il controllo di eventuali violazioni. Riscontrava, quindi, alcune incongruenze, per esempio il fatto che i suddetti principi si applicassero «*soltanto alle organizzazioni americane autocertificate che ricevono dati personali dall'Unione, mentre dalle autorità pubbliche americane non si esige il rispetto di detti principi*»[292]. Inoltre, e soprattutto, la Corte rilevava la previsione di una deroga a quei principi per esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia, esigenze che avrebbero avuto il primato sui principi e che però, a parere della Corte, provocherebbero «*possibili ingerenze (…) nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti*»[293]. Tra le ulteriori valutazioni, aggiungeva poi che la Commissione avesse «*constatato che non esistevano, per le persone di cui trattasi, rimedi amministrativi o giurisdizionali che consentissero, segnatamente, di accedere ai dati che le riguardavano e, se del caso, di ottenerne la rettifica o la soppressione*»[294].

[292] Corte di giustizia, *Schrems I*, p. 82. Prima, il riferimento è ai punti 79-81.
[293] Ibidem, p. 87. Prima, v. punti 81-86.
[294] Ibidem, p. 90, ma si vedano anche i punti precedenti.

Da qui, la Corte iniziava ad esporre le proprie considerazioni a seguito dell'effettuato "controllo stretto" (che però, si precisa, non arrivava a "*esaminare i principi dell'approdo sicuro sotto il profilo del loro contenuto*")[295], a partire dalla definizione di cosa è consentito ed è valido nell'ordinamento dell'Unione, riprendendo a tal fine la propria giurisprudenza – in particolare *DRI* – per poi poter valutare la sussistenza o meno di una "sostanziale equivalenza" del sistema esaminato. Essa effettuava, dunque, un'analisi a partire *dall'interno verso l'esterno*, con una dinamica argomentativa chiaramente (e consapevolmente?) volta a stimolare l'influenza unilaterale dell'Unione, e che dunque in questo caso palesemente iscrive l'intervento della giurisprudenza sovranazionale nel novero degli elementi che concorrono a corroborare (non solo, secondo Anu Bradford, il c.d. *Brussels effect*, ma, più ampiamente) ciò che abbiamo chiamato 'moto opposto'; ed è qui, infatti, che qualcuno ha ravvisato «un passo ulteriore per l'affermazione di una 'sovranità digitale' dell'Unione Europea»[296].

«*Quanto al livello di protezione delle libertà e dei diritti fondamentali garantito all'interno dell'Unione, una normativa della medesima che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta deve prevedere, secondo la giurisprudenza costante della Corte, regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati (...). Inoltre, e soprattutto, la protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario (...). In tal senso, non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione (...). In particolare, si deve ritenere che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta* (…). *Analogamente, una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta. (...)*

[295] Ibidem, p. 98.

[296] V. ZENO-ZENCOVICH, Intorno alla decisione nel caso *Schrems*: la sovranità digitale e il governo internazionale delle reti di telecomunicazione, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali – dai "SafE Harbor principles" al "Privacy Shield"*, Roma Tre-PRESS, 2016, p. 7.

A tal riguardo, l'esistenza stessa di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto (...)»[297].

In questi quattro punti è condensato il nucleo duro della giurisprudenza precedente (soprattutto *DRI*, continuamente citata quanti ai limiti, all'accesso alle comunicazioni elettroniche, al contenuto essenziale del diritto) e, pur con i necessari ritocchi, di quella successiva (in materia, e non solo) di cui abbiamo detto, che palesa il nesso tra protezione dei dati personali e *EU rule of law*.

Risalta subito che il "problema" riguarda il sistema di sicurezza predisposto negli USA specialmente rispetto all'accesso generalizzato della autorità pubbliche ai dati relativi alle comunicazioni elettroniche, e le perplessità che esso presenta in termini di sistema di tutela che possa dirsi "adeguato" al fine di trasferire i dati, in quanto "sostanzialmente equivalente" a quello dell'Unione. Eppure, se, allontanandoci dallo stretto tenore letterale della pronuncia, ci spingiamo a delle riflessioni che dall'esterno, comparativamente sindacato *in teoria*, ritornano verso l'interno del sistema sovranazionale, ci rendiamo subito conto, *in pratica*, che perplessità (almeno) altrettanto gravi possono ravvisarsi anche rispetto a diversi sistemi di sicurezza nazionale degli Stati membri. I casi analizzati sulla direttiva *e-privacy*, a partire da *Tele 2 e Watson* e sino, e soprattutto, a *La Quadrature du Net* sono stati funzionali alla trattazione dell'attuale pronuncia perché testimoniano come simili tensioni non solo siano ben presenti all'interno dell'Unione, ma addirittura paiono ultimamente influenzare la giurisprudenza verso un maggiore riguardo a esigenze securitarie in vista dell'evoluzione tecnologica, con un approccio che parrebbe in qualche modo tendente quasi a giustificare tali sistemi assoggettandoli a garanzie procedurali piuttosto che rifiutarli *in nuce*, in linea con il più consolidato trend della Corte di Strasburgo[298].

Ebbene, due aspetti dell'estratto appena riportato ci sembrano particolarmente meritevoli di attenzione, entrambi relativi al "contenuto essenziale del diritto".

Anzitutto, come accennato, la Corte interpretò per la prima volta tale concetto in *Digital Rights Ireland*, quale richiesto dall'articolo 52 della Carta tra gli elementi da considerare nel novero di ciò che abbiamo individuato come c.d. *justification test for limiting rights* (seguendo la dicitura suggerita da Peers, cfr. *supra*). Tuttavia, in quella prima occasione la Corte, pur riconoscendo un'ingerenza, escluse che le previsioni della direttiva *data retention* (comunque poi annullata per altri motivi) pregiudicassero il contenuto essenziale dei diritti sanciti dagli articoli 7 e 8 della Carta,

[297] Corte di giustizia, *Schrems I*, punti 91-95, sottolineato aggiunto.
[298] Si rinvia, al riguardo, ai commenti già citati, soprattutto di M. ZALNIERIUTE, A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence, *cit.*.; M. MILANOVIC, The Grand Normalization of Mass Surveillance, *cit.* , v. supra.

concludendo piuttosto che la conservazione dei dati consentita alle autorità nazionali rispondesse a un obiettivo di interesse generale[299]. Nel caso *Schrems I*, invece, la Corte ravvisa proprio una violazione del contenuto essenziale del diritto; anzi, due. Infatti, anzitutto emerge come la Corte di giustizia ritenesse chiaramente che misure di accesso generalizzato delle autorità pubbliche alle comunicazioni elettroniche (i.e. sorveglianza di massa) pregiudicano il contenuto essenziale del diritto al rispetto della vita privata *ex* articolo 7 Carta. In questo senso la Corte parrebbe abbastanza assertiva nel ritenere misure di sorveglianza generalizzata come sicuramente lesive del contenuto essenziale. Tuttavia, nella giurisprudenza successiva relativa a sistemi degli ordinamenti degli Stati membri (da *Tele2* a *Privacy International* e *La Quadrature du Net*) la Corte, aldilà degli esiti di quelle pronunce, non è parsa soffermarsi troppo sul rapporto tra le misure ivi previste e il contenuto essenziale dei diritti coinvolti, per cui comprensibilmente è stato notato: «*In the landscape of protection of essence, privacy and data protection therefore play a prominent constitutional role, even though the methodology used by the Court and its conclusions on interference with the essence are contentious and can be subject to criticism. The Court's case law on this issue can be depicted as a muddled maze where the final destination remains concealed due to reasoning that is full of meanders and unpredictable curves*»[300].

Sicuramente deve tenersi in considerazione, in una valutazione parallela dei vari casi su sistemi di sicurezza, il fatto che la Corte è stata interpellata su normative diverse (la decisione di adeguatezza rispetto al sistema di un Paese terzo nel solo caso *Schrems*, mentre le disposizioni della direttiva *e-privacy* ai fini della compatibilità dei sistemi degli Stati membri, negli altri casi) che coinvolgevano misure diverse e che dunque ciò giustificasse degli approcci di analisi diversi. Per esempio, sicuramente è dirimente e non va sottovalutato il fatto che, mentre le questioni sui sistemi di Stati membri riguardavano l'accesso e/o la conservazione sui dati relativi al traffico e all'ubicazione, la normativa statunitense riguardasse misure che consentivano un accesso generalizzato proprio al contenuto delle comunicazioni elettroniche (che, si capisce, è estremamente più invasivo delle altre ipotesi). Tuttavia, aldilà del merito e degli esiti, pare comunque non azzardato rilevare che queste pronunce, lette insieme, farebbero emergerebbe quasi l'esistenza di un paradosso insito nel sistema di protezione dei dati personali costruito a livello sovranazionale. Tale paradosso consisterebbe nel fatto che, mentre per il trasferimento verso l'esterno, i sistemi di sicurezza degli Stati terzi vengono vagliati (potremmo dire, *ex ante*) dalla Commissione per rintracciarne la necessaria adeguatezza, nel caso di sistemi di sicurezza degli Stati membri una simile valutazione non è prevista in partenza,

[299] Corte di giustizia, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland*, 8 aprile 2014, punti 38-44.
[300] M. BRKAN, The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU's Constitutional Reasoning, (2019), *cit*., p. 865.

valendo quasi una sorta di presunzione di conformità, per consentire la circolazione dei dati, ma viene chiaramente prospettata (*ex post*) nel caso di eventuale incompatibilità con le disposizioni sovranazionali (di diritto primario o derivato), rilevabile in diversi modi e in ultima analisi appurata dalla Corte di giustizia. Sicuramente, come abbiamo cercato di esporre nei casi relativi alle esigenze di sicurezza nazionale degli Stati membri, incide molto la ripartizione di competenze tra Stati membri e Unione, per cui la sicurezza nazionale rimane appannaggio dei primi, ma ciò con i limiti e gli aggiustamenti che abbiamo visto e che chiamano, in ultima analisi, la Corte di giustizia a sindacare la compatibilità con i valori fondanti del diritto dell'Unione (in particolare, nel rispetto dei diritti fondamentali). In questo senso, da ultimo, la Corte ribadiva la propria posizione chiarendo il riferimento dell'articolo 4, par. 2 TUE da ultimo in *La Quadrature du Net*: «*sebbene spetti agli Stati membri definire gli interessi essenziali della propria sicurezza e decidere le misure idonee a garantire la loro sicurezza interna ed esterna, la mera circostanza che una misura nazionale sia stata adottata a fini di salvaguardia della sicurezza nazionale non può comportare l'inapplicabilità del diritto dell'Unione e dispensare gli Stati membri dal necessario rispetto di tale diritto*»[301]. Inoltre, come vale anche per i sistemi di sicurezza nazionale degli Stati membri, nel caso *Schrems I* la Corte ha chiarito sotto questo profilo che anche nel caso di trasferimenti verso Paesi terzi le esigenze di sicurezza nazionale, che rimangono appannaggio di quelle entità statali, possono provocare ingerenze nei diritti fondamentali solo laddove limitate allo stretto necessario[302]. Il controllo della Corte in tal senso appare, pertanto, notoriamente espressivo della costruzione di un'*Unione di diritto* e proprio nel caso *Schrems I* essa ribadiva la propria competenza esclusiva a sindacare gli atti sovranazionali e, quindi, il nucleo dei principi della *EU rule of law*[303]. Comunque, se pur si capisce che la differenza di atteggiamento nei confronti di Stati membri e terzi risponde alla stessa *ratio* del sistema europeo di protezione dei dati sopra menzionata, ossia di "libera circolazione" all'interno dell'Unione e "circolazione controllata" al di fuori, ciò non varrebbe però ad escludere del tutto il "paradosso", che parrebbe emergere per esempio dai nuovi negoziati con gli USA, o specie quando, in pratica, si crea quella straordinaria situazione per cui uno Stato prima membro diventi terzo successivamente, trovandosi così assoggettato ad uno scrutinio più serrato da parte dell'Unione di quanto non fosse avvenuto nella situazione precedente. Il caso Brexit, perciò,

[301] Corte di giustizia, La Quadrature du Net, cit. p. 99.
[302] Corte di giustizia, *Schrems I*, punti 87-88 e 91-94, che verranno ripresi anche nella sentenza successiva.
[303] Corte di giustizia, *Schrems I*, pp. 60-61: «*A tal riguardo, occorre richiamare la giurisprudenza costante della Corte secondo la quale l'Unione è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali (…). Le decisioni della Commissione adottate in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 non possono pertanto sfuggire ad un siffatto controllo. Ciò premesso, la Corte è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione, quale una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, della direttiva 95/46; la natura esclusiva di tale competenza ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione (…)*».

risulta particolarmente significativo, anche in vista delle recenti pronunce sul sistema britannico sia della Corte di Lussemburgo che di Strasburgo nonché delle decisioni di adeguatezza recentemente adottate dalla Commissione, in termini di considerazioni e prospettive della sovranità digitale, che verranno meglio affrontate nel prosieguo.

Invero, riflessioni del genere sono state rilevate all'indomani della sentenza *Schrems I*, come Kuner prontamente rilevava: «*The unclear delineation and definition of "national security" can produce confusion about the standards that should apply to Member State activities (…). Following the Schrems judgment, some commentators (particularly those in the US) argued that it is hypocritical for EU policymakers and the CJEU to concern themselves with the standards of data protection for intelligence surveillance outside the EU, when the standards that apply in the EU seem lacking in many respects. In addition, there is widespread sharing of information by intelligence agencies of the Member States with the US, both under the "Five Eyes" intelligence-sharing network (which includes Australia, Canada, New Zealand, the UK, and the US), and under bilateral arrangements involving Member States, such as France and Germany*»[304]. Al riguardo, l'autore forniva un importante chiarimento e prospettava un'interessante soluzione, che parrebbe effettivamente (specie alla luce delle complessità emerse dalla pur più recente giurisprudenza sulle comunicazioni elettroniche) quella auspicabile, nonostante le comprensibili implicazioni in termini di sovranità: «*Strictly speaking, the data protection standards of Member State intelligence agencies are irrelevant for judging the standard of protection offered by third countries, and a violation of fundamental rights by a third country cannot be excused because Member State standards may be lacking. Yet, in a moral and political sense, the legitimacy of EU fundamental rights protection is undermined if the EU is viewed as holding third countries to standards that it is not willing to abide by itself. It would enhance the legitimacy of EU law in the eyes of third countries if national security was clearly brought within the ambit of EU fundamental rights law*»[305]. Eppure, l'avvio di nuovi negoziati tra UE e USA, a seguito, come diremo, dell'invalidità dell'ultima decisione di adeguatezza *Privacy Schield*, starebbe facendo emergere proprio nodi su questi aspetti. Come Christakis ci consente di rilevare nel suo interessante commento, pare che gli USA cerchino di insistere sull'opportunità di escludere questioni di sorveglianza internazionale dall'ambito della nuova decisione di adeguatezza[306]. Si avrà modo di rilevare che ciò che abbiamo denominato "paradosso" corrisponde a quella sensazione palesata dagli USA di "due pesi e due misure" che

[304] C. KUNER, Reality and Illusion in EU Data Transfer Regulation Post Schrems, in *German Law Journal*, Vol 18, No. 4, 2017, pp. 898-899.
[305] Ibidem, p. 899.
[306] T. CHRISTAKIS, Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy negotiations (Part 1), in *European Law Blog*, 12 April 2021.

potrebbe emergere dal raffronto tra sorveglianza interna e sorveglianza internazionale[307]. Questi stimoli saranno sviluppati in riflessioni successive.

Il secondo aspetto della sentenza *Schrems I* che merita attenzione quanto al contenuto essenziale del diritto è quello della "doppia violazione", su cui si sofferma particolarmente Hofmann. Per la prima volta, infatti, nella più alta manifestazione dei principi della *EU rule of law*, la Corte di giustizia ha rintracciato non solo un pregiudizio derivante dalla normativa del Paese terzo al contenuto essenziale di un diritto, ma addirittura di due: non solo del diritto al rispetto della vita privata, sancito dall'articolo 7 della Carta, ma anche del diritto ad una tutela giurisdizionale effettiva, sancito dall'articolo 47 della stessa. Di qui, si capisce l'impatto della pronuncia rispetto a questioni di *EU rule of law*, laddove ne intacca il nucleo centrale. Al riguardo, Hofmann spiegava: «*This double violation of the very essence of the right, which is the first in the case-law of the Court of Justice, helps to understand what does it mean to have the essence of a right and on the other hand clearly drew lines as to how far can a EU institution go in the area of limitation of fundamental rights*»[308]. Un aspetto importante che possiamo cogliere da queste brevi notazioni consiste nell'attenzione, che forse abbiamo sin ora sottaciuto, rispetto allo scrutinio della Corte sull'operato di un'istituzione dell'Unione. Infatti, quando la Corte esprime considerazioni sulla normativa del Paese terzo, essa sta in realtà sindacando la valutazione di adeguatezza che spetta alla Commissione, come effettivamente emerge dalla pronuncia: «*l'adozione, da parte della Commissione, di una decisione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 richiede la constatazione, debitamente motivata, da parte di tale istituzione, che il paese terzo di cui trattasi garantisce effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'ordinamento giuridico dell'Unione (...). Orbene, occorre rilevare che la Commissione, nella decisione 2000/520, non ha affermato che gli Stati Uniti d'America «garantiscono» effettivamente un livello di protezione (...). Di conseguenza, e senza che occorra esaminare i principi dell'approdo sicuro sotto il profilo del loro contenuto, si deve concludere che l'articolo 1 di tale decisione viola i requisiti fissati all'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce della Carta, e che esso è, per tale motivo, invalido*"[309]. In ciò è ravvisabile, chiaramente (e come abbiamo largamente affermato commentando *DRI*), un aspetto imprescindibile della *EU rule of law*, consistente nel sindacato della Corte di giustizia sull'operato delle istituzioni

[307] ID., Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2), in *European Law Blog*, 13 April 2021.
[308] Dall'intervista del Prof. H. Hoffman, realizzata dal *Blog Droit européen*, *Retour sur le premier arrêt Schrems – Interview de Herwig Hofmann, partie 4*, 21 Novembre 2017, minuti 5:42-6:05, disponibile qui: https://blogdroiteuropeen.com/2017/11/21/retour-sur-le-premier-arret-schrems-interview-de-herwig-hofmann-partie-4/ .
[309] Corte di giustizia, *Schrems I*, pp. 96-98.

dell'Unione, e dunque un ulteriore esempio, se vogliamo, di coerenza dell'azione (interna ed esterna) dell'Unione.

Inoltre, ancor di più, nella ravvisata "doppia violazione" si coglie l'essenza del nesso, che stiamo cercando di far risaltare in questo lavoro, tra principi della *EU rule of law* e protezione dei dati personali, in quanto tale evocativo della propensione verso una sovranità digitale dell'Unione europea, specie laddove simili considerazioni della Corte stabiliscono «*how European fundamental rights have to be exercised in the digital age*»[310]. Nel risaltare quest'altro importante aspetto, Hofmann infatti rilevava la difficoltà di incardinare i trasferimenti di dati nell'era digitale nelle classiche categorizzazioni sulla portata territoriale del diritto e, in maniera interessante, per rispondere alla domanda "*what is the territorial reach of a right such as the right to privacy and data protection?*" effettuava un parallelo con categorie proprie del diritto della concorrenza, per spiegare che «*if the effect of a violation is in Europe, European law is applicable*»[311]. Peraltro, calando le riflessioni teoriche sulla portata (extra)territoriale sopra esposte a questa specifica pronuncia, la Scott rilevava come «*the CJEU has been willing to adopt a robust interpretation of legislation giving rise to country-level territorial extension*», riconoscendo quindi qui una "*permissive stance to territorial extension*", senza però negare altri casi in cui la Corte si è effettivamente mostrata sensibile al rischio che tale estensione territoriale potesse comportare dei conflitti con le legislazioni dei Paesi terzi[312].

Infine, l'ultima cosa da rilevare su questa pronuncia, che tornerà utile anche nella valutazione dell'ultima sentenza della *saga Schrems*, è quello che Kuner individua come "approccio dinamico alla protezione dei diritti fondamentali" che la Corte avrebbe palesato nella sua argomentazione: «*the Court's dynamic approach to fundamental rights protection in* Schrems *can also be seen in its choice of 'essential equivalence' with EU law as the measure of 'adequate protection', even though when the DPD was adopted, the EU legislator specifically preferred the term 'adequate protection' over 'equivalent protection'. This indicates that in cases involving the validity of adequacy decisions (and possibly other data transfer mechanisms as well), the CJEU will make a 'dynamic assessment' and evaluate whether they meet legal standards in force at the time that it makes its judgment and not just those that applied when the case was brought*»[313]. Viene così, peraltro, fornito uno stimolo a più ampie riflessioni sulla protezione equivalente, che spontaneamente derivano da questioni del genere, e che verranno esposte nel prosieguo.

[310] Intervista a H. Hofmann, cit., minuto 6:17.
[311] Ibidem, minuti 7:43-7:49, mentre la domanda al minuto 7:18.
[312] J. SCOTT, The Global Reach of the EU Law, 2019, *cit.*, p.37.
[313] C. KUNER, Article 45, cit., p. 782.

Tutte queste considerazioni sugli aspetti più rilevanti, ai nostri fini, della sentenza *Schrems I* spiegano a sufficienza, a nostro avviso, l'inevitabile impatto che essa ha avuto sul successivo andamento del processo di integrazione europea nel suo complesso, comprensivo dell'azione interna ed esterna dell'Unione. Con queste consapevolezze, procediamo, dunque, ad esporne i principali sviluppi.

Conseguenze Schrems I e interventi nella prassi

Una volta dichiarata invalida la decisione di adeguatezza relativa al sistema USA, la Commissione si mise subito al lavoro per adottarne una nuova che rispondesse ai requisiti richiesti dalla Corte. In realtà, il dialogo con le autorità statunitensi era già cominciato dal 2014, proprio a seguito delle succitate Comunicazioni del 2013 (la 846 e la 847), seguite alle rivelazioni di Snowden e palesanti la necessità di revisionare il regime di approdo sicuro; nondimeno, a seguito della sentenza *Schrems* esso venne rinvigorito per rintracciare un regime che potesse rispondere alle esigenze di adeguatezza. Tale dialogo sfociò in una serie di documenti (che si trovano allegati alla decisione 2016/1250) che, insieme con i principi in materia di protezione dei dati, costituirono il nuovo regime, c.d. *scudo UE-USA per la privacy* (*Privacy Shield*)[314]. Nel luglio 2016, a meno di un anno dalla sentenza Schrems e dopo qualche mese dal pacchetto di riforma che includeva soprattutto il GDPR, la Commissione si trovò quindi ad adottare una seconda decisione di adeguatezza per il trasferimento di dati verso gli USA, con cui, in sostanza, riteneva adeguato il nuovo regime di *Privacy Shield*.

Dalla decisione si leggeva: "*Lo scudo UE-USA per la privacy si fonda su un sistema di autocertificazione in base al quale l'organizzazione statunitense s'impegna a rispettare un insieme di principi in materia di privacy, ossia i principi del regime dello scudo UE-USA per la privacy, comprensivi dei principi supplementari (…) emanati dal Dipartimento del Commercio degli USA e riportati nell'allegato II della presente decisione. Lo scudo si applica sia ai titolari sia ai responsabili del trattamento (procuratori), con la specificità che un contratto deve vincolare il responsabile del trattamento ad agire esclusivamente secondo le istruzioni del titolare del trattamento dell'UE e a prestargli assistenza per rispondere alle persone che esercitano i loro diritti nell'ambito dei principi. Fermo restando il rispetto delle disposizioni nazionali adottate in applicazione della direttiva 95/46/CE, la presente decisione ha l'effetto di autorizzare il*

[314] Cfr. Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, 12 luglio 2016 (non più in vigore), punto 12. Si vedano, però, più in generale anche i punti 7-13.

trasferimento dei dati personali dai titolari o responsabili del trattamento nell'Unione alle organizzazioni presenti negli USA che si sono autocertificate come aderenti ai principi presso il Dipartimento del Commercio e si sono impegnate a conformarsi agli stessi"[315]. Peraltro, interessante anche ai fini della successiva analisi su *Schrems II*, il nuovo regime prevedeva l'istituzione del c.d. Mediatore dello scudo (di seguito anche solo "Mediatore"), quale nuovo meccanismo di vigilanza sulle ingerenze delle autorità statunitensi per motivi di sicurezza nazionale, definito indipendente dai servizi di *intelligence*[316].

Già prima dell'adozione della nuova decisione di adeguatezza, nell'aprile 2016 il Gruppo di Lavoro Articolo 29 interveniva ad individuare le c.d. *garanzie essenziali europee* proprio a seguito degli stimoli dati da *Schrems I*, al fine di chiarire quali interferenze non fossero consentite poiché oltrepassanti i limiti dello stretto necessario. Esso individuava tali garanzie essenziali in quattro punti: regole di trattamento precise, chiare e accessibili; necessità e proporzionalità; un meccanismo di controllo indipendente; rimedi effettivi per gli individui[317].

Inoltre, pochi mesi dopo l'adozione di tale documento, sempre il Gruppo di Lavoro interveniva a chiarire le caratteristiche del nuovo regime, fornendo ausilio alle imprese europee sui requisiti per il trasferimento di dati personali negli USA e su quelli richiesti alle società statunitensi per aderirvi[318].

Ad ulteriore ausilio degli operatori e non solo, il Gruppo di Lavoro interveniva finalmente nel novembre 2017 ad adottare i suddetti "*criteri di riferimento per l'adeguatezza*", che indichiamo nella versione emendata del febbraio 2018. Con gli stessi, il Gruppo di Lavoro interveniva ad aggiornare il documento del 1998 sul trasferimento di dati verso Paesi terzi (WP12, *supra*), tenendo conto delle conclusioni della Corte di giustizia sul caso *Schrems I* soprattutto quanto alle garanzie sostanziali per l'accesso ai fini di sicurezza nazionale (e facendo richiamo già alle disposizioni del GDPR)[319].

Intanto, come si è detto, la Commissione nel gennaio dello stesso anno aveva adottato la Comunicazione sullo *Scambio e protezione dei dati personali in un mondo globalizzato* e, nella

[315] Ibidem, punti 14-15.
[316] Ibidem, p. 65.
[317] (documento non disponibile in italiano) WP29, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237, Adopted on 13 April 2016, part. p. 6, available here: https://ec.europa.eu/newsroom/article29/items/640363/en .
[318] Gruppo di lavoro Articolo 29 – WP245 del 13 dicembre 2016, LO SCUDO UE - USA PER LA PRIVACY ("PRIVACY SHIELD") FAQ PER LE IMPRESE EUROPEE, disponibile qui: https://www.garanteprivacy.it/documents/10160/0/PRIVACY+SHIELD+-+FAQ+PER+LE+IMPRESE+EUROPEE+-+WP+245.pdf/a2ed84f7-e161-424b-9730-c8accc88dd09?version=1.0 .
[319] Gruppo di Lavoro Articolo 29*, Criteri di riferimento per l'adeguatezza* – Adottati il 28 novembre 2017, Versione emendata e adottata il 6 febbraio 2018, WP 254 rev.01, cit.

parte dedicata alle decisioni di adeguatezza, ne sottolineava l'importanza per consentire il libero flusso di dati verso Paesi terzi senza necessità di garanzie supplementari da parte dell'esportatore e poi, dopo aver richiamato le specificazioni di *Schrems*, precisava quanto alle decisioni su Canada e USA che si trattasse di decisioni "parziali": «*La decisione di recente adozione sullo scudo UE-USA per la privacy è un caso specifico nel senso che, in assenza di una legislazione generale sulla protezione dei dati negli Stati Uniti, essa si basa sull'assunzione di impegni da parte delle imprese partecipanti ad applicare gli elevati standard di protezione dei dati stabiliti dal presente accordo che sono, a loro volta, azionabili in forza del diritto statunitense. Inoltre, lo scudo per la privacy si fonda sulle specifiche osservazioni e garanzie espresse dal governo degli Stati Uniti per quanto riguarda l'accesso a fini di sicurezza nazionale, che sono alla base dell'accertamento di adeguatezza. Il rispetto degli impegni sarà oggetto di attento monitoraggio da parte della Commissione e parte integrante del riesame annuale sul funzionamento del quadro*»[320]. Nello stesso documento, la Commissione faceva riferimento anche al fatto che ultimamente diversi Paesi terzi si stessero dotando di nuove normative in materia di tutela dei dati personali e vita privata. A tal proposito, va almeno accennato il fatto che, sempre come ulteriore conseguenza della sentenza *Schrems I*, nel dicembre 2016 la Commissione adottava una decisione per modificare le già esistenti decisioni di adeguatezza relative ad alcuni Paesi terzi proprio alla luce dei criteri fissati dalla Corte di giustizia[321].

Insomma, questi pochi cenni di prassi istituzionale denotano già la portata dell'impatto della prima pronuncia *Schrems* sull'operato delle istituzioni coinvolte nel settore, stimolando una rinnovata sensibilità delle stesse nel conformarsi ai dettami della Corte e nel chiarire e incentivare il conseguente intervento degli operatori privati.

Intanto in Lussemburgo…

Tra le molte conseguenze della sentenza *Schrems I*, alcune delle quali si sono accennate, fondamentale risulta sicuramente la c.d. sentenza *Schrems II*, che della prima appare inevitabile prosieguo. In realtà, va precisato che tra la prima sentenza e quella che qui chiameremo *Schrems II* è intercorso un altro caso che ha visto scontrare *Schrems* contro Facebook ed è stato deciso dalla Corte di giustizia nel 2018. Non ci occuperemo di quel caso (tecnicamente, dunque, il secondo)

[320] Comunicazione della Commissione, COM (2017) 7 final, 10 gennaio 2017, *cit.*, pp. 7-8.

[321] Decisione di esecuzione (UE) 2016/2295 della Commissione, del 16 dicembre 2016, che modifica le decisioni 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE, 2011/61/UE e le decisioni di esecuzione 2012/484/UE, 2013/65/UE *riguardanti l'adeguatezza della protezione dei dati personali da parte di taluni paesi*, a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, 17 dicembre 2016.

poiché relativo a questioni procedurali e alla possibilità per gli individui di agire contro Facebook in maniera da potenziare il loro diritto alla tutela dei dati personali sotto l'egida del diritto dell'Unione[322].

Passando, invece, alla causa che ha un filo diretto con la prima, si ricorderà che la pronuncia del 2015, oltre ad aver invalidato la decisione di adeguatezza della Commissione, aveva, soprattutto, chiaramente ribadito il riconoscimento del controllo sui trasferimenti di dati verso Paesi terzi da parte delle autorità nazionali, che quindi non potevano esimersi dai poteri conferitigli dal diritto dell'Unione per il solo fatto che esistesse una decisione di adeguatezza della Commissione rispetto al Paese terzo destinatario di quei trasferimenti[323]. Si ricorderà, inoltre, che quella causa originava da un reclamo proposto da Schrems all'autorità garante irlandese (competente, per i trasferimenti effettuati da Facebook, poiché azienda avente sede europea in Irlanda) con cui chiedeva di vietare a Facebook Ireland di trasferire i propri dati negli USA a causa delle perplessità emerse sul sistema di tutele di quel Paese. L'autorità irlandese (c.d. *Data Protection Commissioner*, di seguito anche DPC) rigettava tale reclamo in virtù dell'esistenza, appunto, di una decisione di adeguatezza della Commissione al riguardo. Così il signor Schrems impugnava quella decisione dinanzi alla High Court, che proponeva rinvio pregiudiziale alla Corte di giustizia che portò agli esiti suddetti, invalidando quella decisione di adeguatezza. Ebbene, da lì, la High Court irlandese annullava la decisione del DPC e la rinviava allo stesso, che apriva quindi finalmente un'apposita indagine, dalla quale emergeva che in realtà la principale base giuridica per i trasferimenti dei dati da parte di Facebook consistesse nelle c.d. *clausole tipo di protezione*, previste nell'apposita decisione della Commissione 2010/87/CE (e che dunque legittimavano i trasferimenti pur in mancanza di una decisione di adeguatezza; di seguito anche decisione CPT); pertanto, l'autorità invitava Schrems a riformulare il proprio reclamo.

Questo veniva riformulato e così ripresentato già nel dicembre 2015, dunque ben prima dell'adozione della decisione *Privacy Shield* e, soprattutto, riguardava altri metodi di legittimazione dei trasferimenti rispetto a quest'ultima. In questo contesto il DPC, poiché dubitava sulla validità della decisione CPT della Commissione, adiva finalmente la High Court affinché, in ossequio agli insegnamenti di *Schrems I*, sollevasse rinvio pregiudiziale alla Corte di giustizia, cosa che avvenne

[322] Cfr. Corte di giustizia, C-498/16, *Maximilian Schrems c. Facebook Ireland Limited*, sentenza del 25 gennaio 2018. Per un commento si rinvia, *ex multis*, a G.E. CORSARO, Schrems contro Facebook: gli incerti confini della categoria dei consumatori, in C. PICIOCCHI, M. FASAN; C. M. REALE (a cura di), *Le (in)certezze del diritto: atti delle giornate di studio 17-18 gennaio 2019*, QUADERNI DELLA FACOLTÀ DI GIURISPRUDENZA, Università degli Studi di Trento, 2021, pp. 339-359.

[323] Corte di giustizia, *Schrems I*, punti 51-59. Cfr. *supra*, Parte III.

nel maggio 2018[324]. Ci stiamo dilungando su questi passaggi fattuali per palesare come, in realtà, la nuova decisione di adeguatezza non fosse stata affatto oggetto della controversia principale tra Schrems e Facebook dinanzi al DPC irlandese. Piuttosto, come si legge dalla pronuncia della Corte del 2020, la decisione *Privacy Shield* risaltò solo in un secondo momento (e dunque, evidentemente, non era affatto l'oggetto principale, né tantomeno secondario, della doglianza di Schrems rispetto alla tutela dei propri dati trasferiti in USA): « *Nella sua domanda di pronuncia pregiudiziale, il giudice del rinvio precisa altresì che le parti del procedimento principale hanno posizioni divergenti, in particolare, quanto alla questione dell'applicabilità del diritto dell'Unione a trasferimenti, verso un paese terzo, di dati personali che possono essere trattati dalle autorità di tale paese segnatamente a fini di sicurezza nazionale, nonché quanto agli elementi da prendere in considerazione ai fini della valutazione del livello di protezione adeguato garantito da detto paese. In particolare, tale giudice rileva che, secondo Facebook Ireland, le constatazioni della Commissione riguardanti l'adeguatezza del livello di protezione garantito da un paese terzo, come quelle contenute nella decisione «scudo per la privacy», vincolano le autorità di controllo anche nel contesto di un trasferimento di dati personali fondato sulle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT*»[325]. È per questa via, dunque, che la Corte di giustizia arrivava a sindacare per la seconda volta una decisione di adeguatezza della Commissione sugli USA. Sia ben chiaro, però, che, come si è cercato di introdurre, la sentenza sul caso *Schrems II* riguarda soprattutto gli altri strumenti che legittimano i trasferimenti verso Paesi terzi (quelli di cui all'articolo 46, in base ai quali di fatto avviene la maggior parte dei trasferimenti), mentre, nonostante la chiara rilevanza mediatica, l'attenzione sulla decisione di adeguatezza assume importanza sotto profili più giuridici che pratici, oltre che essere ovviamente funzionale alla questione sugli altri strumenti. Si riprenderà questa sentenza per gli aspetti peculiari relativi alle clausole tipo, quando si tratterà degli strumenti alternativi alla decisione di adeguatezza. Per il momento, analizziamo la sentenza *Schrems II* limitatamente alla decisione *Privacy Shield*.

[324] Chiarimenti sui passaggi relativi al ricorso del DPC alla High Court irlandese sono forniti da H. Hofmann, nell'intervista realizzata dal *Blog Droit européen*, *La saga Schrems continue – Interview de Herwig Hofmann, partie 5*, 28 Novembre 2017, dal minuti 6:18, disponibile qui: https://blogdroiteuropeen.com/2017/11/28/la-saga-schrems-continue-interview-de-herwig-hofmann-partie-5/ .
Qui, in particolare, il Professore spiega, chiarendo un aspetto altrimenti incomprensibile, la bizzarra circostanza per cui secondo il diritto irlandese ogni ricorso deve prevedere il nome di entrambe le parti. Nel caso specifico, poiché il ricorso alla High Court venne presentato dal DPC irlandese, questi indicò sé stesso come ricorrente ed entrambi i contendenti, dunque sia Schrems che Facebook, come resistenti, nonostante questi avessero chiaramente una posizione opposta rispetto al reclamo proposto allo stesso DPC e, chiaramente, nonostante avessero ambizioni opposte quanto all'esito della valutazione della High Court; cfr. minuti 8:40 ss. Ciò spiega perché la causa C-311/18 dinanzi alla Corte di giustizia abbia la nomenclatura che vede Facebook e Schrems come entrambi parti resistenti.
[325] Corte di giustizia, C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems*, 16 luglio 2020, p. 66 (di seguito: *Schrems II*), sottolineato aggiunto.

Invero, tale decisione, ancorché molto giovane, fu subito oggetto di "contestazione giurisdizionale", nel senso che fu proposto un ricorso in annullamento a settembre 2016 da *Digital Rights Ireland*, che venne dichiarato irricevibile dal Tribunale nel novembre 2017[326]. Inoltre, un altro ricorso in annullamento venne proposto da *La Quadrature du Net e altri* dinanzi al Tribunale il 25 ottobre 2016, che venne sospeso in virtù della pendenza alla Corte sulla stessa decisione, e che si concluse infatti con un'ordinanza del dicembre 2020 di non luogo a procedere[327]. Infine, qualche perplessità emergeva anche dall'EDPB, come si evince dalla relazione di riesame della decisione a cui partecipò insieme con la Commissione, adottata nel 2019[328].

Il caso Schrems II e (l'invalidità del)la decisione Privacy Shield

Anzitutto, va detto (o meglio, ripetuto, cfr. Parte III), che la Corte affrontò le questioni pregiudiziali alla luce del GDPR e non della direttiva madre, ancorché fosse quest'ultima la normativa in vigore al momento di proposizione del rinvio pregiudiziale, poiché «*sebbene le questioni pregiudiziali facciano riferimento alle disposizioni della direttiva 95/46, è pacifico che il Commissario non aveva ancora adottato una decisione definitiva su tale denuncia allorché tale direttiva è stata abrogata e sostituita dal RGPD, con effetto dal 25 maggio 2018*»[329].

La pronuncia, ancorché abbastanza prevedibile poiché in totale continuità con la precedente, ha una portata dirompente, che continuerà ad avere forte risonanza nel prossimo futuro. Di particolare interesse gli aspetti relativi alla decisione sulle clausole tipo di protezione (rimasta valida) e al ruolo della autorità di controllo, di cui diremo successivamente. Qui ci limitiamo ad esporre e commentare sommariamente le considerazioni sulla decisione di adeguatezza della Commissione, dichiarata dalla Corte per la seconda volta invalida.

Chiamata all'interpretazione e al sindacato sulla validità della decisione *Privacy Shield*, rispetto alla quale il giudice di rinvio chiedeva entro che limiti vincolasse le autorità di controllo, la Corte ne giustificava l'attenzione considerando: "*il giudice del rinvio ha sottolineato di essere tenuto a*

[326] Tribunale causa T-670/16, *Digital Rights Ireland Ltd c. Commissione*, ordinanza del 22 novembre 2017.
[327] Tribunale, T-738/16, *La Quadrature du Net e.a. c. Commissione*, ordinanza del 14 dicembre 2020.
[328] EDPB, *EU - U.S. Privacy Shield - Second Annual Joint Review*, Adopted on 22 January 2019, disponibile qui: https://edpb.europa.eu/sites/default/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf, in cui si legge, per esempio: «*The absence of substantial checks remains a concern of the EDPB. Other areas that require further*
attention are the application of the Privacy Shield requirements regarding onward transfers, HR Data and processors, as well as the recertification process. In addition, the EDPB recalls the remaining issues with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016», p.7.
[329] Corte di giustizia, *Schrems II*, p. 77.

prendere in considerazione le modifiche della normativa intercorse tra la proposizione del ricorso e l'udienza tenutasi dinanzi ad esso. Appare, pertanto, che tale giudice abbia l'obbligo di prendere in considerazione, per dirimere la controversia di cui al procedimento principale, il mutamento di circostanze risultante dall'adozione della decisione «scudo per la privacy» nonché dagli eventuali effetti vincolanti di quest'ultima. In particolare, l'esistenza degli effetti vincolanti connessi alla constatazione, da parte della decisione «scudo per la privacy», di un livello di protezione adeguato negli Stati Uniti è rilevante ai fini della valutazione tanto degli obblighi (...) che incombono al titolare del trattamento e al destinatario di un trasferimento di dati personali verso un paese terzo effettuato sulla base delle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT, quanto degli obblighi che gravano, eventualmente, sull'autorità di controllo di sospendere o vietare un trasferimento siffatto"[330].

Dunque, anzitutto la Corte ripeteva quanto rilevato in *Schrems I* rispetto a decisione di adeguatezza e autorità di controllo, ribadendo che queste ultime, per quanto vincolate dagli atti dell'Unione, devono comunque trattare i reclami che discutono simili decisioni e, nel caso in cui appaiano fondati, adire un giudice affinché venga sollevato rinvio pregiudiziale alla Corte di giustizia per sindacarne (quale unica competente) la validità. Quindi, si procedeva all'interessante esame del contenuto della decisione 2016/1250. Diciamo subito che sono due gli elementi fondamentali emergenti da tale esame: intanto, ancora una volta, come in *Schrems I*, l'accesso delle autorità statunitensi per esigenze di sicurezza nazionale, con le ingerenze che esso comporta; quindi, elemento di novità (ma in realtà in linea con le considerazioni della prima sentenza sulla tutela giurisdizionale effettiva), la posizione della nuova figura del Mediatore. Si tratta di due elementi, invero, correlati e che comunque, alla fine, riprendono pedissequamente il ragionamento condotto nella sentenza precedente.

Sul contenuto, la Corte di giustizia immediatamente constatava che, per quanto la Commissione avesse ritenuto che gli USA garantissero un livello di tutela adeguato in virtù dei principi emanati dal Dipartimento del Commercio statunitense che fanno parte del regime *Privacy Shield*, la stessa Commissione precisava però "*che l'adesione a tali principi può essere limitata «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia». Pertanto* [rilevava la Corte], *detta decisione, al pari della decisione 2000/520, sancisce il primato delle suddette esigenze rispetto a tali principi, primato in forza del quale le organizzazioni statunitensi autocertificate che ricevono dati personali dall'Unione sono tenute a disapplicare, senza limiti, tali principi allorché questi ultimi interferiscono con tali esigenze e*

[330] Ibidem, pp. 153-154, sottolineato aggiunto.

risultano dunque incompatibili con le medesime. Alla luce del suo carattere generale, la deroga (...) rende pertanto possibili ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti"[331]. Seppure la Commissione, a seguito di valutazioni, riteneva tali ingerenze come limitate allo stretto necessario, il giudice di rinvio sollevava invece perplessità rispetto alla garanzia effettiva di un livello di tutela adeguato predisposto dal sistema statunitense, invocando l'articolo 45 GDPR letto alla luce della Carta (articolo 7, 8 e 47) e quindi, in particolare, ponendo in dubbio il ruolo dell'istituito Mediatore rispetto a rimedi e garanzie necessarie in casi di possibili ingerenze soprattutto in luce dell'articolo 47 della Carta.

Ebbene, la Corte richiamava la propria giurisprudenza più rilevante in materia, sull'importanza dei diritti di cui agli articoli 7 e 8 Carta ma anche sulla possibilità di limitazioni, sul rispetto del contenuto essenziale e sull'esigenza di proporzionalità, per poi specificare che "*l'articolo 45, paragrafo 2, lettera a), del RGPD precisa che, nel valutare l'adeguatezza del livello di protezione garantito da un paese terzo, la Commissione prende in considerazione in particolare «i diritti effettivi e azionabili degli interessati» i cui dati personali sono trasferiti*"[332]. Da qui, la Corte passava a valutare sia le constatazioni della Commissione che i dubbi sui programmi di sorveglianza da cui deriverebbero le ingerenze, per rilevare che questi non rispondessero ai "*requisiti minimi connessi, nel diritto dell'Unione, al principio di proporzionalità, cosicché non si può considerare che i programmi di sorveglianza basati su tali disposizioni siano limitati allo stretto necessario*"[333]. Insistendo sull'importanza della previsione di rimedi effettivi rispetto a simili ingerenze, che poi costituisce il fulcro della *EU rule of law*, la Corte affermava che «*L'esistenza di tali effettive possibilità di ricorso nel paese terzo considerato riveste un'importanza particolare nel contesto di un trasferimento di dati personali verso tale paese terzo, in quanto, come risulta dal considerando 116 del RGPD, gli interessati possono trovarsi di fronte all'insufficienza dei poteri e dei mezzi delle autorità amministrative e giudiziarie degli Stati membri per poter dare utilmente seguito ai loro reclami fondati su un asserito trattamento illecito, in tale paese terzo, dei loro dati in tal modo trasferiti, il che può costringerli a rivolgersi alle autorità e ai giudici nazionali di siffatto paese terzo*»[334].

[331] Corte di giustizia, *Schrems II*, punto 164.
[332] Ibidem, p. 177. Si vedano anche i punti precedenti.
[333] Ibidem, p. 184.
[334] Ibidem, p. 189, sottolineato aggiunto.

Quest'ultimo punto, fondamentale sotto diversi aspetti, pare darci esattamente la misura della portata extraterritoriale del diritto europeo alla protezione dei dati personali, testimoniando esattamente quanto diceva Hofmann sugli effetti del diritto dell'Unione: "*se gli effetti di una violazione si producono nell'Unione europea, il diritto dell'Unione è applicabile*". Ciò ci sembra la più alta conferma dell'inclinazione della Corte verso la sovranità digitale dell'Unione, una sovranità che va oltre il territorio e segue…l'effettiva protezione dei diritti fondamentali riconosciuti in quell'ordinamento sovranazionale. Avremo modo di riflettere su simili valutazioni.

Tornando alla pronuncia, è da qui che la Corte passava a valutare la posizione del Mediatore, rilevando che la sua istituzione come garanzia nel nuovo regime comunque «*non può colmare le lacune constatate dalla Commissione stessa per quanto riguarda la tutela giurisdizionale delle persone i cui dati personali sono trasferiti verso tale paese terzo*»[335]. Quindi, esaminava l'idoneità del meccanismo di mediazione, ribadendo le basilari esigenze di tutela giurisdizionale effettiva, per constatare infine che lo stesso «*non fornisce mezzi di ricorso dinanzi a un organo che offra alle persone i cui dati sono trasferiti verso gli Stati Uniti garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta*»[336]. Tanto bastava ad invalidare l'articolo della decisione che constatava che gli USA garantissero un livello di protezione adeguato, poiché in contrasto con gli articoli 45 GDPR e 7, 8 e 47 Carta, inficiando così la validità dell'intera decisione.

Alcune valutazioni su questi estratti, prima di procedere all'analisi successiva. Anzitutto, appare senz'altro peculiare che per la seconda volta di fila la Corte abbia "sanzionato" la valutazione di adeguatezza operata dalla Commissione, che la dice lunga in termini di operato dell'istituzione sovranazionale, soprattutto se si considera che, come abbiamo visto, le censure sono esattamente sugli stessi aspetti della prima sentenza. Infatti, specie nella prospettiva di una nuova decisione della Commissione, qualcuno a caldo rilevava: «*The second consecutive invalidation of the Commission's adequacy decision has important legal and political significance and raises the bar for the Commission to "do things right" this time*»[337]. Eppure, non può certo dirsi, alla luce soprattutto dei più recenti interventi della Commissione (molti dei quali si sono esposti in questo Capitolo e nei precedenti) che essa non sia sensibile alle questioni di tutela nella dimensione digitale, tanto che qualcuno addirittura ha letto la pronuncia in linea con l'impegni dell'istituzione nell'azione esterna: «*The judgment seems also to be in line with the European Commission's commitment to promoting global convergence in the area of data protection by placing the EU*

[335] Ibidem, p. 190.
[336] Ibidem, p. 197. Si vedano anche punti precedenti.
[337] T. CHRISTAKIS, After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe, in *European Law Blog*, 21 July 2020.

standards as a reference point at the international level»[338]. Invero, l'apparente contraddittorietà rivela un importante aspetto da non sottovalutare, e cioè che per quanto le decisioni di adeguatezza siano, formalmente, un atto della Commissione europea, motivo per cui le consideriamo come strumenti di influenza unilaterale dell'Unione nella protezione dei dati personali verso l'esterno, in realtà pronunce del genere palesano come si tratti di atti che costituiscono il risultato di importanti e non semplici negoziazioni che la Commissione conduce con i Paesi terzi. E che quindi, in quanto tali, pongono complessità non dissimili a quelle che si sono esposte trattando della conclusione di accordi internazionali in materia. Pertanto, non si può non concordare con quanto commentava Kuner al riguardo: «*The invalidation of the Privacy Shield also raises questions about how adequacy decisions are negotiated and issued. There is a disconnect between the political pressure to reach an accommodation with the US to which the Commission seems to be subject, and the Court's insistence on a high standard of data protection, which can be seen in the Commission's willingness to accept formulations that seem obviously questionable*»[339]. È vero che, come nel caso del parere sull'accordo PNR con il Canada, la Corte non può che ribadire il proprio ruolo di garante dei valori fondanti del suo ordinamento, palesando con queste pronunce (che si pongono in totale continuità) la coerenza del suo operato coi dettami della *EU rule of law*. È vero anche, però, che la reiterazione di pronunce che correggono la Commissione praticamente sugli stessi aspetti la dice lunga in termini di coerenza tra azione interna ed esterna dell'Unione, pur riconoscendo le difficili dinamiche dei dialoghi e compromessi che sono richiesti. Sicuramente, la pronuncia rappresenta un monito alla Commissione in questo senso: «*Greater transparency and accountability in the negotiations might result in the Commission adopting adequacy decisions of a higher quality*». Pertanto, piuttosto che riproporre una strategia di "scelta rapida", che si è rivelata con il Privacy Shield evidentemente non vincente, qualche autore suggeriva un modo di avanzare "più credibile" affrontando le principali questioni sollevate dalla Corte per arrivare a un prossimo negoziato UE-USA conforme e più duraturo, che però, in sostanza, richiederebbe una profonda revisione del sistema statunitense: *«(…) to try hard to address the main issues raised by the CJEU and conclude a long-lasting EU-US arrangement providing a valid legal basis and legal certainty for years to come. For a European observer this should not be "mission impossible" (…). Of course, several US and other commentators have expressed their pessimism about any chance that the US political*

[338] Così I. OLDONI, The future of data transfer rules in the aftermath of Schrems II, in *SIDIBlog*, 23 ottobre 2020.
[339] C. KUNER, The Schrems II judgment of the Court of Justice and the future of data transfer regulation, in *European Law Blog*, 17 July 2020.

economy will allow for a re-calibration of US law at the expense of surveillance capabilities, while extending US protections to foreigners has been presented as an "anathema to US law"»[340].

Queste considerazioni ci consentono di passare oltre la specifica questione trattata nella pronuncia e avviarci a concludere la trattazione sulle decisioni di adeguatezza con valutazioni di più ampio respiro sulla portata delle previsioni del GDPR. È vero, infatti, che, nella più genuina espressione del suddetto *Brussels effect*, la previsione nella normativa europea di decisioni di adeguatezza come principale base giuridica per legittimare il trasferimento dei dati verso Paesi terzi ha prodotto, riprendendo Anu Bradford, una sorta di "*proliferation of the EU-style privacy regimes around the world*": ciò deriverebbe da «*the countries' desider to obtain an "adequacy decision" from the EU*»[341]. Tuttavia, come il caso dimostra, non è così automatico, in pratica, che un Paese terzo, per quanto affascinato dal modello europeo e interessato agli scambi con quel mercato, possa prontamente adattarsi ai livelli di tutela richiesti da quegli standard: «*Promoting the GDPR in other regions with different legal and cultural traditions requires the EU to walk a fine line: the standard of protection should be high in order to make it a desirable model, but it must be set at a level that is possible for third countries to attain. Striking the right balance is made more difficult by the apparent tension between the Court, which has tightened the legal standards for data transfers in recent years, and the Commission, which almost seemed to welcome the invalidation of the Privacy Shield as an opportunity to negotiate a yet another data transfer agreement with the US (see the statement of Commissioner Reynders following the judgment)*»[342]. Al riguardo, non è infatti improbabile che, come conseguenza della sentenza *Schrems II*, i Paesi terzi diventino, al contrario, più restii a portare avanti complessi negoziati per ottenere un'agognata decisione di adeguatezza che poi, però, possa venire "facilmente" invalidata dalla Corte di giustizia; sono riflessioni che lo stesso Kuner aveva sollevato, come ricordiamo, anche rispetto alla conclusione di accordi internazionali in materia (*supra*, par. 3.2): «*However, the judgment may cause some third countries to question whether it is worthwhile to strive to reach the EU's data protection standards and to engage in protracted negotiations only to have the agreement, or the adequacy decision based on it, invalidated later on. Having now ensured that data transfers must meet a high standard, the EU should also take care not to set the bar too high, or it may make the GDPR a less attractive model*

[340] T. CHRISTAKIS, After Schrems II, *cit*.
Nello stesso senso anche C. KUNER, Schrems II Re-Examined, in *Verfassungsblog*, 25 August 2020, che rilevava: «*With the Court taking such a strict position in Schrems II, any hope of a stable and viable accommodation for data transfers between the EU and the US can only be based on changes to US law*».
[341] A. BRADFORD, The Brussels Effect, *cit*., p. 149.
[342] C. KUNER, Schrems II Re-Examined, *cit*.

for third countries»[343]. Più in generale, poi, sono state riscontrate incertezze derivanti dalla pronuncia quanto al futuro delle altre decisioni di adeguatezza[344], che ci accingiamo a presentare.

Prime conseguenze di Schrems II sulle decisioni di adeguatezza

Una fondamentale conseguenza della pronuncia consiste sicuramente nella reazione dell'EDPB. Il Comitato europeo, infatti, ha adottato ben due raccomandazioni a seguito di *Schrems II* essenzialmente per assistere titolari e responsabili del trattamento nell'ardua individuazione e attuazione delle misure da adottare in caso di trasferimenti di dati verso Paesi terzi per i quali non esista una decisione di adeguatezza. Pertanto, si capisce che tratteremo questo aspetto nel prosieguo. Qui, però, assumono rilievo le *Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza*, che intervengono invece ad "aggiornare" quanto proposto dal Gruppo di Lavoro Articolo 29 all'indomani della sentenza *Schrems I* (cfr. *supra*, WP237) e cercano quindi, a loro volta, di "*individuare le garanzie essenziali europee che devono essere rispettate al fine di garantire che, in rapporto al trasferimento di dati personali, le ingerenze nei diritti al rispetto della vita privata e alla protezione dei dati personali mediante misure di sorveglianza non eccedano quanto è necessario e proporzionato in una società democratica*"[345], seguendo appunto *Schrems II* e, più in generale, basate sulla giurisprudenza di Lussemburgo e anche di Strasburgo. Il rilievo in questa sede si capisce perché si tratta di garanzie che, per come individuate, dovranno essere prese in considerazione anche dalla Commissione nell'adozione di decisioni di adeguatezza, come si legge dalle stesse: "Nel valutare l'adeguatezza del livello di protezione, ai sensi dell'articolo 45 del RGPD, *la Commissione dovrà valutare se le garanzie essenziali europee siano soddisfatte* nel quadro degli elementi da considerare per garantire che la legislazione del paese terzo nel suo insieme offra un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE"[346].

Il problema che, però, si porrebbe (tanto per la Commissione quanto per gli esportatori di dati chiamati ad attenersi a tali garanzie) in pratica, allorché, cioè dalla "semplice individuazione" di tali

[343] Ibidem.
[344] Cfr. T. CHRISTAKIS, After Schrems II, *cit.*, laddove parla di incertezze che avrebbero potuto mettere a rischio le decisioni sul Regno Unito, cosa che in parte è stata rispetto alle valutazioni dell'EDPB, ma che si è conclusa con la loro recente adozione; ma anche delle rispetto a quelle già esistenti quanto ad altri Stati terzi: «*It would be interesting to follow future developments, including the Commission's periodic reviews or eventual legal challenges at the CJEU, in relation with some of the past adequacy decisions, especially the one with Israel – a country that conducts extensive surveillance for national security purposes – potentially running afoul of the CJEU's standards*».
[345] EDPB, Raccomandazioni 2/2020 *relative alle garanzie essenziali europee per le misure di sorveglianza*, Adottate Il 10 novembre 2020.
[346] Ibidem, pag. 15 (punto 52), enfasi aggiunta.

garanzie si passi alla loro concreta applicazione. Ancora una volta, si ripropone l'asimmetria che abbiamo visto sussistere tra l'intervento della Corte e quello della Commissione in materia. Ci riferiamo al fatto che, come è evidente leggendo le Raccomandazioni, alcuni autori hanno subito notato come sia difficile che diversi Paesi terzi possano assolvere alle "*garanzie essenziali europee*" [347].

Infatti, quanto ai possibili interventi della Commissione rispetto a un'ulteriore decisione di adeguatezza USA, i nuovi negoziati UE-USA stanno proprio palesando le difficoltà derivanti dalle conseguenze di *Schrems II*, nonché dalla rigidità delle garanzie individuate dall'EDPB. Queste ultime, se da un lato fissano gli standard che devono applicarsi, nel caso di specie, agli Stati Uniti affinché possano essere considerati un sistema "sostanzialmente equivalente" a quello europeo, dall'altro lato, come è stato acutamente notato, non prevedono (come neanche la sentenza *Schrems II*) una distinzione tra sorveglianza interna e sorveglianza internazionale e dunque potrebbero sollevare dubbi di coerenza nel caso in cui possano riscontrarsi misure di sorveglianza di Stati membri non del tutto in linea con quelle rigorose garanzie, alimentando la sensazione USA di "due pesi e due misure" nell'approccio UE[348]. In quest'ottica, si comprende la risoluzione del maggio 2021 con cui il Parlamento europeo chiedeva alla Commissione di predisporre linee guida sui trasferimenti di dati verso gli Stati Uniti, puntualizzando che nessuna nuova decisione dovrebbe essere assunta senza seguire quanto definito dalla Corte nell'ultima sentenza *Schrems II*[349].

Con specifico riguardo all'impatto di queste Raccomandazioni rispetto all'adozione di una decisione di adeguatezza da parte della Commissione *ex* articolo 45 GDPR, emergono poi suggestioni sul rapporto tra EDPB e Commissione, che assumono particolare rilievo ai nostri fini per valutare i risvolti pratici delle prospettazioni teoriche che abbiamo avanzato nella Parte III quanto alla predisposizione di un articolato sistema istituzionale dedicato alla protezione dei dati personali a livello sovranazionale, in rispondenza (quantomeno, teorica) ai dettami della *EU Rule of law*.

---

[347] Si segnala T. CHRISTAKIS, "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1), in *European Law Blog*, 13 November 2020, che, tra i primissimi a pronunciarsi sulle "EEG", ironicamente esordiva la propria analisi: «*For the thousands of companies and other data controllers or data processors around Europe faced with the herculean task of assessing whether countries to which they wish to transfer personal data meet the EEG requirements, here is some quick advice: start with the assumption that, in principle, they don't!*».

[348] Così notava T. CHRISTAKIS, Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2), *cit*., 13 April 2021.

[349] Data Protection: MEPs call for clear guidelines on transfer of data to the US, press relase here: https://www.europarl.europa.eu/news/en/press-room/20210518IPR04206/data-protection-meps-call-for-clear-guidelines-on-transfer-of-data-to-the-us .
See also: European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18, here: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.html .

Infatti, ci eravamo promessi di esaminare le implicazioni pratiche delle previsioni teoriche di tale impianto, come ristrutturato dal GDPR anche con la nuova figura del EDPB, e queste vicende legate alla sentenza *Schrems II* paiono fornirci gli elementi fondamentali per un simile esame. A tal riguardo, paiono particolarmente interessanti, ancora, le riflessioni di Christakis anzitutto laddove, nel commentare la sentenza, considerava già l'EDPB come "*the Grand Assessor of Global Legal Adequacy*", ancorché essenzialmente con riguardo alle misure supplementari[350], di cui diremo. Ma queste Raccomandazioni dello scorso novembre 2020 paiono proprio confermare quelle riflessioni, che infatti l'autore ha sviluppato anche in vista del rapporto, che qui più ci interessa, tra l'EDPB, nell'individuare le garanzie europee, e la Commissione, nell'adottare decisioni di adeguatezza. Commentando il punto delle Raccomandazioni che abbiamo riporta sopra, l'autore lo considerava come un "avvertimento" che la Commissione non può permettersi di ignorare nelle sue prossime valutazioni, quindi provocatoriamente affermava: «*the message is that future adequacy decisions should ensure that the requirements found in the "EEG Recommendations" are met in the foreign country. The Commission now has an updated "user's manual" for adequacy decisions that should be taken into consideration. Going even further, a devil's advocate might argue that the "EEG Recommendations" could be a valuable tool in the hands of activists, as a means of challenging the validity of existing adequacy decisions through action at the CJEU. Do the twelve States or entities that have until now benefited from adequacy decisions all meet these EEG requirements? Does Israeli or Japanese surveillance law, for instance, really meet the EEG requirements? And what should the consequences be if they do not?*»[351].

Lasciando aperte queste provocazioni, che ci forniscono suggestioni per riflessioni che si tratteranno nel prosieguo, esse ci danno anche l'occasione per passare all'ulteriore punto sulle decisioni di adeguatezza, indicando quelle in vigore e quelle eventuali.

Le decisioni di adeguatezza attualmente in vigore e quelle mancanti

Una volta invalidata la decisione di adeguatezza della Commissione sugli Stati Uniti, sono attualmente dodici le decisioni vigenti, molte delle quali adottate sotto il vigore della direttiva madre, relative ai seguenti Paesi terzi: Andorra, Argentina, Faer Oer, Giappone, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, nonché sulla legge canadese *Personal Information Protection and Electronic Documents Act*. Tali decisioni non coprono i trasferimenti legati all'attività di contrasto, per cui si applica la direttiva 2016/680. Il 16 giugno 2021 la

[350] T. CHRISTAKIS, After Schrems II, *cit*.
[351] Ibidem.

Commissione ha iniziato la procedura per l'adozione di una decisione relativa alla Corea del Sud (mentre il 28 giugno successivo ha adottato delle decisioni sull'adeguatezza del Regno Unito, come diremo a breve)[352]. Si è detto che a seguito della sentenza *Schrems I* la Commissione adottò una decisione nel 2016 per emendare gran parte delle decisioni già assunte al fine di renderle conformi ai dettami della Corte di giustizia. Gli sviluppi del caso *Schrems II*, come si è visto, potrebbero similmente comportare ulteriori aggiustamenti. Inoltre, non sono ad oggi presenti decisioni relative ad organizzazioni internazionali[353].

Le accennate considerazioni della Bradford sull'effetto incentivante della previsione di decisioni di adeguatezza rispetto a Paesi terzi che non ne sono ancora destinatari, quale ulteriore espressione dell'*effetto Bruxelles*, per quanto sia stato presentato insieme a critiche relativi a possibili rischi di disincentivi, parrebbe invero avere qualche riscontro nella realtà. Nel suo lavoro, aggiornato al 2019, l'autrice rilevava: «*To date, nearly 120 countries have adopted privacy laws, most of them resembling the EU data protection regime. These countries range from large economies and regional leaders such as Brazil, Japan, South Africa, and South Korea to midsize economies such as Columbia and Thailand; and even to small economies and tiny island nations such as Bermuda*»[354]. Interessante, a tal fine, è peraltro la breve ma chiara analisi comparata di Goretta, che di recente ha spiegato come avvengono i trasferimenti di dati verso Paesi che hanno un rilievo preponderante nel mercato globale ma che non godono di decisioni di adeguatezza: Cina, Brasile, India e Russia[355].

Quanto alla Cina, sebbene non dotata di una normativa apposita né di accordi nel settore con l'Unione, essa ha ultimamente, come noto, incrementato esponenzialmente gli scambi commerciali con l'Unione, e dunque inevitabilmente anche il trasferimento (chiaramente senza decisione di adeguatezza, difficilmente ipotizzabile in considerazione del sistema di sorveglianza ivi presente) di dati personali. Ebbene, pare che «nell'ottobre 2020 i parlamentari hanno incominciato a discutere la Legge sulla tutela delle informazioni personali – *Personal Information Protection Law* (PIPL) – apparentemente ispirata dal GDPR (…) – per regolamentare la raccolta e l'uso di dati personali»[356]. Quanto all'India, con una tradizione giuridica molto lontana da quella cinese, il GDPR pare sia stato davvero assunto a modello per importanti interventi legislativi (soprattutto di riforma rispetto a previsioni precedenti), mentre ciò è già espressamente avvenuto in Brasile, con l'adozione nel 2018

[352] Si rinvia alla pagina della Commissione dedicata con gli hyperlink per ciascuna decisione: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[353] C. KUNER, Article 45, *cit*., p. 786.
[354] A. BRADFORD, *op. cit.*, p. 148.
[355] R. GORETTA, Gdpr e trasferimento dati extra Ue: i casi di Cina, India, Brasile e Russia, in *Agenda Digitale*, 22 marzo 2021.
[356] Ibidem.

della *Lei General da Proteção de Dados*, che entrerà a breve in vigore[357]. In entrambi i casi, dunque, sembrano esserci i presupposti per delle trattative nel senso di una prospettiva di futura adeguatezza, come peraltro la Commissione aveva caldeggiato nella suddetta Comunicazione del 2017[358]. Sulla Russia, infine, l'autore rileva le peculiarità di un sistema che ha da poco rinnovato le previsioni legislative in materia nel senso di una maggiore protezione dei cittadini e che, tra gli altri ha previsto «la modifica apportata alla medesima Legge federale n. 152-FZ il 9 luglio 2014 da una legge di pari rango, la n. 242-FZ (Data Localisation Law), che ha introdotto l'obbligo per coloro che raccolgono i dati personali dei cittadini russi di archiviare tali dati personali utilizzando esclusivamente database localizzati in Russia»[359] scartando così qualsivoglia possibilità di trasferimenti di dati verso l'esterno.

Ebbene, escludendo l'ultimo esempio, lo sviluppo di sistemi molto lontani dalle tradizioni giuridiche europee verso un allineamento al sistema di protezione dei dati personali proposto dall'Unione, se da un lato costituisce un chiaro esempio di emulazione di quello "modello globale" dato dal GDPR, dall'altro lato contribuisce ad avvicinare quegli ordinamenti verso un percorso che, come avvenuto di recente con il Giappone o la Corea del Sud, potrebbe condurre ad una decisione di adeguatezza per facilitare gli scambi. Il tutto, ovviamente, deve fare i conti con le conclusioni di *Schrems II* e, quindi, con le rigide aggiornate *garanzie essenziali europee*.

La prospettata decisione di adeguatezza per un "nuovo" Paese terzo: aggiornamenti sul Regno Unito

Sulla singolare vicenda del Regno Unito ci soffermeremo successivamente con valutazioni complessive che, raccogliendo tutti gli elementi esposti sin ora rispetto al Paese e spiegando meglio la situazione dopo il recesso dall'Unione europea, indagheranno possibili prospettive.

Qui basti segnalare che, a partire dal gennaio 2021 in cui ha avuto termine il periodo di transizione, il Regno Unito ha assunto la posizione di qualsiasi altro Paese terzo e dunque i trasferimenti di dati

[357] Ibidem.
[358] Cfr. Commissione, COM(2017) 7 final, 10 gennaio 2017, *cit.*: «*la Commissione intende impegnarsi attivamente con i principali partner commerciali in Asia orientale e sudorientale, a partire dal Giappone e dalla Corea nel 2017 e, in funzione dei progressi compiuti verso la modernizzazione della normativa in materia di protezione dei dati, con l'India, ma anche con i paesi dell'America latina, in particolare con i paesi del Mercosur, e con il vicinato europeo, che hanno manifestato l'interesse a sottoporsi ad un "accertamento di adeguatezza". Inoltre, la Commissione accoglie con favore le manifestazioni di interesse da parte di altri paesi terzi disposti a impegnarsi su queste tematiche. Le discussioni su un eventuale accertamento di adeguatezza sono un dialogo interattivo durante il quale fornire tutti i necessari chiarimenti in merito alle norme UE sulla protezione dei dati ed esplorare le modalità per accrescere la convergenza della legislazione e della prassi dei paesi terzi*», p. 9.
[359] R. GORETTA, *op. cit.*, 22 marzo 2021.

dall'Unione europea rientrano nelle previsioni del Capo V del GDPR (e del Capo V della direttiva 2016/680). Infatti, dal gennaio 2020 il Regno Unito ha definitivamente lasciato l'Unione europea e da allora è iniziato un "periodo di transizione" (regolato dal c.d. *Withdrawal Agreement*) sino al 31 dicembre 2020 in cui, quanto allo specifico settore, continuava ad applicarsi anche a quello Stato il GDPR. Allo scadere del periodo di transizione intervenne però un ulteriore accordo (EU-*UK Trade and Cooperation Agreement*) per regolare ancora alcuni settori di cooperazione con l'Unione e in esso veniva prevista la libera circolazione dei dati tra UE e Regno Unito sino a che la Commissione non avrebbe adottato una decisione di adeguatezza, per la quale era però previsto un termine di sei mesi (con scadenza, quindi, al 30 giugno scorso). Di fronte alle paventate possibilità che ciò non sarebbe avvenuto nei tempi, con necessità di altri strumenti di legittimazione e misure supplementari previste dall'EDPB, la Commissione presentò a febbraio 2021 delle bozze di decisioni di adeguatezza (una ai sensi del GDPR e l'altra ai sensi della direttiva 2016/680), avviando la procedura per la loro adozione. Intanto, in linea con le previsioni dell'articolo 70, par. 1, lett. s), GDPR, ad aprile 2021 l'EDPB interveniva con due pareri sulle bozze di adeguatezza della Commissione sindacandole in maniera serrata e rilevando aspetti su cui sollecitava la stessa ad approfondire le proprie valutazioni, in conformità con la giurisprudenza *Schrems*[360]. Quindi, nel maggio 2021 il Parlamento europeo adottava una Risoluzione sull'adeguatezza del Regno Unito, invitando la Commissione ad adottare una decisione di adeguatezza solida, in grado di superare un eventuale vaglio della Corte di giustizia, e a tal fine "a elaborare un piano d'azione per affrontare quanto prima le criticità identificate nei pareri dell'EDPB"[361]. Ebbene, a pochissimo dal termine del periodo transitorio, il 28 giugno 2021 la Commissione ha finalmente adottato le due decisioni, confermando quindi l'adeguatezza del sistema del Regno Unito ai fini di un trasferimento dei dati personali che non sarà perciò soggetto a misure supplementari. Se questa soluzione potrebbe da un lato apparire scontata rispetto al sistema di un Paese che sino a ieri era membro dell'Unione, e dunque – almeno in teoria – ne condivideva i valori fondanti, le perplessità sorte prima

[360] EDPB, Opinion 14/2021 *regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, Adopted on 13 April 2021: https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf .
EDPB, Opinion 15/2021 *regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom*, Adopted on 13 April 2021, https://edpb.europa.eu/system/files/2021-04/edpb_opinion152021_ukadequacy_led_en.pdf .

[361] Risoluzione del Parlamento europeo del 21 maggio 2021 sull'adeguata protezione dei dati personali da parte del Regno Unito (2021/2594(RSP)), punto 38. Si veda anche, più in generale, il punto 40: "si rammarica del fatto che la Commissione abbia ignorato gli inviti del Parlamento a sospendere lo scudo per la privacy fino a quando le autorità statunitensi non rispetteranno le sue condizioni, e che abbia invece sempre preferito "monitorare la situazione" senza alcun risultato concreto in termini di protezione dei dati per le persone né certezza giuridica per le imprese; esorta la Commissione a imparare dai suoi errori del passato prestando attenzione agli inviti del Parlamento e degli esperti relativi alla conclusione e al monitoraggio delle precedenti decisioni di adeguatezza, e a non lasciare che sia la GCUE, sulla base delle denunce presentate dai singoli, ad occuparsi dell'adeguata applicazione della legislazione dell'Unione europea in materia di protezione dei dati".

dell'adozione (che, quanto a "rapidità" potrebbe rievocare lo stesso errore commesso con il *Privacy Shield*), soprattutto nella misura in cui (oltre alle lecite critiche di attivisti in vista anche dei casi a Strasburgo e Lussemburgo sul sistema di sorveglianza britannico) venivano avanzate da attori istituzionali (Parlamento e EDPB), ci offrono argomenti per porre in dubbio le scelte della Commissione, che si avrà modo di esporre in seguito.

5. Sulle garanzie adeguate…e sulle deroghe

Previsioni normative e correlati sviluppi nella prassi istituzionale

L'articolo 46 del GDPR, rubricato "Trasferimento soggetto a garanzie adeguate", comprende gli strumenti che costituiscono base giuridica per il legittimo trasferimento di dati verso l'esterno quando manchi una decisione di adeguatezza rispetto al Paese terzo o all'organizzazione destinatari. In tali casi, il trasferimento è consentito solo se il titolare o responsabile del trattamento hanno "fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi"[362]. L'articolo 46 del GDPR, che ha un corrispettivo nell'articolo 37 della direttiva 680/2016 (pur con le ovvie differenze date dal diverso ambito di applicazione), trova il suo antecedente nell'articolo 26 della direttiva madre – che al paragrafo 1 prevedeva i casi di deroga e al paragrafo 2 indicava, invece, le "garanzie sufficienti" – confermandone l'impianto ma ampliando gli strumenti a disposizione. L'articolo 26, par. 2, infatti, prevedeva espressamente soltanto il riferimento alle "clausole contrattuali appropriate", quali esempio di "garanzie sufficienti" che il responsabile del trattamento doveva presentare affinché lo Stato membro potesse autorizzare il trasferimento[363]. In realtà, ancorché non espressamente richiamate dalla norma, a partire circa dagli inizi del 2000 alcune autorità garanti nazionali cominciarono ad approvare anche le cd. *norme vincolanti d'impresa*, quali garanzie sufficienti ai sensi dell'articolo 26 della direttiva[364].

[362] GDPR, Articolo 46 – *Trasferimento soggetto a garanzie adeguate*

[363] Direttiva 95/46, Articolo 26 – *Deroghe*

2. Salvo il disposto del paragrafo 1, uno Stato membro può autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo che non garantisca un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 2, qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate.

[364] Così chiarisce C. KUNER, Article 46. Transfers subject to appropriate safeguards, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2020, p. 799, in cui si legge: «*Under the DPD, two main types of 'adequate safeguards' were recognised, namely contractual clauses and binding corporate rules ('BCR', though they were not mentioned explicitly in the DPD)*».

Nonché ID., Article 47. Binding corporate rules, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2020, p. 815, in cui si legge: «*The DPD did*

Nel suo parere n. 1/2001 sulla proposta di decisione della Commissione relativa alle clausole tipo, il Gruppo di Lavoro, oltre ad accoglierla con favore, ivi precisava gli aspetti caratteristici di tali clausole: "Per definizione il destinatario dei dati personali trasferiti in base alle clausole contrattuali tipo approvate dalla Commissione è residente in un paese in cui non esiste un sistema adeguato di tutela dei dati personali. Le clausole contrattuali tipo consentono di ovviare a questo problema a condizione che l'importatore dei dati ne rispetti rigorosamente le disposizioni"[365]. Successivamente, nel 2005, in un documento di lavoro, il Gruppo segnalava che la Commissione avesse adottato decisioni in materia proprio per facilitare il ricorso alle clausole contrattuali[366]. Infatti, queste ultime costituivano il principale strumento per il trasferimento dei dati sotto il vigore della direttiva madre[367]. Nello stesso periodo, il Gruppo di Lavoro definiva e precisava poi l'utilizzo di *norme contrattuali d'impresa*, laddove rispondenti alle necessarie garanzie in accordo con i principi di protezione stabiliti dalla direttiva: "*From this perspective, as a general principle, the implementation of binding corporate rules within the Community does not pose any problem provided that the rules comply with the national data protection legislation. If these conditions were met, this would allow corporate groups to have a truly global privacy policy*"[368].

Come si anticipava, relativamente alle clausole tipo, la Commissione adottava nel 2001 due decisioni: la decisione 2001/497/CE, su "*clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi*", che dichiarava le clausole allegate come garanzie sufficienti ai sensi dell'articolo 26 della direttiva madre, e però specificava di non applicarsi "al trasferimento di dati personali operato da responsabili del trattamento, aventi sede nella Comunità, a destinatari aventi sede al di fuori della Comunità, che costituiscano meri incaricati di trattamenti tecnici"[369]; e la decisione 2001/16/CE, "*clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento residenti in paesi terzi*", che si applicava solo ai trasferimenti aventi come destinatari soggetti residenti fuori della Comunità che agissero "esclusivamente in veste di incaricati

---

not explicitly mention BCRs. However, beginning in approximately 2002, some DPAs began approving BCRs as adequate safeguards under Article 26(2) DPD (…). The first meeting of the WP29 ever with outside stakeholders took place in The Hague in November 2004 and focused on BCRs».

[365] Gruppo di Lavoro Articolo 29, Parere 1/2001 sul progetto di decisione della Commissione ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi in conformità all'articolo 26(4) della direttiva, WP38, Adottato il 26 gennaio 2021

[366] Gruppo di Lavoro Articolo 29, Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva95/46/CE del 24 ottobre 1995, Adottato il 25 novembre 2005, WP114, disponibile qui: https://www.garanteprivacy.it/documents/10160/10704/ARTICOLO+29+-+WP+114+-+Interpretazione+articolo+26+direttiva+9546.pdf/784bb47e-ed63-4c9c-911b-27671b34b60b?version=1.1. Le decisioni della Commissione sono disponibili qui: http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm .

[367] Cfr. C. KUNER, Article 46, *cit*., p. 799.

[368] Working Party A29, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Adopted on 3 June 2003, WP 74, p. 8, available here: https://naih.hu/files/D_bcr_wp074_en.pdf .

[369] Decisione della Commissione 2001/497/CE, del 15 giugno 2001, *relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE*, Articolo 2, c. 2.

del trattamento"[370]. La prima veniva, poi, modificata nel 2004[371], mentre la seconda veniva abrogata e sostituita con la decisione 2010/87/UE, che è stata sottoposta al vaglio della Corte proprio nel caso *Schrems II*, ma non è stata invalidata (la c.d. decisione CPT). Nel 2016, un'ulteriore decisione della Commissione (la n. 2297) interveniva a modificare la prima decisione del 2001 e quella del 2010, dunque entrambe le vigenti normative sulle clausole contrattuali tipo (rispettivamente, per trasferimenti da responsabili a responsabili, e da responsabili a incaricati), essenzialmente sostituendone una parte con la previsione di un'informativa dello Stato membro alla Commissione nel caso in cui un'autorità nazionale di controllo decida di sospendere o vietare un trasferimento[372]. Da ultimo, proprio lo scorso 4 giugno 2021, la Commissione ha adottato la decisione di esecuzione n. 2021/914, con cui ha rilevato la necessità di aggiornare le clausole contrattuali tipo vigenti, adottate sulla base della direttiva madre, per individuarne di nuove rispondenti ai requisiti e alle garanzie di cui al GDPR (articolo 46, par. 2, lett. c)[373]. Tale decisione è entrata in vigore venti giorni dopo la pubblicazione, mentre le decisioni 2001/497/CE e 2010/87/UE sono abrogate con effetti a partire dal settembre 2021. Avremo modo di soffermarci su questi interventi.

Passando al GDPR, abbiamo visto che nel periodo che lo separa dalla direttiva madre si ebbero già importanti sviluppi in tema di garanzie adeguate. Pertanto, sin dal suo Considerando 108 è previsto espressamente, tra le garanzie adeguate, il riferimento alle *norme vincolanti d'impresa*, a cui segue quello alle *clausole tipo di protezione dei dati* adottate dalla Commissione o da un'autorità di controllo, e alle *clausole contrattuali* autorizzate da un'autorità di controllo[374]. Peraltro, oltre a riconoscere le norme vincolanti d'impresa nella lista di cui all'articolo 46, il Regolamento dedica alle stesse appositamente l'articolo 47[375]. L'impostazione del nuovo articolo 46, che aggiungerebbe quattro nuove forme di garanzie rispetto al sistema precedente[376], distingue in due paragrafi

[370] Decisione della Commissione 2002/16/CE, del 27 dicembre 2001, *relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento residenti in paesi terzi, a norma della direttiva 95/46/CE,* Articolo 2, c. 2 [non più in vigore dal 2010, cfr. Decisione 2010/87/UE].
[371] Decisione della Comissione2004/915/CE, del 27 dicembre 2004, *che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi.*
[372] Decisione di esecuzione (UE) 2016/2297 della Commissione, del 16 dicembre 2016, che modifica la decisione 2001/497/CE relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE, e la decisione 2010/87/UE della Commissione relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio.
[373] Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio.
[374] GDPR, Considerando 108.
[375] GDPR, Articolo 47 – *Norme vincolanti d'impresa*, in cui è previsto che l'autorità di controllo competente possa approvare norme vincolanti d'impresa secondo il meccanismo di coerenza *ex* articolo 63, purché soddisfino le condizioni che sono elencate nell'articolo.
[376] C. KUNER, Article 46, *cit*., pp. 800 e 806.

garanzie adeguate che non richiedono una previa autorizzazione dell'autorità nazionale di controllo (par. 2) da quelle che la richiedono (par. 3). Nella prima categoria, di cui al par. 2, rientrano: strumenti giuridicamente vincolanti ed esecutivi tra soggetti pubblici (lett. a); norme vincolanti d'impresa (lett. b); clausole tipo, adottate dalla Commissione ovvero da un'autorità di controllo e poi approvate dalla Commissione (lett. c e d); codici di condotta (lett. e); meccanismi di certificazione (lett. f). Nella seconda categoria, di cui al par. 3, rispetto ai quali l'autorità di controllo applica il meccanismo di coerenza *ex* art. 63 (cfr. par. 4, art. 46), rientrano: clausole contrattuali c.d. *ad hoc*, ossia tra titolari e responsabili esportatori e destinatari nel Paese terzo o nell'organizzazione internazionale (lett. a); accordi amministrativi tra autorità o organismi pubblici (lett. b). Il par. 5 dell'articolo 46 disciplina gli effetti delle autorizzazioni rilasciate da Stati membri o autorità di controllo ovvero delle decisioni della Commissione adottate sotto la vigenza della direttiva madre[377].

Dunque, ricapitolando, rispetto a quest'ultima, le garanzie introdotte *ex novo* dal GDPR sarebbero: gli strumenti vincolanti tra soggetti pubblici; gli accordi amministrativi tra questi; i codici di condotta; i meccanismi di certificazione. Inoltre, l'articolo 48 si dedica ai casi in cui sentenze o decisioni amministrative di uno Stato terzo consentano trasferimenti solo se basati su un accordo tra quello Stato e l'UE. Non ci soffermeremo sull'analisi di questi strumenti, ma è bene averne conoscenza anche in vista del fatto che qualcuno ne avrebbe incoraggiato il ricorso, poiché valide alternative rispetto alle perplessità sorte di recente sulle clausole tipo[378]. Come si accennava, a seguito dello stimolo dato dalla sentenza *Schrems II* quanto alle garanzie adeguate (ancorché limitatamente alle clausole contrattuali tipo) l'EDPB è intervenuto a novembre 2020 con delle Raccomandazioni. In particolare, interessano qui le Raccomandazioni n. 1/2020 su "*misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE*" che, in sostanza, snocciolando le conclusioni della Corte nel caso suddetto (di cui diremo a beve), cercano di aiutare gli esportatori ad individuare le eventuali misure supplementari adeguate quando debbano effettuare trasferimenti verso Paesi terzi che non godono di una decisione di adeguatezza[379]. Proporremo qualche commento rispetto alle stesse dopo aver analizzato, sotto il profilo delle garanzie adeguate, il caso *Schrems II* e le sue implicazioni al riguardo.

[377] GDPR, Articolo 46 – *Trasferimento soggetto a garanzie adeguate*.
[378] Il riferimento è ad alcuni commenti sopra riportati rispetto alla decisione *Schrems II*, nonché alle nuove Raccomandazioni 1/2020 dell'EDPB, di cui però si dirà meglio. Per una breve analisi delle quattro nuove forme di garanzie adeguate previste dall'articolo 46 GDPR, si rinvia a C. KUNER, Article 46, cit., pp. 806-809.
[379] EDPB, Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, Adottate il 10 novembre 2020.

Il caso Schrems II e le clausole contrattuali tipo

Come dicevamo, il rinvio pregiudiziale che diede luogo al c.d. caso *Schrems II* originava essenzialmente dal dubbio sulla validità della decisione della Commissione relativa proprio alle clausole tipo, che costituivano invero la base giuridica per i trasferimenti di *Facebook Ireland* verso gli Stati Uniti.

Ricordiamo infatti che, a seguito della sentenza *Schrems I*, il giudice di rinvio irlandese annullava il rigetto del reclamo proposto da Schrems al *Data Protection Commissioner* e lo rinviava a quest'ultimo, che quindi apriva finalmente un'indagine da cui rilevava che gran parte dei dati veniva trasferita da Facebook sulla base delle clausole tipo di protezione previste nell'allegato della apposita decisione della Commissione 2010/87/UE (decisione CPT). Pertanto, come sappiamo, chiedeva a Schrems di riformulare il reclamo in vista di tale considerazione. Seguendo le sollecitazioni derivanti, il DPC predisponeva una bozza di decisione da cui emergevano effettivamente perplessità circa la compatibilità del sistema di sorveglianza USA con le previsioni della Carta UE, rispetto alle quali le clausole tipo sulla cui base avvenivano i trasferimenti «*non sono idonee a porre rimedio a tale carenza, in quanto esse conferiscono agli interessati unicamente diritti contrattuali nei confronti dell'esportatore e dell'importatore dei dati, senza tuttavia vincolare le autorità statunitensi*»[380]. In tal senso, il DPC poneva in dubbio la validità della decisione CPT e, a tali fine, adiva il giudice irlandese perché sollevasse rinvio pregiudiziale. Dunque, la questione del secondo caso sorse, come dicevamo, essenzialmente rispetto alle clausole tipo. Abbiamo, però, anche già detto che la Corte di giustizia non ha invalidato la contestata decisione CPT. Prima di vedere con quali argomenti veniva risolta la questione di validità della decisione, è molto utile esaminare gli altri aspetti, preliminarmente trattati dalla Corte, relativi a tali clausole tipo: quello degli elementi per valutare l'adeguatezza nel caso di trasferimenti fondati su di esse; quello de(lla portata de)i poteri delle autorità di controllo al riguardo.

Quanto al primo punto, il giudice di rinvio domandava quali elementi andassero considerati per stabilire se il livello di protezione richiesto dal GDPR nel caso di trasferimenti basati su clausole tipo adottate dalla Commissione, dunque *ex a*rt. 46, par. 2, lett. c), GDPR, possa dirsi garantito nello specifico contesto. Nel definire il livello di protezione, la Corte rispondeva richiamando, in sostanza, altre previsioni del Regolamento anche per valutare lo specifico trasferimento realizzato sulla base di clausole tipo, ribadendo che il principio di continuità della tutela di cui all'articolo 44

[380] Corte di giustizia, *Schrems II*, p. 56, ma si vedano anche i pp. 53-55.

deve ritenersi operante per tutte le disposizioni previste dal Capo V. Quindi, specificava: «*La valutazione richiesta, a tal fine, nel contesto di un trasferimento siffatto deve, in particolare, prendere in considerazione tanto le clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo considerato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali trasferiti, gli elementi rilevanti del sistema giuridico di quest'ultimo. Relativamente a quest'ultimo aspetto, gli elementi che occorre prendere in considerazione nel contesto dell'articolo 46 di tale regolamento corrispondono a quelli enunciati, in modo non esaustivo, all'articolo 45, paragrafo 2, di detto regolamento*»[381].

Al riguardo, come è stato notato da qualcuno, la Corte ha interpretato le disposizioni del Capo V GDPR «*to create a common baseline for standards, despite differences in wording between Arts 45 and 46 GDPR*»[382], e ciò attraverso una lettura congiunta a partire del principio dell'articolo 44. Invero, qualcuno ha criticato che la Corte non abbia tenuto conto della "gerarchia" prospettata tra le varie misure nel Capo V del GDPR: «*The Court thus abandoned the hierarchy between these two data transfer mechanisms, despite the express language of the GDPR and the long-standing practice of the DPAs. One could even ask what point there is of the Commission assessing third countries for adequacy if appropriate safeguards based on the same standards are available, in light of the fact that they can be implemented much more quickly than an adequacy decision can be approved*»[383].

In ogni caso, da ciò emerge che la determinazione del livello di protezione garantito rispetto ai casi di trasferimento dei dati verso l'esterno, qualunque sia lo strumento utilizzato (tra quelli previsti dai vari articoli del Capo V) dovrà tener conto degli stessi elementi: «*l'articolo 46, paragrafo 1, e l'articolo 46, paragrafo 2, lettera c), del RGPD devono essere interpretati nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti da tali disposizioni devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta*»[384]. Ciò che cambia, potremmo dedurre, è il soggetto tenuto a tale valutazione a seconda dello strumento che viene utilizzato come base giuridica per il trasferimento, ovvero nei casi in cui si debba procedere a sospendere o vietare il trasferimento come conseguenza di carenze

[381] Corte di giustizia, Schrems II, pp. 103 e 104.
[382] Così L WOODS, "You Were Only Supposed to Blow the Bloody Doors Off!": Schrems II and external transfers of personal data, in *EU Law Analysis*, 16 July 2020.
[383] C KUNER, Schrems II Re-Examined, *cit*., 25 August 2020.
[384] Ibidem, p. 105.

(anche sopravvenute) emerse dalla valutazione. Quest'ultimo riferimento ci consente il passaggio al secondo punto di rilievo, mentre il primo si lega meglio alla questione di validità della decisione CPT, che tratteremo subito dopo.

Infatti, giudice di rinvio chiedeva lumi sull'interpretazione dell'articolo 58, par. 2, lett. f) e j) GDPR per capire se nei casi di trasferimenti basati su CPT i poteri attribuiti da quelle norme alle autorità dovessero considerarsi limitati a ipotesi eccezionali. La Corte rilevava al riguardo: «*tale autorità è tenuta a sospendere o a vietare un trasferimento di dati personali verso un paese terzo qualora ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le clausole tipo di protezione dei dati non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione non possa essere garantita con altri mezzi, ove il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo*»[385]. Il riferimento al "complesso delle circostanze proprie del trasferimento" conferma, quindi, applicando il chiarimento suddetto sugli elementi da considerare per determinare se il livello di protezione sia garantito in un dato contesto, che anche le autorità di controllo devono sindacare quegli gli elementi per sospendere o vietare un trasferimento[386].

A tal fine, la Corte, utilizzando un ragionamento analogo a quello formulato in *Schrems I* (*mutatis mutandis*, perché in quel caso si riferiva alla decisione di adeguatezza), chiariva che il potere di esecuzione riconosciuto alla Commissione quando emette una decisione per adottare clausole tipo *ex* art. 46, par. 2, lett. c), GDPR non deve limitare i poteri conferiti dall'articolo 58 GDPR alle autorità di controllo, quanto a possibili sospensioni o divieti di trasferimento. Invece, l'esistenza di una decisione di adeguatezza della Commissione, laddove da un lato vincola le autorità di controllo, dall'altro non esime le stesse dal trattare reclami correlati e sollevare eventuali dubbi rivolgendosi a un giudice per proporre questioni pregiudiziale alla Corte di giustizia, in ciò riprendendo pedissequamente *Schrems I*, ma in maniera funzionale a distinguere l'atteggiamento che le autorità di controllo devono tenere rispetto alle due diverse tipologie di decisioni della Commissione e in vista dei peculiari compiti conferitigli al riguardo[387].

[385] Ibidem, p. 113.
[386] Cfr. F. D'ATH, Arrêt « Schrems II » : sur la légalité des transferts de données personnelles fondés sur une décision d'adéquation ou moyennant des garanties appropriées, in *Journal de droit européen*, 2020, p. 442 : « *De façon connexe, la Cor confirme également qu'une autorité de contrôle demeure compétente pour examiner si l'usage des clauses types suffit, ou s'il y a lieu d'ordonner la suspension ou l'interdiction d'un transfert car le niveau de protection requis n'est pas respecté. Lors de cette analyse, l'autorité de contrôle doit prendre en compte tant les stipulations contractuelles convenues entre l'exportateur et l'importateur des données que « les éléments pertinents du système juridique [du pays tiers]* ».
[387] Cfr. Corte di giustizia, *Schrems II*, punti 115 e 119.

Dunque, la Corte passava finalmente a sindacare la validità della decisione della Commissione CPT alla luce della Carta, che il giudice di rinvio poneva in dubbio in vista delle perplessità riscontrate rispetto al sistema di sorveglianza statunitense e poiché le clausole tipo non vincolerebbero le autorità pubbliche di quel Paese. La Corte anzitutto chiariva che le CPT non possono per definizione vincolare le autorità pubbliche, non essendo esse parti del contratto, che riguarda invece solo il titolare del trattamento stabilito nell'Unione e il destinatario nel Paese terzo; tuttavia, prendeva atto del fatto che: «*Pur se esistono* (…) *situazioni in cui, a seconda dello stato del diritto e delle prassi vigenti nel paese terzo interessato, il destinatario di un trasferimento siffatto è in grado di garantire la protezione dei dati necessaria sulla base delle sole clausole tipo di protezione dei dati, sussistono altre situazioni in cui quanto pattuito in tali clausole potrebbe non costituire un mezzo sufficiente che consenta di garantire, in pratica, la protezione effettiva dei dati personali trasferiti nel paese terzo interessato. Ciò si verifica, in particolare, qualora il diritto di tale paese terzo permetta alle autorità pubbliche di quest'ultimo ingerenze nei diritti delle persone interessate relativi a tali dati*»[388]. Quindi, dopo aver sottolineato l'importanza dell'effettività della tutela in casi di trasferimento, la Corte affrontava la questione rintracciando possibili garanzie rispetto alle autorità pubbliche.

Nel farlo, essa partiva intanto distinguendo bene le decisioni *de quo* (CPT) da quelle di adeguatezza per ribadire che solo nel secondo caso è richiesta alla Commissione una valutazione di adeguatezza del Paese terzo o organizzazione internazionale destinatari; quando adotta, invece, una decisione CPT, la Commissione non deve effettuare nessuna valutazione preliminare al riguardo. Piuttosto in tali casi, in cui cioè una decisione di adeguatezza mancherebbe, la Corte precisava che «*spetta al titolare del trattamento o al responsabile del trattamento stabiliti nell'Unione prevedere segnatamente garanzie adeguate*», cosa che si traduce, come suggerito anche dai Considerando (soprattutto 109) al GDPR, nella necessità, in vista delle peculiarità del Paese terzo verso cui i dati sono trasferiti, di adottare *ulteriori misure supplementari* che possano consentire di mantenere il livello di protezione garantito dal GDPR. Insomma, la Corte insisteva in tali casi "*sull'attribuzione della responsabilità al titolare del trattamento o al responsabile del trattamento stabiliti nell'Unione e, in subordine, all'autorità di controllo competente*"[389].

Così veniva dunque spiegato il ragionamento che salvava la validità della decisione della Commissione CPT: le clausole in essa previste «*mirano unicamente a fornire ai titolari del trattamento o ai responsabili del trattamento stabiliti nell'Unione garanzie contrattuali che si applicano in modo uniforme in tutti i paesi terzi e, pertanto, indipendentemente dal livello di*

[388] Corte di giustizia, Schrems II, p. 126.
[389] Ibidem, punto 134 e prima punti 130-132.

protezione garantito in ciascuno di essi. Poiché tali clausole tipo di protezione dei dati non possono, tenuto conto della loro natura, fornire garanzie che vadano al di là di un obbligo contrattuale di vegliare a che sia rispettato il livello di protezione richiesto dal diritto dell'Unione, esse possono richiedere, in funzione della situazione esistente nell'uno o nell'altro paese terzo, l'adozione di misure supplementari da parte del titolare del trattamento al fine di garantire il rispetto di tale livello di protezione (...). Incombe pertanto, anzitutto, a tale titolare del trattamento o al responsabile del trattamento verificare, caso per caso, e, eventualmente, in collaborazione con il destinatario del trasferimento, se il diritto del paese terzo di destinazione garantisca una protezione adeguata, alla luce del diritto dell'Unione, dei dati personali trasferiti sulla base di clausole tipo di protezione dei dati, fornendo, se necessario, garanzie supplementari rispetto a quelle offerte da tali clausole. Qualora il titolare del trattamento o il responsabile del trattamento, stabiliti nell'Unione, non possano adottare misure supplementari sufficienti a garantire tale protezione, essi o, in subordine, l'autorità di controllo competente, sono tenuti a sospendere o mettere fine al trasferimento di dati personali verso il paese terzo interessato. Pertanto, il solo fatto che clausole tipo di protezione dei dati contenute in una decisione della Commissione (...) come quelle contenute nell'allegato della decisione CPT, non vincolino le autorità dei paesi terzi verso i quali dati personali possono essere trasferiti non può inficiare la validità di tale decisione»[390]. Sindacando poi, nello specifico, le clausole allegate nella decisione CPT, la Corte concludeva che essa «*prevede meccanismi efficaci che consentono, in pratica, di garantire che il trasferimento verso un paese terzo di dati personali sulla base delle clausole tipo di protezione dei dati contenute nell'allegato di tale decisione sia sospeso o vietato qualora il destinatario del trasferimento non rispetti dette clausole o si trovi nell'impossibilità di rispettarle*»[391], rispondendo quindi, infine, che dall'esame complessivo della decisione non emergessero elementi di invalidità.

Ci siamo forse dilungati nell'esporre gli estratti della sentenza relativi alle clausole tipo, ma li riteniamo indispensabili per avere la chiarezza necessaria ai fini della comprensione dei delicati passaggi, e, dunque, soprattutto, delle confusioni e perplessità che ne sono derivate all'indomani sotto disparati aspetti, che hanno anche portato gli interventi istituzionali cui si è fatto cenno. Ma ciò costituisce una conseguenza inevitabile di una pronuncia in cui, potremmo dire, "ce n'è per tutti".

Diciamo subito che la pronuncia *Schrems II* ci pare massimamente emblematica del nesso tra protezione dei dati personali e *EU rule of law* poiché da essa, ad un'analisi complessiva, (ri)emerge chiaro il ruolo "sovrano" della Corte nel manovrare il complesso meccanismo costruito con il

[390] Ibidem, punti 133-136, sottolineato aggiunto.
[391] Ibidem, p. 148.

GDPR, tanto nella sua specifica architettura istituzionale – che coinvolge attivamente, come abbiamo visto, le autorità di controllo (finanche nella loro composizione collegiale all'EDPB) e la Commissione – che nel rilievo e nella responsabilità riconosciuti agli operatori privati, affinando, così, quanto avevamo in qualche misura riscontrato già commentando *Google c. CNIL*. Intendiamo dire che nell'analisi delle due decisioni della Commissione sottoposte al vaglio di validità, in *Schrems II* la Corte non ha risparmiato nessuno degli attori coinvolti.

Se con l'analisi sulla decisione *Privacy Shield*, come abbiamo detto, la Corte parrebbe "richiamare" la Commissione rispetto alla propria valutazione di adeguatezza, con l'analisi sulla decisione CPT – che sembrerebbe, invece, "salvare" la Commissione – essa ribadisce l'importanza dei compiti delle autorità di controllo e la responsabilità degli esportatori nei casi di trasferimenti fuori dall'Unione. Non è soltanto la Commissione, quindi, ad essere tenuta a controllare la continuità delle garanzie predisposte nell'ordinamento dell'Unione quando avvengono trasferimenti verso l'esterno, ma anche le autorità di controllo e finanche gli operatori del mercato interessati all'esportazione dei dati devono intervenire attivamente per assicurare il principio che sta alla base dei trasferimenti, per come palesato nell'articolo 44 GDPR, e quindi, più in generale, la coerenza tra l'azione interna e l'azione esterna dell'Unione quanto al suo sistema valoriale.

Eppure, se passiamo dalla prospettiva teorica all'applicazione concreta dei principi ribaditi dalla Corte, anche le conclusioni in questo caso lasciano, come dicevamo, margini di confusione. Infatti, proprio il giorno dopo la sentenza, l'EDPB rilevava rispetto ai trasferimenti basati su clausole tipo che «*While the SCCs remain valid, the CJEU underlines the need to ensure that these maintain, in practice, a level of protection that is essentially equivalent to the one guaranteed by the GDPR in light of the EU Charter. The assessment of whether the countries to which data are sent offer adequate protection is primarily the responsibility of the exporter and the importer, when considering whether to enter into SCCs (…). If the result of this assessment is that the country of the importer does not provide an essentially equivalent level of protection, the exporter may have to consider putting in place additional measures to those included in the SCCs. The EDPB is looking further into what these additional measures could consist of*»[392]. Invero, come abbiamo anticipato, l'EDPB pubblicava poi nel novembre successivo raccomandazioni volte a fare chiarezza su tali misure, come diremo meglio.

[392] EDPB, Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, 17 July 2020, available here: https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en .

Ma difficoltà emergono, quanto a questo passaggio, anche laddove la Corte, oltre ad insistere sulla necessità che gli esportatori prevedano "misure supplementari", richiede prima agli stessi di effettuare l'ardua valutazione sul livello di protezione garantito nel Paese terzo. Invero, qualcuno ha ritenuto al riguardo che "*cette obligation de se livrer à un examen « au cas par cas » du niveau de protection garanti par le droit du pays tiers devrait dès lors être considérée comme une obligation de moyen, plutôt qu'une obligation de résultat*"[393].

Oltre alle incombenze sui soggetti esportatori (se del caso di concerto con gli importatori), la Corte puntava poi anche sulle responsabilità delle autorità di controllo, laddove ribadiva che il loro controllo deve coprire l'intero processo di trasferimento fondato su clausole tipo, e che esse possono così sospenderlo o vietarlo non appena lo considerino non capace di garantire il livello di protezione adeguato. Da qui, dunque, derivano le paventate incertezze a seguito della sentenza *Schrems II* rispetto alla possibilità di continuare a utilizzare con la stessa frequenza lo strumento sin ora più diffuso per legittimare i trasferimenti in mancanza di una decisione di adeguatezza. Infatti, laddove la Corte ribadisce tale controllo delle autorità, che esprimerebbe il funzionamento dei meccanismi di sospensione e divieto che renderebbero legittime le previsioni sulle clausole tipo, richiedendo quindi alle autorità una la valutazione di sostanziale equivalenza del sistema di garanzie del Paese terzo, essa implica inevitabili ripercussioni sui trasferimenti attualmente in atto, fondati su clausole tipo, rispetto a Paesi che sembrerebbero poter non rispondere a quelle garanzie: «*this assessment, under the control of DPAs, could shut down data transfers to an important number of States (starting with China and Russia) whose legal systems offer substantially less guarantees than the US in relation with government access to data. Indeed, one can hardly imagine how personal data transfers to China could continue via TikTok or other companies after Schrems II*»[394].

Inoltre, sempre su queste considerazioni, la dichiarata invalidità della decisione *Privacy Shield* ha delle inevitabili conseguenze, che la Corte aveva infatti posto a giustificazione del suo scrutinio e come si anticipava, sui trasferimenti verso gli Stati Uniti basati sulle clausole tipo. Infatti, pur avendo salvato la decisione CPT, la Corte, nella misura in cui con l'invalidità della decisione *Privacy Shield* ha acclarato che quel sistema non risponde alle garanzie richieste, ha così orientato le valutazioni a cui sono tenuti autorità di controllo ed esportatori, nel verificare la sostanziale equivalenza del sistema, ai fini di eventuali sospensioni o divieti del trasferimento. L'alternativa per continuare i trasferimenti basati su clausole tipo verso gli USA, allo stato attuale, è dunque quella di predisporre le c.d. misure supplementari, quali garanzie aggiuntive per sopperire ai rischi di quel sistema; cosa che, però, potrebbe risultare alquanto complessa, specie se, come qualcuno ha notato,

[393] F. D'ATH, Arrêt « Schrems II » : sur la légalité des transferts de données personnelles, *cit*., p. 445.
[394] T. CHRISTAKIS, After Schrems II, *cit*., 21 July 2020.

le carenze rilevate dalla Corte in quel sistema riguardano soprattutto la mancanza di rimedi giurisdizionali effettivi: «*If one considers, for instance, that one of the main concerns of the Court was that the US system of surveillance does not offer effective judicial remedies to EU citizens, it is hard to imagine how any "additional safeguards" introduced by the data controller could change this*»[395]. E questo è, ancora, un altro nodo problematico della pronuncia (ed è forse per questo che, all'indomani della stessa, Facebook ha utilizzato una base giuridica diversa da quelle previste dall'articolo 46, cfr. *infra*).

La Corte, infatti, per quanto vi insista, si limita a un semplice riferimento vago a tali misure (pur usando diversi termini, cfr. parr. 133-137), rispetto al quale è facile immaginare come gli operatori possano trovarsi spiazzati. È per questo che, al fine di chiarire tale passaggio, mentre già si suggeriva il ricorso a garanzie alternative (quali norme contrattuali d'impresa, deroghe o codici di condotta), che pure presentavano incertezze[396], ovvero il riferimento a possibili strumenti supplementari (come misure tecniche o organizzative)[397], l'EDPB è intervenuto con le sue Raccomandazioni.

Le (prime) conseguenze di Schrems II: misure supplementari individuate dall'EDPB e clausole tipo aggiornate dalla Commissione 2021

Come si diceva, il 10 novembre 2020 l'EDPB ha adottato due tipi di Raccomandazioni per fornire delle linee guida a seguito della sentenza *Schrems II*. Abbiamo già parlato in parte di quelle relative alle *garanzie essenziali europee*, che riprenderemo. Qui, invece, qualche considerazione sulle Raccomandazioni n. 1/2020 "*relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE*".

Partendo proprio dalle statuizioni della Corte, laddove precisava la responsabilità degli esportatori a verificare caso per caso l'efficacia delle garanzie adeguate rispetto a un dato sistema esterno,

[395] T. CHRISTAKIS, After Schrems II, *cit*., 21 July 2020.

[396] A caldo, C. KUNER proponeva le alternative dei codici di condotta o dei meccanismi di certificazione, cfr. The Schrems II judgment of the Court of Justice, *cit.*, 17 July 2020. Si veda, però, T. CHRISTAKIS, After Schrems II, *cit*., 21 July 2020, in cui l'autore prospettava le seguenti incertezze rispetto alle norme vincolanti d'impresa: «*their negotiation and implementation can take years and is particularly onerous. As a result, BCRs are only used by large companies with wide-ranging data transfer obligations. (…) they will be met by exactly the same difficulty as SCCs, namely that the transfer in both cases will be impossible if the third country's laws do not meet the EU protection standards (…). The essentially equivalent level of protection standard applies to all legal mechanisms of transfer, not just SCCs*». Inoltre, rilevava perplessità nel caso di ricorso sia alle deroghe che ai codici di condotta o ai meccanismi di certificazione, concludendo che «*it is hard to imagine how codes of conduct or certification mechanisms could work any better than SCCs and permit to address the problem of the absence of equivalent protection in the country of destination*».

[397] Cfr., *ex multis*, C. KUNER, che indicava a titolo di esempio "*legal measures, technical measures; organisational measures*", in Schrems II Re-Examined, *cit*., 25 August 2020.

l'EDPB prendeva atto delle difficoltà che simili responsabilità (ancorché in linea con l'articolo 5 GDPR) comportano, e così adottava le raccomandazioni per aiutare tali operatori "nel complesso compito di valutare i paesi terzi e di individuare, se necessario, misure supplementari adeguate"[398]. Nel farlo, l'EDPB strutturava il lavoro indicando i "passi da seguire", potenziali informazioni utili nonché alcuni esempi di possibili misure supplementari da adottare. In breve, l'EDPB suggeriva: di conoscere i propri trasferimenti; dunque, verificare lo strumento che li legittima, tra quelli previsti dal GDPR; quindi, valutare se la legge o la prassi del Paese terzo destinatario inficia l'efficacia delle garanzie adeguate, in tal senso indicando il riferimento alle altre Raccomandazioni sulle garanzie essenziali europee; in caso affermativo, individuare e adottare misure supplementari e, se nessuna si rivela adeguata, procedere a sospendere o vietare il trasferimento; adottare eventuali procedure formali richiesti dalle misure supplementari; infine, rivalutare a intervalli regolari il livello di protezione del Paese terzo e controllarne gli sviluppi. Quindi, l'EDPB ribadiva il compito di monitoraggio delle autorità di controllo quanto alla corretta applicazione del GDPR e ribadiva il loro dovere di sospendere o vietare un trasferimento nel caso in cui rilevino, a seguito di un'indagine o reclamo, che non sia (più) garantito un livello di tutela sostanzialmente equivalente[399]. Quindi, l'EDPB prevedeva nell'allegato l'importante, ancorché non esaustiva, lista di possibili misure supplementari.

Ebbene, poco dopo la loro adozione, Christakis individuava già profili di difficoltà, ritenendo in sostanza che da esse emergerebbe che per l'EDPB nessun trasferimento debba avvenire verso Paesi terzi che non possano considerarsi garantire una tutela essenzialmente equivalente[400]. Dalla sua analisi delle Raccomandazioni, l'autore evinceva tre punti che, a suo modo di vedere, sarebbero critici e renderebbero dunque difficile la concreta applicazione di quanto indicato dall'EDPB: "*The EDPB Ignores the Risk-Based Approach*"; "*The EDPB is Highly Suspicious of the Use of Solely Non-Technical Measures*"; "*The EDPB's Technical Measures: Make the Data Unreadable!*".

In particolare sul primo punto, l'autore segnalava che a fronte del rifiuto dell'approccio basato sul rischio (che pure sarebbe previsto dal GDPR) da parte dell'EDPB, diverse società e organizzazioni stimolavano quest'ultimo a considerare piuttosto i rischi reali, comprovando (anche con documenti che vengono riportati dall'autore) che molto raramente le autorità straniere richiederebbero l'accesso ai dati e che dunque il rischio per la protezione dei dati sarebbe particolarmente limitato, rispetto alle ben più ampie esigenze di commercio internazionale: *«None of these arguments have*

[398] EDPB, Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE – Adottate il 10 novembre 2020, p. 2.
[399] Ibidem, pp. 2-4.
[400] Cfr. T. CHRISTAKIS, "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2), in *European Law Blog*, 16 November 2020.

convinced the EDPB. Not only does the Board not endorse a risked-based approach, but it also gives the impression that it wishes to reject it in para. 42 (…). The debate between a risk-based approach and a rights-based approach is an old one as far as the EU is concerned (…). The EDPB post-Schrems II "Recommendations" clearly show a preference for the rights-based approach, despite the fact that the risk-based approach also forms part of the data protection GDPR iceberg. The rejection of the risk-based approach by the EDPB is odd. Combined with the interpretation of "supplementary measures" by the Board (…), it might lead to important disruption for business activities that could be incompatible with the respect of the principle of proportionality.»[401].

Quanto, poi, al terzo aspetto, l'autore concludeva che, a suo modo di vedere, nella visione molto rigida dell'EDPB i trasferimenti potrebbero considerarsi legittimi, verso Paesi che non assicurano una protezione essenzialmente equivalente, solo se i dati sono illeggibili[402]. Da questi aspetti di forte rigidità nella posizione dell'EDPB, l'autore concludeva prospettando tre possibili scenari, che cerchiamo qui di sintetizzare. A suo modo di vedere, le conseguenze potrebbero essere: una sorta di "zona grigia" in cui le aziende solo lievemente prendono in considerazione le indicazioni del Comitato, continuando la maggior parte dei trasferimenti in maniera non conforme; la "localizzazione dei dati", che sarebbe una conseguenza del fatto che questi sostanzialmente non possono essere trasferiti all'esterno, e che ci sembrerebbe peraltro abbastanza in linea con le proposte di *cloud-computing* europeo (ci riferiamo al progetto GAIA-X) o con le considerazioni più recenti del Commissario Breton, di cui diremo; infine, il terzo scenario sarebbe quello che l'autore riferisce come "*Change the World*", ossia la prospettiva di un'azione dell'Unione così forte e convincente, nella sua rigidità, da incentivare cambiamenti nei sistemi di sorveglianza dei Paesi terzi che li rendano, di fatto, tali da assicurare una tutela sostanzialmente equivalente a quella europea[403]. In quest'ultimo caso, si tratterebbe della massima attuazione della strategia unilaterale dell'Unione nella promozione dei suoi valori verso l'esterno e, così, nel suo contributo a modellare l'ordine internazionale (tramite il *Brussels effect*, e non solo). Tralasciando quest'ultima prospettiva, le prime due inglobano, in qualche modo, le perplessità che l'autore rilevava a fronte delle innegabili difficoltà derivanti dalle Raccomandazioni. Sono valutazioni da tenere in considerazione perché, aldilà della scelta di condividerle o meno, aiutano a comprendere meglio le diverse posizioni, fornendo una prospettiva pragmatica, e si rivelano legate ai discorsi che faremo sulla

[401] Ibidem.
[402] [402] Cfr. T. CHRISTAKIS, "Schrems III"? (Part 2), *cit.*, 16 November 2020; ID., "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 3), in *European Law Blog*, 17 November 2020.
[403] Cfr. T. CHRISTAKIS, "Schrems III"? (Part 3), *cit.*, 17 November 2020.

sovranità digitale dell'Unione europea, per cui saranno utili per sviluppare in maniera più compiuta le successive riflessioni.

Passando, infine, a esaminare l'ultimo intervento istituzionale che pare direttamente legato alla pronuncia *Schrems II* quanto alle clausole tipo, se è chiaro che la Corte non ha invalidato la decisione CPT, è chiaro anche, però, che la pronuncia e l'intera vicenda ne abbiano fatto emergere il carattere obsoleto. Pertanto, la Commissione si mise subito a lavoro, con un progetto di decisione già disponibile a fine 2020 che ha portato lo scorso giugno all'adozione della nuova Decisione 2021/914 sulle clausole tipo di protezione.

Come si diceva, nel novembre 2020 la Commissione presentava un progetto di decisione (o meglio, un progetto di decisione di esecuzione sulle clausole contrattuali tipo e un progetto di allegato a tale decisione) che otteneva il parere congiunto dell'EDPB e dell'EDPS. O meglio, si trattava di due pareri, ma che erano in continuità e che venivano sviluppati a partire da questa prospettiva: "*L'EDPB e il GEPD sono del parere che clausole che si limitino a ribadire le disposizioni dell'articolo 28, paragrafi 3 e 4, del GDPR e dell'articolo 29, paragrafi 3 e 4, dell'EUDPR, non costituiscono adeguate clausole contrattuali tipo. Il comitato e il GEPD hanno quindi deciso di analizzare il documento nella sua interezza, comprese le appendici. Secondo il parere del comitato e del GEPD, un contratto conforme all'articolo 28 del GDPR o all'articolo 29 dell'EUDPR dovrebbe stabilire e chiarire ulteriormente come adempiere alle disposizioni in oggetto. È in questa prospettiva che verrà analizzato il progetto di clausole contrattuali tipo presentato al comitato e al GEPD per il previsto parere*»[404]. Senza soffermarci sull'analisi dei pareri congiunti, basti dire che dalla decisione definitiva adottata a giugno scorso emerge che la Commissione ne abbia seguito gli orientamenti, come la stessa dichiara espressamente nel Considerando 25 della Decisione 2021/914[405]. Inoltre, anche il NOYB – organizzazione non a scopo di lucro fondata da Schrems e, chiaramente, incentrata sulla tutela dei dati personali – aveva commentato la proposta della Commissione, con una parte soprattutto che ci pare utile riportare poiché relativa alle implicazioni pratiche delle previsioni proposte: «*we would like to recognize that most smaller organisations will be unable to conduct a proper assessment of the laws of a third country. Such an assessment is highly complex and requires cross-jurisdictional expertise. Usually experts for (partly very exotic)*

[404] Parere congiunto 1/2021 dell'EDPB e del GEPD sulla decisione di esecuzione della Commissione europea relativa alle clausole contrattuali tipo tra titolari e responsabili del trattamento, 14 gennaio 2021, p. 5, disponibile qui: https://edpb.europa.eu/system/files/2021-04/edpb-edpsjointopinion01_2021_sccs_c_p_it.pdf . Si veda anche il Parere congiunto 2/2021 dell'EDPB e del GEPD sulla decisione di esecuzione della Commissione europea relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi, 14 gennaio 2021, a cui peraltro si riferisce espressamente la Commissione nella Decisione (Considerando 25), disponibile qui: https://edpb.europa.eu/system/files/2021-05/edpb_edps_jointopinion_202102_art46sccs_it.pdf .

[405] Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021, *cit*., Considerando 25.

other jurisdictions are not available in most Member States and local experts in the given third country are not aware of the requirements under the SCCs, GDPR and CFR. We would therefore encourage the Commission to think about ways to provide such assessments for the most important trading partners of the Union, be it via the EDPB, SAs or via independent researchers. A relatively small investment in such publicly available assessments may ensure that these assessments are accurate but also realistically available to smaller organisations»[406]. Un'utile suggestione che non pare però aver avuto grande riscontro.

Nel prevedere le nuove clausole tipo, la Commissione prendeva atto degli sviluppi tecnologici, dell'incremento del commercio internazionale e, con esso, della necessità del trasferimento di dati; quindi, introduceva nuove clausole che rispondessero alle rinnovate esigenze e fossero in linea con le previsioni del GDPR; incoraggiava poi i soggetti interessati (esportatori e importatori) a corredare le clausole di misure supplementari laddove necessario. Sicuramente è importante il richiamo alla valutazione periodica cui la Commissione è tenuta "poiché le esigenze dei portatori di interessi, la tecnologia e i trattamenti possono cambiare" e che quindi andrebbe fatta "alla luce dell'esperienza"[407]. Rispetto alle valutazioni cui sono tenute le parti, considerando i riferimenti nel Considerando 20 e nei punti relativi alla "sicurezza del trattamento" di cui alla clausola 8 (in tutti i moduli in essa previsti) non parrebbe del tutto accolto il sollecito di NOYB[408]. Senza dilungarci su complesse previsioni, non resta da vedere quali saranno i riscontri pratici dell'attuazione di questa recentissima decisione.

Le deroghe di cui all'articolo 49 GDPR

L'articolo 49 del GDPR prevede ora le deroghe che, sotto la previgente normativa, erano anche contenute nell'articolo 26, par. 1 della direttiva madre, che consentiva agli Stati membri di disporre un trasferimento verso un Paese terzo che non garantiva una tutela adeguata al ricorrere di certe condizioni[409]. Il Gruppo di Lavoro Articolo 29 predisponeva nel 2005 un documento sull'articolo

[406] NOYB, noyb's comments on the proposed Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679, December 2020, p. 3, available here: https://noyb.eu/sites/default/files/2020-12/Feedback_SCCs_nonEU.pdf

[407] Decisione di esecuzione (UE) 2021/914, cit., Considerando 23, ma si veda anche Articolo 3.

[408] Peraltro, al riguardo, si segnalano le dichiarazioni non troppe entusiaste che Schrems ha rilasciato, attraverso la sua organizzazione NOYB, il 16 luglio 2021 in occasione dell'anniversario della sentenza *Schrems II*, v. NOYB, *Statement by Max Schrems on the "Schrems II" Anniversary*, July 16, 2021: "*The European Commission is muddying the waters by issuing new transfer tools, like "Standard Contractual Clauses", that carefully bypass a clear say on EU-US transfers and allow industry lawyers to keep spinning new compliance theories and avoid long-term solutions. At the same time, the Commission does not seem to believe in a timely solution with the US*", disponibili qui: https://noyb.eu/en/statement-max-schrems-schrems-ii-anniversary

[409] Direttiva 95/46/CE, Articolo 26 – *Deroghe.*

26, di cui si è già detto, che riguardava principalmente le deroghe, per fornire indicazioni volte ad evitare che lo stesso fosse oggetto di interpretazioni che portavano a un'applicazione non uniforme tra gli Stati membri[410].

L'attuale previsione del GDPR, che trova un corrispettivo per l'ambito relativo all'attività di contrasto nell'articolo 39 della direttiva 680/2016, stabilisce le condizioni in presenza delle quali il trasferimento è ammesso pur non ricorrendo le ipotesi degli articoli 45 e 46, ovvero non vi sia una decisione di adeguatezza di quel Paese terzo o organizzazione internazionale né sia possibile predisporre garanzie adeguate. Rinviando all'articolo per l'elenco di deroghe previste (la prima tra le quali è il consenso esplicito dell'interessato)[411], va ricordato che esse vanno interpretate restrittivamente e non abusate: «*Use of the derogations of Article 49 by their nature provides no extra protection for data transfers. However, any relevant provisions of the GDPR continue to apply when personal data are transferred based on a derogation. In addition, such provisions must*

---

1. In deroga all'articolo 25 e fatte salve eventuali disposizioni contrarie della legislazione nazionale per casi specifici, gli Stati membri dispongono che un trasferimento di dati personali verso un paese terzo che non garantisce una tutela adeguata ai sensi dell'articolo 25, paragrafo 2 può avvenire a condizione che:
a) la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto, oppure
b) il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa, oppure
c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo, oppure
d) il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per costatare, esercitare o difendere un diritto per via giudiziaria, oppure
e) il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure
f) il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione.

[410] Gruppo di Lavoro Articolo 29, Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva95/46/CE del 24 ottobre 1995, Adottato il 25 novembre 2005, WP114.

[411] GDPR, Articolo 49 – *Deroghe*
1. In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:
a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
d) il trasferimento sia necessario per importanti motivi di interesse pubblico;
e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

be read in light of the Charter, since, as the CJEU has found, the applicability of EU law entails the applicability of the Charter»[412]. Nel 2018 l'EDPB forniva degli orientamenti sull'applicazione dell'articolo 49, che ricordavano proprio come l'esportatore sia sempre tenuto a osservare le altre disposizioni del GDPR: «*Si rende pertanto necessaria una verifica articolata in due fasi: innanzitutto il trattamento dei dati deve essere fondato su una base giuridica, nel rispetto di tutte le disposizioni pertinenti di cui al RGDP; in secondo luogo occorre ottemperare alle disposizioni di cui al Capo V*»[413].

Senza poterci soffermare sulla disamina di tali linee guida, diciamo che l'articolo 49 GDPR assume rilievo per il richiamo "criptico"[414] che ne fa la Corte di giustizia nella *sentenza Schrems II*. Prima di chiudere l'articolata analisi sulle varie questioni pregiudiziali propostele, la Corte di giustizia affronta quella sugli effetti della decisione *Privacy Shield* invalidata e, a tal fine, si riferisce all'articolo 49: "*Quanto alla questione se occorra mantenere gli effetti di tale decisione al fine di evitare la creazione di una lacuna giuridica (...), occorre rilevare che, in ogni caso, tenuto conto dell'articolo 49 del RGPD, l'annullamento di una decisione di adeguatezza come la decisione «scudo per la privacy» non è idoneo a creare una lacuna giuridica siffatta. Tale articolo stabilisce, infatti, in modo preciso, a quali condizioni possono aver luogo trasferimenti di dati personali verso paesi terzi in assenza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, di detto regolamento o di garanzie appropriate ai sensi dell'articolo 46 del medesimo regolamento*"[415]. Rispetto a questo passaggio, Christakis rilevava che, pur a fronte della rigida posizione (nelle linee guida 2/2018 e non solo) dell'EDPB rispetto alla necessità di non considerare le deroghe in modo sistematico per coprire i casi in cui non siano possibili le basi giuridiche *ex* artt. 45-46, da questo punto della pronuncia della Corte potrebbe invero derivare, in attesa di migliori alternative, che le imprese possano essere tentate di fare un ricorso maggiore all'articolo 49[416]. Anche Kuner rilevava che, nonostante l'incontestata restrittività con cui considerare le deroghe, detto punto della sentenza parrebbe equivoco nell'implicare un utilizzo delle stesse per compensare

[412] C. KUNER, Article 49. Derogations for specific situations, in in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2020, p. 846-847.
[413] EDPB, Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679, Adottate il 25 maggio 2018, p. 3, ma si veda anche a p. 4: « *Nel considerare il trasferimento di dati personali verso paesi terzi od organizzazioni internazionali gli esportatori di dati dovrebbero pertanto promuovere soluzioni che offrano agli interessati la garanzia di continuare a beneficiare, dopo il trasferimento, dei diritti fondamentali e delle garanzie cui hanno titolo in materia di trattamento dei dati. Poiché le deroghe non forniscono una tutela e garanzie adeguate per i dati personali trasferiti e poiché i trasferimenti fondati su una deroga non necessitano di alcuna autorizzazione preventiva dell'autorità di controllo, il trasferimento di dati personali verso paesi terzi sulla base delle deroghe comporta maggiori rischi per i diritti e per le libertà degli interessati*», https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_it.pdf .
[414] Così lo considera C. KUNER, Schrems II Re-Examined, *cit*., 25 August 2020.
[415] Corte di giustizia, *Schrems II*, p. 202.
[416] Cfr. T. CHRISTAKIS, After Schrems II, *cit*., 21 July 2020.

l'invalidità della decisione *Privacy Shield*, concludendo tuttavia al riguardo che «*the derogations cannot fill the gap created by invalidation of the Privacy Shield, except in a few limited cases*»[417].

Su questi pochi limitati casi vogliamo un attimo soffermarci perché pare che tra essi rientrino ora proprio i trasferimenti effettuati da Facebook verso gli Stati Uniti (saltando così le condizioni sia dell'articolo 45 che dell'articolo 46) e che la questione stia emergendo nel prosieguo della vicenda, dopo la pronuncia della Corte di giustizia, in Irlanda. In particolare, ciò sarebbe avvenuto proprio all'indomani della sentenza *Schrems II*, da quando Facebook avrebbe cominciato a utilizzare come base giuridica per i trasferimenti di dati verso gli USA l'articolo 49, par. 1, lett. b, GDPR[418]. Vale la pena di percorrere i punti salienti. Dopo la sentenza della Corte di giustizia, Schrems chiedeva ripetutamente al DPC irlandese di dare attuazione alle statuizioni di Lussemburgo, senza particolari riscontri al riguardo. Invero, nell'agosto 2020, l'autorità irlandese comunicava che avrebbe aperto una nuova indagine, distinta da quella partita dal reclamo, per indagare sull'utilizzo di clausole tipo da parte di Facebook, mentre informava inoltre che avrebbe sospeso l'indagine partita dal reclamo di Schrems. Il punto è che, poiché Facebook ha cominciato ad utilizzare una nuova base giuridica per i trasferimenti verso gli USA, che consiste proprio in una deroga *ex* articolo 49, l'indagine sulle clausole tipo non avrà più rilievo: «*This means that any "preliminary order" or "second investigation" by the DPC on the SCCs alone will in fact not stop Facebook from arguing that its EU-US data transfers continue to be legal. In practice Article 49(1)(b) GDPR may be an appropriate legal basis for very limited data transfers (e.g. when an EU user is sending an message to a US user), but cannot be used to outsource all data processing to the US*»[419].

Ad ogni modo, nel settembre 2020 il DPC emetteva l'ordine preliminare con cui intimava a Facebook di interrompere i trasferimenti di dati verso gli USA, mentre poco dopo la High Court autorizzava Facebook a presentare un riesame giudiziario contro il DPC e sospendeva così la nuova indagine da questo avviata[420]. Tuttavia, nel maggio 2021 la High Court stabiliva che il DPC avesse diritto di aprire quella nuova indagine. Dunque, da quel momento sono in corso due "indagini parallele" contro Facebook condotte dall'autorità irlandese: quella a seguito del reclamo di Schrems del 2013, che ha portato ai casi della Corte di giustizia; quella nuova, avviata spontaneamente

[417] C. KUNER, Shrems II Re-Eamined, *cit.*, 25 August 2020.
[418] Così risultava, per esempio, da aggiornamenti NOYB del settembre 2020, cfr. NOYB, Is the DPC actually stopping Facebook's EU-US data transfers? Maybe…half-way, 09 September 2020, here: https://noyb.eu/en/dpc-actually-stopping-facebooks-eu-us-data-transfers-maybe-half-way .
[419] Ibidem.
[420] NOYB, Irish High Court: Judicial Review against DPC admitted, September 14, 2020, available here: https://noyb.eu/en/irish-high-court-judicial-review-against-dpc-admitted .

dall'autorità per verificare la legittimità dei trasferimenti di dati[421]. Nel frattempo, poco prima, a fronte dell'inerzia del DPC rispetto al reclamo di Schrems, questi convenivano un accordo in cui il DPC si impegnava a decidere rapidamente il relativo reclamo[422]. A seguito dell'ultima pronuncia della Corte irlandese, la chiusura delle indagini e la soluzione del reclamo relativo ai trasferimenti di dati effettuati da Facebook dovrebbe avvenire (dopo quasi otto anni dall'inizio) veramente a breve.

Seguendo anche queste vicende, a fine maggio 2021 il Parlamento europeo adottava una risoluzione chiedendo alla Commissione di avviare una procedura d'infrazione nei confronti dell'Irlanda, relativa proprio alla gestione dei reclami da parte dell'autorità irlandese in violazione del GDPR[423]. Da essa, in particolare, si legge che il Parlamento "*si rammarica del fatto che il Commissario irlandese per la protezione dei dati (DPC) abbia avviato un procedimento contro Maximilian Schrems e Facebook dinanzi alla Corte suprema irlandese, anziché adottare una decisione nell'ambito dei suoi poteri ai sensi dell'articolo 4 della decisione 2010/87/UE e dell'articolo 58 del RGPD; ricorda, tuttavia, che il DPC si è avvalso del ricorso giuridico che consente alle autorità di protezione dei dati di portare all'attenzione di un giudice nazionale le preoccupazioni sulla validità di una decisione di esecuzione della Commissione al fine di avviare una domanda di pronuncia pregiudiziale alla CGUE; esprime profonda preoccupazione per il fatto che diverse denunce di violazione del RGPD presentate il 25 maggio 2018, il giorno in cui il RGPD è entrato in vigore, e altre denunce da parte di organizzazioni a tutela della privacy e gruppi di consumatori, siano ancora in attesa di una decisione del DPC, che è l'autorità capofila per i casi in questione; esprime preoccupazione per il fatto che il DPC interpreti "senza indugio" all'articolo 60, paragrafo 3, del RGPD – contrariamente all'intenzione dei legislatori – come periodo superiore a mesi; esprime preoccupazione per il fatto che le autorità di controllo non abbiano adottato misure proattive ai sensi dell'articolo 61 e 66 del regolamento generale sulla protezione dei dati per costringere il DPC a rispettare i suoi obblighi a norma del regolamento generale sulla protezione dei dati; è altresì preoccupato per il numero insufficiente di specialisti in ambito tecnologico che lavorano per il DPC e per il loro utilizzo di sistemi obsoleti; deplora le implicazioni del tentativo fallito del DPC di trasferire i costi del procedimento giudiziario al convenuto, il che avrebbe avuto un forte effetto*

[421] NOYB, Decision by Irish High Court – DPC must now implement CJEU decision and stop EU-US transfers, May 13 2021, available here: https://noyb.eu/en/decision-irish-high-court-jr .
High Court of Ireland, Judgment n. 126 delivered on the 14th of May 2021, available here: https://noyb.eu/sites/default/files/2021-05/High%20Court%20Judgement%202021-05-14.pdf

[422] Accordo tra Schrems e DPC, 12 gennaio 2021, disponibile qui: https://noyb.eu/sites/default/files/2021-05/Settelement%20-%20DPC%20-%20Schrems.pdf .

[423] Risoluzione del Parlamento europeo del 20 maggio 2021 sulla sentenza della Corte di giustizia dell'Unione europea del 16 luglio 2020 – Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems ("Schrems II") – Causa C-311/18, qui: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_IT.html .

dissuasivo; invita la Commissione ad avviare una procedura di infrazione nei confronti dell'Irlanda per non aver applicato correttamente il RGPD"[424].

Queste riflessioni, ci danno un'idea della complessità di un sistema che quanto più è perfezionato nelle sue previsioni (come il GDPR appare, tanto per condizioni e garanzie imposte ai trasferimenti che per funzioni e compiti dei soggetti coinvolti), tanto più si complica al momento dell'applicazione pratica, perché basta il minimo disfunzionamento di una parte per "ingarbugliare" l'intero circuito. Il caso dell'autorità irlandese lo spiega chiaramente, non solo per lo specifico della vicenda Schrems e di come la "gerarchia" di basi giuridiche per il trasferimento di dati verso Paesi terzi si riveli macchinosa in sostanza, ma anche perché essa nelle vicende coinvolgenti Facebook costituisce la c.d. autorità capofila, figura che abbiamo prospettato come funzionale nelle sue previsioni teoriche (*supra*, Parte III), ma che in pratica mostra le carenze del meccanismo in cui si colloca. Ciò ci conduce, quindi, oltre che ad affrontare discorsi più ampi sul principio di coerenza, a prospettarne anche di più specifici sul funzionamento concreto del meccanismo di coerenza tra autorità di controllo introdotto dal GDPR, che peraltro è stato di recente oggetto di sindacato dalla Corte di giustizia in un altro caso contro Facebook deciso in Lussemburgo proprio lo scorso giugno 2021.

[424] Ibidem, punto 4.

CAPITOLO III

ALCUNE RIFLESSIONI

SUI PRINCIPI DI PROTEZIONE EQUIVALENTE E COERENZA

NELLA PROTEZIONE DEI DATI PERSONALI DELL'UNIONE EUROPEA

1. Livello di protezione adeguato significa sostanzialmente equivalente?

A partire dal punto 73 della sentenza *Schrems I* pare sia ormai indiscutibile che, quando si tratta di trasferimenti di dati personali fuori dall'Unione, la "adeguatezza" del livello di protezione che il sistema terzo deve *effettivamente* garantire vada intesa come "sostanziale equivalenza" rispetto a quello garantito all'interno dell'Unione.

Nell'evocare e ribadire, quasi come un *mantra*, il "livello di protezione sostanzialmente equivalente" che l'Unione così pretende dal Paese terzo, sia per adottare (ad opera della Commissione) decisioni di adeguatezza, sia, quando ciò non è possibile, per condurre le valutazioni degli esportatori o delle autorità di controllo rispetto ad eventuali sospensioni o divieti del trasferimento, sia ancora nel caso di conclusione di accordi internazionali in materia, la Corte pare operare in piena attuazione del principio di coerenza tra azione interna ed esterna dell'Unione nel settore della protezione dei dati personali, in affermazione e promozione dei valori su cui essa si fonda. La coerenza sarebbe infatti, anzitutto interna, laddove esprime l'ormai totale assunzione delle tradizioni giuridiche europee.

Con ciò intendiamo, da un lato, che la stessa terminologia utilizzata rievoca chiaramente la *dottrina* elaborata dalla Corte di Strasburgo sin dal caso *Bosphorus* (in quel caso, basata su una presunzione) per gestire i rapporti con l'ordinamento sovranazionale in caso di collisioni rispetto a questioni relative a Stati che fossero, al contempo, parti della CEDU e membri delle Comunità. Ma intendiamo anche, dall'altro, il riferimento a quelle dinamiche che, a partire dalla "opposizione" di c.d. *controlimiti* da parte di Corti costituzionali degli Stati membri (particolarmente, tedesca e italiana), stimolarono la Corte di giustizia, al tempo in cui i diritti fondamentali non trovavano riconoscimento nell'ordinamento sovranazionale, a divenire sempre più sensibile rispetto alla loro tutela.

Da queste spinte (esterne, Consiglio d'Europa, ed interne, Stati membri) emerse, com'è noto, quello che è divenuto l'impianto attuale del processo di integrazione, fortemente imperniato, pur senza perdere l'afflato funzionale alle esigenze del mercato unico, sul riconoscimento di valori comuni, tra cui spicca la tutela dei diritti fondamentali garantiti a livello sovranazionale. E ciò emerse proprio, più o meno esplicitamente, attraverso, potremmo dire, l'*adeguamento* tra i diversi livelli di tutela dei diritti fondamentali riconosciuti nel contesto regionale europeo – ossia quello degli Stati, quello sovranazionale e quello internazionale della CEDU – che passava proprio dal riconoscimento di una *tutela sostanzialmente equivalente* tra di essi.

In tal senso, nello specifico settore della protezione dei dati personali, il GDPR ci fornisce una chiara conferma, sin dal Considerando 10 che prevede: "*Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione*"[425]. Ciò risulta, come abbiamo visto, ben ribadito dai giudici nella saga *Schrems*[426].

In linea con tale coerenza interna, l'operato della Corte pare poi coniugare anche la coerenza nella azione esterna dell'Unione, utilizzando sempre – e in maniera più esplicita, potremmo dire – la formula che richiama la protezione sostanzialmente equivalente. Infatti, in molti casi relativi a questioni che, nell'esercizio dell'azione esterna dell'Unione, coinvolgono in qualche misura sistemi di Paesi terzi, la Corte si trova spesso ad insistere sulla tutela dei diritti fondamentali quale caratteristica imprescindibile del proprio ordinamento e, così, a pretendere che le proprie istituzioni acclarino che una tutela "sostanzialmente equivalente" possa riscontrarsi anche nel sistema con cui entrano in contatto[427].

Il fatto che tale giurisprudenza abbia così influenzato le previsioni del GDPR sul trasferimento dei dati verso l'esterno e, da lì, abbia confermato il suo approccio nell'ultimo caso *Schrems II* può considerarsi una dimostrazione, in pratica, che la Corte suole dare piena attuazione del principio – esposto in teoria – tra coerenza dell'azione interna ed esterna. E non solo. Con il suo operato essa pare influenzare anche le istituzioni coinvolte, per cui vanno lette in piena continuità le ultime

[425] GDPR, Considerando 10.
[426] Corte di giustizia, *Schrems I*, punti 73, 74 e soprattutto 91; *Schrems II*, punti 100, 101 e 178.
[427] Come si è detto *supra* (Capitolo III, Parte III), il riferimento è soprattutto alle misure adottate nell'ambito PESC. Tra queste, segnaliamo ancora una volta lo specifico approfondimento sul rapporto tra le misure restrittive antiterrorismo e tutela dei diritti fondamentali, che richiama proprio riflessioni sulla protezione equivalente, cfr. G. LO TAURO, Diritti fondamentali e misure antiterrorismo nell'Unione europea, *cit.*, part. pp. 175-182.

Raccomandazioni dell'EDPB sulle *garanzie essenziali europee*, che erigerebbero il Comitato, con il modello della Corte, ad ulteriore portavoce della *EU rule of law* nello specifico settore.

Nondimeno, e pur confermando tutto quanto appena sviluppato, è proprio dall'analisi dell'impatto di quelle Raccomandazioni sugli operatori e sui casi concreti che il principio di coerenza, letto dalla prospettiva della protezione sostanzialmente equivalente, parrebbe non funzionare in pratica.

Come dicevamo, le Raccomandazioni 2/2021 contengono le *garanzie essenziali europee* che devono essere riscontrare nel caso di trasferimenti di dati personali fuori dall'Unione europea, per evitare ingerenze nei diritti degli interessati che possano travalicare lo stretto necessario. Si tratta di garanzie, come si evince sin dal titolo, nei confronti delle misure di sorveglianza del sistema terzo destinatario dei dati personali provenienti dall'Unione. Vale la pena illustrarne alcuni passaggi per rilevarne il tenore e sviluppare alcune possibili criticità, in parte anticipate, che potrebbero far emergere i limiti che, sotto questo profilo, il principio di coerenza tra azione interna ed esterna dell'Unione potrebbe mostrare in pratica nel nesso tra *EU rule of law* e protezione dei dati personali.

Abbiamo già detto di quali garanzie si tratta, ma le riproponiamo brevemente. I limiti ai diritti derivanti dalle misure di sorveglianza devono: basarsi su regole chiare, precise e accessibili; rispondere a necessità e proporzionalità rispetto agli obiettivi legittimi perseguiti; essere controllati da un meccanismo di controllo indipendente; consentire l'accesso per gli interessati a misure di ricorso efficaci. Da ciò, appare subito che tali garanzie essenziali costituiscono la trasposizione dei principi fondamentali della *EU rule of law* allo specifico settore della protezione dei dai personali. Quindi, l'EDPB precisava al riguardo: "*le garanzie essenziali europee fanno parte della valutazione da effettuare per stabilire se un paese terzo fornisca un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE, ma non mirano a definire di per sé tutti gli elementi necessari a ritenere che un paese terzo fornisce tale livello di protezione in conformità dell'articolo 45 del RGPD. Analogamente, esse non mirano a definire di per sé tutti gli elementi che potrebbero essere tenuti presenti nel valutare se il regime giuridico di un paese terzo impedisca all'esportatore e all'importatore di dati di assicurare le adeguate garanzie di cui all'articolo 46 del RGPD. Pertanto, gli elementi forniti nel presente documento dovrebbero essere considerati come le garanzie essenziali da individuare in un paese terzo nel valutare l'ingerenza nei diritti al rispetto della vita privata e alla protezione dei dati derivante dalle misure di sorveglianza applicate in tale paese terzo, e non già un elenco di elementi atti a dimostrare che il regime giuridico di un paese*

terzo nel suo insieme fornisce un livello di protezione sostanzialmente equivalente"[428]. E ancora: "*Le quattro garanzie essenziali europee sono da considerarsi elementi fondamentali (…). Esse non dovrebbero essere valutate in modo indipendente, essendo in realtà strettamente interconnesse, bensì complessivamente, esaminando la legislazione pertinente in relazione alle misure di sorveglianza, al livello minimo di garanzie per la protezione dei diritti degli interessati e ai mezzi di ricorso previsti dalla legislazione nazionale del paese terzo. Tali garanzie richiedono un certo grado di interpretazione, soprattutto perché la legislazione del paese terzo non deve necessariamente essere identica al quadro giuridico dell'UE*"[429].

Da queste precisazioni potrebbe intanto dedursi che tali Raccomandazioni vogliano costituire una guida ai soggetti chiamati ad effettuare la valutazione del sistema del Paese terzo, diretta rispettivamente agli operatori privati e alle autorità di controllo (nei casi di garanzie adeguate *ex* art. 46) e alla Commissione (per l'adeguatezza *ex* art. 45). Inoltre, nello spiegarne il contenuto, emerge spesso il riferimento giurisprudenza delle Corti europee, soprattutto più recente, e al riguardo ci interessa rilevare che, per spiegare la seconda garanzia (su necessità e proporzionalità delle misure) l'EDPB faccia esplicito riferimento a *La Qaudrature du Net*, finanche nel passaggio che, come dicevamo, ha destato perplessità quanto a possibili "ammorbidimenti" della Corte rispetto ai meccanismi di sorveglianza degli Stati membri: "*In La Quadrature du Net et al., si può osservare che la CGUE ha stabilito, in relazione al diritto di uno Stato membro e non al diritto di un paese terzo, che l'obiettivo di salvaguardia della sicurezza nazionale è, per la sua importanza, idoneo a giustificare misure che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero essere giustificate da altri obiettivi, come la lotta alla criminalità. Essa ha tuttavia constatato che ciò vale fintantoché ricorrano circostanze sufficientemente concrete tali da consentire di ritenere che lo Stato interessato si trovi dinanzi a una minaccia grave alla sicurezza nazionale, che si dimostri reale e attuale o prevedibile, e a condizione che siano soddisfatti gli altri requisiti di cui all'articolo 52, paragrafo 1, della Carta*"[430]. Veniva poi aggiunto in nota che: "*nella causa La Quadrature du Net et al., la Corte ha rilevato che l'analisi automatizzata dei dati relativi al traffico e all'ubicazione appare come un'ingerenza particolarmente grave in quanto riguarda in modo generalizzato e indifferenziato i dati delle persone che si avvalgono dei mezzi di comunicazione elettronica; una tale misura può soddisfare il requisito di proporzionalità solo in situazioni nelle quali lo Stato membro interessato si trovi di fronte ad una minaccia grave per la*

[428] EDPB, Raccomandazioni 2/2020, *cit.*, parr. 8-9.
[429] Ibidem, parr. 48-49.
[430] Ibidem, par. 34.

sicurezza nazionale che risulti reale e attuale o prevedibile e, in particolare, a condizione che la durata di tale conservazione sia limitata allo stretto necessario (§§ 174-177)"[431].

Ebbene, da quanto riportato potrebbe dedursi che l'EDPB assuma le conclusioni della giurisprudenza e le prospetti per condurre le valutazioni necessarie nei casi di trasferimenti di dati verso Paesi terzi, molto spesso puntualizzandone il riferimento al fatto che i casi giurisprudenziali riportati si riferiscano ai soli Stati membri, e però applicandone i principi anche per la valutazione dei sistemi di Stati terzi. Tutto ciò parrebbe, in realtà, abbastanza in linea con l'orientamento conforme alla *EU rule of law* e al principio di coerenza, che abbiamo esposto.

Eppure, come anticipavamo, sono state sollevate delle criticità rispetto al fatto che, in pratica, tali garanzie essenziali difficilmente potrebbero funzionare, nel senso che difficilmente sistemi di Paesi terzi potrebbero soddisfare quanto richiesto, risultando pertanto inevitabilmente non idonei a fornire un livello di protezione sostanzialmente equivalente, con la necessità dunque di adottare misure supplementari alle garanzie adeguate (di cui si occupano le altre Raccomandazioni 1/2020) e, se non adattabili, di sospendere o vietare i trasferimenti di dati che già si effettuano.

Ci riferiamo alle riflessioni avanzate da Christakis, anzitutto, all'indomani dell'adozione delle Raccomandazioni, laddove rilevava che proprio dall'analisi della giurisprudenza delle Corti europee in materia, e pur riconoscendo che quella di Strasburgo è stata tendenzialmente più permissiva su questioni di sorveglianza rispetto a quella di Lussemburgo, emergerebbe che la maggior parte degli stessi Stati europei non supererebbe il vaglio delle garanzie essenziali: «*In more general terms, the ECtHR, even applying its less strict standards than the CJEU, has found that almost all the surveillance laws of Members of the Council of Europe that have been brought under its scrutiny since 2001 have violated the ECHR. This was the case for Hungary, Russia, Romania (…), Bulgaria, Moldova, Turkey and more recently the UK in the Big Brother Watch case* [il riferimento si legga alla sentenza del 2018, non aggiornato alla Grande Camera] *(…). If one now turns to the CJEU, it is worth recalling that in its October 6, 2020 data retention/collection judgments it found that the laws of France, Belgium and the UK did not meet the European standards either. One can conclude from this first section that surveillance laws rarely survive the scrutiny of European tribunals. If the surveillance laws of European countries themselves most often do not respect the "EEG requirements", how many States around the world could be expected to do so?*»[432]. Queste considerazioni, che denotano come l'autore considerasse da subito le garanzie dell'EDPB particolarmente rigide, si legano poi a quelle dello stesso tenore avanzate, come si accennava,

[431] Ibidem, nota 36 (pag. 10).
[432] T. CHRISTAKIS, "Schrems III"? (Part 1), *cit.*, 13 November 2020.

rispetto ai nuovi negoziati tra UE e USA per una prossima decisione di adeguatezza, che emergerebbero più in generale dai commenti avanzati proprio dagli USA rispetto alle Raccomandazioni dell'EDPB (ancorché a quelle sulle misure supplementari)[433].

Sempre lo stesso autore, infatti, faceva notare come, nel partecipare alle consultazioni pubbliche dell'EDPB, gli Stati Uniti avrebbero palesato di voler lasciare fuori dalle valutazioni sulla sostanziale equivalenza del sistema (e quindi di escludere da una eventuale decisione di adeguatezza) le questioni di sorveglianza internazionale (in particolare, quella condotta dall'intelligence USA al di fuori del territorio e prevista dall'Ordine Esecutivo 12333 emesso nel 1981 ed emendato l'ultima volta nel 2008), a partire da un distinguo tra accesso governativo ai dati indiretto e obbligatorio (che imporrebbe ai fornitori di servizi di comunicazione elettronica di consentire l'accesso ai dati) e quello diretto e non obbligatorio, relativo ai casi in cui il Governo acquisisce i dati direttamente con propri mezzi, senza rivolgersi ai fornitori di servizi), basandosi proprio sulla recente giurisprudenza di Lussemburgo *Privacy International* e *La Quadrature du Net*. Il riferimento sarebbe in particolare al passaggio in cui la Corte chiariva: «*quando gli Stati membri attuano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche, senza imporre obblighi di trattamento ai fornitori di detti servizi di comunicazione, la protezione dei dati delle persone interessate non ricade nell'ambito della direttiva 2002/58, bensì unicamente in quello del diritto nazionale, fatta salva l'applicazione della direttiva (UE) 2016/680 (…) relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (…), di modo che le misure in questione devono rispettare in particolare il diritto nazionale di rango costituzionale e i requisiti della CEDU*»[434].

Ebbene, da qui, la posizione degli USA risulta chiara dal seguente estratto: «*under LQdN no EU legislation governs direct access by Member State authorities to personal data for national security purposes—not the e-Privacy Directive, not GDPR, and not the Law Enforcement Directive. Since EU law provides no privacy protections relating to EU Member State governments' direct access to personal data for national security purposes, a data exporter would have no comparative standard by which to assess whether privacy protections offered by a destination country for the same type of activities are "essentially equivalent" to protections required by EU law. The EDPB should not interpret Schrems II to create a double standard under which non-EU countries' direct access*

[433] US COMMENTS ON PROPOSED EDPB RECOMMENDATIONS 01/2020, 21 December 2020, available here: https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.12.21_-_us_comments_on_edpb_supp_measures_final.pdf .
[434] Corte di giustizia, *La Quadrature du Net*, punto 103.

measures are subject to strict EU data protection rules while comparable Member State direct access measures are not subject to EU law at all. Such an interpretation would be discriminatory and inconsistent with the Court's ruling that appropriate safeguards under Article 46 of the GDPR *"must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter". We recommend that references to governments' "direct access" to data without imposing processing obligations on private entities be removed from the Recommendations. Otherwise, data exporters will be placed in the impossible situation of assessing whether privacy protections relating to foreign direct access measures are "essentially equivalent" to a non-existent EU standard*»[435]. Ebbene, Christakis riconosceva le ragioni dell'insistenza degli USA nell'escludere i casi di accesso diretto ai dati da valutazioni sull'adeguezza, anche se ne riscontrava i limiti, tra i quali condividiamo particolarmente quello derivante dall'interpretazione teleologica del GDPR: «*The exclusion of EO 12333 from the adequacy/essential equivalence equation could thus be helpful for the US in order to reach an agreement with the EU and allow transatlantic data flows. Furthermore, it is difficult for the US to understand why its international surveillance activities would be placed under close scrutiny by the EU, when international surveillance by EU Member States themselves (…) is entirely excluded from the scope of EU law. The feeling that "double standards" are prevailing, and that the EU is intruding, for reasons that can barely be justified, on key US national security activities, haunts US government officials (…). One of the most important objections to the US arguments must be based on a teleological interpretation of Chapter V of the GDPR (…). The entire logic of the GDPR is that European personal data should travel with protection. If European data can be intercepted legally by the US Government while transiting from Europe to the US without any application of European surveillance safeguards, then there is no protection. What is the point of introducing safeguards once the data have already been transmitted to the US (…), if bulk interception of the same data can take place with no European equivalent protection, by accessing the transatlantic cables? (…) the protective mechanism of Chapter V would either mean that the data is not transferred at all or that robust encryption is used in order to protect the data during the transit*»[436].

Queste considerazioni, che qui si sono riportate provocatoriamente per dare un'idea della complessità che la valutazione sull'adeguatezza implica in concreto, forniscono più di uno spunto per dubitare del funzionamento in pratica del principio di coerenza tra l'azione interna ed esterna

[435] Ibidem. pp. 8-9.
[436] T. CHRISTAKIS, Squarin the circle? (Part 1), *cit*., 12 April 2021.

dell'Unione nel settore della protezione dei dati personali. per quanto, infatti, come la Corte ha chiarito nel passaggio suddetto in *La Quadrature du Net*, le misure nazionali di accesso diretto rientrano nell'ambito del diritto nazionale, riferendosi allo stesso e alla CEDU per la protezione dei diritti degli interessanti in tali casi; è vero anche, però, che le perplessità avanzate dagli USA a partire dalla distinzione tra sorveglianza interna e sorveglianza internazionale in termini di "doppio standard" potrebbero trovare rispetto a quelle indicazioni un concreto riscontro, per esempio, nel sistema francese, come ha rilevato Christakis con riguardo alla legge del 2015 sulle misure di sorveglianza delle comunicazioni elettroniche internazionali[437]. L'autore, in particolare, proponeva un'analisi dell'atto legislativo francese alla luce delle garanzie essenziali europee per riscontrare che lo stesso non parrebbe soddisfare le condizioni richieste e dunque concludere: «*A situation where the EU requests that the US complies immediately with all the "European Essential Guarantees for surveillance measures" (as they appear in the EDPB EEG Recommendations), when EU Member State's international surveillance laws do not seem to meet these same safeguards, could only reinforce the US feeling of "double standards" and could hinder the fruitful conclusion of the EU-US negotiations which is absolutely essential for the continuation of transatlantic data transfers*»[438].

Ancora, ulteriori suggestioni al riguardo ci sovvengono, come si anticipava, dalla prospettata adeguatezza nei confronti del Regno Unito, neo Paese terzo. Data l'importanza, prevista dal GDPR, alla continuità di tutela anche nel caso di trasferimenti successivi, le decisioni di adeguatezza della Commissione nei confronti del Regno Unito devono tenere in considerazione anche gli accordi internazionali di quest'ultimo che comportino un trasferimento di dati. Tralasciando il meccanismo di condivisione tra servizi di intelligence UK-USA, che pure, tra le varie perplessità dei più, è stato salvato dalla Corte di Strasburgo (sia sezione che Grande Camera, *Big Brother Watch*), la questione è stata posta in particolare dall'EDPB in sede di parere, favorevole ma condizionato, alle proposte di decisioni di adeguatezza. In particolare, il Comitato avanzava perplessità quanto al noto *Cloud Act Agreement*, ovvero l'accordo tra Regno Unito e USA (basato sul *Cloud Act* adottato da questi ultimi nel 2018) sulla trasmissione delle prove elettroniche, esortando la Commissione a esaminare l'interazione del Regno Unito nei suoi accordi internazionali in linea con il principio di continuità della tutela del GDPR, nonché di monitorare in particolare se quell'accordo assicura adeguate garanzie aggiuntive "*taking into account the level of sensitivity of the categories of data concerned*

[437] LOI no 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, https://www.legifrance.gouv.fr/download/file/ua_habBuhVRZYt1WFbF5Hglgj8aUOv1MZCf1HPdWY3s=/JOE_TEXTE .

[438] T. CHRISTAKIS, Squaring the circle? (Part 2), *cit*., 13 April 2021.

and the sole requirements of the transfer of electronic evidence directly by service providers rather than between authorities, also assessing under which circumstances safeguards may be provided by an appropriate implementation of the adaptation of the EU-US Umbrella Agreement"[439]. Abbiamo poi anche fatto cenno al monito del Parlamento europeo, che con specifico riguardo a questo passaggio dichiarava: «*prende atto dell'accordo di accesso transfrontaliero ai dati tra il Regno Unito e gli Stati Uniti, ai sensi del CLOUD Act statunitense, che facilita i trasferimenti a fini di contrasto; esprime profonda preoccupazione per il fatto che ciò consentirà alle autorità statunitensi di accedere indebitamente ai dati personali dei cittadini e dei residenti dell'UE; condivide la preoccupazione dell'EDPB in merito al fatto che le garanzie previste dall'accordo quadro tra l'Unione europea e gli Stati Uniti, applicate mutatis mutandis, potrebbero non soddisfare i criteri di chiarezza, precisione e accessibilità delle norme per quanto riguarda l'accesso ai dati personali o che detto accordo sancisca tali garanzie in modo insufficiente a renderle efficaci e impugnabili ai sensi del diritto del Regno Unito*»[440] Ebbene, la Commissione, con l'adozione delle decisioni di adeguatezza lo scorso 28 giugno 2021, parrebbe aver preso atto di tali avvertenze e, dopo una disamina delle peculiarità quanto all'ambito di applicazione e degli aspetti da tenere sotto controllo a seguito dell'entrata in vigore dell'accordo USA-UK (non ancora avvenuta), concludeva al riguardo che «*any relevant development as regards the entry into force and application of the Agreement will be duly taken into account in the context of the continuous monitoring of this decision, including with respect to the necessary consequences to be drawn in case of any indication that an essentially equivalent level of protection is no longer ensured*», così impegnandosi a monitorare gli sviluppi, come richiesto al suo ruolo dal GDPR[441].

Tutti questi sviluppi, e le loro possibili prospettive, confluiscono a stimolare i discorsi e le riflessioni sulla sovranità digitale, che ci accingiamo a trarre.

Prima di farlo, un ultimo aspetto relativo alla coerenza merita (anche in continuità con quanto esposto in teoria, *supra*, Capitolo III, Parte III) di essere affrontato nell'analisi del riscontro pratico: il coordinamento tra autorità di controllo, tramite i meccanismi di cooperazione e coerenza, e in particolare il meccanismo di c.d. *sportello unico* per la gestione di trattamenti transfrontalieri.

[439] EDPB, Opinion 14/2021, *cit*., Adopted on 13 April 2021, p. 19, ma si vedano punti 18-20.
[440] Risoluzione del Parlamento europeo del 21 maggio 2021, (2021/2594(RSP)), cit., p. 25.
[441] COMMISSION IMPLEMENTING DECISION of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, para 153.

2. Cooperazione e coerenza tra le autorità di controllo, in pratica

Abbiamo detto che il Capo VII del GPDR (articoli 60-76) è rubricato a cooperazione e, disciplinando gli appositi meccanismi che dovrebbero gestire i rapporti tra autorità di controllo e tra queste ed EDPB nonché Commissione, per un coerente funzionamento dell'architettura istituzionale predisposta dal GDPR a garanzia della protezione dei dati personali. A tal fine, per quanto riguarda i trattamenti transfrontalieri, come abbiamo detto il GDPR ha introdotto la figura della c.d. autorità capofila, descritta all'articolo 56 come quella competente in quanto autorità dello stabilimento principale o unico del titolare del trattamento. La previsione di tale nuova figura introduce, con il GDPR, il c.d. *meccanismo di sportello unico*, pur con eccezioni, per la trattazione di trattamenti transfrontalieri. La norma, invero, nel coordinare le competenze tra questa e le altre autorità di controllo, fa salve le previsioni sulla competenza di cui all'articolo 55 e poi, al par. 6, precisa che "*L'autorità di controllo capofila è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale titolare del trattamento o responsabile del trattamento*"[442].

Orbene, le ultime vicende riportate sugli sviluppi della saga *Schrems*, ma anche la recente proposta del Parlamento di avviare una procedura di infrazione contro l'Irlanda, danno una misura delle difficoltà che la previsione del meccanismo di sportello unico potrebbe comportare quando, come nel caso dell'autorità irlandese (che peraltro, secondo questo meccanismo, sarebbe capofila per diversi titolari), si creerebbero delle situazioni di accumulo di reclami che non vengono trattati con la richiesta speditezza e che, quindi, inficiando la cooperazione e coerenza che dovrebbero sorreggere l'architettura istituzionale del GDPR, si pongono in violazione dello stesso e, al contrario, paiono ostacolare l'obiettivo di una tutela effettiva.

La questione, pur con altri termini, è stata invero di recente affrontata dalla Corte di giustizia nel caso Facebook. Con il rinvio pregiudiziale sollevato dal giudice belga, veniva chiesto alla Corte: se un'autorità di controllo che non fosse quella capofila potesse intentare un'azione dinanzi al giudice del suo Stato membro rispetto alla asserita violazione del Regolamento laddove questa avvenga nell'ambito di un trattamento transfrontaliero; se tale eventualità richieda che il titolare abbia il proprio stabilimento principale nel territorio del suo Stato membro, oppure anche altro stabilimento; se, nel caso in cui tale autorità potesse agire, dovesse farlo nei confronti dello stabilimento principale del titolare ovvero contro lo stabilimento che si trova nel proprio Stato membro; se,

[442] GDPR, Articolo 56 – *Competenza dell'autorità di controllo capofila*.

considerando che l'azione era stata esperita prima dell'entrata in vigore del GDPR (e dunque dell'istituzione dello sportello unico) tale eventualità potesse influire sulle condizioni di esercizio per l'autorità del suo potere di agire in sede giurisdizionale; se l'articolo 58, par. 5 (che prevede il potere dell'autorità di agire in giudizio) abbia effetto diretto; se, in caso affermativo, l'esito di un procedimento giudiziario così intentato possa ostare a una decisione dell'autorità capofila che possa giungere alla soluzione contraria (dichiarata irricevibile).

La sentenza della Corte, da alcuni definita "equilibrata"[443], da altri considerata in linea con l'orientamento, che qui stiamo sindacando, volto a forzare le maglie dell'integrazione europea per tramite del diritto europeo alla protezione dei dati personali[444], assume rilievo sotto diversi profili, quanto alla nozione di stabilimento, al ruolo delle autorità, alle loro competenze e all'importanza della loro cooperazione. Per quel che ci interessa, la Corte sin da subito pone l'accento sulla necessaria cooperazione tra le autorità per l'effettivo funzionamento dello sportello unico: «*da un lato, in materia di trattamento transfrontaliero di dati personali, la competenza dell'autorità di controllo capofila ad adottare una decisione che constati che un siffatto trattamento viola le norme relative alla tutela dei diritti delle persone fisiche con riguardo al trattamento di dati personali contenute nel regolamento 2016/679 costituisce la regola, mentre la competenza delle altre autorità di controllo interessate ad adottare una tale decisione, anche in via provvisoria, costituisce l'eccezione. D'altro lato, pur se la competenza di principio dell'autorità di controllo capofila è confermata all'articolo 56, paragrafo 6, del regolamento 2016/679 (...), tale autorità deve esercitare siffatta competenza nell'ambito di una stretta cooperazione con le altre autorità di controllo interessate. In particolare, l'autorità di controllo capofila non può sottrarsi, nell'esercizio delle sue competenze (...), a un dialogo indispensabile nonché a una cooperazione leale ed efficace con le altre autorità di controllo interessate. A tal riguardo, dal considerando 10 del regolamento 2016/679 risulta che quest'ultimo mira, in particolare, a garantire un'applicazione coerente ed omogenea delle norme in materia di protezione delle libertà e dei diritti fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione e a rimuovere gli ostacoli ai flussi di dati personali all'interno di quest'ultima. Orbene, siffatto obiettivo e l'effetto utile del meccanismo dello «sportello unico», potrebbero essere compromessi se un'autorità di controllo, che, riguardo a un trattamento di dati transfrontaliero, non è l'autorità di controllo capofila, potesse esercitare il potere previsto all'articolo 58, paragrafo*

[443] Cfr. L. WOODS, Who has jurisdiction over Facebook Ireland? The CJEU rules on the GDPR 'one stop shop', in *EU Law Analysis*, 16 June 2021.
[444] Così M. GÖMANN, A Hidden Revolution, in *Verfassungsblog*, 17 June 2021, che apriva la sua analisi rilevando: «*its revolutionary aspects do however not catch the eye, but lie in the consequences of what may at first glance appear as a rather technical ruling*.».

5, del regolamento 2016/679 al di fuori dei casi in cui essa è competente ad adottare una decisione come quella di cui al punto 63 della presente sentenza. Infatti, l'esercizio di un potere siffatto mira a giungere ad una decisione giurisdizionale vincolante, la quale è altrettanto idonea a pregiudicare detto obiettivo nonché detto meccanismo quanto una decisione adottata da un'autorità di controllo che non è l'autorità di controllo capofila»[445]. Sulle altre questioni, di interpretazione dell'articolo 58, par. 5, la Corte essenzialmente ha stabilito che l'esercizio del potere dell'autorità di controllo non capofila di intentare un'azione giudiziaria non esige che il titolare del trattamento disponga di uno stabilimento nel suo Stato membro; può essere effettuato nei confronti di qualsiasi stabilimento, purché l'azione riguardi un trattamento effettuato nell'ambito dell'attività di detto stabilimento e purché l'autorità sia competente ad esercitare tale potere; che la norma ha effetto diretto e che dunque ogni autorità può invocarla rispetto ai privati anche se mancano specifiche disposizioni interne di attuazione[446].

Dunque, dall'estratto riportato pare palese l'orientamento della Corte che, attento a fornire un'interpretazione che lega il dato letterale delle norme del GDPR allo spirito che ne permea l'intera costruzione, non pare invero avere una portata rivoluzionaria, ma assume un certo peso laddove insiste sulla necessità di salvaguardare il meccanismo dello sportello unico – anche laddove i dati fattuali potrebbero far protendere per un ridimensionamento – soprattutto perché lo considera in linea con la *coerenza* che deve guidare la gestione delle relazioni tra le autorità di controllo e, dunque, sostenere l'intero sistema istituzionale di protezione dei dati. Tuttavia, se delle perplessità possono sorgere, dalla soluzione delle altre questioni, quanto alla "imprevedibilità" derivante per i titolari del trattamento rispetto alle possibilità delle autorità di intentare azioni giudiziarie[447], secondo le modalità derivanti dall'interpretazione data all'articolo 58, par. 5 dalla Corte, vi è chi ha ritenuto questa pronuncia manchevole laddove non tratterebbe "l'elemento chiave per un'applicazione coerente della normativa": « *By not addressing which national adaptation law is to be applied to a certain processing operation and, thus, enforced by the competent DPA, the ECJ in its most recent decision ignores the key element for a coherent and consistent application of data protection law under the GDPR. This is especially regrettable given that the Court appears*

[445] Corte di giustizia, C-645/19, *Facebook Ireland Limited*, 15 giugno 2021, punti 63-65 (ma si vedano anche i punti 52, 53, 60), sottolineato aggiunto.
[446] Ibidem, punti 84, 96, 105, 113.
[447] Così ritiene infatti L. WOODS, Who has jurisdiction over Facebook Ireland?, cit.: «*What is potentially problematic from the perspective of the data controller is the greater unpredictability of the data protection regime. This may be less about fragmenting standards (especially if the decision is referred to the EDPB) but about where enforcement actions may start; this agenda may not rest entirely in the hands of the lead authority*».

particularly concerned to ensure a sufficient intra-European connection between the processing operation at stake and the data protection authority (subsidiarily) competent for its supervision»[448].

Insomma, una questione che si aggiunge ulteriormente a far riflettere sull'esigenza di coerenza (in teoria), nell'impianto del GDPR ma anche nella più ampia risonanza che esso assume, e sulle effettive difficoltà della sua concreta applicazione (in pratica), che pure, come le considerazioni precedenti, concorre ad arricchire più ampie valutazioni relative al nesso tra *EU rule of law* e protezione dei dati personali per condurci, finalmente, a tirare le somme sulla decantata tendenza verso una sovranità digitale dell'Unione europea.

[448] M. GÖMANN, A Hidden Revolution, cit.

CAPITOLO IV

EU RULE OF LAW E PROTEZIONE DEI DATI PERSONALI *IN FIERI*: PROSPETTIVE DELLA SOVRANITÀ DIGITALE DI UN ORDINAMENTO AUTONOMO

1. Sovranità e legittimazione

Conclusa questa densa parte di analisi, abbiamo finalmente a disposizione tutti gli elementi necessari per suggerire una possibile soluzione alla domanda di ricerca, ossia quella con cui vogliamo indagare se la tendenza dell'Unione verso una sovranità digitale possa costituire un (valido) tentativo per superare le crisi di legittimazione che la destabilizzano.

A tal fine, riteniamo utile tirare le fila proprio dagli iniziali discorsi teorici sulla natura dell'Unione, sulle teorie dell'integrazione europea e sulle relazioni con gli Stati membri in termini di "sovranità condivisa e potere da separare". Quei discorsi, si ricorderà, ci hanno condotto a riconoscere l'Unione come un *ordinamento giuridico autonomo*, singolare nel presentare elementi tanto di normativismo quanto di istituzionalismo, e dotato di peculiarità che lo rendono *sui generis* nel panorama internazionale, fondato su un sistema proprio di valori comuni agli Stati membri e che trova, in ultima analisi, nel *diritto* il proprio *potere*, che ne modella l'architettura interna e ne permette l'affermazione all'esterno, alla cui conformità rispondono tanto gli Stati membri quanto le istituzioni, mediante un meccanismo di controllo che è costruito sull'intreccio tra sistemi giurisdizionali nazionali e sovranazionale che garantisce così rimedi effettivi ai cittadini: elementi, tutti, che caratterizzano ciò che abbiamo chiamato *EU rule of law*.

Se è vero, infatti, che «*the term "sovereignty" (let alone a digital one) appears nowhere in the EU constitutive treaties*»[449], cosa che, in qualche modo, ribadisce il c.d. modello di *integrazione senza*

[449] T CHRISTAKIS, 'European Digital Sovereignty': Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy', *Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute*, e-book, December 2020, p. 9, in cui invero l'autore ritiene l'esatto opposto di quanto noi proponiamo per affrontare la sovranità digitale dell'Unione: «*The very fact that the EU speaks about "sovereignty" is rather puzzling. Without re-opening the debate about the legal nature of the EU, the different theories of integration, federalism and "division of sovereignty", or the important transfers of powers from the sovereign member states to the EU, it will be enough to highlight that the term "sovereignty" (let alone a digital one) appears nowhere in the EU constitutive treaties*». La scelta da noi proposta spiega le differenti premesse e le differenti conclusioni.

sovranità [450], è vero anche, però, che, da quanto abbiamo esposto, non parrebbe così improbabile ravvisare qualche elemento di "sovranità", o almeno di tendenza alla stessa, dell'Unione europea, che troverebbe infatti conferma nell'attuale discussione sulla sovranità digitale. Ci riferiamo, in particolare, ad alcuni elementi distintivi che emergono da quell'analisi generale e che sembrerebbero ritornare nella dimensione digitale. Ne riprendiamo brevemente alcuni, mentre altri emergeranno più chiaramente con riferimento a quella specifica dimensione.

Anzitutto, tra le esposte teorie dell'integrazione europea, l'analisi condotta sull'evoluzione della protezione dei dati personali e sui suoi recenti sviluppi ci consentirebbe di riscontrare nel momento attuale dell'evoluzione del processo di integrazione alcuni elementi propri del *costruttivismo,* nonché del *governance approach*, e del *post-funzionalismo*.

Nella misura in cui, infatti, il costruttivismo (calato all'integrazione europea, ma radicato nelle concezioni di teoria delle relazioni internazionali) insisteva sull'influenza delle istituzioni europee nel modellare preferenze e attitudini degli Stati membri e dei cittadini, rilevando l'impatto trasformativo del costrutto europeo rispetto ai sistemi domestici, esso spiegherebbe i risultati derivati dalla previsione di un apposito apparato istituzionale per la protezione dei dati personali, con le autorità nazionali di controllo quali attori di spicco del contesto *sovra*nazionale, specie per come coordinati dal EDPB, nonché con la centralità riconosciuta alla Commissione.

Ma ritornano anche le valutazioni di *governance approach*, per esempio quanto alle criticità emerse dalla giurisprudenza sui casi relativi alla sicurezza nazionale oppure rispetto alla conclusione di accordi internazionali, che giustificherebbero nel settore di riferimento le perplessità avanzate da quell'approccio rispetto al fatto che l'Unione affronterebbe solo tangenzialmente alcuni settori politici che sono invece cruciali a livello nazionale per legittimare i governi. Inoltre, l'analisi sulla *governance* ha il particolare pregio di mettere in risalto un aspetto molto rilevante nella protezione dei dati personali, ossia quello delle dimensioni *trasformative* della governance europea, dalle quali emergerebbe lo "stile normativo dominante" che insisterebbe sull'uso del diritto a livello sovranazionale come strumento fondamentale per guidare le economie e le società degli Stati membri. Questo, peraltro, avrebbe un particolare riscontro anche rispetto all'influenza unilaterale *esterna* operata dall'Unione nella protezione dei dati personali, trovando ivi piena applicazione il c.d. *normative/regulatory power Europe*, consistente nella capacità persuasiva che l'Unione eserciterebbe nella sua azione verso l'esterno e che ne paleserebbe la "differenza normativa" nel contesto internazionale, data dalle sue "norme costituzionali", dal suo sistema di valori, che così ne definirebbe all'esterno l'identità. L'analisi sulle dinamiche relative ai trasferimenti di dati personali

[450] Cfr. E. CANNIZZARO, *La sovranità oltre lo Stato*, cit., p. 89.

verso Paesi terzi, pur con le prospettate contraddittorietà, risulta particolarmente dimostrativa di questo aspetto.

Infine, un altro ausilio che ci deriva dalle teorie dell'integrazione europea, per rintracciare la tendenza dell'Unione verso una sovranità digitale come fonte di legittimazione, è quello dato dal *post-funzionalismo*, precisamente laddove (riprendendo il *neofunzionalismo*) quella teoria rilevava l'*interdipendenza* come tipica della governance multilivello (senza approfondire sulle discrepanze che riscontrava al riguardo). Ebbene, la caratteristica dell'interdipendenza, così come è chiaramente connaturata all'architettura interna del costrutto europeo, costituisce anche, come abbiamo visto, elemento centrale nella spiegazione delle dinamiche internazionali tra Stati (soprattutto in un contesto globalizzato) proposta nella teoria delle relazioni internazionali dal *liberalismo*, e che rimanda quindi inevitabilmente alle valutazioni sul rapporto tra sovranità e diritto internazionale.

Infatti, ricordiamo di aver detto che l'*interdipendenza* comporterebbe un ridimensionamento del concetto classico di sovranità (implicante, nella sua dimensione esterna, proprio l'*indipendenza* reciproca degli Stati) e connoterebbe, invero, la fase c.d. *post-westfaliana* delle relazioni tra Stati e soggetti di diritto internazionale[451]. In quest'ordine di considerazioni, ne derivava un aspetto che qui vogliamo particolarmente enfatizzare, ossia, com'è ben noto, che l'emersione della sensibilità verso la tutela dei diritti umani sarebbe correlata proprio allo sviluppo dell'interdipendenza globale[452].

Ciò potrebbe indurre a considerare la sovranità come quasi contrapposta alla tutela dei diritti, e invece l'attuale contesto globale, in cui la "rinnovata" concezione di sovranità si caratterizza proprio per l'interdipendenza tra "sovrani", ci dimostra che è proprio all'opposto. Infatti, in questa rinnovata concezione, la sovranità, ormai lontana dalla hobbesiana concezione di autorità assoluta, non coinciderebbe neppure con la schmittiana identificazione di chi decide sullo stato di eccezione, ma piuttosto parrebbe, nell'attuale contesto di interdipendenza internazionale, compenetrata alla tutela dei diritti: potremmo dire in questo senso, con qualche azzardo e pur consapevoli della complessità e dell'ampiezza della questione che esula dal presente lavoro, che, con riferimento allo specifico profilo qui trattato, *è sovrano chi garantisce la tutela dei diritti*.

---

[451] N. WALKER, *Late Sovereignty in the European Union*, in N. WELKER (ed.), *Sovereignty in transition – essays in European law*, Hart Publishing, 2003, p. 19 ss.

[452] In particolare, si ricorderà che per spiegare l'interdipendenza postwesfaliana (cfr., Capitolo II, Parte I), riprendevamo il padre del *funzionalismo*, Mitrany, che, nell'analisi proposta da De Wilde, la riteneva causa di due contrastanti sviluppi, ossia la sempre maggiore unificazione economica contro la crescente frammentazione politica; quindi, riportavamo le valutazioni di De Wilde laddove tracciava un legame tra quelle premesse e sviluppi più recenti, che ci sembrano infatti proprio calzanti per spiegare le dinamiche che accompagnano la tendenza verso la sovranità digitale, che stiamo perciò riproponendo: «the development from cosmopolitism via state sovereignty and national sovereignty to human rights closely relates to the development towards global interdependence», cfr. J. DE WILDE, *Saved from oblivion: interdependence theory in the first half of the 20th Century – A study on the causality between war and complex interdependence*, Dartmouth, 1991*p. cit.*, pp. 193-194.

Allora, se assumiamo questa "rinnovata" concezione della sovranità (legata alle garanzie di tutela dei diritti), si capisce quanto queste considerazioni siano in linea con l'intera analisi condotta su *EU rule of law* e protezione dei dati personali: da essa rileva, infatti, non solo l'importanza dell'interdipendenza nelle dinamiche attuali, specie in considerazione degli sviluppi dell'Unione in termini di sovranità digitale; ma, soprattutto, da essa emergerebbe come tale rinnovata considerazione della sovranità nel contesto internazionale più valere per l'Unione europea come fonte di legittimazione nella dimensione digitale. Ciò, in particolare, risulta chiaro adottando quella specifica "caratterizzazione funzionalista della sovranità" che infatti vogliamo qui sposare: una sovranità intesa «come *legittimazione sul piano giuridico di una effettività che fonda se stessa*»[453] . Da qui, l'importanza di queste premesse per tentare una plausibile soluzione alla controversa questione della sovranità digitale, come declinata in termini di (possibile soluzione a) crisi di legittimazione.

Intesa in questo senso, ossia di sovranità come *veicolo* per acquisire legittimazione, la tendenza alla sovranità digitale dell'Unione europea consentirebbe a quest'ultima di (auto)legittimarsi in virtù di questo particolare tipo di legittimazione[454], ossia una legittimazione fondata sulla *effettività* del proprio operato e, soprattutto, della *tutela* garantita dal proprio ordinamento giuridico, che ne costituirebbe, proprio nella dimensione digitale, l'elemento distintivo, specie rispetto agli altri attori (pubblici e privati) ivi operanti.

Per comprendere meglio questi passaggi e pervenire alle conseguenti conclusioni, è necessario risolvere tre aspetti:

- anzitutto, cosa intendiamo per "sovranità digitale" rispetto all'Unione europea;
- quindi, se e in che misura, dall'analisi prospettata, possiamo già riscontrare indizi di sovranità digitale dell'Unione europea;
- infine, perché, laddove riscontrati, questi indizi o tentativi dovrebbero spiegare (o frenare) una possibile soluzione alla crisi di legittimazione dell'Unione.

[453] Ricordiamo che la caratterizzazione funzionalista della sovranità veniva prospettata da Quaglioni rispetto all'affermazione dello Stato moderno, cfr. D. QUAGLIONI, *La sovranità*, Laterza, 2004, p. 14.

[454] E non già, invece, in virtù di uno dei tre tipi di legittimazione che, come abbiamo esposto (*supra*, Capitolo II, Parte I), Weiler proponeva per spiegare l'evoluzione del processo di integrazione europea e rispetto alle quali, però, riscontrava gli esiti fallimentari. Il riferimento è a: *input legitimacy*, *output legitimacy*, *political messianism*. Cfr. J.H.H. WEILER, In the face of crisis: Input Legitimacy, Output Legitimacy and the Political Messianism of European Integration, in *Journal of European Integration*, 34:7, 2012.

2. Tre aspetti da chiarire

Definire la sovranità digitale dell'Unione europea

Come abbiamo avuto modo di esporre all'inizio del lavoro, sono davvero molto recenti i tentativi di definizione, non del tutto univoci, della formula "sovranità digitale", alla quale il mondo accademico pare ora prestare attenzione, e che è stata, ed è ancora sempre più, utilizzata soprattutto a livello politico (e finanche mediatico) specie da ultimo nel novero delle iniziative della Commissione per il Futuro Digitale dell'Unione europea. Ebbene, quelle definizioni sono funzionali al nostro discorso, perché ci consentono di rintracciare dei profili comuni, che potrebbero trovare riscontro nell'analisi qui condotta, a partire dai quali proporre un nostro significato di sovranità digitale dell'Unione europea e, per questa via, la sua pertinenza rispetto a questioni di legittimazione dell'Unione.

Da quelle suggestioni, ricaviamo anzitutto che l'ambizione alla sovranità digitale, nell'era della rivoluzione tecnologica, sarebbe ravvisabile non solo nei soggetti "classicamente" sovrani, ossia gli Stati, ma anche enti e organizzazioni e finanche privati, in quello che viene inteso come un "*nuovo spazio in cui le regole restano ancora da definire*" [455], e in cui, dunque, risulta comprensibilmente singolare l'intervento regolativo dell'Unione europea: un *normative/regulatory power* esercitato nella dimensione digitale, tanto indispensabile, per gli Stati membri (al fine di gestire la nuova realtà) e per i cittadini (al fine di ivi ottenere una tutela effettiva), quanto funzionale alla stessa Unione per trovare, così, possibili elementi di legittimazione.

Inoltre, tale ambizione celerebbe anche la necessità di mantenere un *controllo* sulle società e sugli effetti che su di esse produce l'evoluzione tecnologica, che potrebbe aversi solo sopperendo all'asserita mancanza di indipendenza dell'Unione in termini di servizi e infrastrutture digitali, per cui si è parlato di "sovranità strategica", al fine di difendere i propri cittadini nella nuova era di competizione geopolitica[456]. In questo senso, diversi insistono sulla necessità, proprio in vista delle

[455] F. GUEHAM, Digital Sovereignty – Steps towards a new system of Internet Governance, *Fondation pour l'innovation politique*, January 2017, pp. 9 e 11: «*The quest for digital sovereignty is therefore a goal shared by companies, public authority stakeholders and, more recently, Internet users, citizens and consumers (…). The balance of power between governments, citizens, companies and consumers is forging a new Internet of sovereignties, a new space whose rules remain to be defined*».

[456] Così C. HOBBS (Ed.), Europe's Digital Sovereignty: from rulemaker to superpower in the afe of US-China rivalry, in European Council on Foreign Relations – Essay Collection, July 2020, in cui veniva data la seguente definizione di "*strategic sovereignty*": «*Strategic sovereignty implies that the EU and its member states need to preserve for themselves the capacity to act in the world, even as they remain deeply interdependent*», p. 7.

Insiste su questi aspetti anche E. CELESTE, Digital Sovereignty in the EU: Challenges and Future Perspectives, in F. FABBRINI, E. CELESTE, J. QUINN (Eds), *Data Protection Beyond Borders: Transatlantic Perspectives on*

recenti *spinte esterne* che (ancora e di nuovo) modellano il processo di integrazione europea nel suo *moto perpetuo*[457], che l'Unione acquisisca una "autonomia strategica" per essere capace di gestire le nuove dinamiche geopolitiche al fine di proteggere i propri cittadini nel contesto digitale.

Quindi, da queste esigenze di regolazione e controllo emergerebbe un intento più profondo dell'Unione, ossia quello di *preservare i propri valori fondanti*, specie in termini di democrazia e diritti umani, che la rivoluzione tecnologica potrebbe mettere a repentaglio[458]. Quest'ultimo passaggio ben si sposa, in effetti, con la nostra insistenza sul nesso tra *EU rule of law* (e complessivo sistema di valori dell'Unione), da un lato, e protezione dei dati personali, dall'altro. Ad avallare questo ordine di considerazioni, dai recenti interventi delle istituzioni europee, che pure hanno evidenziato la necessità di potenziare il profilo di autonomia strategica[459], emerge sempre più chiaramente l'attitudine verso un "approccio antropocentrico" nel promuovere il modello europeo nella dimensione digitale[460].

Dunque, sarebbero due i profili che connoterebbero la definizione di "sovranità digitale" dell'Unione europea: quello relativo al suo *potere regolatorio* nella dimensione digitale, e quello tendente a raggiungere un'*autonomia strategica* in quella dimensione[461]. Entrambi questi profili

---

Extraterritoriality and Sovereignty, Oxford: Hart Publishing, 2020, pp. 217-218: «*the market for digital products and services is dominated by American and Chinese multinational corporations. Multiple risks are identified in the European inability to fully control its data and digital infrastructures. Regaining sovereignty of its portion of the digital ecosystem is seen in the EU as a potential solution to preserve its unique DNA of rights and values*».

[457] F. G. BURWELL, K. PROPP, The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?, *Atlantic Council – Issue Brief*, June 2020, p. 3: «*The current European focus on digital sovereignty has its roots in a much broader discussion about Europe's ability to protect its citizens from an increasingly hostile and challenging world. The financial crisis of 2009–2012, followed by Russian aggression in Ukraine in 2015 and the migration crisis later that same year, led to an awareness of the deterioration in the European Union's external circumstances. The return of geopolitics prompted a review of Europe's strategic position and, at least within EU institutions, gave rise to a belief that Europe should seek greater "strategic autonomy," strengthening its capacity to act externally on its own, especially in the defense realm*».

[458] E. CELESTE, op. cit., p. 220: «*By invoking control over personal data and digital infrastructures, the EU is seeking to maintain its fundamental values of respect for democracy and human rights unaltered in the face of the challenges of the global digital society*».

[459] Cfr. T. BRETON, European Commission, Europe: Keys to sovereignty, presse release, 11.09.2020, available here: https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en .

[460] European Council, Special meeting – 1 and 2 October 2020, Conclusions, EUCO 13/20, par. 7: « *To be digitally sovereign, the EU must build a truly digital single market, reinforce its ability to define its own rules, to make autonomous technological choices, and to develop and deploy strategic digital capacities and infrastructure. At the international level, the EU will leverage its tools and regulatory powers to help shape global rules and standards. (…) Digital development must safeguard our values, fundamental rights and security, and be socially balanced. Such a human-centred approach will increase the attractiveness of the European model*», available here: https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf .

Si veda soprattutto, ancor più di recente, la Comunicazione della Commissione al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, 9 marzo 2021, COM/2021/118 final: «*la nostra ambizione dichiarata è più che mai pertinente: perseguire politiche per il digitale che conferiscano ai cittadini e alle imprese l'autonomia e la responsabilità necessarie per conseguire un futuro digitale antropocentrico, sostenibile e più prospero (…). Così facendo l'Europa potrà conseguire la sovranità digitale (…)*».

[461] Invero, così vengono suggeriti proprio da T CHRISTAKIS, 'European Digital Sovereignty': Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy', *Multidisciplinary Institute on Artificial*

parrebbero confluire, in ultima analisi, nel medesimo approccio che l'Unione sta utilizzando per promuovere il proprio modello nella dimensione digitale, ossia quello che mette *al centro l'essere umano* e i valori fondanti di quel sistema, che accomunano le tradizioni costituzionali degli Stati membri.

Così intesa la tendenza alla sovranità digitale dell'Unione europea, vediamo, dunque, se e in che misura è possibile reperirne riscontri nella prassi e nella giurisprudenza analizzata.

Indizi di sovranità digitale dell'Unione europea: punti di forza, punti deboli e prospettive

Dall'analisi compiuta nel corso di questo lavoro è possibile ravvisare più un elemento che faccia ritenere che l'Unione europea sia già, in parte, dotata di una qualche sovranità digitale.

Intanto, abbiamo potuto constatare varie attuazioni del c.d. *Brussels effect*: l'influenza del GDPR come modello emulato da Stati terzi, sia per esigenze stimolate dalle multinazionali aventi sede principale in quegli Stati ma operanti nel mercato dell'Unione, sia per ambire a future decisioni di adeguatezza della Commissione, sia, più in generale, per individuare i criteri in base ai quali uno Stato terzo può considerarsi dotato di un sistema di garanzie sostanzialmente equivalente a quello europeo.

Ancora, ulteriori elementi confermano espressioni di sovranità digitale: la capacità della Corte di giustizia di influenzare, con il proprio operato, direttamente gli Stati membri e le istituzioni europee e, così, indirettamente le multinazionali straniere, ma anche gli operatori privati più modesti, e gli Stati terzi, in uno con la contaminazione – non sempre al rialzo – con la giurisprudenza di Strasburgo, indicativa anche del c.d. *Strasburg effect* riscontrabile (aldilà del merito) nelle recenti pronunce sui casi relativi ai sistemi di sorveglianza in Europa; la portata *extraterritoriale* del diritto alla protezione dei dati personali, riscontrabile nei casi sul diritto all'oblio come su quelli relativi ai trasferimenti verso Paesi terzi, che, oltre a testimoniare l'influenza dell'Unione verso l'esterno, confermerebbe anche l'*effettività* della tutela (pur con le remore che si sono esposte rispetto al caso *Google c. CNIL*) dei diritti garantiti dall'ordinamento sovranazionale, ovunque questi siano attaccati; il funzionamento dell'apparato costituito dalle autorità di controllo, specie nel rilievo ultimamente ad esse riconosciuto dalla Corte di giustizia quanto all'enfasi del loro intervento anche rispetto ai trasferimento verso Paesi terzi, meccanismo il cui funzionamento, pur con le perplessità

Intelligence/Grenoble Alpes Data Institute, e-book, December 2020, *Executive Summary – i*: «*sovereignty as regulatory power; and, sovereignty as strategic autonomy and the ability to act in the digital sphere without being restricted to an undesired extent by external dependencies*».

che sta presentando in pratica, parrebbe essere incoraggiato dall'ultima pronuncia sul caso *Facebook*; il sempre più scrupoloso intervento dell'EDPB, ad ausilio di operatori privati e non solo, per un'implementazione quanto più coerente ed efficace delle previsioni sulla protezione dei dati personali. Tutti interventi che, in qualche modo, trovano massima espressione nella saga *Schrems* e nei suoi ulteriori sviluppi (ci riferiamo alle vicende relative all'autorità garante irlandese), e che più in generale, come abbiamo dimostrato, hanno un notevole impatto performativo verso l'esterno.

Ma ancora, tra gli interventi delle varie istituzioni univocamente rivolte alla sovranità digitale dell'Unione (pur, invero, con le diverse prospettive che si sono evidenziate, per esempio, tra Parlamento e Commissione), la chiara presa di posizione della nuova Commissione con la prospettazione, tra le priorità dell'Agenda, di *Plasmare il Futuro Digitale dell'Europa,* con importanti interventi riformatori verso un sempre maggiore incremento del Mercato Unico Digitale, attraverso l'adozione di Comunicazioni e soprattutto di Proposte legislative parecchio significative in tal senso. Tra tutte, ricordiamo da ultimo il proposto *Data Governance Act,* espressivo della sensibilità della Commissione di creare "*un nuovo modo europeo di governance dei dati*" per facilitarne la condivisione e rafforzare la fiducia tra gli intermediari.

Se tutti questi esempi possono dirsi già, pacificamente, sintomatici di una sovranità digitale dell'Unione, uno degli ambiti in cui si avrebbero perplessità, sempre seguendo l'analisi condotta, è quello della cooperazione internazionale. Abbiamo detto che nel settore della protezione dei dati personali la cooperazione internazionale si esplicherebbe nella promozione di standard elevati di tutela a livello globale, attraverso la collaborazione con i vari attori coinvolti. Abbiamo anche visto, però, le difficoltà che si pongono per la conclusione di accordi con Stati terzi che riescano a soddisfare gli interessi, anche di commercio internazionale, che imporrebbero il trasferimento dei dati e le garanzie di protezione fissate dagli standard propriamente europei. Difficoltà che si palesano in un atteggiamento non sempre univoco tra le istituzioni sovranazionali, con una Corte di giustizia (avallata dal Parlamento) che cerca di essere coerente ai valori dell'Unione e, dall'altro lato, una Commissione che a fatica gestisce le dinamiche di compromesso con le controparti internazionali. Da qui, chiaramente, emergerebbe che, se l'Unione può già vedere dei risultati nell'esercizio del suo *regulatory power*, ciò che stenta a realizzarsi, e rende, dunque, ancora incompiuta la tendenza verso la sovranità digitale, è il profilo di *strategic autonomy*.

E ciò, in qualche modo, si ripercuote anche nelle dinamiche interne, per poi palesarsi in quelle esterne. Dal punto di vista interno, l'analisi giurisprudenziale ha fatto emergere che i limiti dell'intervento dell'Unione nel settore riguardano proprio i casi di sicurezza nazionale, ossia quelli in cui le prerogative sovrane degli Stati membri si rendono particolarmente ostative di una compiuta

attuazione pratica del nesso tra *EU rule of law* e protezione dei dati personali. Invero, anche rispetto ai casi di trasferimenti di dati fuori dall'Unione, sono sempre le questioni di sicurezza nazionale a porre difficoltà e, dunque, i casi di più genuina espressione della sovranità nazionale anche degli Stati terzi, che pongono freni a una sovranità, ancorché digitale, dell'Unione europea.

Una riprova ulteriore di tali ostacoli derivanti da prerogative sovrane statali emergerebbe da due questioni rilevanti nel digitale, che ci limitiamo qui a citare: quella della risposta alle preoccupazioni del 5G; quella dell'imposta sui servizi digitali[462].

Inoltre, le questioni legate alla sicurezza nazionale, in uno con gli aspetti di cooperazione internazionale, fanno sorgere perplessità anche quanto alle vicende legate, come abbiamo accennato, al peculiare caso del Regno Unito. Se è comprensibile che le decisioni di adeguatezza della Commissione nei suoi confronti siano arrivate in tempi rapidi perché si trattava di uno Stato membro sino a ieri, che dunque condivideva i valori e gli standard propri dell'Unione, è anche vero che già prima della Brexit quel sistema presentava perplessità, sia rispetto al sistema di sicurezza interna, più volte denunciato, come i casi a Strasburgo e Lussemburgo dimostrano, e sia rispetto a quello di sicurezza internazionale e alle conseguenti collaborazioni implicanti scambi di dati con Paesi terzi, quali gli USA (il caso *Big Brother Watch*, ben oltre gli esiti della sentenza, fa proprio emergere i punti deboli di quel sistema). L'episodio fa riflettere in termini di coerenza del sistema europeo di protezione dei dati personali, laddove questo, tra imposizioni normative, statuizioni giurisprudenziali e raccomandazioni dell'EDPB, potrebbe apparire in sostanza più rigido nei confronti di sistemi di sorveglianza di Paesi terzi, facendo dubitare che le sue finalità non siano esclusivamente legate all'effettiva esigenza di tutela dei diritti fondamentali degli interessati e che potrebbero forse invece sottacere strategiche dinamiche geopolitiche. Situazioni del genere, piuttosto che palesare un'abilità dell'Unione nel gestire situazioni delicate che tali dinamiche implicherebbero, denoterebbero una qualche debolezza e instabilità dell'Unione espressiva di una sovranità digitale ancora incompiuta.

Un'ulteriore vicenda che ha fatto emergere perplessità in termini di sovranità digitale sia sul versante interno che esterno, palesando la carenza di *strategic autonomy*, sarebbe proprio la pandemia da Covid-19. Dal punto di vista interno, infatti, gli interventi sovranazionali hanno puntato a un coordinamento dell'azione degli Stati membri che non avrebbe goduto a pieno di

[462] Per l'approfondimento di entrambe, proprio nell'ottica delle prerogative sovrane statali, si rinvia a T. CHRISTAKIS, 'European Digital Sovereignty', *cit*., che al riguardo dispone: «*it remains to be seen how far the EU is ready to go on exercising regulatory influence on the 5G issue and, indeed, on other issues related to national security considerations. (…) in other important areas affecting important Member State "sovereign functions", internal infighting has torpedoed the regulatory efforts of the EU*», pp. 27-28.

effettiva risposta. Ci riferiamo sempre a questioni che relative a misure statali di sorveglianza, in particolare relative all'uso di tecnologie per monitorare e cercare di gestire la diffusione del virus.

L'adozione di tali misure da parte degli Stati membri comporta l'applicazione della normativa sovranazionale, in particolare del GDPR per certi aspetti e della direttiva *e-privacy* per altri. Ebbene, i casi che destano perplessità in termini di bilanciamento con i diritti fondamentali sono proprio quelli relativi alle misure di geolocalizzazione che, al pari di quelle della casistica analizzata, sono assunte per esigenze di sicurezza, rientrando così nelle deroghe dell'articolo 15 della direttiva *e-privacy*. Rispetto alla possibilità di utilizzare tali tecniche invasive, ma necessarie, dalla primavera del 2020 diversi interventi dell'EDPB[463] e della Commissione[464] hanno cercato di indirizzare gli Stati membri per ribadire la necessità di accompagnare dette misure con relative garanzie adeguate, nonché per avviare un approccio comune e coordinato degli Stati rispetto all'utilizzo ditali misure digitali.

Ebbene, anche qui pare potersi rilevare che l'intervento come *regulatory power* sembrerebbe aver trovato riscontri pur nella situazione emergenziale, tanto che è stato rilevato «*The GDPR, its principles and obligations, passed the first major test of their short existence, demonstrating to the world how high privacy standards can be maintained even in emergency circumstance. (…) businesses and organisations may have discovered that compliance with the security-related requirements of the GDPR already provided the necessary technical and organisational measures to combat the rise in cybercrime during the pandemic*»[465]. Dall'altro lato, però, nell'adozione concreta di tali misure e di altre correlate, l'approccio degli Stati membri non è parso così coordinato a livello sovranazionale come le premesse avrebbero fatto sperare, e di ciò si è avuto conferma anche rispetto agli interventi relativi alla circolazione delle persone tra Stati membri, che hanno destato anche in prospettiva non poche perplessità[466]. Invero, quest'ultimo ambito parrebbe di recente aver trovato una soluzione concertata con il nuovo *certificato verde digitale*, volto

[463] EDPB, Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020, pp. 2-3, available here: https://edpb.europa.eu/sites/default/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[464] Commissione europea, Raccomandazione "*relativa a un pacchetto di strumenti comuni dell'Unione per l'uso della tecnologia e dei dati al fine di contrastare la crisi Covid-19 e uscirne, in particolare per quanto riguarda le applicazioni mobili e l'uso di dati anonimizzati sulla mobilità*"…
Communication from the Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, C(2020) 2523 final, 16.04.2020, https://ec.europa.eu/info/sites/default/files/5_en_act_part1_v3.pdf Si veda, *ex multis*, C. FIORILLO, La protezione dei dati personali nel diritto UE di fronte all'emergenza del COVID-19, in L'emergenza sanitaria Covid-19 e il diritto dell'Unione europea. La crisi, la cura, le prospettive, *Eurojus – numero speciale*, 2020, p.

[465] Così E. VENTRELLA, Privacy in emergency circumstances: data protection and the COVID-19 pandemic, in *ERA Forum*, 28 September 2020.

[466] Si rinvia per approfondimenti in tal senso a O. J. GSTREIN, D. V. KOCHENOV, A. ZWITTER, A Terrible Great Idea? COVID-19 'Vaccination Passports' in the Spotlight, COMPAS, *Working Paper* n. 153, March 2021.

facilitare la libertà di circolazione durante la pandemia attraverso l'adozione di un quadro comune a livello europeo. La proposta della Commissione del marzo 2021 fu oggetto di parere congiunto dell'EDPB e EDPS il successivo aprile[467], da cui emergeva un forte monito alla conformità del certificato alla normativa sulla protezione dei dati personali, cercando di ridurre i possibili rischi derivanti dal suo utilizzo rispetto ai diritti fondamentali degli interessati. Com'è noto, il relativo Regolamento è entrato in vigore il 1° luglio scorso, per cui l'effettivo funzionamento dell'intero meccanismo e i prospettati vantaggi sono ancora da verificare.

Ma, ancora di più, l'emergenza pandemica ha rivelato le carenze di *strategic autonomy* dell'Unione nella dimensione esterna, palesando una forte dipendenza rispetto ad aziende tecnologiche straniere, in particolare statunitensi e cinesi.

In realtà, si tratterebbe di una dipendenza che esisteva già e che il Covid-19 ha fatto solo emergere in maniera lampante, palesando dipendenze in settori cruciali rispetto ai quali gli Stati membri e l'Unione risulterebbero dipendenti quanto a servizi e infrastrutture digitali, con un impatto geopolitico non da poco, poiché «*These dependencies create insecurity, and generate several concerns, including the fear of losing control of data or of being increasingly vulnerable to external pressure*»[468]. Tra le varie preoccupazioni, dunque, l'emergenza pandemica avrebbe messo in luce la necessità per l'Unione di diventare più competitiva e meno dipendente in settori chiave, e le iniziative e le prospettive (in parte accennate) delle istituzioni europee sembrerebbero particolarmente espressive di questa consapevolezza[469].

Al riguardo, sarebbero cinque i settori chiave in cui l'Unione, anche a partire dal *recovery plan* prospettato rispetto al Covid-19, dovrebbe agire per potenziare la propria *strategic autonomy* da attori esterni: *Quantum Computing*; *High-end Microchips*; *Cloud Comupting*; *Cybersecurity*; *Artificial Intelligence*[470]. Limitandoci a un doveroso cenno sul settore di *Cloud Computing*, rileviamo come degni di nota, oltre ai recenti approfondimenti della Commissione in materia[471], il progetto di infrastruttura europea Gaia-X, proposto da Germania e Francia nel giugno 2020, come anche la *Cloud Declaration* di 25 Stati membri, dichiarazione congiunta che mira alla costruzione

[467] https://edpb.europa.eu/system/files/2021-07/edpb_edps_joint_opinion_dgc_it.pdf .
[468] T. CHRISTAKIS, 'European Digital Sovereignty', *cit*., p. 45.
[469] Cfr. E. KELLY, Decoding Europe's new fascination with 'tech sovereignty', in Science Business, 3 September 2020, che, nel rilevare questa rinnovata attenzione verso un'indipendenza dalle tecnologie cinesi e statunitensi, sollevava anche qualche dubbio rispetto a una visione coerente di "sovranità tecnologica", cfr. "*Since COVID-19, EU leaders are pushing for greater independence from US and Chinese technology. But what would that mean*?".
Cfr. anche Atlantic Council, cit. pp. 4-5: «*if the EU wanted to be able to play a role in shaping global affairs, it had to address shortcomings in its industrial and technological base, as well as its critical infrastructure*».
[470] Così vengono individuati, infatti, da T. CHRISTAKIS, alla cui analisi rinviamo per approfondimenti,cfr. 'European Digital Sovereignty', *cit*., pp. 50-52.
[471] Cfr. https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/cloud-computing_it ; anche: https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe .

di una prossima generazione *cloud* europea, che è stata di recente accolta con favore dalla Commissione[472].

In questo ordine di interventi, particolarmente significativa è l'ultima iniziativa adottata dalla Commissione nell'ambito della sua *Strategia europea in materia di dati* proposta nel febbraio 2020. Abbiamo già detto che tale strategia è volta a "*Fare in modo che l'UE assuma il ruolo di modello e di guida per una società più autonoma grazie ai dati*", nella consapevolezza che "*i dati rappresentano il fulcro della trasformazione digitale*"[473]; ebbene, lo scorso 19 luglio 2021 la Commissione ha compiuto un ulteriore passo annunciato proprio nell'ambito di tale strategia, anche in virtù degli "Insegnamenti tratti dalla crisi della Covid-19"[474], ossia il lancio di una *Alleanza europea per i dati industriali, edge e cloud* che si aggiunge a quella per i *processori e le tecnologie dei semiconduttori*. Tali due nuove alleanze dovrebbero rafforzare le infrastrutture e i servizi digitali critici dell'Unione: "*The alliances will bring together businesses, Member State representatives, academia, users, as well as research and technology organisations*"[475].

Insomma, ultimamente l'Unione pare ben consapevole delle carenze in termini di *strategic autonomy* e della necessità di potenziare questo aspetto per ottenere una compiuta sovranità digitale, pur con dei settori ancora da irrobustire e pur con i rischi, paventati da molti, che interventi del genere, soprattutto di *data localisation*, potrebbero comportare in termini di protezionismo o di erezione di una sorta di "*fortress Europe*"[476].

Sovranità digitale come possibile soluzione a "legitimacy crisis" dell'Unione europea

Da tutto quanto detto emergono chiare testimonianze di una sovranità digitale dell'Unione europea esplicantesi nell'esercizio del *normative/regulatory power* particolarmente performativo della dimensione digitale.

Ciò deriverebbe dalla capacità dell'Unione, attraverso l'utilizzo (ancora) del suo *diritto* come *potere*, di affermare le proprie regole in quella dimensione in un modo che è *proprio* dell'Unione, e

[472] European Commission: "The Commission, together with Member States, aims to create more synergies between national and cross-border initiatives to enhance and broaden their interoperability, scale-up and scope" https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-member-states-declaration-eu-cloud-federation .
[473] Si rinvia alla pagina della Commissione dedicata: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_it .
[474] Così si evince dalla Strategia industriale europea, cfr. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_it .
[475] European Commission, press release – Digital Sovereignty: Commission kick-starts alliances for Semiconductors and industrial cloud technologies, 19 July 2021: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3733 .
[476] Questo il termine usato dall'Atlantic Council, nelle prospettive illustrate nel lavoro, cit. Sui rischi legati al protezionismo si rinvia anche a Christakis, p. 52 ss.

che dunque è distintivo del suo intervento e ne costituisce valore aggiunto in quella dimensione: rispetto agli Stati membri, poiché essi, pur condividendo il medesimo assetto valoriale, non hanno, in quanto tali e presi singolarmente, gli strumenti e le capacità necessari a far valere quei valori nella dimensione digitale; quanto agli Stati terzi, specie quelli pur più competitivi dell'Unione in termini di infrastrutture e servizi tecnologici, perché ad essi mancherebbe invece quell'assetto valoriale che è proprio dell'Unione e dei suoi Stati membri insieme e che risulta particolarmente efficace per ordinare la caotica dimensione digitale e per garantire in essa le necessarie tutele, aspetto che abbiamo identificato nella *EU rule of law*: «*Europe has been able to convince the world that its rules are both ethically desirable and normatively justified – as they can promote social welfare and (in the field of data protection) individual self-determination. The regulation of the digital sphere by Europe appears to many people as a natural and healthy consequence of the earlier mistake of conflating globalization with deregulation, and digitalization with a "free for all" attitude leading, in the private sphere, to what Shoshana Zuboff called "Surveillance Capitalism" and, in the public sphere, to "Surveillance States" such as China*»[477].

Questo già potrebbe valere, in qualche misura, a rispondere alle questioni di legittimazione dell'Unione, che dalla spiegata insostituibilità di tale intervento nella dimensione digitale troverebbe più di un argomento per legittimarsi, tanto all'interno (rispetto alle recenti crisi, soprattutto dei valori, che la porrebbero in dubbio) quanto, quindi, all'esterno, nel contesto internazionale.

Tuttavia, proprio rilievi di "autonomia strategica" farebbero invece ancora dubitare rispetto al ruolo *effettivo* dell'Unione in quel contesto, e così, di riflesso, anche nella sua dimensione interna. Pertanto, occorre capire se anche questo profilo della sovranità digitale può fornire, se non attualmente, almeno in prospettiva, delle possibilità di legittimazione dell'Unione tramite una eventuale compiuta sovranità digitale.

Ebbene, l'ambizione ad una autonomia strategica nel contesto internazionale ci fa ritornare alle riflessioni esposte in apertura quanto alla caratteristica dell'attuale contesto internazionale che abbiamo visto essere l'*interdipendenza*. Invero, alcuni studiosi hanno proprio enfatizzato che la tendenza verso una autonomia strategica dovrebbe essere accompagnata dalla consapevolezza di una necessaria "interdipendenza strategica"[478]. In questo senso, le suddette attuali carenze in termini

[477] T. CHRISTAKIS, European Digital Sovereignty, *cit.*, pp. 38-39.
[478] Ibidem, che cita Timmers a Cerulus, p. 87.

di cooperazione internazionale andrebbero superate con un approccio dell'Unione più proteso verso soluzioni concertate, ma senza abbandonare il suo carattere distintivo[479].

La caratteristica interdipendenza del contesto internazionale, e la necessità per l'Unione di gestirne le dinamiche, potrebbero apparire contrastanti rispetto alle ultime iniziative che, come abbiamo visto, protenderebbero per una *localizzazione* dei dati, mentre l'insistenza sulla protezione dei dati potrebbe anche portare a paventati rischi di *protezionismo*[480].

Invero, queste preoccupazioni paiono ridimensionate dagli ultimi interventi delle istituzioni europee. Infatti, non solo le Conclusioni del Consiglio europeo dell'ottobre 2020 sono chiare in tal senso, ma anche, per esempio, il Commissario Hogan, in un discorso tenuto all'EUI poco prima, parlava chiaramente di una "*autonomia strategica aperta*": «*Open Strategic Autonomy means reaffirming our global leadership ambitions across a range of areas, in line with the aims of a more geopolitical European Commission; It means building stronger alliances with like-minded partners; It means shaping a better type of globalisation – fairer, and more sustainable; It reflects our commitment to strong and up-to-date multilateral rules; It recalls our belief in "the opportunity of openness". While at the same time:It advocates for a tougher, more assertive approach to protect our businesses and consumers, notably through stronger trade defence and enforcement; And it calls for the diversification of supply chains to assure our strategic independence*»[481].

Dunque, a fronte di queste prospettive, parrebbe pacifico che «*L'autonomia non deve essere confusa con un ripiego verso l'isolazionismo o il protezionismo. L'apertura dell'Europa e l'interdipendenza che ne deriva sono l'essenza stessa del progetto di integrazione europea*»[482]; eppure, permangono delle perplessità e preoccupazioni proprio sull'effettiva portata delle prospettive, che farebbero ancora dubitare su "*what model Europe wishes to promote*"[483].

---

[479] Ibidem, p. 96: «*Beyond using international law to resolve specific problems with specific countries, strategic partnerships seem to be an interesting option in order to be able to promote certain important values in cyberspace*».
[480] Ibidem, p. 98: «*The bottom line is that Europe should focus not on "data localisation" but on "data protection". Nevertheless, data protection considerations can easily be misused or abused as a vehicle to further domestic business interests and protectionism. The one million dollar question is how to distinguish between data protection and data protectionism (or "nationalism")*».
[481] Speech by Commissioner Phil Hogan at Launch of Public Consultation for EU Trade Policy Review - Hosted by EUI Florence, 16 June 2020, available here: https://ec.europa.eu/commission/commissioners/2019-2024/hogan/announcements/speech-commissioner-phil-hogan-launch-public-consultation-eu-trade-policy-review-hosted-eui-florence_en .
[482] Così M LEONARD, J. SHAPIRO, Un'Europa sovrana in un mondo pericoloso: proteggere la capacità d'azione dell'Europa in cinque aree chiave, in *European Council on Foreign Relations – Policy Brief*, 1 Dicembre 2020, versione italiana disponibile qui: https://ecfr.eu/rome/publication/sovereign-europe-dangerous-world-five-agendas-to-protect-europes-capacity-to-act/ .
[483] T. CHISTAKIS, *op. cit.*, pp 86 e 99.

3. La sovranità digitale come sfida dell'Unione europea

Cogliendo quest'ultima provocazione, possiamo proporre risposta alla nostra domanda di ricerca.

Il modello che l'Unione vuole promuovere nella dimensione digitale è quello che ha ribadito da ultimo la Commissione, ossia quello basato sull'approccio *antropocentrico*, che fa ancora, e anche rispetto ad interventi di autonomia strategica, dei suoi valori e della tutela dei diritti fondamentali il suo baluardo e il perno della sua azione. Dunque, un modello, potremmo dire, *proprio* del suo stile, che conferma come l'anelito verso la sovranità digitale non sia altro che un'affermazione, nella dimensione digitale, delle peculiarità tipiche dell'Unione e della *EU rule of law*.

E però, lo ripetiamo, tale anelito verso la sovranità digitale, nei due profili proposti, non solo parrebbe comune ad altri attori che concorrono in quella dimensione, ma soprattutto si farebbe strada in un contesto internazionale caratterizzato da *interdipendenza*, che parrebbe dunque in antitesi con ambizioni autonomiste e con i caratteri classici della sovranità. Abbiamo però anche detto che peculiare dello sviluppo di quell'interdipendenza è stata l'emersione della cultura dei diritti umani, e della "rinnovata" concezione della sovranità in tale contesto, che abbiamo voluto proporre con la formula per cui *è sovrano chi garantisce la tutela dei diritti*.

Ebbene alla luce dei riscontri nell'analisi proposta, nonché delle prospettive illustrate (e pur tenendo conto delle perplessità) quanto agli interventi dell'Unione nella dimensione digitale, possiamo concludere che, abbracciando la suddetta concezione "funzionalista" della sovranità come "*legittimazione sul piano giuridico di una effettività che fonda se stessa*", la pretesa sovranità digitale dell'Unione europea si risolverebbe nella garanzia da essa apprestata alla tutela dei diritti nella dimensione digitale, che trova nell'*effettività* di quella tutela la sua (nuova) ragione di legittimazione.

Se, dunque, assumiamo la sovranità come *veicolo* per acquisire legittimazione, la tendenza alla sovranità digitale dell'Unione europea consentirebbe a quest'ultima di (auto)legittimarsi in virtù dell'*effettività* del proprio e peculiare operato nella dimensione digitale, caratterizzato dall'attenzione alle tutele degli individui quale elemento distintivo, tanto negli interventi regolatori che di potenziamento della propria autonomia nell'innovazione tecnologica, rispetto agli altri attori.

Di ciò si avrebbe conferma nell'approccio *antropocentrico* ribadito dalla Commissione, che non fa altro che richiamare ciò su cui la Corte di giustizia insiste da parecchio, circa l'imprescindibilità del

controllo giurisdizionale effettivo[484], che anche altri ordinamenti devono garantire affinché la tutela apprestata dall'Unione possa dirsi *effettiva ovunque*, e la necessità che la sua intera azione sia soggetta al controllo di conformità ai diritti fondamentali, quale genuino significato della *Unione di diritto*[485].

Nella misura in cui queste peculiarità, proprie della *EU rule of law*, trovano *effettivo* compimento nella dimensione digitale, esse consentono (già) di superare alcune criticità della legittimazione dell'Unione, come gli interventi di *regulatory power* testimonierebbero. Laddove, invece, manca ancora tale effettività, ecco che la sovranità digitale rimane incompiuta e mantiene quelle criticità, che si palesano soprattutto in ostacoli derivanti dalle prerogative sovrane degli Stati, tanto membri quanto terzi.

La capacità dell'Unione, intesa come insieme di Stati membri, dovrebbe essere quella di rendersi più flessibile e aperta con le controparti internazionali, potenziando gli investimenti nei punti deboli per aumentare la propria competitività, ma gestendo quelle dinamiche in maniera fedele alla tradizioni comuni agli Stati membri, senza arretrare sull'*effettività* delle garanzie riconosciute nel proprio ordinamento giuridico, che ne contrassegna, a livello internazionale, l'identità, e che in ultima analisi può consentirle, ancora una volta, di superare, più o meno apparenti, crisi di legittimazione.

In pratica, a fronte di una sempre maggiore consapevolezza circa la necessità di rimuovere tali ostacoli, permangono le perplessità rispetto a un'effettiva rimozione, che richiederebbe, in ultima analisi, maggiori attribuzioni da parte degli Stati membri a favore all'Unione. Se è vero che da tempo in diversi settori dell'integrazione tale aspetto si è fatto evidente, la dimensione digitale, che penetra e ingloba, più o meno direttamente, ormai tutti i settori, lo rende ora particolarmente impellente.

[484] Corte di giustizia, *Schrems I*, p. 95.
[485] Ibidem, p. 60.

Conclusioni

Il lavoro di ricerca proposto in questa tesi ha cercato di dimostrare che lo stato attuale dell'integrazione europea presenta, da un lato, profonde criticità che ripropongono dubbi sulla legittimazione dell'Unione europea, e però anche, dall'altro, enormi potenzialità di cui quest'ultima può ancora godere, che troverebbero nella nuova dimensione digitale lo "spazio" ideale per la loro realizzazione.

A partire dalla domanda di ricerca, abbiamo legato l'ambizione alla sovranità digitale dell'Unione europea al tentativo dell'ente di trovare rinnovati elementi di legittimazione.

Dalla disamina condotta è emerso che la sovranità digitale si connoterebbe, rispetto all'Unione europea, per due aspetti: quello legato al *potere normativo/regolatorio*, inteso come capacità dell'ente di ordinare la dimensione digitale e di stabilire le regole per il suo funzionamento; quello legato alla *autonomia strategica*, in termini di capacità di dominare l'innovazione tecnologica e gestire proprie infrastrutture e servizi digitali senza dover dipendere da attori esterni.

Per rispondere alla domanda di ricerca abbiamo assunto come caso di studio il diritto alla protezione dei dati personali e ne abbiamo rintracciato i punti di contatto con l'insieme delle caratteristiche essenziali e distintive dell'Unione europea che abbiamo individuato nella *EU rule of law*.

Da tale analisi, dunque, sono emersi sia nelle previsioni teoriche, tanto normative quanto dottrinali, che nella prassi delle istituzioni e soprattutto nella giurisprudenza, molteplici indici che consentono di confermare sufficientemente il primo aspetto della sovranità digitale: l'utilizzo del diritto come potere nella dimensione digitale ha già consentito all'Unione europea di affermarsi nel contesto internazionale come modello regolatorio, particolarmente rispetto alla protezione dei dati personali.

Dall'altro lato, però, da quella analisi sono emerse incongruenze, sia nella dimensione interna, rispetto per esempio alle prerogative securitarie degli Stati membri, che in quella esterna, rispetto alle difficoltà di una efficace cooperazione per la conclusione di accordi con Stati terzi e ancora, più in generale, rispetto alla capacità dell'Unione di presentarsi in maniera univoca alle controparti internazionali (ci riferiamo ai diversi approcci riscontrabili tra le istituzioni sovranazionali quanto ai casi che riguardano, in generale, trasferimenti di dati verso l'esterno), facendo sorgere dubbi sulla coerenza dell'azione dell'Unione.

Nondimeno, le più ampie riflessioni sui risultati dell'intera ricerca, comprensiva tanto delle premesse teoriche sulla natura e sulle peculiarità dell'ordinamento giuridico *sui generis* dell'Unione (come anche, ancorché per pillole, sulla sovranità in generale) quanto anche degli ultimissimi sviluppi sugli interventi delle istituzioni anche a seguito della crisi pandemica, specie in termini di approccio antropocentrico per la promozione del modello europeo nella dimensione digitale, hanno portato a concludere come segue: nelle attuali sembianze del contesto internazionale caratterizzato da interdipendenza tra soggetti e dall'attenzione verso i diritti umani, garantire la tutela di questi ultimi costituisce un elemento imprescindibile della "rinnovata" concezione di sovranità. Abbracciando la concezione funzionalista che spiega la sovranità in termini di effettività, abbiamo così dedotto che nella dimensione digitale, la pretesa sovranità digitale dell'Unione europea si risolverebbe nella garanzia da essa apprestata alla tutela dei diritti nella dimensione digitale, che trova nell'*effettività* di quella tutela la sua (nuova) ragione di legittimazione.

E ciò varrebbe nella duplice accezione riconosciuta alla sovranità digitale dell'Unione europea, tanto come potere regolatorio che in termini di autonomia strategica.

Gli esiti del nostro lavoro hanno dimostrato che possiamo già ravvisare una compiuta sovranità digitale come *effettività* del potere normativo dell'Unione nella dimensione digitale, che infatti in questa accezione parrebbe coerente alla garanzia di protezione dei dati personali e che dunque, in questo, troverebbe già motivi di legittimazione. Gli ambiti in cui, invece, tale ambizione rimane incompiuta sono quelli in cui non si ravviserebbe detta effettività, in ultima analisi riconducibili all'aspetto della autonomia strategica, specie rispetto ad attori esterni (pubblici e privati), ma anche nella sua peculiare declinazione nella dimensione interna dell'integrazione, che rivelerebbe criticità ogni qualvolta l'intervento dell'Unione stride con le prerogative sovrane degli Stati membri.

Il processo di integrazione europea, però, e come abbiamo assunto sin dall'inizio, consisterebbe proprio in un moto perpetuo, guidato da continue spinte e rotture che, al netto di rovinose previsioni di breve periodo, rileverebbero un ente (senza forma, ma forse grazie a questo) in un continuo movimento che, a nostro avviso, sottace miglioramento. Le diffuse consapevolezze da ultimo palesate sulle criticità che l'Unione presenta nella dimensione digitale farebbero protendere verso fertili prospettive che, a partire da quella dimensione (e nonostante i molti scetticismi), potrebbero rinvigorire il processo di integrazione nel prossimo futuro.

Bibliografia

ADAM R., TIZZANO A., *Lineamenti di Diritto dell'Unione europea*, Giappichelli, 2016.

ARENA A., La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento? Commento a Corte Giust. Sentenza 8 aprile 2014, *Digital Rights Ireland*, cause riunite C-293/12 e C-594/12, in *Quaderni costituzionali*, n. 3/2014, pp. 722- 725.

ARENA A., *Le «situazioni puramente interne» nel diritto dell'Unione Europea*, Editoriale Scientifica, 2019.

AZOULAI L., VAN DER SLUIS M., Institutionalizing personal data protection in times of global institutional distrust: *Schrems*, in *Common Market Law Review*, 53, 2016, pp. 1343-1372.

BALDUCCI ROMANO F., La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo, in *Rivista Italiana di Diritto Pubblico Comunitario*, Fasc. 6-2015, pp. 1618-1659.

BARTOLE S., CONFORTI B., RAIMONDI G. (a cura di), *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, CEDAM, 2001.

BARTOLE S., DE SENA P., ZAGREBELSKY V. (a cura di), *Commentario breve alla CEDU - Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali*, CEDAM, 2012.

BASILICO A. E., *Le autorità indipendenti tra diritto dell'Unione e sistema interno dei poteri*, Università degli Studi di Milano – Scuola di dottorato in scienze giuridiche, XXV ciclo (IUS/08), AA. 2011/2012.

BELLANGER P., De la souveraineté en général et de la souveraineté numérique en particulier, in *Les Echos*, 30.08.2011.

BENSOUSSAN, A., *Règlement européen sur la protection des données - Textes, commentaires et orientations pratiques*, 2e édition, Bruyant, 2018.

BESSON S., Sovereignty, in *Max Planck Encyclopedias of International Law*, Oxford Public International Law, latest updated April 2011.

BESTAGNO F., Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali, in *Il Diritto dell'Unione europea*, n. 1/2015, pp.25-56.

BIFULCO R., CARTABIA M., CELOTTO A. (a cura di), *L'Europa dei diritti - Commento alla Carta dei diritti fondamentali dell'Unione Europea*, Il Mulino, 2001.

BIFULCO R., NATO A., The concept of sovereignty in the EU – past, present and the future, in *Reconnect – Europe*, 2020.

BRADFORD A., *The Brussels Effect – How the European Union rules the world*, Oxford University Press, 2020.

BRKAN M., The Court of Justice of the EU, privacy and data protection: Judge-made law as a leitmotif in fundamental rights protection, in M. BRKAN, E. PSYCHOGIOPOULOU (Eds), *Courts, privacy and data protection in the digital environment*, Elgar, 2017.

BRKAN M., The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU's Constitutional Reasoning, in *German Law Journal*, vol. 20, no. 6, 2019, p. 864-883.

BURWELL F. G., PROPP K., The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?, *Atlantic Council – Issue Brief*, June 2020.

BYGRAVE L. A., The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, Vol. 40, 2021 38, pp.1-24.

CAGGIANO G., Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione, in *MediaLaws – Rivista di Diritto dei Media*, n. 2/2018, pp. 1-19.

CAGGIANO G., La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali, in *Studi sull'integrazione europea*, n. 1/2018, pp. 9-28.

CANNIZZARO E., *Diritto Internazionale*, Quinta edizione, Giappichelli, 2020.

CANNIZZARO E., *Il diritto dell'integrazione europea – L'ordinamento dell'Unione*, Terza edizione, Giappichelli, 2020.

CANNIZZARO E., Il ruolo della Corte di giustizia nella tutela dei valori dell'Unione europea, in *Liber Amicorum Antonio Tizzano – De la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, Giappichelli, 2018, pp. 158-169.

CANNIZZARO E., *La sovranità oltre lo Stato*, Il Mulino, 2020.

CARPANELLI E., LAZZERINI N., PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU, in *Air and Space Law*, 42, no. 4&5 (2017), pp. 377-402.

CARTER C., SCOTT A., Legitimacy and Governance beyond the European nation State: conceptualising governance in the European Union, in *European Law Journal*, Vol. 4, No.4, December 1998, pp. 429-445.

CASTELLANETA M., *Corte Ue e obblighi di rimozione di contenuti illeciti dal web – EU Court ruling on Facebook duty to take down illegal content*, in *marinacastellaneta.it*, 15 ottobre 2019.

CELESTE E., Digital Sovereignty in the EU: Challenges and Future Perspectives, in F. FABBRINI, E. CELESTE, J. QUINN (Eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford: Hart Publishing, 2020.

CELLERINO C., *Soggettività internazionale e azione esterna dell'Unione Europea – fondamento, limiti e funzioni,* Aracne editrice, 2015.

CHRISTAKIS T., 'European Digital Sovereignty': Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy', *Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute*, e-book, December 2020.

CHRISTAKIS T., "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1), in *European Law Blog*, 13 November 2020.

CHRISTAKIS T., "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2), in *European Law Blog*, 16 November 2020.

CHRISTAKIS T., "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 3), in *European Law Blog*, 17 November 2020.

CHRISTAKIS T., After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe, *European Law Blog*, 21 July 2020.

CHRISTAKIS T., Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy negotiations (Part 1), in *European Law Blog*, 12 April 2021.

CHRISTAKIS T., Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2), in *European Law Blog*, 13 April 2021.

CHRYSSOCHOOU D.H., TSINISIZELIS M.J., STAVRIDIS S., IFANTIS K., *Theory and reform in the European Union*, Manchester University press, 2003.

COLE M. D., Weltimmo Reloaded: CJEU Further Clarifies the Concept of Establishment, in *European Data Protection Law Review*, n. 3/2016, pp. 377-380.

COLE M.D., VANDENDRIESSCHE A., From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR made of the deep pass by the CJEU in the recent cases on mass surveillance, in (2016) *European Data Protection Law Review* 121.

CORTESE B., Articolo 16 TFUE, in A. TIZZANO (a cura di), *I Trattati dell'Unione europea*, Giuffrè, 2014.

CORTESE B., Articolo 39 TUE, in A. TIZZANO (a cura di), *I Trattati dell'Unione europea*, Giuffrè, 2014.

CORTESE B., Riflessioni sull'autonomia come limite: l'equilibrio tra libertà e condizionamento nel diritto dell'Unione europea, tra Unione, Stati membri ed individui, in *Liber Amicorum Antonio Tizzano – De la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, Giappichelli, 2018, pp. 222-246.

CRAIG P., The EU, democracy and institutional structure: Past, present and future, in W. HEUSEL, J-P REGEADE (Eds), *The Authority of EU Law – Do we still believe in it*?, Springer, 2019, pp. 311-334.

CREMONA M., Extending the Reach of EU Law – The EU as an International Legal Actor, in C. CREMONA, J. SCOTT (Eds), *EU law beyond EU border – The Extraterritorial Reach of EU Law*, Oxford University Press, 2019.

CREMONA M., SCOTT J., Introduction - EU Law Beyond EU Borders, in M. CREMONA, J. SCOTT (Eds), *EU Law Beyond EU Borders – The Extraterritorial Reach of EU Law*, Oxford University Press, 2019.

CREMONA M., *Values in EU Foreign Policy*, in E. SCISO, R. BARATTA, C. MORVIDUCCI (a cura di), *I valori dell'Unione europea e l'azione esterna*, Giappichelli, 2017.

D'ATH F., Arrêt « Schrems II » : sur la légalité des transferts de données personnelles fondés sur une décision d'adéquation ou moyennant des garanties appropriées, in *Journal de droit européen*, 2020.

D'ORAZIO R., La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, 2019.

DE BURCA G., Sovereignty and the Supremacy Doctrine of the European Court of Justice, in N. WALKER (Ed.) *Sovereignty in Transition*, Hart Publishing, 2003, pp. 449-460.

DE BURCA G., The Quest for Legitimacy in the European Union, in *The Modern Law Review*, 59:3, 1996, p. 349-376.

DE HERT P., CZERNIAWSKI M., Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, in *International Data Privacy Law*, Vol. 6(3), 2016, pp. 230-243.

DE HERT P., GUTWIRTH S., Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, in S. GUTWIRTH, Y. POULLET, P. DEHERT-J. NOUWT, C. DE TERWAGNE (Eds), *Reinventing data protection*?, Springer Science, Dordrecht, 2009.

DE HERT P., SAJFERT J., The Role of the Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data, in C. BRIÈRE and A. WEYEMBERGH (Eds), *The Needed Balances in EU Criminal Law: Past, Present and Future*, Oxford, 2018, pp. 243-255.

DE HERT P., V. PAPAKONSTANTINOU, The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals, in *Computer Law and Security Review* (28), 2012, pp. 130-142.

DE SENA P., Dignità umana in senso oggettivo e diritto internazionale, in *Diritti umani e diritto internazionale*, n. 3/2017, pp. 573-586.

DE VANNA F., L'ordinamento giuridico di Santi Romano e il pluralismo oltre l'orizzonte dello Stato: alcuni percorsi interpretativi, in *Jura Gentium*, XV (2018), 2.

DE WILDE J., *Saved from oblivion: interdependence theory in the first half of the 20th Century – A study on the causality between war and complex interdependence*, Dartmouth, 1991.

DE WITTE B., Sovereignty and European Integration. The Weight of Legal Tradition, *Maastricht Journal*, 2, 1995.

DELLA MORTE G., *Big Data e protezione internazionale dei diritti umani – regole e conflitti*, Editoriale Scientifica, 2018.

DELLAVALLE S., Il potere dell'Unione europea, in *Teoria politica. Nuova Serie*, Annali VI, 2016, pp. 193-223.

DEVUYST Y., The European Union's Institutional Balance after the Treaty of Lisbon: Community Method and Democratic Deficit Reassessed, 39(2) *Georgetown Journal of International Law*, 2008.

DI FRANCESCO MAESA C., Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR). In *Eurojus.it*, 24.05.2016.

DI MATTEO F., La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella direttiva PNR?, in *Diritti Umani e Diritto Internazionale*, n. 1/2017, pp. 234-235.

DI STEFANO A., *Convenzione europea dei diritti dell'uomo e principio di sussidiarietà – contributo ad una lettura sistematica degli articoli 13 e 35*, ed.it, 2009.

DOCKSEY C., HIJMANS H., The Court of Justice as a Key Player in Privacy and Data protection, in *European Data Protection Law*, n. 3, 2019, pp. 300-316.

DOCKSEY C., Ministerio Fiscal: Holding the line on ePrivacy, in *Maastricht journal of European and comparative law*, n. 4 (vol 26) 2019, pp. 585-594.

ECKES C., Protecting Supremacy from External Influences: A Precondition for a European Constitutional Legal Order, *European Law Journal*, vol. 18, no. 2, March 2012, p. 230-250.

ERDEM E. I., European Integration and International Relations Theory, in *Florida International University – Working Paper*, December 2006.

ESTRADA CAÑAMARES M., Building Coherent EU Responses': Coherence as a Structural Principle in EU External Relations, in M. CREMONA (Ed.), *Structural Principles in EU External Relations Law*, Hart Publishing, 2018, pp.243-262.

F. FABBRINI, Il diritto dell'Ue e l'indipendenza delle autorità nazionali garanti della protezione dei dati, in *Giornale di diritto amministrativo*, n. 10/2010.

FALCHETTA T., Intelligence Sharing and the Right to Privacy after the European Court Judgment in Big Brother Watch v. UK, in *EJIL: Talk!*, September 24, 2018.

FICHERA M., *The foundations of EU as a polity*, Elgar, 2018.

FIORAVANTI M., Stato e costituzione, in M. FIORAVANTI (a cura di), *Lo Stato moderno in Europa – Istituzioni e diritto*, Laterza, 2011.

FORMICI G., L'incerto futuro della data retention nell'Unione europea: osservazioni a partire dalla sentenza H.K. v Prokuratuur, in *SIDIblog*, 27 aprile 2021.

FRA-COE-EDPS, *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, 2018.

GAJA G., ADINOLFI A., *Introduzione al diritto dell'Unione europea*, Quarta edizione, Bari-Roma, 2020.

GIANFRANCESCO E., Article 17 [The European Commission], in in H.-J. BLANKE, S. MANGIAMELI (Eds), *The Treaty on European Union (TEU)-A Commentary*, Springer, 2013.

GIURGIU A., LARSEN T. A., Roles and Powers of National Data Protection Authorities, in *European Data Protection Law Review* (EDPL), vol. 2, n. 3, 2016, p. 351

GÖMANN M., A Hidden Revolution, in *Verfassungsblog*, 17 June 2021.

GONZÁLEZ FUSTER G., *The emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014.

GORETTA R, Gdpr e trasferimento dati extra Ue: i casi di Cina, India, Brasile e Russia, in *Agenda Digitale*, 22 marzo 2021.

GRAGLIA P., *L'Unione europea – perché stare ancora insieme*, Il Mulino, 2019.

GRIMM D., Does Europe need a Constitution?, in *European Law Journal*, 1 (1995), pp. 282-302.

GSTREIN J., The Judgment That Will Be Forgotten – How the ECJ Missed an Opportunity in Google vs CNIL (C-507/17), in *Verfassungsblog*, 25 September 2019.

GUEHAM F., Digital Sovereignty – Steps towards a new system of Internet Governance, *Fondation pour l'innovation politique*, January 2017.

GUTWIRTH S., LEENES R., DE HERT P. (Eds), *Data Protection on the Move – Current Developments in ICT and Privacy/Data Protection*, Springer, 2015.

GUTWIRTH S., LEENES R., DE HERT P. (Eds), *Data Protection on the Move – Current Developments in ICT and Privacy/Data Protection*, Springer, 2015, Preface.

GUY PETERS B., PIERRE J., Governance Approaches, in A. WIENER, T. DIEZ (Eds), *European Integration Theory – Second edition*, Oxford University Press, 2009, pp. 91-104.

GYŐZŐ SZABÓ E., The Weltimmo case in light of the future General Data Protection Regulation. One-stop-shop – burden or catalyst among cooperating data protection authorities? – selected intervention from the PHAEDRA Final Conference, in P. DE HERT, D. KLOZA AND P. MAKOWSKI (Eds), *Enforcing privacy: lessons from current implementation and perspectives for the future*, Warszawa, 2015.

HABERMAS J., Democracy in Europe: Why the Development of the EU into a Transnational Democracy Is Necessary and How It Is Possible, *European Law Journal*, Vol. 21, No. 4, July 2015, pp. 554-555.

HABERMAS J., Remarks on Dieter Grimm's 'Does Europe need a Constitution?', in *European Law Journal*, 1 (1995), pp. 303-307.

HART H.L.A., *The concept of Law*, Oxford, 1961.

HIJMANS H., *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU*, (PhD Thesis) University of Amsterdam, 2016.

HIJMANS H., PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators, 3 *European Data Protection Law Review*, pp. 406-412 (2017).

HIJMANS H., Article 51. Supervisory Authority, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020.

HOBBS C. (Ed.), Europe's Digital Sovereignty: from rulemaker to superpower in the afe of US-China rivalry, in European Council on Foreign Relations – Essay Collection, July 2020.

HOBBS C., L'Europa alla ricerca di una sovranità digitale: sfide e interessi in gioco, in *Agenda Digitale*, 8 ottobre 2020.

HOOGHE L., MARKS G., A Postfunctionalist Theory of European Integration: From Permissive Consensus to Constraining Dissensus', in *British Journal of Political Science*, published online by Cambridge University Press, 2008, pp. 1-23.

HOOGHE L., MARKS G., Grand Theories of European integration in the twenty-first century, (2019), in *Journal of European Public Policy*, 26:8, 1113-1133.

JACQUÉ J.P., The Principle of constitutional balance, in *Common Market Law Review*, 41, 2004.

KELLY E., Decoding Europe's new fascination with 'tech sovereignty', in Science Business, 3 September 2020.

KELSEN H, *Lineamenti di dottrina pura del diritto*, 1934, Einaudi (1952).

KELSEN H., Sovereignty and International Law, *Georgetown Law Journal*, vol. 48, no. 4, 1960.

KLAMERT M., Article 16 TFEU, in M KELLERBAUER, M KLAMERT, J TOMKIN (Eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Oxford University Press, 2019.

KLAMERT M., Article 2 TEU, in M KELLERBAUER, M KLAMERT, J TOMKIN (Eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Oxford University Press, 2019.

KOKOTT J., SOBOTTA C., The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International data privacy law*, 2013, Vol. 13, No. 4, pp. 222-228.

KRANENBORG H., Article 2. Material Scope, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020.

KRASNER S.D., Sovereignty, *Foreign Policies*, No. 122, 2001.

KÜHNHARDT L., *European Union – The Second Founding. The Changing Rationale of European Integration*, Nomos, 2008.

KUNER C., Extraterritoriality and International Data Transfers in EU Data Protection Law, in *Legal Studies Research Paper Series* – Paper No. 49/2015, University of Cambridge.

KUNER C., International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR, in *Common Market Law Review*, 55, 2018.

KUNER C., International Organizations and the EU General Data Protection Regulation, University of Cambridge Faculty of Law Research Paper No. 20/2018.

KUNER C., Reality and Illusion in EU Data Transfer Regulation Post Schrems, in *German Law Journal*, Vol. 18, No. 4, 2017.

KUNER C., Article 44. General principle for transfers, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020.

KUNER C., Article 45. Transfers on the basis of an adequacy decision, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020.

KUNER C., Article 46. Transfers subject to appropriate safeguards, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020.

KUNER C., Article 47. Binding corporate rules, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University, 2020.

KUNER C., Article 49. Derogations for specific situations, in in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020.

KUNER C., Article 50. International cooperation for the protection of personal data, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020.

KUNER C., BYGRAVE L.A., DOCKSEY C., Background and Evolution of the EU General Data Protection Regulation (GDPR), in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020.

KUNER C., The GDPR and International Organisations, *American Journal of International Law AJILUnbound*, 114, 2020, pp. 15-19.

KUNER C., The Internet and the Global Reach of EU Law, in CREMONA M., SCOTT J. (Eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, Oxford University Press, 2019.

KUNER C., The Schrems II judgment of the Court of Justice and the future of data transfer regulation, in *European Law Blog*, 17 July 2020.

KUNER C., Schrems II Re-Examined, in *Verfassungsblog*, 25 August 2020.

KWASNY S., Convention 108, a Trans-Atlantic DNA?, in D. SVANTESSON, D. KLOZA (Eds), *Trans-atlantic data privacy relations as a challenge for democracy*, Intersentia, 2017.

LANCHESTER F., Legittimità e legittimazione: la prospettiva del costituzionalista, in *Il Politico*, Vol. 6, No. 4, 1998, pp. 547-565.

LAZZERINI N., *La Carta dei diritti fondamentali dell'Unione europea – I limiti di applicazione*, Franco Angeli, 2018.

LEANERTS K, Some Thoughts on the State of the European Union as a Rights-Based Legal Order, in *Il Diritto dell'Unione europea*, n. 1/2015, pp. 5-24.

LINDAHL H., Sovereignty and Representation in the European Union, in N. WALKER (Ed.) *Sovereignty in transition*, Hart Pulishing, 2003, pp. 115-144.

LINDROOS-HOVINHEIMO S., Who controls our data? The legal reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojavaltuutettu v Jehovan todistajat*, in *Information & Communications Technology Law*, Vol. 28, 2/2019.

LOUGHLIN M., Ten Tenets of Sovereignty, in N. WALKER (Ed.), Sovereignty in Transition, Hart Publishing, 2003, pp. 56-59.

LOWE V., *International Law: A Very Short Introduction*, Oxford University Press, 2015.

LYNSKEY O., *The foundations of EU Data Protection Law*, Oxford University Press, 2015.

MACCORMICK N., Beyond the Sovereign State, in *Modern Law Review*, vol. 56, no. 1, 1993, p. 1-18.

MACCORMICK N., The Maastricht-Urteil: Sovereignty now, *European Law Journal*, 1(2), 1995, 259-266.

MAGEN A., PECH L., The rule of law and the European Union, in MAY C., WINCHESTER A. (Eds), *Handbook on the Rule of Law*, Elgar, 2018, pp. 235-256.

MAHER R., International Relations Theory and the Future of European Integration, in *International Studies Review*, 2019, 0, pp. 1-26.

MANCINI G.F., Europe: The case for Statehood, in *European Law Journal*, vol. 4, no. 1, 1998, pp. 29-42.

MANNERS I., Normative Power Europe: A Contraddiction in Terms?, in *Journal of Common Market Studies*, 2002, Vol 40. No 2.

MANNONI S., Relazioni internazionali, in M. FIORAVANTI (a cura di), *Lo Stato moderno in Europa – Istituzioni e diritto*, Laterza, 2011.

MARRANI D., Dati personali e cybersicurezza: la decisione Breyer della Corte di giustizia, in *SIDIBlog*, Aprile 2017.

MARTINES F., Humans Rights Clauses in EU Agreements, in S. POLI (Ed.), *Protecting Human Rights in the European Union's External Relations*, CLEER PAPERS 2016/5, pp. 37-62.

MASTROIANNI R., Le garanzie dei valori nell'azione esterna e il ruolo della Corte di giustizia, in SCISO E., BARATTA R., MORVIDUCCI C. (a cura di), *I valori dell'Unione europea e l'azione esterna*, Giappichelli, 2016.

MASTROIANNI R., L'effettività della tutela giurisdizionale alla prova della Carta dei diritti fondamentali, in *Liber Amicorum Antonio Tizzano – De la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, Giappichelli, 2018, pp. 586-600.

MASTROIANNI R., Sui rapporti tra Carte e Corti: nuovi sviluppi nella ricerca di un sistema rapido ed efficace di tutela dei diritti fondamentali, in *European Papers*, Vol. 5, 2020, No. 1, pp. 493-522.

MIGLIO A., Enforcing the Right to Be Forgotten Beyond EU Borders, in E. CARPANELLI and N. LAZZERINI (Eds), *Use and Misuse of New Technologies – Contemporary Challenges in International and European Law*, Springer, 2019.

MILANOVIC M., The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa, in *EJIL.Talk!*, May 26, 2021

MOORE D., Article 96. Relationship with previously concluded Agreements, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU Gkeneral Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020.

MOORHEAD T., *The Legal Order of the European Union – The Institutional Role of the Court of Justice*, Routledge, 2014.

NARDONE V., The Passenger Name Record Case: Profiling Privacy and Data Protection Issues in Light of CJEU's Opinion 1/15, in E. CARPANELLI, N. LAZZERINI (Eds), *Use and Misuse of New Technologies – Contemporary Challenges in International and European Law*, Springer, 2019.

NERVI A., Il perimetro del Regolamento europeo: portata applicativa e definizioni, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, 2019.

NINO M., *Terrorismo internazionale, privacy e protezione dei dati personali*, Editoriale Scientifica, 2012.

OETER S., Article 21 TEU [The Principles and Objectives of the Union's External Action], in H.-J. BLANKE, S. MANGIAMELI (Eds), *The Treaty on European Union (TEU) – A Commentary*, Springer, 2013.

OJANEN T., Right-based Review of Electronic Surveillance after *Digital Rights Ireland* and *Schrems* in the European Union, in D. COLE, F. FABBRINI, S. SCHULHOFER (Eds), *Surveillance, Privacy and Trans-Atlantic Relations*, Hart Publishing, 2017.

OLDANI I., The future of data transfer rules in the aftermath of Schrems II, in *SIDIBlog*, ottobre 2020.

OROFINO M., Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione, *MediaLaws*, n. 2/2018.

PALOMBELLA G., Beyond Legality – Before Democracy. Rule of Law Caveats in the EU Two-Level System, in C. CLOSA, D. KOCHENOV (Eds), *Reinforcing Rule of Law Oversight in the European Union*, Cambridge University Press, 2016, pp. 36-58.

PASSAGLIA P., Il sistema delle fonti normative in materia di tutela dei dati personali, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I Dati personali nel diritto europeo*, Giappichelli, 2019, pp. 85-118.

PECH L, *The Rule of Law in the EU: The Evolution of the Treaty Framework and Rule of Law Toolbox*, RECONNECT Working Paper No. 7, March 2020.

PEERS S., PRECHAL S., Article 52, in S. PEERS, T. HERVEY, J. KENNER, A. WARD (Eds), *The EU Charter of Fundamental Rights - A Commentary*, Hart Publishing, 2014.

PELLET A., *Les fondements juridiques internationaux du droit communautaire*, Academy of European Law (Ed.) – Collected Courses of the Academy of European Law, Volume V, Book 2, Kluwer Law International, 1997, pp. 193-271.

PIETROPAOLI S., Ordinamento giuridico e Konkrete Ordnung – Per un confronto tra le teorie istituzionalistiche di Santi Romano e Carl Schmitt, in *Jura Gentium*, n. 2/2012, pp. 1-22.

PISAPIA A., *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli, 2018.

PITEA C., TOMASI L., Articolo 8 – Diritto al rispetto della vita privata e familiare, in S. BARTOLE, P. DE SENA, V. ZAGREBELSKY (a cura di), *Commentario breve alla CEDU - Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali*, CEDAM, 2012, pp. 297-369.

PIZZETTI F., Article 39 TEU [Protection of Individuals with Regard to the Processing of Personal Data by the Member States], in H.-J. BLANKE, S. MANGIAMELI (Eds), *The Treaty on European Union (TEU) – A Commentary*, Berlin - Heidelberg - New York, 2013, pp. 1159-1160.

PIZZETTI F., *Privacy e diritto europeo alla protezione dei dati personali – Dalla Direttiva 95/46 al nuovo Regolamento europeo* – I –, Giappichelli, 2016.

PIZZETTI F., Il futuro dell'Europa di regge sui dati. Pizzetti: "Così l'UE ha cambiato approccio", in *Agenda Digitale*, 5 agosto 2020.

POIARES MADURO M., Three claims of Constitutional Pluralism, in M. AVBELJ, J. KOMÁREK (Eds), *Constitutional Pluralism in Europe and beyond*, Hart Publishing, 2012, pp.67-84.

POLI S., L'evoluzione del controllo giurisdizionale sugli atti PESC intesi a consolidare la rule of law: il caso delle misure restrittive sullo sviamento di fondi pubblici, in *Il Diritto dell'Unione europea*, n. 2/2019, pp. 301-334.

POLLACK M.A, Institutionalism and European Integration, Preliminary draft of a paper to be published in A. WIENER, T. BÖRZEL, T. RISSE (Eds), *European Integration Theory* (3rd edition), 11 July 2018.

POLLACK M.A., Theorizing the European Union: International Organization, Domestic Polity, or Experiment in New Governance?, in *Annual Review of Political Science*, 2005.

POLLICINO O., BASSINI M., Articolo 8, in R. MASTROIANNI, O. POLLICINO, ALLEGREZZA, F. PAPPALARDO, RAZZOLINI (a cura di), *La Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, 2016.

POLLICINO O, Il "senso" della Corte di giustizia per la tutela dei dati personali, in *Liber Amicorum Antonio Tizzano – De la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, Giappichelli, 2018, pp. 751-768.

POLLICINO O., L' "autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale, *Federalismi.it*, n. 19, ottobre 2019.

PSYCHOGIOPOULOU E., The European Court of Human Rights, privacy and data protection in the digital era, in M. BRKAN, E. PSYCHOGIOPOULOU (Eds), *Courts, privacy and data protection in the digital environment*, Elgar, 2017.

QUAGLIONI D., *La sovranità*, Laterza, 2004.

QUINN J., *Google v CNIL*: Circumscribing the Extraterritorial Effect of EU Data Protection Law, in F. FABBRINI, E. CELESTE, J. QUINN (Eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford, 2020.

RICCIO G.M., *Model Contract Clauses* e *Corporate Binding Rules*: valide alternative al *Safe Harbor Agreement*?, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali – Dai "Safe Harbourprinciples" al "Privacy Shield"*, Roma Tre Press, 2016.

RICCIO G.M., PEZZA F., Trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali, in E. TOSI (a cura di), *Privacy Digitale – Riservatezza e protezione dei dati tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, 2019.

RISSE T., Social Constructivism and European Integration, in A. WIENER, T. DIEZ (Eds), *European Integration Theory* (second edition), Oxford University Press, 2009, pp. 144-155.

ROCHE J.-J., *Théories des relations internationales*, 4e édition, Montchrestien, 2001.

RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Il Mulino, 1973.

ROJAS-HUTINEL N., *La séparation du pouvoir dans l'Union européenne*, mare&martin, 2017.

ROMANO S., *L'ordinamento giuridico*, Quodlibet, 2018.

ROSAMOND B., *Theories of European Integration*, MacMillan, 2000.

ROSSI DAL POZZO F., La tutela dei dati personali nella giurisprudenza della Corte di giustizia, in *Eurojus*, 2018, pp. 1-24.

ROSSI E., Forget me…or not? La Corte di giustizia torna sul diritto di farsi dimenticare. Prima lettura di due recenti pronunce sul «diritto all'oblio», in *SidiBlog*, Novembre 2019.

ROSSI L.S., Rango, primato ed effetti diretti della Carta dei diritti fondamentali dell'Unione europea, in *Il Diritto dell'Unione europea*, n. 2/2019, pp. 329-356.

ROVELLI S., Case *Prokuratuur*: Proportionality and the Independence of Authorities in Data Retention, in *European Papers*, Vol. 6, 2021, No. 1.

RUGANI G., La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della Direttiva (UE) 2016/680: frammentazione ed incertezza applicative, in *Freedom, Security & Justice: European Legal Studies*, 2019, n. 1, pp. 75-92.

RUOTOLO G.M., *Scritti di diritto internazionale ed europeo dei dati*, Cacucci editore, 2021.

RUOTOLO G.M., Digital Services Act e Digital Markets Act tra responsabilità dei fornitori e rischi di ne bis in idem, in *SIDIblog*, 29 marzo 2021.

SAJFERT J., Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy, in *European Law Blog*, 26 October 2020.

SAJFERT, J., The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?, in *European Law Blog*, 8 June 2021.

SALERNO G., *European Rule of Law*: un principio in cerca d'autore, in *Federalismi*, 17 giugno 2020.

SAMONTE M., Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law, in *European Law Blog*, 29 October 2019.

SAPIENZA R., Sul margine di apprezzamento statale nel sistema della Convenzione europea dei diritti dell'uomo, in *Rivista di Diritto Internazionale*, LXXIV/ 1991, pp. 573-614.

SAPIENZA R., I 50 anni della Convenzione europea dei diritti dell'uomo, in *Aggiornamenti Sociali*, 6, 2000, pp. 515-523.

SAPIENZA R., *Elementi di diritto internazionale*, Giappichelli, 2002.

SAPIENZA R., Verso la deterritorializzazione del diritto internazionale della transizione infinita. Una premessa schmittiana ad un programma di ricerca, *Fogli di lavoro per il Diritto internazionale*, n. 2.2, 2009.

SAPIENZA R., *Diritto Internazionale – Quattro pezzi facili*, Giappichelli, 2013.

SAPIENZA R., Oltre i territori. Diritto internazionale, giurisdizioni e "nuove geografie", in A. DI STEFANO (a cura di), *Un diritto senza terra? Funzioni e limiti del principio di territorialità nel diritto internazionale e dell'Unione europea*, Atti e contributi del X Incontro di Studio fra i giovani cultori delle materie internazionalistiche – Catania, 24-25 gennaio 2013, I, Giappichelli, 2015, p. 139-142.

SAURON J-L., L'UE: quelle légitimité ? Quel avenir ?, in The Authority of European law: do we still believe in it?, in W. HEUSEL, J-P REGEADE (Eds), *The Authority of EU Law – Do we still believe in it?*, Springer, 2019.

SCHWARTZ P. M., Global Data Privacy: The EU Way, *New York University Law Review*, Vol. 94, No. 4, 2019, pp. 771-818.

SCHWOK R., *Théories de l'intégration européenne – Approches, concepts et débats*, Editions Montchrestien, 2005.

SCISO E., BARATTA R., MORVIDUCCI C. (a cura di), *I valori dell'Unione europea e l'azione esterna*, Giappichelli, 2016.

SCOTT J., Extraterritoriality and Territorial Extension in EU Law, in *American Journal of Comparative Law*, Vol. 62, 2014, pp. 87-126.

SCOTT J., The Global Reach of the EU Law, in M. CREMONA, J. SCOTT (Eds), *EU Law Beyond EU Borders – The Extraterritorial Reach of EU Law*, Oxford University Press, 2019.

SILVA PEREIRA P., The European Union's never-ending search for legitimacy, in W. HEUSEL, J.P. RAGEADE (Eds), The Authority of EU Law, Springer, 2019.

SORO A., La tutela di un diritto fondamentale: un primo bilancio applicativo – Prefazione, in E. TOSI (a cura di), *Privacy Digitale – Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè, 2019.

STROZZI G., MASTROIANNI R., *Diritto dell'Unione europea – parte istituzionale*, Ottava edizione, Giappichelli, 2020.

SVANTESSON D.J.B., Article 3. Territorial scope, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020.

SZYDŁO M., Principles underlying independence of national data protection authorities: *Commission v. Austria*, in *Common Market Law Review*, 50, 2013.

TANZARELLA P., Il margine di apprezzamento, in M. CARTABIA (a cura di), *I diritti in azione – Universalità e pluralismo dei diritti fondamentali delle Corti europee*, Il Mulino, 2007.

TERRASI A., *La protezione dei dati personali tra diritto internazionale e diritto dell'Unione europea*, Giappichelli, 2008.

TERRASI A., *Protection of Personal Data and Human Rights between the ECHR and the EU Legal Order*, in A. CALIGIURI (Ed.), *Legal Technology Transformation. A Practical Assessment*, Editoriale Scientifica, 2020, pp. 21-32.

TIZZANO A. (a cura di), *Trattati dell'Unione Europea*, II edizione, Giuffrè, 2014.

TOKÁR A., Something Happened. Sovereignty and European Integration, in *Extraordinary Times – IWM Junior Visiting Fellows Conferences*, Vol. 11, Vienna 2001.

TOSI E., Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo codice privacy, in E. TOSI (a cura di), Privacy Digitale – Riservatezza e protezione dei dati personali tra GDPR e nuovo codice privacy, Giuffrè Francis Lefebvre, 2019, pp. 1-54.

TOSONI L., BYGRAVE L.A., Article 4. Definitions, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY, L. DRECHSLER (Eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020.

TZANOU M., *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Hart Publishing, 2017.

VAN DER SLOOT B., Legal Fundamentalism: Is Data Protection Really a Fundamental Right?, in LEENES R., VAN BRAKEL R., GUTWIRTH S., DE HERT P. (Eds), *Data Protection and Privacy: (In)visibilities and Infrastructures*, Springer, 2017, pp. 3-30.

VEDASCHI A., MARINO NOBERASCO G., From DRD to PNR: Looking for a New Balance Between Privacy and Security, in D. D. COLE, F. FABBRINI AND S. SCHULHOFER (Eds), *Surveillance, Privacy and Transatlantic Relations,* Hart Publishing, 2017, pp. 67–88.

VILLANI U., Una rilettura della sentenza Van Gend&Loos dopo cinquant'anni, *Studi sull'integrazione europea*, n. 2/2013.

VITALE G., Il principio di effettività della tutela giurisdizionale nella Carta dei diritti fondamentali, in *Federalismi.it*, 28 febbraio 2018.

VON DANWITZ T., The Rule of Law in the Recent Jurisprudence of the ECJ, in *Fordham International Law Journal*, Vol. 37, 5, 2014, pp. 1311-1348.

WALKER N., The Idea of Constitutional Pluralism, in EUI Working Paper LAW, No 2002/1.

WALKER N., Late Sovereignty in the European Union, in N. WALKER (Ed.), *Sovereignty in transition – essays in European law*, Hart Publishing, 2003, pp. 3-32.

WARREN S. D., BRANDEIS L D., *The right to privacy*, Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890).

WATT E., Much Ado About Mass Surveillance – the ECtHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK, in *Strasbourgobservers*, June 28, 2021.

WEILER J.H.H., The Transformation of Europe, in *The Yale Law Journal*, Vol. 100, 1991.

WEILER J.H.H., After Maastricht: Community legitimacy in Post-1992 Europe, in W.J. Adams (ed.), Singular Europe: Economy and Polity of the European Community After 1992, *The University of Michigan Press*, 1995.

WEILER J.H.H., Does Europe Need a Constitution? Demos, Telos and the German Maastricht Decision, in *European Law Journal*, vol. 1, no. 2, 1995.

WEILER J.H.H., HALTERN U., MAYER F., *European democracy and its critique – Five uneasy pieces*, in The Jean Monnet Centre for International and Regional Economic Law&Justice, September 1995.

WEILER J.H.H., HALTERN U. R., The autonomy of the community legal order-through the looking glass, in *Harvard International Law Journal*, 37(2), 1996.

WEILER J.H.H., Europe: The Case Against the Case for Statehood, in *European Law Journal*, vol. 4, no. 1, 1998, pp. 43-62.

WEILER J.H.H., In the face of crisis: Input Legitimacy, Output Legitimacy and the Political Messianism of European Integration, in *Journal of European Integration*, 34:7, 2012.

WEILER J.H.H., Epilogue: Living in a glass house – Europe, Democracy and the Rule of Law, in C. CLOSA, D. KOCHENOV (Eds), *Reinforcing Rule of Law Oversight in the European Union*, Cambridge University Press, 2018.

WEILER J.H.H., The Authority of European law: do we still believe in it?, in W. HEUSEL, J-P REGEADE (Eds), The Authority of EU Law – Do we still believe in it?, Springer, 2019.

WHITMAN J. Q., The Two Western Cultures of Privacy: Dignity Versus Liberty, *The Yale Law Journal*, Vol. 113, 2003.

WIENER A., DIEZ T., Introducing the Mosaic of Integration Theory, in A. WIENER, T. DIEZ (Eds), *European Integration Theory* (second edition), Oxford University Press, 2009, pp. 1-24.

WILKINSON M., Beyond the Post-Sovereign State? The Past, Present and Future of Constitutional Pluralism, in *Cambridge Yearbook of European Legal Studies*, 21, (2019), pp. 6-23.

WOODS L., Data protection: the CJEU clarifies the applicable law and jurisdiction, in *EU Law Analysis*, 13 October 2015.

WOODS L., Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber), in *EU law Analysis*, 21 December 2016.

WOODS L., Analysis of the ECtHR judgment in Big Brother Watch: part 2, in *EU Law Analysis*, 20 September 2018.

WOODS L., "You Were Only Supposed to Blow the Bloody Doors Off!": Schrems II and external transfers of personal data, in *Eu Law Analysis*, 16 July 2020.

WOODS L., Who has jurisdiction over Facebook Ireland? The CJEU rules on the GDPR 'one stop shop', in *EU Law Analysis*, 16 June 2021.

WOODS L., Big Brother Watch v UK: the ECtHR Grand Chamber rules on mass surveillance, in *EU Law Analysis*, 17 June 2021.

ZALNIERIUTE M., A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence, in *EJIL:Talk!*, June 4, 2021.

ZALNIERIUTE M., A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union, in *Modern Law Review*, Vol 85(1) 2022 *forthcoming*, [2021] UNSWLRS 34.

ZENO-ZENCOVICH V., Articolo 8 – Diritto al rispetto della vita privata e familiare, in S. BARTOLE, B. CONFORTI, G. RAIMONDI (a cura di), *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, CEDAM, 2001, pp. 307-318.

ZENO-ZENCOVICH V., Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali – dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TRE-Press, 2016, pp. 7-22.

ZUBOFF S., *Il capitalismo della sorveglianza – il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, 2019.

Indice dei casi

Corte Internazionale di Giustizia

Corte di giustizia dell'Unione europea

Corte di giustizia

Causa C-524/06, *Heinz Huber c. Bundesrepublik Deutschland*, sentenza del 16 dicembre 2008;

Causa C-518/07, *Commissione c. Germania*, sentenza del 9 marzo 2010;

Causa C-28/08 P, *Commissione europea c. The Bavarian Lager Co. Ltd*, sentenza del 29 giugno 2010;

Causa C-614/10, *Commissione c. Austria*, sentenza del 16 ottobre 2012;

Cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd*, sentenza del 8 aprile2014;

Causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, sentenza del 13 maggio 2014;

Causa C-212/13, *František Ryneš c. Úřad pro ochranu osobních údajů*, sentenza del 11 dicembre 2014;

Parere n. 2/13, *Adesione dell'Unione europea alla CEDU*, 18 dicembre 2014;

Causa C-230/14, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, sentenza del 1 ottobre 2015;

Causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, sentenza del 6 ottobre 2015;

Causa C-191/15, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, sentenza del 28 luglio 2016;

Causa C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland*, sentenza del 19 ottobre 2016;

Cause riunite C-203/15 e C-698/15, *Tele2 Sverige* e *Watson e a.*, sentenza del 21 dicembre 2016;

Causa C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, sentenza del 9 marzo 2017;

Parere n. 1/15, *Accordo PNR UE-Canada*, 26 luglio 2017;

Causa C-434/16, *Peter Nowak c. Data Protection Commissioner*, sentenza del 20 dicembre 2017;

Causa C-73/16, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky*, sentenza del 27 dicembre 2017;

Causa C-498/16, *Maximilian Schrems c. Facebook Ireland Limited*, sentenza del 25 gennaio 2018;

Causa C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, sentenza del 5 giugno 2018;

Causa C-25/17, *Jehovan todistajat*, sentenza del 10 luglio 2018;

Causa C-207/16, *Ministerio Fiscal*, sentenza del 2 ottobre 2018;

Parere n. 1/17, *Accordo CETA UE-Canada*, 30 aprile 2019;

Causa C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, sentenza del 24 settembre 2019;

Causa C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, sentenza del 3 ottobre 2019;

Causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems*, sentenza del 16 luglio 2020;

Causa C-623/17, *Privacy International*, sentenza del 6 ottobre 2020;

Cause riunite C-511/18, C-512/18, C-520/18, *La Quadrature du Net e altri*, sentenza del 6 ottobre 2020;

Causa C-746/18, *Procedimento penale a carico di H.K (Prokuratuur)*, sentenza del 2 marzo 2021;

Causa C-505/19, *WS c. Bundesrepublik Deutschland*, sentenza del 12 maggio 2021;

Causa C-645/19, *Facebook Ireland Limited*, sentenza del 15 giugno 2021.

Tribunale

Causa T-194/04, *Bavarian Lager*, sentenza del 8 novembre 2007

Causa T-670/16, *Digital Rights Ireland Ltd c. Commissione*, ordinanza del 22 novembre 2017;

Causa T-738/16, *La Quadrature du Net e.a. c. Commissione*, ordinanza del 14 dicembre 2020.

Conclusioni di Avvocati Generali

AG A. Tizzano, causa C-101/01, *Bodil Lindqvist c. Åklagarkammaren i Jönköping*, 19 settembre 2002;

AG A. Tizzano, causa C-465/00, *Rechnungshof c. Österreichischer Rundfunk e a.* e cause riunite C-138/01 e C-139/01, *Neukomm e Lauermann c. Österreichischer Rundfunk*, 14 novembre 2002;

AG E. Sharpston, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR* e *Harmurt Elfert c. Land Hessen*, 17 giugno 2010;

AG J. Kokott, causa C-137/12, *Commissione c. Consiglio* (*Convenzione sui servizi ad accesso condizionato*), 27 giugno 2013;

AG P. Cruz Villálon, C-230/14, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 25 giugno 2015;

AG M. Szpunar, C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, 10 gennaio 2019;

AG M. Szpunar, C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, 4 giugno 2019.

Corte europea dei diritti umani

Ricorsi n. 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64, *Belgian linguistic*, 23 luglio 1968;

Ricorsi n. 2832- 2835- 2899/66, *De Wilde, Ooms, Versyp c. Belgio*, 18 giugno 1971;

Ricorso n. 5029/71, *Klass e a. c. Germania*, 6 settembre 1978;

Ricorso n. 7525/76, *Dudgeon c. Regno Unito*, 22ottobre 1981;

Ricorso n. 8691/79, *Malone c. Regno Unito*, 2 agosto 1984;

Ricorso n. 9248/81, *Leander c. Svezia*, 26 marzo 1987;

Ricorso n. 10454/83, *Gaskin c. Regno Unito*, 7 luglio 1989;

Ricorso n. 11801/85, *Klusin c. Francia*, 24 aprile 1990;

Ricorso n. 27798/95, *Amann c. Svizzera*, 16 febbraio 2000;

Ricorso n. 28341/95, *Rotaru c. Romania*, 4 maggio 2000;

Ricorso n. 48539/99, *Allan c. Regno Unito*, 5 novembre 2002;

GC, ricorsi nn. 30562/04 e 30566/04, *S&Maper c. Regno Unito*, 4 dicembre 2008;

Ricorso n. 26839/05, *Kennedy c. Regno Unito*, 18 agosto 2010;

GC, ricorso n. 47143/06, *Zakharov c. Russia*, 4 dicembre 2015;

Ricorso n. 37138/14, *Szabó e Vissy c. Ungheria*, 12 gennaio 2016;

Ricorsi n. 58170/13, 62322/14 e 24960/15, *Big Brother Watch and others v. UK*, 13 settembre 2018;

GC, ricorsi nn. 58170/13, 62322/14 e 24960/15, *Big Brother Watch e altri*, 25 maggio 2021;

GC, ricorso n. 35252/08, *Centrum for Rattvisa c. Svezia*, 25 maggio 2021.

Indice dei principali documenti

Consiglio d'Europa

Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, n. 5, Roma, 4 novembre 1950;

Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, n. 108, Strasburgo, 28 gennaio 1981;

Convenzione sulla criminalità informatica, n. 185, Budapest, 23 novembre 2001;

Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici, n. 189, Strasburgo, 28 gennaio 2003;

Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, n. 223, Strasburgo, 10 ottobre 2018.

Unione europea

Disposizioni normative

Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23.11.1995 (non più in vigore, dal 24.05.2018);

Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati, GU L 77 del 27.3.1996;

Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, GU L 167 del 22.06.2001;

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), GU L 201 del 31.7.2002;

Direttiva 2004/48/CE del Parlamento europeo e del Consiglio del 29 aprile 2004 sul rispetto dei diritti di proprietà intellettuale, GU L 157 del 30.4.2004;

Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, GU L 105 del 13.4.2006 (non più in vigore);

Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, GU L 337 del 18.12.2009;

Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio – GU L 119 del 4.5.2016;

Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, GU L 119/132 del 4.5.2016;

Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione – GU L 194 del 19.7.2016;

Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio, GU L 88 del 31.3.2017;

Direttiva (UE) 2017/1564 del Parlamento europeo e del Consiglio, del 13 settembre 2017, relativa a taluni utilizzi consentiti di determinate opere e di altro materiale protetto da diritto d'autore e da diritti connessi a beneficio delle persone non vedenti, con disabilità visive o con altre difficoltà nella lettura di testi a stampa, e che modifica la direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione – GU L 242 del 20.9.2017;

Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico PE/28/2019/REV/1, GU L 172 del 26.6.2019.

Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati – GU L 8 del 12.1.2001;

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (Testo rilevante ai fini del SEE) PE/31/2018/REV/1, GU L 295 del 21.11.2018;

Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, PE/53/2018/REV/1, GU L 303 del 28.11.2018;

Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), GU L 151 del 7.06.2019.

Altri documenti

WP A29

Working Document WP 74, Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Adopted on 3 June 2003;

Parere 4/2007 - WP 136, sul concetto di dati personali, adottato il 20 giugno 2007;

Parere 1/2014 - WP 211, sull'applicazione dei principi di necessità e proporzionalità nell'azione di contrasto, adottato il 27 febbraio 2014;

Parere 05/2014 - WP 216, sulle tecniche di anonimizzazione, adottato il 10 aprile 2014;

Linee Guida sull'attuazione della sentenza della Corte di giustizia dell'Unione europea nel caso C-131/12 "Google Spain e Inc. contro Agencia Espanola de la Proteccion de datos (AEPD) e Mario Costeja Gonzalez", WP 225, adottate il 26 novembre 2014;

Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237, Adopted on 13 April 2016;

Documento di lavoro WP 254 rev.01, sui criteri di riferimento per l'adeguatezza, 18/IT, 28 novembre 2017, versione emendata e adottata il 6 febbraio 2018,.

EDPB

Linee guida 2/2018, sulle deroghe di cui all'articolo 49 del regolamento 2016/679, adottate il 25 maggio 2018;

EU - U.S. Privacy Shield - Second Annual Joint Review, Adopted on 22 January 2019;

Linee-guida 3/2018, sull'ambito di applicazione territoriale del RGPD (articolo 3), Versione 2.1 – adottate il 12 novembre 2019;

Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020;

Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, 17 July 2020;

Decisione 01/2020 relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente Twitter International Company ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD, adottata il 9 novembre 2020;

Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, adottate il 10 novembre 2020;

Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza, adottate il 10 novembre 2020;

Parere congiunto 1/2021 dell'EDPB e del GEPD sulla decisione di esecuzione della Commissione europea relativa alle clausole contrattuali tipo tra titolari e responsabili del trattamento, adottato il 14 gennaio 2021;

Parere congiunto 2/2021 dell'EDPB e del GEPD sulla decisione di esecuzione della Commissione europea relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi, adottato il 14 gennaio 2021;

Opinion 14/2021 *regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, Adopted on 13 April 2021;

Opinion 15/2021 *regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom*, Adopted on 13 April 2021;

Parlamento europeo

Risoluzione sulla tutela dei diritti degli individui di fronte al crescente sviluppo tecnico nel settore dell'informatica, GU C 87/39, 5 aprile 1982;

Relazione su un approccio globale alla protezione dei dati personali nell'Unione europea, 15 marzo 2011, (2011/2025(INI));

Risoluzione sull'adeguata protezione dei dati personali da parte del Regno Unito, 21 maggio 2021 (2021/2594(RSP)).

Commissione europea

Communication of the Commission to the Council, *Community Policy on Data Processing*, SEC(73) 4300 final, Brussels, 21 November 1973;

Raccomandazione concernente una convenzione del Consiglio d'Europa sulla protezione delle persone per quanto riguarda l'elaborazione automatica dei dati a carattere personale, 81/679/CEE, 29 luglio 1981;

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni - *Un approccio globale alla protezione dei dati personali nell'Unione europea* /* COM/2010/0609 def. */, Bruxelles, 4 novembre 2010;

Comunicazione della Commissione, EUROPA 2020 – *Una strategia per una crescita intelligente, sostenibile e inclusiva*, COM/2010/2020 def, Buxelles, 3 marzo 2010;

Comunicazione della Commissione al Parlamento europeo, al Consiglio, *Scambio e protezione dei dati personali in un mondo globalizzato*, COM (2017) 7 final, 10 gennaio 2017;

Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM(2017) 10 final, 2017/0003 (COD);

Proposta di Decisione del Consiglio che autorizza gli Stati membri a firmare, nell'interesse dell'Unione europea, il protocollo che modifica la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STE 108) COM/2018/449 final - 2018/0237 (NLE);

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economicoe sociale europeo e al Comitato delle Regioni, *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final, 19 febbraio 2020;

Communication from the Commission, *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*, C(2020) 2523 final, 16 April 2020;

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economicoe sociale e al Comitato delle Regioni, *Relazione sullo Stato di diritto 2020 – La situazione dello Stato di diritto nell'Unione europea*, COM(2020) 580 final, Bruxelles, 30 settembre 2020;

Proposta di Regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (*Atto sulla governance dei dati*), COM(2020) 767 final, 25 novembre 2020;

Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (*legge sui servizi digitali*) e che modifica la direttiva 2000/31/CE, COM(2020) 825 final, 15 dicembre 2020;

Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (*legge sui mercati digitali*), COM(2020) 842 final, 15 dicembre 2020;

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM/2021/118 final, 9 marzo 2021;

Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (*Legge sull'intelligenza artificiale*) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final, 21 aprile 2021;

Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, C/2021/3972.

Consiglio dell'Unione europea

Conclusions on the Communication from the Commission to the European Parliament and the Council - A comprehensive approach on personal data protection in the European Union, 3071st JUSTICE and HOME AFFAIRS Council meeting Brussels, 24 and 25 February 2011.

Consiglio europeo

Special meeting of the European Council – 1 and 2 October 2020, Conclusions, Brussels, 2 October 2020, EUCO 13/20, CO EUR 10, CONCL 6.