Tesi di Dottorato di ricerca in Scienze Giuridiche
(Università di Siena – Università di Foggia)
Ciclo XXXI

IL DIRITTO ALL'OBLIO E I SUOI CONFINI:
quando il dovere del ricordo annebbia l'ombra del tempo

Tutor: Ch.mo Prof. Francesco Astone

Dottoranda: Francesca Miccoli

... A mamma,

stella polare del mio cammino.

«La felicità è l'oblio.

Chi non sa fermarsi sulla soglia dell'istante,

dimenticando tutto il passato,

non saprà mai in che cosa consista la felicità;

peggio: non farà mai nulla che renda felici gli altri».

Friedrich Wilhelm Nietzsche

INDICE

SEZIONE II: Il trattamento dei dati personali nell'evoluzione normativa europea, dalla Convenzione di Strasburgo 108/1981: un lento affermarsi, nel quadro europeo, del diritto alla protezione dei dati personali

1) Il ruolo del ricordo e l'importanza dell'oblio: il diritto alla memoria e l'opposto diritto alla cancellazione dei dati non più necessari
2) Le prime leggi di protezione dei dati personali in Europa
3) La stigmatizzazione del diritto nella nuova normativa comunitaria: la centralità della Direttiva 95/46 CE ed il riconoscimento nel diritto positivo europeo del diritto all'oblio
4) Il diritto alla protezione dei dati personali nel panorama normativo nazionale
5) La difficoltà di capire l'importanza della nuova normativa di protezione dei dati in molti Stati membri e in particolare in Italia
6) La Carta di Nizza e il Trattato sul Funzionamento dell'Unione Europea
7) Gli esiti dirompenti della sentenza CGUE, C/131/12 del 13 maggio 2014, in materia di trattamento dati ed oblio
8) Il diritto all'oblio e al trattamento dei dati personali nelle Linee Guida del WP29

SEZIONE III: Le difficoltà nel garantire il diritto alla protezione dei dati a seguito dell'affermazione delle più recenti innovazioni tecnologiche ed informatiche

1) Il diritto alla protezione dei dati nella dialettica e interazione con i social network
2) La tutela dei dati e delle informazioni personali in Google
3) La sfida lanciata al diritto alla protezione dei dati dai nuovi servizi offerti dalla Rete.
   3.1) Il Cloud Computing
      3.1.1) Vantaggi e criticità del Cloud Computing in materia di protezione dei dati personali
   3.2) L'IOT: Internet of Things
   3.3) 'La smart grid' e la tutela dei dati personali
   3.4) I contatori intelligenti
   3.5) Reperimento dei dati in Rete e comunicazioni indesiderate: lo SPAM
   3.6) Il fenomeno del Telemarketing
   3.7) La regolamentazione in materia di cookie

CAPITOLO SECONDO

LA LIBERTA' DI INFORMAZIONE, QUALE DIRITTO FONDAMENTALE SPETTANTE ALLA COLLETTIVITA', ALLA LUCE DEL REGOLAMENTO EUROPEO 2016/679

SEZIONE I: Il nuovo Regolamento Europeo sulla protezione dei dati personali: un ponte tra presente e futuro

9) Un’analisi critica: l’ambiguità del testo e i problemi applicativi
10) Il Consiglio d’Europa, nell’ottica del Regolamento 2016/679 UE, aggiorna la Convenzione 108/1981

SEZIONE II: Il diritto all’esercizio delle libertà fondamentali spettante alla collettività ed il diritto all’oblio: forme di tensione

1) Le tensioni tra il diritto alla protezione dei dati personali e la libertà di espressione e di informazione
2) Applicabilità ai motori di ricerca dell’eccezione giornalistica
3) La libertà di stampa e il diritto all’oblio: premessa
4) La libertà di stampa nelle sue estrinsecazioni del diritto ad informare e ad essere informati:
   a) il diritto ad informare
   b) il diritto ad essere informati e il diritto di accesso alle informazioni
5) Il diritto di cronaca e il diritto all’oblio: confini ridisegnati dalla sentenza CEDU ‘Affaire M.L. ET W.W c/ Allemagne’ del 28 giugno 2018 e la palese distorsione del diritto all’oblio operata dalla Corte di Cassazione con la pronuncia 24 giugno 2016, n. 13161.
6) La ricerca di un giusto equilibrio tra tutela dei dati personali e libertà d’informazione estrinsecantesi nell’attività giornalistica:
   a) verità oggettiva della notizia pubblicata
   b) continenza della notizia
   c) interesse pubblico alla conoscenza dei fatti
7) I criteri utili per un corretto bilanciamento tra diritto all’oblio e diritto di cronaca, espressi dai giudici di legittimità nell’Ordinanza del 20 marzo 2018, n. 6919 e i dubbi manifestati dalla III Sezione della Suprema Corte, nell’Ordinanza di rimessione alle Sezioni Unite del 5 novembre 2018, n. 28084
8) I poteri del Garante in materia di trattamento dei dati per finalità giornalistiche

CAPITOLO TERZO

I 'DIRITTI DIMENTICATI' DAL LEGISLATORE EUROPEO: LA TUTELA DELLA MEMORIA STORICA E DEI TERZI INTERESSATI AL RICORDO

SEZIONE I: La tutela della memoria storica collettiva a presidio dei diritti alla conoscenza e all'informazione

1) L'esercizio del diritto all'oblio e il vulnus nella memoria collettiva
   1.1) La memoria storica prevale sul diritto all'oblio di un ex terrorista
2) La Rete come bene pubblico
3) Il dato: un bene giuridico/economico
4) Opinioni discordi in merito all'immortalità o vita a tempo determinato del dato immesso in Rete
   4.1) La difficoltosa tutela della memoria storica: la "Digital Preservation" e l'ambizioso progetto "Internet Archive"
   4.2) Morte dell'oblio o tutela solo provvisoria?
5) Le ragioni socio-economiche che impedirebbero il decollo del diritto all'oblio
6) La nuova Governance europea in materia di protezione dei dati personali: le ragioni politiche alla base del Regolamento europeo 2016/679

SEZIONE II: 'Terzi interessati al diritto alla memoria' dimenticati dal Legislatore europeo: diritti e tutele.

La de-indicizzazione dei dati e le possibili soluzioni alternative

Premessa

1) Nozione di terzo/destinatario e di destinatario/terzo
2) Titolare del sito sorgente: "terzo" interessato alla permanenza della notizia in Rete?
3) Possibili soluzioni utili a tutelare indirettamente il diritto alla memoria dei terzi
   3.1) La possibilità di disporre di 15 millimetri di buona memoria
   3.2) L'opportunità per il motore di ricerca di garantire una search neutrality
   3.3) La possibilità di disporre di uno spazio reputazionale
   3.4) Le tecniche di anonimato e la pseudonimizzazione dei dati

INTRODUZIONE

Il diritto all'oblio, quale pretesa a riappropriarsi della propria storia personale, a recuperare il dominio sui fatti personali, dopo che questi siano stati legittimamente divulgati, e a reimpadronirsi del potere di disporne, dopo un lungo e tortuoso cammino, nel corso del quale un profondo e attento contributo è stato fornito dal lavoro svolto dalla giurisprudenza, non solo di legittimità, e dalla dottrina, ha finalmente visto un riconoscimento legislativo espresso, a livello europeo, nell'art. 17 GDPR 2016/679 che ne ha definitivamente sancito la vigenza, perimetrandone in maniera puntuale l'estensione, al fine di proteggere gli interessi di tutte le parti coinvolte nella dialettica giuridica.

Alcuni studiosi sostengono, da tempo, che bisognerebbe preoccuparsi meno di come ricordare e più di come dimenticare. In tempi ormai lontani, l'inadeguatezza biologica della memoria umana era in realtà un pregio e sicuramente semplificava le relazioni umane e sociali: le indiscrezioni passate, gli errori, i gossip, i motivi di conflitto erano di solito smarriti in un arco temporale alquanto ridotto, consentendo la possibilità di superare le imperfezioni nelle varie vite e di ricominciare, o semplicemente, di lasciarsi alle spalle un passato non più rilevante.

La grande opportunità, concessa all'uomo dalla Natura, di poter perdere conoscenza e memoria del ricordo è stata inesorabilmente erosa con l'avvento delle moderne tecnologie: caselle di posta elettronica, archivi online, social network costituiscono sempre più supporti infallibili per la memoria umana miseramente limitata, sicché l'informazione non sarà più perduta, seppur non incasellata nelle anguste maglie del ricordo. E', pertanto, sempre più complesso per l'uomo redimersi da un passato scomodo e doloroso, sempre pronto a raggiungerlo, azzerando limiti di spazio e tempo.

Eppure, in alcuni ambiti, si pensi a quello penale, il dimenticare non è solo considerato accettabile e socialmente utile, ma è ritenuto vitale. Le annotazioni di reati piuttosto modesti, sono, di solito, rimosse dai documenti ufficiali dopo un certo periodo, così come piccole infrazioni commesse da minori vengono cancellate prima che diventino adulti. La logica sottesa a tali previsioni è sicuramente condivisibile: le imperfezioni di gioventù e le infrazioni meno pericolose non possono, né devono, impedire all'uomo di redimersi, abbandonare un passato non propriamente edificante e reintegrarsi in società, fornendo

un'immagine edulcorata di sé, più vicina alla sua nuova e mutata personalità. Ma la tecnologia sempre più difficilmente offre questa seconda possibilità, determinando l'immortalità digitale, che consente di essere ricordati per sempre, superando il limite dei pochi ricordi che la mente umana è in grado di trattenere ed affidandoli a computer ed intelligenza artificiale, in grado di rimpolpare, aggiornare, rinnovare e riproporre costantemente tali informazioni.

A fronte dell'incedere incalzante della tecnologia, l'affermazione del diritto all'oblio è stata oggetto di un lungo processo evolutivo che ne ha comportato l'espansione, per cui, dall'iniziale interesse della persona a non subire lesioni alla propria sfera personale, causate dalla reiterazione della pubblicazione del contenuto di una notizia, legittimamente pubblicata in passato, ma successivamente priva di un interesse pubblico tale da giustificarne un'ulteriore diffusione (paladino quindi della identità e dignità della persona), si è passati al diritto all'autodeterminazione informativa e protezione dei dati personali, onde apprestare idonee garanzie al soggetto, cui i dati si riferiscono, di poter esercitare in ogni momento, il controllo sugli stessi, ivi compreso il potere di modificare il flusso e la direzione della loro circolazione.

Il *novum* del contenuto del diritto all'oblio, rispetto alla sua accezione iniziale, è, senza dubbio, proiezione e conseguenza dell'avvento di Internet, e, più in generale, delle tecnologie informatiche più avanzate, che hanno reso possibile a chiunque l'inserimento di dati e informazioni personali su piattaforme digitali, più o meno consapevoli della loro contestuale circolazione e fruizione da parte di chiunque, in tempo reale e senza limiti di spazio. Dati immediatamente ingoiati dai motori di ricerca per essere perennemente riproposti, in una dimensione atemporale, come se si vivesse sempre in un eterno presente/passato.

Il riconoscimento e la relativa tutela giuridica del 'diritto a dimenticare' sono volti sicuramente ad apprestare tutela tanto al protagonista di vicende ormai coperte dalla polvere del tempo ma che, in un lontano passato, hanno interessato la cronaca, quanto al titolare di dati e informazioni, dallo stesso e da terzi immessi nei circuiti della Rete, affinché non ne perda la gestione, nei limiti e con il bilanciamento del diritto all'informazione e alla conoscenza di quei dati, spettante alla collettività.

Per cui, ogniqualvolta il diritto al silenzio del protagonista dei fatti di cronaca o del titolare delle informazioni, dovesse collidere con l'interesse ad informare, informarsi ed essere

informati della collettività, interesse che, tra l'altro, oltre ad essere costituzionalmente garantito, rappresenta la massima espressione di democrazia di uno Stato di diritto, si presenta come indispensabile l'opera di bilanciamento tra interessi contrapposti, di uguale spessore e rango costituzionale.

All'esito dell'opera di bilanciamento si avrà la prevalenza dell'uno o del contrapposto interesse, in considerazione della scelta operata dal Legislatore, oggettivatasi nel porre al centro del sistema giuridico la 'persona' nella sua dimensione individuale e sociale, con l' ovvia conseguenza che tutti i diritti e le libertà, riconosciuti dalla Carta costituzionale o da altre disposizioni di legge, debbano essere finalizzati al suo sviluppo e la consapevolezza che tra quei diritti non possa esservi in alcun modo confliggenza, ma integrazione, in quanto tutti convergenti verso la medesima finalità, quale quella di consentire il pieno sviluppo della persona.

La legislazione comunitaria e quella nazionale sono state attente nel delineare le responsabilità e le tutele spettanti ai vari attori e protagonisti del diritto all'oblio, avendo previsto una normativa via via più attenta e minuziosa, tanto per i soggetti titolari della manipolazione delle informazioni, che dei destinatari, vittime della 'gogna mediatica'.

Non risultano, per contro, disposizioni normative dirette ad apprestare tutela agli eventuali 'controinteressati', ossia agli individui che dalla reiterazione della riproposizione, anche a distanza di tempo, di notizie ormai archiviate, ne trarrebbero vantaggio, perché il fatto di cronaca li ha visti positivamente protagonisti.

Il taglio del link alla notizia, così come stabilito dalla CGUE nel 2014, sentenza C-131 Costeja Gonzales, poi confermato dal legislatore comunitario, sebbene nei limiti e nel rispetto dei paletti stabiliti dall'art. 17 RGPD 2016/679, senza dubbio non gioverebbe loro perché farebbe cadere nell'oblio comportamenti e azioni meritevoli sempre e comunque di memoria.

La posizione di questi soggetti, interessati al diritto alla memoria, non ha destato l'interesse degli operatori tecnici e/o giuridici che, pertanto, non si sono prodigati nel cercare soluzioni tecnico/informatiche o forme di tutela giuridica, anche solo risarcitoria, che potessero salvaguardare il loro diritto a 'non vedersi dimenticati'.

Il lavoro, oltre a delineare la nuova dimensione giuridica europea del diritto all'oblio e la sua estrinsecazione dinamica, quale diritto alla protezione dei dati personali, è volto ad individuare eventuali forme di tutela tecnica, ed in ultima analisi giuridica, per i

‘protagonisti positivi’ di vicende passate che potrebbero altrimenti essere definitivamente coperte dalla fitta coltre del tempo.

CAPITOLO PRIMO

DAL DIRITTO A DIMENTICARE AL DIRITTO ALL'AUTODETERMINAZIONE E PROTEZIONE DEI DATI PERSONALI: IL VOLTO DINAMICO DEL DIRITTO ALL'OBLIO

SEZIONE I: L'evoluzione dinamica del diritto all'oblio

1) La nascita di un diritto tra riservatezza e diritto di cronaca

Il diritto all'oblio, nato dalla necessità di offrire tutela alla dignità della persona, a fronte dell'esercizio dei fondamentali diritti di libertà d'informazione, stampa e manifestazione del pensiero, è stato inizialmente ritenuto una costola del diritto alla riservatezza, tanto che, nelle prime controversie aventi ad oggetto la sua lesione, i ricorrenti si sono visti riconoscere una tutela cautelare, ma in forza della violazione del 'diritto al riserbo', piuttosto che di quello ad essere dimenticati[1], anche se parte della dottrina, già dagli anni '90 del secolo scorso, ha fatto propria l'opinione secondo cui " il diritto all'oblio, sebbene appartenga alla ragioni e alle regioni del diritto alla riservatezza, e pur presentando alcuni argomenti comuni a quella, non è tuttavia sovrapponibile al diritto al riserbo, poiché presenta la specifica caratteristica di aver ad oggetto la nuova pubblicazione di notizie già pubblicate in passato e che per questo erano già fuori dall'area della riservatezza[2].

Due diritti contigui ma differenti: il diritto alla riservatezza, volto ad impedire la divulgazione di notizie e fatti appartenenti alla sfera intima della persona, non destinati ad essere resi noti e la cui diffusione sarebbe illecita fin dall'origine, uno *ius ad excludendi alios* dall'intrusione nella propria sfera privata; il diritto all'oblio, un diritto volto ad impedire che fatti, già resi di pubblico dominio (e quindi sottratti al riserbo),

---

[1] Controversia tra la RAI e Trigona, Pretura di Roma, 25 gennaio 1979, in *Riv. dir. comm.,* 1979, II, 253, con nota di NUZZO. Nella pronuncia la Pretura di Roma ha avuto modo di affermare che «*la tutela della riservatezza trova precisi limiti in relazione all'interesse generale, nell'attività di cronaca, nell'indagine storica e nell'elaborazione creativa di vicende già note*». Solo quest'ultimo era il punto che presentava un riferimento al diritto all'oblio.

[2] G. B. FERRI, *Diritto all'Informazione e diritto all'oblio*, in *Riv. Dir. Civ.*, 1990, I, 808. Per l'Autore «*ciò spiega come gli argomenti utilizzabili in tema di oblio sono necessariamente comuni a quelli che emergono con riguardo alla riservatezza*». Due tematiche contigue, quelle della riservatezza e dell'oblio, che ripropongono un comune tema di fondo, ossia il rapporto tra riserbo e notizia. Anche l'oblio vede, come suo interlocutore naturale e non antagonista, il diritto di cronaca, entrambi funzionali allo sviluppo della persona.

possano essere rievocati, richiamando su di essi, ora per allora, l'attenzione del pubblico e riproiettando la persona, all'improvviso e senza il suo consenso, verso una nuova notorietà indesiderata. Azionando la tutela dell'oblio, l'individuo verrebbe a chiedere di non infrangere quella nuova identità che si è ricostruito con l'aiuto del tempo, che ne ha sbiadito, se non cancellato, i ricordi.

Due diritti quindi, autonomi, ma non del tutto separati[3], legati da un filo sottile che, muovendo dal riserbo, giunge all'oblio ed ulteriormente collegati dal condiviso limite dell'esercizio dei diritti di cronaca e di informazione. Tanto il diritto al riserbo, quanto quello ad essere dimenticati, infatti, vedono, quale limite naturale, "l'interesse pubblico alla conoscenza di fatti oggettivamente rilevanti per la collettività[4]", sicché, in forza dell'esigenza di tutela della reputazione e dell'identità personale dei protagonisti di fatti e accadimenti, l'intrusione nella loro vita privata sarebbe giustificata solo dalla presenza di un interesse pubblico alla conoscenza di quei fatti e di quegli accadimenti.

Per cui, se è vero che la collettività vanta il diritto ad un'informazione tempestiva, finalizzata a conoscere l'accaduto in tempo reale e con completezza, allorquando informata, il suo interesse cessa, e la reiterata riproposizione dell'accadimento non solo sarebbe inutile, dal momento che la collettività ne sarebbe già in possesso, ma anche dannosa per i protagonisti in negativo della vicenda che, in tal modo, potrebbero subire un'ulteriore e profonda lesione della loro reputazione. Lesione, inizialmente giustificata dall'esigenza d'informare il pubblico su fatti nuovi, che viene successivamente a perdere ogni ragion d'essere, allorquando i fatti siano stati ampiamente acquisiti e digeriti e risultino, in quanto tali, meritevoli di oblio.

Con dei limiti: vi sono accadimenti talmente gravi, da destare perenne interesse pubblico alla loro riproposizione nel tempo; si pensi ai 'crimini contro l'umanità', in merito ai quali, riconoscere ai responsabili un diritto all'oblio, significherebbe cancellare la memoria, creando buchi neri nella storia, che, così facendo, verrebbe a perdere l'imprimatur di testimone del passato.

Per altri fatti, ugualmente gravi, potrebbe sorgere la necessità di riproporli affinché non vengano dimenticati: è il caso di tutte quelle vicende che hanno modificato il corso degli

---

[3] M. FERRARA – E. SANTAMARIA, *Il Diritto all'illesa intimità privata*, in *Riv. dir. priv.*, 1937, I, 173; A. RAVÀ, *Istituzioni di Diritto Privato*, Padova, 1938, 157 e ss.

[4] Cass. Pen., sentenza del 6 dicembre 1998, n. 1473, in *Giust. pen.*, 1999, 687. Non è sufficiente la sola curiosità del pubblico a giustificare la diffusione di notizie sulla vita privata altrui, occorrendo invece che quelle informazioni siano di oggettivo interesse per la collettività.

eventi, diventando 'storia', come il Caso Moro, l'attentato al Papa o la Tangentopoli lombarda. La gravità di questi accadimenti è tale da non consentire che possano mai diventare privati, anzi è la mancata riproposizione degli stessi che si verrebbe a porre in contrasto con l'interesse pubblico alla loro conoscenza, interesse che, pertanto, verrà sempre a prevalere sul diritto del singolo a non essere più ricordato[5].

Ancora: essendo il diritto all'oblio subordinato al perdurare della mancanza dell'interesse pubblico, può accadere che, a distanza di tempo, sorga l'interesse alla riproposizione del medesimo fatto. E' il caso di chi, essendo stato condannato per stupro molti anni prima, commetta altra violenza sessuale appena uscito dal carcere. Legittima, a questo proposito, sarebbe non solo la diffusione della notizia relativa all'ultima violenza, ma anche la rievocazione del vecchio delitto, anche solo per stimolare nell'opinione pubblica considerazioni circa la funzione rieducativa del carcere e soprattutto la necessità di adottare misure cautelari ulteriori, per impedire il ripetersi di simili accadimenti[6].

Legittima sarebbe, pertanto, la rievocazione a distanza di trent'anni dal 'massacro del Circeo' dopo che Angelo Izzo, uno degli aguzzini, appena uscito dal carcere, ha replicato il feroce comportamento, violentando e massacrando un'altra donna e la di lei figlia quattordicenne.

Il perdurare dell'interesse pubblico, infine, è *in re ipsa* relativamente a tutti quei casi ancora 'aperti', sebbene siano trascorsi decenni dal loro accadimento[7], la cui riproposizione verrebbe ancor oggi a soddisfare un'indubbia esigenza informativa, per il duplice ordine di motivi insiti, da un lato, nell'interesse della collettività ad essere aggiornata sullo stato delle indagini e, dall'altro, in quello di stimolare un dibattito, permettendo la partecipazione del pubblico alla soluzione del caso.

Tra l'altro, in relazione ai 'casi aperti' sarebbe anche errato parlare di diritto all'oblio, in quanto ancora irrisolti: il diritto all'oblio, infatti, sorge laddove il diritto all'informazione e il diritto di cronaca sbiadiscono, essendo venuta meno qualsiasi utilità ad informare o aggiornare il pubblico.

---

[5] Il Tribunale di Roma, 1 febbraio 2001, non accolse il ricorso di Eva Mikula, contraria alla messa in onda, da parte di Canale 5, dello sceneggiato dal titolo *Uno bianca*, considerato dall'interessata lesivo della sua onorabilità e del diritto all'oblio, poiché, secondo quei giudici, «*non è lesivo della personalità altrui uno sceneggiato televisivo basato su fatti di cronaca che, per la loro eccezionalità e per l'efferatezza dei delitti rievocati, necessitano di essere ricordati e tramandati, non potendosi invocare il diritto all'oblio rispetto a vicende per le quali l'interesse pubblico non è mai venuto meno*».

[6] Tribunale Roma, sentenza 29 luglio 1976.

[7] Si pensi alla scomparsa di Emanuela Orlandi e agli omicidi e stupri commessi dal mostro di Firenze.

2) Evoluzione giurisprudenziale e concettuale del diritto all'oblio: dal diritto a dimenticare all'autodeterminazione e protezione dei dati

Il diritto all'oblio, nella sua prima e tradizionale applicazione, nasce come estrinsecazione del diritto alla riservatezza, strumento da azionare per tutelare la dignità della persona, attraverso la perimetrazione della diffusione di notizie e dati, qualora la loro conoscibilità non risultasse utile all'esigenza di conoscenza della collettività o di una parte di essa, ma si rivelasse, invece, lesiva della sfera intima della persona.

Intesa in tal senso, la tematica, nelle sue applicazioni iniziali, non ha avuto un vero legame con quella della protezione dei dati personali; così anche la giurisprudenza degli anni '90, e per un buon decennio, si è sviluppata muovendo dalla sola necessità di trovare un punto di equilibrio tra il diritto alla riservatezza e quello al rispetto della dignità della persona da un lato e la libertà di manifestazione del pensiero e d'informazione dall'altro.

La necessità di protezione dei dati personali ha iniziato a trovare residenza nel nostro diritto positivo con la Dir. 95/46 CE che, agli artt. 6 e 7[8], sanciva la protezione di quel bene, non in via autonoma, ma in quanto paladino del diritto alla riservatezza e di quello all'identità personale, indicando le finalità e le modalità in forza delle quali i dati avrebbero potuto essere trattati, l'obbligo del loro aggiornamento, il riconoscimento di

[8] Direttiva 95/46 CE, art. 6: «*1. Gli Stati membri dispongono che i dati personali devono essere: a) trattati lealmente e lecitamente; b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate; c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati; d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati; e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici.2. Il responsabile del trattamento e tenuto a garantire il rispetto delle disposizioni del paragrafo 1*».

Articolo 7: «*Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando: a) la persona interessata ha manifestato il proprio consenso in maniera inequivocabile, b) è necessario all'esecuzione del contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di tale persona, c) è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento, d) è necessario per la salvaguardia dell'interesse vitale della persona interessata, e) è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati, f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1*».

precisi diritti all'interessato: tutte condizioni in assenza delle quali quest'ultimo avrebbe potuto opporsi al loro trattamento ed eventualmente, ex art. 22, Dir. 95/46, agire in via amministrativa o giurisdizionale per far valere le sue ragioni, dal momento che si andava sempre più consolidando l'idea che la stragrande maggioranza delle scelte operate e delle azioni compiute lasciavano tracce importanti, che consentivano la mappatura e, con essa, la formazione di un identikit della persona.

Nel panorama giuridico italiano, il Legislatore nazionale, in recepimento della Dir. 95/46, ha emanato la Legge 675/96[9] (integrata e corretta da numerose e successive leggi e decreti legislativi), comunemente denominata 'Legge sulla Privacy', nella quale, per la prima volta, ha affrontato, in maniera organica, il tema della protezione della sfera privata, che ogni persona ha il diritto di potersi costruire, superando la concezione tradizionale della privacy come 'diritto ad essere lasciati soli', per giungere a configurarlo come possibilità di accesso alle informazioni riguardanti la propria persona, al fine di controllare la correttezza della loro acquisizione e del loro impiego nel corso del tempo.

Normativa che, in sede applicativa, non ha avuto il successo sperato, anche a causa del retaggio culturale italiano, che portava le imprese a mal digerire l'obbligatorio svolgimento di adempimenti inderogabili, per ottemperare alle disposizioni della legge e la Pubblica Amministrazione, con la sua elefantiaca struttura burocratica, ad adeguarsi con grande fatica al dettato di quella normativa. Era altresì diffusa nell'opinione pubblica l'idea di considerare il diritto alla privacy come un diritto delle elites, di quei privilegiati che erano sotto gli occhi dei riflettori e reclamavano la libertà di starsene per conto loro. Un diritto inteso come superfluo per la gente comune.

Al centro della Legge 675/96 vi era la 'persona' ed è anche per questo che è stata considerata una conquista della civiltà giuridica, una preziosa garanzia apprestata alla sfera privata degli individui, anche se di non facile applicazione, a causa delle numerosissime leggi corollario che avevano creato non poche difficoltà agli operatori giuridici, anche solo per capire quali fossero le norme applicabili al caso concreto. Difficoltà che hanno spinto il Legislatore nazionale a lavorare per produrre un Testo Unico in materia di protezione dati che, sempre nel rispetto delle linee guida della Direttiva 95/46, organizzasse tutto il materiale normativo presente nelle varie leggi e

[9] L. 31 dicembre 1996, n.675, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, in *G.U.* n. 5, 8 gennaio 1997.

decreti che si erano susseguiti dal 1996 al 2001, con previsioni precise, chiare e non sovrapponibili tra loro. Il 30 giugno 2003 è entrato così in vigore il T.U. 196, in materia di protezione dati che, nell'abrogare la legge 675/96, ha dato finalmente vita ad una legislazione diretta alla protezione dei dati personali, il cui articolo di esordio, rubricato "Diritto alla protezione dei dati personali[10]", s'inserisce nel solco tracciato dalla Carta di Nizza allorché specifica che "chiunque ha diritto alla protezione dei dati personali che lo riguardano": norma d'inestimabile valore sistematico, per buona parte della dottrina[11], e di mera declamazione solenne, priva di portata innovativa, essendosi limitata a riportare i medesimi contenuti e limiti già presenti nella Direttiva-madre, per altra e contrapposta parte.

Rispetto alla precedente normativa interna, la legge 196/2003 presenta alcuni punti fermi che attengono, per la maggior parte, alla semplificazione degli adempimenti e delle procedure, intesa come razionalizzazione dei processi di acquisizione e tutela dei dati, all'armonizzazione dei diritti da tutelare, al potenziamento dell'apparato sanzionatorio. In generale, ha generato una risistemazione delle norme in materia di privacy e un provvidenziale snellimento delle procedure e dei vincoli non più così stringenti, come nella vecchia normativa, soprattutto in materia di consenso.

In molti Stati europei il Legislatore si è attivato molti anni prima che in Italia, nel tentativo di legiferare in materia di trattamento dei dati personali. Il ritardo italiano è attribuito in larga parte, anche ad una certa resistenza, da parte della sensibilità giuridica nazionale, verso una normativa erroneamente percepita, almeno inizialmente, come camicia di forza,

---

[10] D. Lgs. 30 giugno 2003, n.196, *Codice della privacy*, in *G.U. suppl. ord*., 2003, n.174, art. 1: «*1.Chiunque ha diritto alla protezione dei dati personali che lo riguardano*».

[11] M. GRAZIADEI, *Diritto Soggettivo, Potere, Interesse*, in *La parte generale del diritto civile. 2. Il diritto soggettivo*, in *Trattato di Diritto Civile*, diretto da R. SACCO, Torino, 2001, 3. L'articolo 1, D. Lgs 30 giugno 2003, n.196, parla di diritto alla protezione dei dati personali, formula che non compare nella L. 31 dicembre 1996 n.675, dove si discute piuttosto di «*tutela delle altre persone e di altri soggetti rispetto al trattamento dei dati personali*», nonché di diritti e libertà fondamentali e dei limiti alla circolazione delle informazioni. Il Legislatore dedica a tale posizione soggettiva la norma di apertura del T.U. sulla privacy, ma la centralità di tale collocazione, sebbene abbia un innegabile valore sistematico, non lascia agevolmente capire, a parere dell'Autore, quali siano gli esatti confini ed il concreto contenuto della suddetta posizione soggettiva. Le modifiche apportate dalla Legge 196/2003, rispetto ai contenuti della normativa comunitaria, non sono di poco conto e rientrano in un più ampio disegno del Legislatore delegato, che non guarda al T.U. come ad una semplice occasione di semplificazione e razionalizzazione dell'esistente, ma assegna a tale strumento una funzione progettuale ben più ambiziosa. Il Codice rappresenta il momento terminale di una parabola, iniziata con il riconoscimento giurisprudenziale dei diritti alla riservatezza ed all'identità personale e proseguita con l'emanazione della Legge 675/96 aprendo, in tal modo, un nuovo capitolo nella teoria dei diritti fondamentali.

destinata a limitare la circolazione delle informazioni e a rendere, in generale, più farraginose le comunicazioni intersoggettive.

L'evoluzione tecnologica dei mezzi attraverso cui avvenivano le comunicazioni intersoggettive, avendo comportato la trasformazione del diritto alla riservatezza in diritto alla protezione dei dati personali, quale diritto ad una corretta gestione dell'uso delle informazioni, per bilanciare il potere di controllo sugli individui detenuto dai possessori delle banche dati, ha fatto sorgere la necessità di nuove forme di tutela, finalizzate a porre limiti ai trattamenti, divenute ormai indispensabili a seguito dell'avvento di Internet che, avendo eliminato le barriere del 'luogo' in cui le informazioni erano conservate, del 'tempo' necessario per raggiungerle e della capacità di ricerca e di reperimento delle stesse, non solo aveva notevolmente velocizzato, rendendola istantanea, la fruizione delle notizie, quanto, soprattutto, aveva manifestato tutti i rischi conseguenti alle potenzialità d'immagazzinamento, oltre che di trasmissione dei dati, per la sua planetaria e capillare diffusione.

Il potenziale informativo, concentrato nelle mani di pochi soggetti, aveva, tra l'altro, consentito ad un numero esiguo di aziende di possedere un patrimonio di conoscenze gigantesco, in grado non solo di accrescere il loro potere economico attraverso la sua vendita, ma anche d'indirizzare la loro influenza su ogni individuo, condizionandone le scelte, incidendo pesantemente sulle garanzie e libertà riconosciute alla persona, esponendo i diritti della stessa al rischio di violazioni di varia natura, rispetto a quanto potesse avvenire in precedenza, allorquando le informazioni circolavano attraverso la carta stampata.

Informazioni che, pertanto, avevano assunto la veste di un vero e proprio 'bene giuridico', suscettibile di sfruttamento economico da parte di imprese e società specializzate che, incrociando i dati in loro possesso, relativi a milioni di persone, sono state sempre più in grado di ottenere profili molto precisi di ciascuno, da destinare alla vendita. Un vero e proprio business, avente ad oggetto la raccolta, l'aggregazione e l'analisi dei dati dei propri clienti, attuali e potenziali, per trasformarli in informazioni che, in quanto destinate alla circolazione, rappresentano la valuta dell'attuale mercato digitale, l'oro nero dell'economia di Internet.

Dati che, tra l'altro, intercettati e raccolti da società pubbliche, si prestavano, e si prestano, a consentire forme di controllo dello Stato sui cittadini, un controllo apparentemente

finalizzato a garantire il rispetto delle regole e a tutelare la struttura statale dai nemici interni ed esterni ma, sostanzialmente orientato a monitorare costantemente la lealtà dei cittadini verso l'Istituzione[12].

E' cambiato completamente il contesto! Si è passati da una prospettiva che poneva al centro la ricerca del corretto equilibrio tra libertà di stampa e manifestazione del pensiero, da un lato, e tutela della riservatezza e dignità della persona, dall'altro, ad altra, che vede i cittadini sudditi di svariate forme di controllo, e non solo private, basate sull'acquisizione d'informazioni, utili e funzionali al sistema politico europeo che, a differenza di quello statunitense[13], e indipendentemente dalle epoche storiche e dalle forme di stato e di governo che si sono alternate, ha visto lo Stato assumere un ruolo predominante e sovrapposto al popolo, depositario del diritto-dovere di controllare costantemente i suoi sudditi.

Tutto questo ha reso quanto mai necessario l'intervento del Legislatore, volto a produrre norme più precise e puntuali, dirette, da un lato, a disciplinare finalità, condizioni e modalità del trattamento dei dati, ivi compresi quelli immessi in Rete dal titolare dei medesimi e della loro trasmissione, affinché non potessero sfuggire al suo controllo e, dall'altro, a costituire strumento di trasparenza nei rapporti interpersonali ed in particolare nei rapporti tra il pubblico e il privato per il corretto funzionamento di una società democratica.

2.1) Dal controllo sui cittadini come elemento strutturale dello Stato autoritario del '900 alla necessità di reperire informazioni utili a contrastare la sfida dello Stato islamico

[12] F. PIZZETTI, *Dalla Direttiva 95/46 al Nuovo Regolamento Europeo*, Torino, 2016, 52: «*Il quadro qui delineato è dichiaratamente connesso alla deriva del '900 verso nuove forme di assolutismo legate allo svilupparsi dello stato totalitario ed alle dittature di destra o di sinistra. Nell'ambito dei regimi autoritari del '900, infatti, il carattere etico ed ideologico dello Stato spinge ad affermare e generalizzare quel principio che è alla base di ogni totalitarismo: "se sei un buon cittadino non hai nulla da nascondere e se hai qualcosa da nascondere è perché non sei un buon cittadino"*».

[13] Vale la pena osservare che nella Costituzione americana il termine *state* o *states* è usato per individuare gli stati che fanno parte della Federazione, non la Federazione come tale. Manca insomma nel sistema federale americano l'idea che la federazione sia il soggetto titolare del potere sovrano. Anzi alla base della Costituzione di Filadelfia sta proprio la divisione dei poteri tra Stati e Federazione, prima ancora che la divisione tra potere legislativo, esecutivo e giudiziario. Tutto questo ha pesato molto sulla storia americana ed ha segnato una profonda differenza rispetto a quella europea, che ha invece, in molti paesi, specialmente dalla metà dell'800 in poi, conosciuto e coltivato a lungo l'idea dello Stato come titolare e punto di riferimento ultimo di ogni potere.

Nel quadro della deriva autoritaria della prima metà del '900, il controllo dello Stato sui cittadini, già capillare, cambia radicalmente prospettiva: seppur ufficialmente diretto a prevenire o punire violazioni di legge, di fatto costituiva un tentativo della 'maggioranza pro tempore' di avvalersi del potere statale per perimetrare il ruolo delle opposizioni, rendendone più difficile l'attività ed imponendo vincoli e limiti alla loro organizzazione. Quindi un controllo non solo finalizzato ad individuare delinquenti, criminali o potenziali sovversivi, ma anche e soprattutto a sorvegliare i cittadini per assicurarsi che orientassero la loro esistenza ed attività in modo conforme alle indicazioni dello Stato o del Partito/Stato.

In questo stesso periodo, e in queste forme di Stato, al controllo totale si ricorre anche per altre e diverse finalità come quella d'individuare, classificare e distinguere i cittadini non solo sulla base delle proprie idee, ma anche in considerazione della loro appartenenza razziale, delle loro tendenze sessuali, delle condizioni di salute fisica e soprattutto psichica, annullando senza scrupolo alcuno, e in un sol colpo, la riservatezza e la dignità della persona. L'unico limite era rappresentato dalla capacità della persona di sfuggire e sottrarsi alle apparecchiature tecniche utilizzate per vigilare su di loro.

Il passaggio dallo Stato autoritario a quello repubblicano - democratico non ha modificato il 'modus operandi' dell'immagazzinamento di dati ed informazioni, finalizzato, in un tempo meno recente a sostenere la sfida lanciata dal terrorismo nazionale e dalla criminalità organizzata, e, in tempi più vicini a noi, a far fronte alla minaccia criminale e sanguinaria lanciata dallo Stato islamico.

Quest'ultima, in particolare, ha comportato ulteriori e notevoli restrizioni all'area della privacy, con controlli assai stringenti del traffico telefonico e telematico per finalità di sicurezza e prevenzione reati. In quest'ottica hanno trovato la loro giustificazione gli obblighi posti in capo alle compagnie aeree di conservare e comunicare agli Stati membri una serie d'informazioni su voli domestici e internazionali (nome e cognome dei passeggeri, numero di volo, strumento di pagamento utilizzato, tratta, bagagli trasportati…). Indagini e rilevamenti massicci per finalità di prevenzione e repressione di minacce terroristiche che, comunque, hanno contribuito a creare un profondo vulnus nella privacy.

Misure che non sono andate esenti da critiche; giudicate troppo massive e sproporzionate rispetto ai canoni costituzionali europei, posti a presidio della riservatezza dei cittadini,

"tentazioni totalitarie dei Governi che, in risposta agli attentati terroristici, tornano ad ipotizzare strumenti di controllo di massa sulle comunicazioni, ben potendo effettuare una 'raccolta selettiva' di dati, imparando a ben esaminarli ed interpretarli, piuttosto che ampliarne a dismisura l'immagazzinamento[14].

Sempre in nome della repressione delle attività legate al terrorismo, in sede di discussione parlamentare della Legge Europea, n. 167 del 20 novembre 2017, sono stati presentati due emendamenti particolarmente incisivi del diritto alla riservatezza e delle consuetudini informatiche dei cittadini. Un primo emendamento, presentato congiuntamente dai deputati del PD e M5S, prevedeva che i dati internet e telefonici di tutti i cittadini italiani avrebbero dovuto essere conservati per sei anni rispetto all'attuale obbligo biennale. In sostanza gli operatori che forniscono l'accesso a internet ed ai servizi telefonici avrebbero dovuto custodire tutti i dati (contenuti di telefonate, messaggi, conversazioni, informazioni condivise attraverso la Rete) per un periodo molto più lungo e con l'obbligo di metterli a disposizione delle Autorità inquirenti, ove loro richiesto; emendamento accolto con favore, essendo stato dilatato il periodo di conservazione dei dati a settantadue mesi. Il secondo emendamento riconosceva all'AGCOM (Autorità per le garanzie delle comunicazioni), il potere di ordinare ai provider la rimozione dei contenuti confliggenti con i copyright. La medesima autorità inoltre, avrebbe potuto impedire, attraverso una sofisticata tecnica informatica, che il medesimo utente potesse nuovamente pubblicare, su ulteriori portali web, i contenuti rimossi. Anche questa seconda proposta ha avuto esito positivo, avendo l'art. 2 della menzionata legge previsto, in attuazione delle Direttive 2021/29 CE e 2004/48 CE, relative all'armonizzazione di alcuni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, su istanza dei titolari dei diritti, che l'Autorità AGCOM possa ordinare in via cautelare, ai prestatori di servizi della società dell'informazione, di porre immediatamente fine alle violazioni del diritto d'autore e dei diritti connessi, e predisporre misure idonee ad impedire la reiterazione delle violazioni.

Le polemiche inizialmente suscitate dagli emendamenti, sono state istantanee e numerose, tutte accomunate dalla medesima denuncia: il rischio di una 'sorveglianza di massa': con il pretesto di contrastare il terrorismo, le Autorità amministrative sarebbero state

[14] A. SORO, *Tentazioni totalitarie dei Governi che in risposta agli attentati terroristici tornano ad ipotizzare strumenti di controllo di massa sulle comunicazioni*, intervista rilasciata al quotidiano *La Repubblica*, 28 giugno 2016.

autorizzate ad intercettare gli individui, contrariamente ai precetti imposti dalla Carta costituzionale e con considerevoli ricadute sul diritto alla riservatezza di ciascuno.
In verità, se in tempi di minaccia globale del terrorismo stragista, trovare un punto di equilibrio accettabile tra le istanze di sicurezza e quelle di libertà è impresa quanto mai difficoltosa, tuttavia, non si può non convenire sulla considerazione che, ove la soluzione dovesse essere quella di restringere la libertà di milioni di individui, ci si auspica che almeno tale restrizione rappresenti una soluzione efficace ed efficiente per la causa.

3) La storia del diritto alla protezione dei dati: la privacy come diritto alla riservatezza anche rispetto ai mezzi d'informazione e l'importanza dell'evoluzione tecnologica legata all'informazione

Alla base dell'espansione del controllo si è rivelato essenziale il ruolo svolto dalle nuove tecniche legate alla consultazione e conservazione delle informazioni, attraverso sistemi automatizzati di archiviazione e trattamento dei dati. Non è un caso che la necessità di proteggere la privacy sia nata in un contesto come quello statunitense, sia perchè la libertà di stampa, comprensiva del diritto ad informare ed essere informati, e quella di manifestazione del pensiero, sono sancite già nel 'first emendament' del Bill of rights, ma anche e soprattutto perché in quella civiltà già dalla fine del 19° secolo erano conosciuti la stampa in offset, la fotografia e il giornalismo d'impresa. Il problema della tutela della privacy è stato, quindi, figlio dell'evoluzione tecnologica delle forme di comunicazione, che hanno moltiplicato le possibilità di diffusione delle informazioni, prescindendo dal consenso dell'interessato, sconosciute in passato e soprattutto sconosciute in Europa[15].
Sul piano delle tecnologie che hanno reso possibili forme di controllo globale più pervasive, un ruolo centrale sicuramente spetta ai trattamenti automatizzati, inizialmente

[15] Si tenga conto di questo fondamentale passo del *Right to privacy*: «*Instantaneous photographs and newspaper enterprise have invaded the sacred percincts of private and domestic life" e quasi feticamente subito dopo aggiunge: "For years there has been a feeling that the law must afford some remedy for unauthorized circulation of portraits of private person; and the evil of invasion of privacy by the newspaper, long keenly felt, has been but recently discussed* »(cfr. S.D. WARREN- L.S. BRANDEIS, *The right to privacy*, in *Harvard Law Review***,** Vol. IV, 1890. E' difficile non sottolineare la lucidità con la quale è messo a fuoco il vero problema della privacy: il suo legame con la tecnologia. Su questo aspetto L.D. BRANDEIS tornerà molte volte, anche con riferimento alle intercettazioni telefoniche. Inoltre, sempre durante la sua vita di giudice, riprese ancora con forza questo tema fino a che, nel 1928, in una famosissima dissenting opinion, scritta nell'ambito della decision assunta dalla Corte Suprema nella causa Olmstead v. United States, 227 US 438 (1928), definì la privacy come «*the most comprehensive of rights and the right most valued by civilized man*».

basati sulle schede perforate e sui sistemi di elaborazione, messi a punto dalla IBM[16] nel nuovo Continente, che hanno consentito, a grandi imprese giornalistiche, l'immagazzinamento e la consultazione, in tempi rapidi, d'informazioni relative a singoli individui o a nuclei familiari, dati poi messi a disposizione degli apparati di controllo nazisti[17]. E' cosa nota che alcune grandi imprese USA abbiano collaborato con il regime hitleriano fornendo tecnologie e apparati operativi essenziali per il disegno del Fuhrer.

Pertanto, se è vero che i diritti nascono e sono legati al contesto in cui operano, il right to privacy non poteva non nascere in quel continente come forma di difesa del cittadino e della sua vita privata dalle potenziali aggressioni delle nuove tecnologie applicate alla stampa, anche se poi la società digitale, diffusasi su scala planetaria, ha costretto tutti a confrontarsi con dimensioni imprevedibili ai tempi della stampa offset. Si pensi alle foto, o altre informazioni personali, postate sui social e ritrasmissibili da ciascuno degli 'amici' o dei 'followers' ad altri, in numero e dimensioni esponenziali e incontrollabili.

Anche nella legislazione europea la privacy non si esaurisce più nella riservatezza, ma è considerata sinonimo di protezione dei dati personali; d'altra parte, la locuzione 'protezione dei dati personali' non è assorbente solo del diritto alla privacy, come protezione dalla diffusione di informazioni inerenti la vita privata dell'individuo, ma comprende altresì il diritto a che ogni informazione, di qualunque genere, che sia direttamente o indirettamente riferibile a una persona, non sia illecitamente raccolta, o trattata, o conservata o diffusa[18].

In sostanza, nel mondo americano il right to privacy, nato per segnare i confini tra la sfera di riservatezza delle persone e i diritti di manifestazione del pensiero e di stampa, solo in seconda battuta, e in forza della sua evoluzione dinamica, viene ad essere utilizzato per

---

[16] I rapporti tra Germania nazista e grandi imprese USA, alcune delle quali collaborarono con il regime hitleriano, anche fornendo tecnologie ed apparati operativi essenziali per il disegno del Führer, sono cosa nota, sulla quale vi è letteratura ampia anche se non di eccellente qualità. In particolare è importante la letteratura sul rapporto tra utilizzazione degli apparati di archiviazione e trattamento dati costruiti dalla IBM e la persecuzione degli ebrei. Su questo si veda per tutti, E. BLACK, *L'IBM e l'olocausto*, trad. it. a cura di R. ZUPPET e S. MANCINI, Milano, 2001, nel quale si sostiene anche che per individuare con maggiore precisione i 7550 negozi di proprietà ebraica distrutti nella notte tra il 9 ed il 10 novembre 1938 in Germania, Austria e Cecoslovacchia furono utilizzati i sistemi IBM, anche grazie ai rapporti tra importanti strutture pubbliche del Terzo Reich e la grande azienda americana.

[17] J. LADOR- LEDERER, *Capitalismo mondiale e cartelli tedeschi tra le due guerre*, Torino, 1959; C. LEVINSON, *Vodka-Cola,* Firenze, 1978.

[18] Non a caso in Europa, dove il problema principale che si è posto nel secolo scorso non è stato tanto la protezione dei cittadini dai media (e quindi dal c.d. quarto potere), quanto direttamente dallo Stato ed in particolare dai partiti- Stato delle dittature del Novecento (e dunque dal potere *tout court*), è prevalso l'uso della più complessa espressione *personal data protection* o *protezione dei dati personali*.

chiedere ed ottenere un trattamento lecito di dati e informazioni relativi all'individuo; nel Vecchio Continente invece, lo sviluppo della "tecnologia del controllo", con la sua sempre più penetrante capacità di raccogliere, trattare, archiviare dati e comportamenti dei cittadini, sudditi di uno Stato prevaricatore, ha fatto sì che il diritto alla privacy si sia subito affermato, oltre che come paladino della riservatezza, anche come diritto alla protezione dei dati personali, ossia come diritto di libertà dell'individuo a non essere sottoposto a controlli, alla raccolta d'informazioni legate alla sua persona senza il suo consenso, in assenza di ragioni di prevenzione e/o repressione di reati che possano altrimenti giustificarne il trattamento[19].

4) La protezione dei dati personali come diritto fondamentale di libertà nella società digitale e delle comunicazioni elettroniche

L'evoluzione tecnologica nel campo delle comunicazioni elettroniche, che è alla base della società digitale e della globalizzazione delle relazioni interpersonali, economiche, finanziarie e sociali, ha comportato un notevole ampliamento del contenuto del diritto alla dignità della persona, facendolo riemergere dalle sue stesse ceneri, prodottesi nel corso della Seconda Guerra Mondiale, fino ad elevarlo a valore fondante, alla pari e forse più della libertà personale, di tutte le Carte dei diritti, da quella dell'ONU[20], alla CEDU[21] fino alla Carta di Nizza e alla Costituzione UE.

Ampliamento che ha consentito, al suo interno, l'inclusione del diritto alla protezione dei dati personali, che oggi forse, rappresenta la sola barriera allo strapotere della società digitale che rende acquisibili e controllabili, in ogni momento, i dati di ognuno circolanti in Rete[22]. Diritto, quindi, che, per volere concorde della scienza giuridica italiana e della

[19] Proprio il fatto che per molti aspetti le forme pervasive di controllo degli Stati autoritari fossero basate su tecniche di trattamento automatizzato dei dati, spiega bene perché, sia in alcune leggi nazionali degli anni '70, sia nella Convenzione 108 del 1981, il diritto alla protezione dei dati personali sia stato incentrato soprattutto su queste tipologie di trattamenti.

[20] Cfr. *Dichiarazione Universale dei Diritti Umani*, proclamata dall'Assemblea generale delle Nazioni Unite, il 1° dicembre 1948 a Parigi. Merita segnalare che il preambolo inizia con queste parole: «*Considerato che il riconoscimento della dignità inerente a tutti i membri della famiglia umana e dei loro diritti uguali ed inalienabili, costituisce il fondamento della libertà, della giustizia e della pace nel mondo*».

[21] Cfr. Convenzione europea dei Diritti dell'Uomo, firmata a Roma il 4 novembre 1950, Preambolo e art. 8 dedicati al *Diritto al rispetto della vita privata e familiare*.

[22] Sul punto S. RODOTÀ', *Il diritto di avere diritti*, Bari, 2012; ID., *Il mondo della rete. Quali i diritti, quali i vincoli*, Bari, 2014.

stessa Corte Costituzionale[23], vede il suo fondamento costituzionale nella tutela della persona e nella necessità di offrire protezione alla sua dignità.

Tutte le informazioni e i dati, ivi compresi quelli immessi in Rete dallo stesso utente, infatti, spontaneamente o su richiesta, in cambio o meno di servizi messi a sua disposizione, vengono captati in circuiti destinati ad una circolazione potenzialmente illimitata nel tempo, nella qualità e nella quantità, facendogli correre il rischio di offrire un'immagine di se difforme da quella reale, fortemente aggressiva della sua dignità.

L'intervento del Legislatore nazionale, prima con la legge 675/96 [24]e successivamente con il T.U 196/2003[25], è la conferma della consapevolezza circa i rischi che la reputazione e la dignità della persona correvano. Rischi che, tuttavia, non si sono attenuati a seguito del nuovo quadro normativo, in quanto l'avvento di 'big data' e 'IOT' hanno rimesso a dura prova il diritto alla protezione della sfera privata.

Tanto i 'big data', che consentono raccolte sempre più smisurate di dati, acquisiti in Rete in modo massiccio e trattati per svariate finalità, a costi sempre più bassi grazie ad elaboratori potenti, che l'IOT (Internet of Things), un insieme di tecnologie, sempre più raffinate, che consente agli esseri umani di trattare le risorse a loro disposizione in modo più efficiente ed organizzato[26], spingendo le persone comuni ad utilizzare la Rete nel quotidiano per ricevere servizi o fare ricerche, comportano, senza che gli utenti se ne rendano conto, una profilazione delle loro persona e dei loro comportamenti. Informazioni che, da chiunque captate, in assenza di adeguate protezioni, portano a conoscere dati sterminati su abitudini, comportamenti e opinioni di ciascuno.

---

[23] Cfr. Corte Cost., sentenza 7 luglio 2005 n.271, in *Dir. Internet*, 2005, 6, 555, con nota di COSTANZO, che considera il diritto alla protezione dei dati personali, non solo collocato nell'ambito del diritto civile, *ex* art. 117, comma 2, lett. l), ma anche come un diritto che si riferisce «*all'intera serie dei fenomeni sociali nei quali questi possono venire in rilievo: da ciò una disciplina che, pur riconoscendo tutele differenziate in relazione ai diversi tipi di dati personali ed alla grande diversità delle situazioni e dei contesti normativi nei quali tali dati vengono utilizzati, si caratterizza essenzialmente per il riconoscimento di una serie di diritti alle persone fisiche e giuridiche, relativamente ai propri dati, diritti di cui sono regolate analiticamente caratteristiche, limiti, modalità di esercizio, garanzie, forme di tutela in sede amministrativa e giurisdizionale*».

[24] L. 31 dicembre 1996 n.675, in *G.U. suppl. ord.,* 1997, n.5, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* (testo consolidato con il d.lgs. 28 dicembre 2001, n. 467).

[25] D. Lgs. 30 giugno 2003 n.196, cit.

[26] Sul tema, cfr. Gruppo Art. 29, Parere n. 8/2014 *Sui recenti sviluppi nel campo dell'Internet degli oggetti*, 16 settembre 2014.

E' per questo che oggi, più che in passato, è ritenuto indispensabile l'intervento attento e capillare delle Autorità, amministrativa e giudiziaria[27], onde contenere e comprimere, quanto più possibile, l'uso improprio delle informazioni raccolte e le forti ingerenze nella vita personale che portano a vanificare ogni forma di libertà personale[28].

Uno dei tanti: è del 2013 lo scandalo del 'Datagate', che ha visto operazioni di spionaggio da parte dell'NSA, nei confronti di alcuni Paesi europei alleati degli USA, i cui dettagli sono stati denunziati da Edward Snowden (ex informatico CIA), relativamente ai programmi di sorveglianza di massa, ad opera della potente NSA (National Security Agency) e che ha sollecitato Viviane Reding, allora Commissario europeo della Giustizia, a porre le questioni generate dal Datagate all'Ordine del giorno del Consiglio europeo del 24 ottobre 2013, al fine di predisporre una risposta europea, forte e univoca, agli USA.

È vero che gli esseri umani questo rischio l'hanno sempre corso, non essendo l'individuo una monade, ma un'animale sociale che forma e sviluppa la sua personalità in un processo di relazioni che si snoda all'interno delle formazioni sociali di cui viene a far parte. E' anche vero che il patrimonio di conoscenze di cui dispone è frutto delle azioni e dei pensieri di coloro che lo hanno preceduto e che gli hanno tramandato l'inevitabile 'rapporto di comunità' che fa sorgere in ciascuno dei suoi membri il bisogno di 'farsi i fatti degli altri'. La differenza rispetto al passato è che, allora, la conservazione dei dati avveniva attraverso gli archivi o la raccolta di documenti che facevano capo a strutture specifiche, pubbliche o private, accessibili a pochi: vi era una circolazione protetta delle informazioni e chi voleva poteva anche nascondere o distruggere i suoi dati.

Oggi, invece, con lo sviluppo massiccio delle tecnologie legate all'archiviazione delle informazioni e con le forme esasperate di controllo, non c'è più un 'luogo in cui nascondersi'[29]: la sfera privata è annientata per vivere la vita degli altri, si avverte

[27] Sin dall'inizio della sua attività, il Gruppo art. 29, ha sempre prestato particolare attenzione ai temi della rete nella prospettiva dei dati, anche per colmare alcune evidenti lacune del contenuto della Direttiva 95/46. Dal momento della sua prima istituzione, nel 1997, i primi Pareri e le prime Raccomandazioni del Gruppo furono dedicati proprio ai problemi che già allora si profilavano rispetto alla protezione dei dati in Rete. Basti ricordare che la prima Raccomandazione del Gruppo, la n. 1/1997, fu dedicata al tema *La legge sulla protezione dei dati personali e i* media (WP n. 1).

[28] Non si creda che le espressioni usate nel testo siano dovute ad un eccesso di retorica: esse rappresentano solo la realtà di oggi ed i pericoli che corrono le nostre libertà. Non per nulla l'art.1 del Regolamento 2016/679 recita al paragrafo 2: "*Dysregulation protects fundamental rights and freedoms of natural persons and in particular their rights to the protection of personal data".*

[29] Cfr. G. GREENWALD, *No place to hide, Edward Snowden e la sorveglianza di massa*, Milano, 2014.

l'oppressione di essere costantemente spiati e monitorati, con un Legislatore che, rassegnato, arranca rispetto ad una evoluzione informatica esasperatamente vorticosa.

4.1) Il caso Snowden

Un trentenne americano, Edward Snowden, ex tecnico della CIA e fino al 2013 collaboratore della Booz Allen Hamilton, azienda di tecnologia informatica consulente della NSA (National Security Agency), ha rivelato ai giornalisti Glenn Greenwald, avvocato costituzionalista americano e opinionista della redazione americana del "The Guardian" e Laura Poitras, documentarista, a suo dire "per questioni di coscienza e per far scattare l'allarme nell'opinione pubblica mondiale su quello che sta accadendo e sulla società in stile Grande Fratello che la NSA ha messo in piedi, e sta consolidando[30]", il programma di sorveglianza di massa sul mondo intero, riferendo numerose informazioni sui planning dell'intelligence secretati, tra i quali, quello delle intercettazioni telefoniche tra USA e UE, relativo ai dati delle comunicazioni, Prisma, Tempora ed altre piattaforme di sorveglianza Internet.

Documenti e informazioni che sono stati pubblicati nell'estate del 2013 dal The Guardian e dal Washington Post[31].

Per la prima volta in assoluto nella storia, Snowden ha permesso di documentare con files "top secret/noforn" (top secret e non rilasciabili a cittadini stranieri) della NSA, come le intercettazioni dell'Agenzia fossero effettivamente di massa. Mai prima, infatti, alcun Insider dell'Agenzia aveva fornito al pubblico questi files top secret, contenenti operazioni massicce, finalizzate a tracciare ogni telefonata, migliaia di dati privati, ed informazioni relative all'altra operazione, Prisma, volta a dirottare verso Fort Mode (sede del quartier generale della NSA) le comunicazioni Internet che entrano ed escono da Google, Apple, Yahoo ed altri giganti della Rete.

Rivelazioni che, a parere di Matthew M. Aid, storico d'intelligence di Washington, hanno semplicemente confermato i sospetti di lunga data che "la sorveglianza dell'NSA negli Usa è più invasiva di quanto pensavamo"[32], così come hanno rafforzato l'idea che oggi la NSA sia in grado d'intercettare tutte le comunicazioni del mondo, registrando i

[30] E. SNOWDEN, *Sfido il Grande Fratello*, in *L'Espresso*, 4 giugno 2014.
[31] G. GREENWALD - E. MAC ASKILL - L. POITRAS, *Edward Snowden: the whistleblower behind the Nsa Surveillance revelations*, in *The Guardian*, 10 giugno 2013.
[32] M. AID, *The Secret Sentry; the untold History of National Security Agency*, in *Bloomsbury Press*, 2010, 231.

contenuti di ogni telefonata, e-mail, chat, video, in considerazione del fatto che le tecnologie d'intercettazione e immagazzinamento dei dati consentono di farlo, anche a costi assolutamente sostenibili. Anzi, secondo quanto dichiarato dal Bill Binney[33], a Bluffdale, nello Utah, l'Agenzia sta costruendo un enorme centro d'immagazzinamento dei dati. Ogni computer 'Narus', usato dall'NSA, è in grado di processare l'equivalente di 100 miliardi al giorno di email da 1000 caratteri. Le dimensioni della struttura di Bluffdale lo portano a stimare che in quel centro possano venire attivati almeno 12,150 computer Narus, in grado d'immagazzinare le informazioni dell'intero mondo per i prossimi 100 anni.

Nessuno sa come vengano usati questi dati, anche se non è difficile immaginarlo, considerato che gli USA hanno avuto una lunga storia di abusi, negli anni '50/60, di sorveglianza e spionaggio ai danni di oppositori e attivisti politici, che ha portato, come risposta, alla produzione di leggi a tutela dei cittadini americani, come il FISA (Foreign Intelligence Surveillance Act) del 1978 che, tuttavia, sono state completamente stravolte e svuotate di contenuto, dopo gli attentati dell'11 settembre.

Informazioni che vengono, tra l'altro, conservate, e non è chiaro per quanto tempo, sul presupposto che un dato, una email, una conversazione telefonica che oggi sembra innocua, potrebbe diventare importante nel giro di poco.

Le rivelazioni hanno dato vita ad un dibattito internazionale sulle conseguenze che una sorveglianza di tali proporzioni ha per la vita privata delle persone interessate, anche considerato il modo in cui i servizi d'intelligence le hanno usate, soprattutto quelle relative alle comunicazioni quotidiane, senza che vi fossero limiti alle proporzioni del controllo.

Il WP29 ha individuato due pilastri per la sicurezza pubblica relativamente ai dati personali: innanzitutto la trasparenza delle modalità di funzionamento dei programmi di sorveglianza, che "contribuisce ad accrescere e ristabilire la fiducia tra i cittadini, governi ed entità private"[34]. Infatti, attraverso l'informativa, gli interessati, qualora i servizi d'intelligence siano autorizzati ad accedere ai loro dati, potendo comprendere le possibili conseguenze dell'uso dei servizi di comunicazione elettronica online e offline, saranno in

[33] B. BINNEY, *Welcome to Utah, the NSA desert home for eavesdropping on America*, in *The Guardian*, 14 giugno 2013.

[34] WP 216, *Parere 4/2014*, sulla sorveglianza delle comunicazioni elettroniche a fini di intelligence e sicurezza nazionale.

grado di proteggersi. In secondo luogo il Gruppo raccomanda una vigilanza più rigorosa delle attività di sorveglianza da parte delle autorità di protezione dei dati, cosicché i servizi d'intelligence non compiano abusi.

Nel predetto Parere il WP29 ha altresì precisato che: "né i principi di approdo sicuro, né le clausole contrattuali tipo, né le norme vincolanti d'impresa possono fungere da fondamento giuridico per giustificare il trasferimento dei dati personali all'autorità di un paese terzo ai fini di una sorveglianza massiccia e indiscriminata" e ciò proprio perché le deroghe previste da questi strumenti di sorveglianza sono comunque interpretate alla luce dei principi di protezione dei dati ed in modo ancor più restrittivo. Infatti, esse non devono mai essere applicate a scapito del livello di protezione garantito dalle norme e dagli strumenti dell'UE che governano i trasferimenti di dati. In tal senso, nel passaggio seguente del medesimo parere, si può comprendere la ratio di quanto affermato dal Gruppo in quell'opinione: "In genere, i programmi di sorveglianza gestiti dagli Stati membri non sono soggetti al diritto dell'Unione, in forza di deroghe, giustificate dalla sicurezza nazionale, previste dai trattati europei nonché da diversi regolamenti e direttive unionali, compresa la Direttiva 95/46 CE. Ciò non significa tuttavia che tali programmi siano soggetti soltanto al diritto nazionale…anche laddove non si applichino il diritto unionale in generale e la direttiva sulla protezione dei dati in particolare, i servizi d'intelligence per agire legalmente, devono non di meno rispettare la maggior parte dei principi di protezione dei dati sanciti dalla CEDU e dalla Convenzione 108 del Consiglio d'Europa sulla protezione dei dati personali. I programmi di sorveglianza basati su un'indiscriminata raccolta a tappeto di dati personali non potranno in alcun modo soddisfare i requisiti di proporzionalità e necessità previsti da detti principi sulla protezione dei dati. Le limitazioni ai diritti fondamentali devono essere interpretate restrittivamente e ciò implica che tutte le ingerenze devono essere necessarie e proporzionate alla finalità perseguita".

Nell'inevitabilità dell'adozione di programmi di sorveglianza, più o meno massivi da parte dei governi, in un'era in cui la lotta al terrorismo si deve necessariamente attuare, anche attraverso elaborazioni automatizzate dei flussi di informazioni digitali, pare auspicabile un significativo passo avanti nelle tutele fondamentali degli individui, rispetto agli algoritmi impiegati dai pubblici poteri nelle società democratiche, sia a livello europeo che internazionale. Pur volendo convenire con quanto affermato da Keith

Alexander, generale e capo dell'NSA, il quale ha pubblicamente difeso il programma di sorveglianza di massa, affermandone la sua utilità, laddove ha permesso di sventare ben 50 complotti terroristici, sono altresì indispensabili norme, di rango costituzionale e sovrannazionale, che fissino criteri minimi di trasparenza e correttezza ex ante e di verificabilità ex post, dirette a regolamentare l'uso che si faccia dei dati massicciamente raccolti.

4.2) Gli Accordi USA – UE: dal Safe Harbour al Privacy Shield

Dopo mesi di trattative, e considerate le profonde differenze normative in materia di tutela dei dati personali, causa di forti tensioni non solo giudiziarie, il 2 febbraio 2016 la Commissione europea e il Governo americano hanno raggiunto un nuovo accordo, denominato Eu-Us Privacy Shield, sul trattamento, la conservazione e l'utilizzo dei dati personali dei cittadini europei negli USA. Lo 'Scudo per la privacy Stati uniti – UE' ha superato e sostituito il Safe Harbour, recepito nel 2000[35]e invalidato il 6 ottobre del 2015 (in seguito ad una sentenza della Corte di Giustizia dell'Unione europea).

La nuova intesa va così a colmare quel vuoto normativo che rischiava di bloccare le transazioni online e di provocare perdite annue del PIL europeo.

Alla fine degli anni '90 emerse la problematica della diversità degli approcci e dei meccanismi di protezione dei dati personali dei propri cittadini, utilizzati da Europa e Stati Uniti. Nel 1998, infatti, la Commissione europea emanò la Direttiva 95/46 CE, relativa alla 'data protection', che vietava il trasferimento di dati personali verso Paesi non appartenenti all'UE, che non rispettavano gli standard previsti dalla normativa comunitaria.

Al fine di colmare le differenze e fornire agli operatori americani uno strumento con cui conformarsi ai requisiti richiesti dalla Direttiva, il Dipartimento del Commercio Americano e la Commissione europea svilupparono l'Accordo denominato Safe Harbour, un compromesso tra le stringenti indicazioni della Direttiva europea e le procedure in atto negli Stati Uniti, decisamente meno vincolanti.

Attraverso l'adesione al programma Safe Harbour, le aziende americane, venendo automaticamente classificate come aziende che non offrivano un adeguato livello di

[35] IL Garante della privacy italiano si è pronunciato il 10 ottobre 2001, *Doc Web n. 30939*, autorizzando il trasferimento di dati personali dal territorio dello Stato verso organizzazioni aventi sede negli USA, in forza dell'Accordo sottoscritto dalla Commissione europea.

protezione dei dati personali, erano obbligate al rispetto degli standard di protezione dei dati richiesti dalla Commissione europea, evitando in tal modo disagi, quali la necessità di ottenere un'autorizzazione specifica da ogni singola Autorità Garante nazionale prima dell'avvio del trasferimento dei dati, il rischio d'interruzione dei rapporti commerciali delle aziende europee con gli Usa, facilitazioni nella soluzione delle problematiche con le Autorità Garanti della privacy nei diversi Stati membri, laddove era previsto che eventuali ricorsi proposti dai cittadini europei contro aziende americane, avrebbero potuto essere gestiti a livello nazionale. Qualora l'Azienda americana avesse deciso di non attenersi al programma del Safe Harbour, sarebbe stato necessario seguire la diversa procedura che prevedeva il rilascio di una specifica autorizzazione, da parte di ogni singola Autorità nazionale, al trasferimento dei dati a quell'Azienda.

Nel novembre del 2001, il Garante nazionale, preso atto dell'intesa USA – UE, e riconoscendo il Safe Harbour, ha autorizzato il trasferimento dei dati personali dall'Italia alle aziende degli Stati Uniti che, in quanto aderenti a quell'Accordo, risultavano iscritte in appositi elenchi periodicamente aggiornati, consentendo, per anni, alle multinazionali americane di immagazzinare e conservare i dati degli utenti europei sia negli USA che nell'UE.

Oltre 4.000 aziende americane hanno aderito al Programma: in un'economia sempre più caratterizzata dall'uso della tecnologia, il trasferimento dei dati era diventato fondamentale, oltre che per le aziende dell'internet economy e dell'Information Technology, anche per quelle relative ad altri settori, quali il turistico, il farmaceutico, il manifatturiero.

Nei suoi quindici anni di vita però l'Accordo ha manifestato tutti i suoi limiti e le carenze, sia nel regolamentare i nuovi social network, molto più sviluppati, che nel frattempo erano sorti (Facebook, Twitter), che nel risolvere le problematiche, legate alla sicurezza e alla privacy che, dopo gli attentati del 2001, si erano manifestate, richiedendo interventi urgenti e massicci.

Il colpo di grazia gli "Accordi" lo hanno ricevuto con lo scoppio del caso Snowden.

Nell'ottobre 2015, alla luce delle rivelazioni di Edward Snowden sulla sorveglianza indiscriminata e illimitata da parte dell'NSA (National Security Agency), la Corte di Giustizia dell'Unione europea ha invalidato la decisione dell'Unione europea sul Safe Harbour (con la sentenza sulla Causa C-362/14, Maximilian Schrems v Data Protection

Commisioner), perché, a parere di quei giudici, non vi erano sufficienti garanzie a che la riservatezza dei dati degli europei fosse tutelata anche in America.

La sentenza della Corte di Giustizia europea, che ha demolito, avendolo ritenuto illegittimo, il trasferimento dei dati personali tra Europa ed America, senza aver introdotto delle più incisive clausole di salvaguardia, ha messo in grosse difficoltà le aziende di dimensione transatlantica che, in tal modo, si sono venute a trovare prive dell'ombrello precedente, costituito dal Safe Harbour.

La Commissione europea e il dipartimento americano per il Commercio hanno immediatamente cominciato a lavorare alacremente per mettere a punto un accordo alternativo, in mancanza del quale i giganti dell'informazione (Google, Facebooh, Yahoo), sarebbero stati impossibilitati a trasferire dati dall'Europa ai server situati negli USA. Urgenza dimostrata dalla straordinaria quantità di dati, che solo nell'anno 2015, per averne un'idea, hanno superato il valore di 240.000.000.000. di dollari[36].

Nel febbraio 2016 la Commissione europea e il governo americano raggiungono l'Accordo politico Eu-Us Privacy Shields che, a differenza della precedente intesa, fondata sulle autocertificazioni, contiene impegni vincolanti e regole stringenti a carico delle aziende americane nonché l'obbligo, posto a carico di queste ultime, di rispettare le decisioni dei Garanti europei in materia di protezione dati e l'esclusione di qualsiasi forma di sorveglianza di massa verso gli europei. E' stato, infatti, esplicitamente dichiarato che le attività di sorveglianza di massa della NSA avrebbero dovuto essere necessariamente messe sotto controllo e il Dipartimento del Commercio ha dato raassicurazioni in questo senso.

Impegni stringenti e regole che il Dipartimento del Commercio, attraverso una serie d'incontri, ha preso l'impegno d'illustrare alle aziende americane, obbligate ad osservarle e che sono stati salutati con soddisfazione dal Gruppo di Lavoro Art. 29, che ha riconosciuto i notevoli miglioramenti apportati dal nuovo Accordo alla materia trattata, rispetto al vecchio quadro normativo di riferimento[37].

---

[36] Dati rilevati da A. BIASOTTI, *Il nuovo Regolamento europeo sulla protezione dei dati. Guida pratica alla nuova privacy e ai principali adempimenti del Regolamento UE 2016/679,* EPC, Roma, 2017, 780.

[37] S. CROLLA, *Dal Safe Harbour al Ue-Us Privacy Shield*, in *Formiche*, marzo 2016, 28-29; L. DE BIASE, *Patto sui dati, successo europeo e della privacy*, in *Il Sole 24 ore*, 3 febbraio 2016, 10; P. LICATA, *Privacy Shields*, *Vera Jourovà: La Commissione al lavoro sulle criticità*, in www.corrierecomunicazioni.it., 13 aprile 2016.

Della stessa opinione non è stato Jan Philipp Albrecht, presidente della Commissione LIBE[38], da sempre attento ed impegnato nello sviluppo del Regolamento generale europeo e di altri documenti afferenti la protezione dei dati personali, secondo il quale le condizioni relative alla conservazione dei dati non sono state redatte con sufficiente precisione, soprattutto relativamente al principio della limitazione delle finalità in base alle quali è possibile raccogliere e trattare dati personali, oltre ad essere piuttosto carenti i riferimenti normativi alle operazioni di vigilanza sul trattamento, nei confronti di aziende residenti negli Stati Uniti[39].

A garanzia di maggiore protezione, il Dipartimento del Commercio americano ha promesso l'istituzione di un Ombudsman americano, dotato di ampi poteri in materia di controlli sia presso le aziende americane che nel settore pubblico, dal momento che l'operatività dell'articolato vale anche per gli Enti statali che raccolgono e trattano dati.

4.3) Le regole sulla protezione dei dati in altre parti del mondo: l'Accordo in APEC

I problemi legati al trasferimento dei dati personali da un Paese all'altro non esistono solo tra Europa e Stati Uniti ma anche nell'estremo opposto del mondo; nelle ragioni asiatiche, esiste un problema similare, in qualche modo risolto su base pattizia.

Nel novembre 2004, infatti, i ministri di ventuno Paesi appartenenti all'Asia Pacific Economy Cooperation' – APEC – hanno approvato un quadro normativo per la tutela della privacy che comprende una serie di norme e linee guida, con relativi manuali applicativi, in modo da assistere le aziende che operano in queste ventuno economie, nello sviluppo di idonei sistemi di protezione dei dati personali, sia in fase di trattamento interno alla stessa nazione, che di trasferimento in altre nazioni.

Norme dirette a consentire alle organizzazioni multinazionali, che raccolgono, trattano e gestiscono dati nelle economie APEC, di sviluppare ed attuare un approccio armonizzato per consentire un accesso globale ai dati personali, nell'osservanza dei sistemi di protezione dalle dannose conseguenze d'intrusioni o utilizzi non autorizzati. Quindi, pur garantendo un flusso continuo d'informazioni fra tutte le economie APEC ed altre economie connesse, l'Accordo è teso a sviluppare meccanismi internazionali che possano

[38] Commissione per le libertà civili, la giustizia e gli affari interni, che si occupa della tutela dei diritti umani e della protezione dei dati personali in Europa.

[39] A BIASOTTI, *IL nuovo regolamento europeo sulla protezione dei dati. Guida pratica alla nuova privacy e ai principali adempimenti del Regolamento UE 2016/679*, op. cit., 781.

permettere di garantire la tutela della privacy, istituendo enti certificatori e di controllo che verifichino il puntuale rispetto delle previsioni normative. In particolare, la verifica della conformità del trattamento alle linee guida, nell'ambito delle varie aziende, è affidata ad un organismo terzo indipendente, una sorta di organismo di certificazione chiamato TRUSTe, competente a rilasciare attestazioni di conformità riconosciute in tutti i ventuno Paesi aderenti, qualora i sistemi di protezione dei dati risultino coerenti con le indicazioni delle linee guida e garantiscano una tutela effettiva agli interessati[40].

Schema applicato su base assolutamente volontaria, nel senso che ogni azienda è libera o meno di prendere parte all'Accordo, sebbene non si può disconoscere l'esistenza di poteri indiretti di pressione su molte aziende (moral suasion), per adottare queste linee guida.

4.4) La protezione dei dati: fragile ma inevitabile barriera al controllo totale

La grande novità della 'Information and Comunication Technology' è che oggi le comunicazioni passano attraverso un sistema molto diffuso e veloce di trasferimento dei dati, sia a causa delle linee di trasmissione, prevalentemente telefoniche, e quindi gestite da provider telefonici, sia per l'assalto delle società multinazionali che, in pochi anni, sono riuscite a concentrare, in un numero molto piccolo di 'ott', il possesso delle piattaforme e larga parte dei servizi accessibili in Rete.

Si sono in tal modo venuti ad accumulare numeri sterminati di dati personali che, considerando la potenza dei server attuali e l'esistenza delle tecniche di big data[41], avvicinano sempre più il nostro mondo alla società del controllo globale.

A questo va ad aggiungersi l'enorme dimensione che ha assunto il fenomeno delle 'app' (app native e web app), il cui uso consente la raccolta, il trattamento e l'invio dei dati degli utenti in quantità cospicua e senza interruzioni e che rende praticamente impossibile

[40] Ad es., nell'agosto 2013 la IBM ha ricevuto l'ambito riconoscimento per le norme a tutela della privacy elaborate dalla società, risultate coerenti con i principi dell'APEC ed entrate in vigore nel novembre 2016. In queste norme di tutela della privacy vengono descritte le procedure di raccolta delle informazioni da parte dei siti web IBM, le modalità di utilizzo dei cookie, web beacon e altre tecnologie nei prodotti software e nelle offerte Software-as-a-Service. Sono applicate per i siti Web IBM che includono un link a queste, mentre non sono applicate ai siti web che hanno norme proprie di tutela della privacy.

[41] La letteratura sui *big data*, termine polisenso, che si riferisce sia allo svilupparsi di server sempre più capaci di conservare e processare una quantità sterminata d dati, sia alla capacità di ottenere dal trattamento di questi dati , grazie ad algoritmi che sappiano interrogare la macchina in modo da avere da essa la risposta voluta o la informazione ricercata, una quantità sempre più sterminata di nuovi dati, che consentano nuove conoscenze e analisi relative ai fenomeni naturali e ai comportamenti umani.

conoscere i titolari, le modalità di uso e conservazione dei dati raccolti e le finalità per le quali sono trattati.

A questi fenomeni, già di per sé complessi, vanno a sommarsi i rischi che si possono correre in Rete, come il furto dei dati da chi non ha il diritto di conoscerli, il loro acquisto per un uso illecito, il rischio di hacheraggio[42]: sicchè i dati possono essere manipolati, falsificati, illecitamente diffusi e assemblati, in modo da trarre, dagli stessi, informazioni ulteriori e diverse da quelle in essi contenute, ovviamente gravemente lesive dei diritti di libertà e reputazione delle persone cui ineriscono.

Tutte queste raffinatezze tecnologiche, in continua evoluzione, lasciano intendere quanto sia difficile rendere effettivo il diritto alla protezione dei dati personali: difficoltà destinate ad aumentare man mano che la società digitale moltiplicherà i mille servizi, in un ormai assai prossimo futuro.

D'altra la parte, la tutela giuridica di quel diritto è la sola e irrinunciabile barriera a presidio della persona umana e dei suoi diritti fondamentali.

5) La stretta di mano digitale

L'esplosione del mondo digitale ha contribuito a rendere pregna di responsabilità l'identità con cui l'individuo si presenta ai social media e, per loro tramite, alle persone, fondando il concetto di 'stretta di mano digitale', quale nuova modalità di conoscenza ottenuta mediante l'acquisizione di un insieme d'informazioni pubbliche, raccolte attraverso Internet, che anticipa, condiziona e a volte impedisce la stretta di mano fisica.

La stretta di mano digitale altro non è che la ricerca su Google del nome e cognome di ciascuno: chiunque sia interessato a conoscere un individuo, per motivi di lavoro, sociali, professionali o altro, attraverso un clic, prima ancora della stretta di mano fisica, ottiene una conoscenza digitale dell'interlocutore che, se dovesse risultare insoddisfacente, potrebbe addirittura impedirne il contatto fisico, senza che l'interlocutore ne sarà mai a conoscenza. Il mondo è percettivo ed è sempre stato così; ha sempre tentato di minimizzare il rischio: se il contatto risulta pericoloso o spiacevole, da vari punti di vista, lo si evita; se dobbiamo affidare i nostri risparmi ad un promotore finanziario che da

[42] Il termine sta ad indicare l'insieme dei metodi, tecniche ed operazioni volte ad accedere ad un sistema hardware o software, conoscere i dati custoditi o trattati ed, eventualmente, modificarli.

ricerche risulta essere stato coinvolto in una truffa, sicuramente non lo chiameremo né per chiedergli spiegazioni, tantomeno per commissionargli l'operazione[43].

La conoscenza, prima ancora che diretta, è data dal 'contatto' con l'identità digitale dell'individuo, con ciò che lo riguarda, con i suoi video, le sue immagini, le sue opinioni, che, fondendosi in modo maldestro e superficiale, costituiscono spesso causa di una commistione della sua sfera privata con quella professionale, ragion per cui sarà opportuno un vaglio coscienzioso, tutt'altro che superficiale e fugace, dei risultati delle ricerche digitali, pur nella consapevolezza che in ogni immagine, in ogni opinione, ci sia pur sempre un fondo di verità.

E' una scelta 'invisibile', in quanto la persona 'studiata' non ha modo di capire che si stiano raccogliendo informazioni sulla sua identità, né chi ne sia l'artefice, quanto 'inevitabile' perché il solo modo per sfuggire alla stretta di mano digitale, è quello di non essere in Rete. Ma l'identità digitale nulla, non paga[44].

E' necessario, invece, che la persona abbia la consapevolezza che tutto ciò che posta non è semplicemente scritto sulla carta stampata, ma è come se fosse inciso sulla pietra: resterà per sempre e sarà sempre accessibile perché "fin che c'è Rete, c'è speranza"[45].

---

[43] A. BARCHIESI, Intervista rilasciata a Enel Radio, in data 18 luglio 2017.

[44] L'identità della persona, immersa in uno scenario tecnologico, si arricchisce di contenuti, a cui ciascuno contribuisce direttamente o indirettamente, che, crescendo di volume ogni giorno di più, restano intrappolati in una Rete che non dimentica. La potenza dell'identità digitale, pertanto, è proporzionata alla quantità dei contenuti, inerenti alla persona, presenti in Rete, destinata a crescere con l'aumento dei dati e delle informazioni, piuttosto che a ridursi.

Le problematiche relative alle difficoltà legate alla gestione di cotanto materiale circolante sulle varie piattaforme telematiche ha, in qualche occasione, fatto sorgere l'esigenza di essere cancellati dalla Rete, acquisendo così un'identità digitale nulla.

Ma tutto ciò è controproducente: oggi non ha senso non avere un profilo, non esistere in Rete non vuol dire essere riservati, ma non aver fatto nulla di rilevante oppure, nel peggiore dei casi, la cosa può destare sospetti, spingendo i terzi a cercare ulteriori informazioni. Non è tra l'altro utile 'sparire', chiudendo la pagina social, perché si lascerebbe la propria reputazione alla mercé degli altri utenti.

Ancora: qualora dovesse essere immesso in Rete un contenuto negativo, relativo ad un determinato individuo, che presenti un'identità digitale nulla, quel contenuto lesivo non potrà competere con eventuali altri contenuti positivi, considerata l'assenza di identità digitale, così l'individuo diverrebbe vulnerabile e sarebbe esposto ad ogni attacco. Al contrario, ove presentasse un'identità digitale robusta, i contenuti positivi presenti tenderebbero a controbilanciare e neutralizzare la potenza di quelli negativi. Così, se si parla poco di ciò che si è fatto, sia relativamente all'aspetto professionale, che ai contributi nel sociale, le notizie negative diventano preponderanti.

Bisogna pertanto selezionare e governare i contenuti delle informazioni e dei dati immessi sulle tante piattaforme e, per poterlo fare, bisogna esserci ed essere influenti.

E', altresì, necessario utilizzare una tecnica di raffinata ingegneria reputazionale, finalizzata alla costruzione di un'identità digitale robusta, perché solo così si potrà sperare in una reputazione digitale resistente che consenta di vivere la presenza in Rete come un'opportunità, piuttosto che come un modo per correre elevati rischi di vulnerabilità della propria immagine.

[45] A. BARCHIESI, *La tentazione dell'oblio*, Milano, 2016, 35.

E' altresì una stretta di mano fortemente condizionante, tanto da portare ad evitare il contatto sociale, qualora dai dati raccolti si percepisca che il soggetto presenti caratteristiche antitetiche a quelle che da lui ci si aspettava, sulla base della relazione che s'intendeva instaurare.

Il solo modo per ridurre i rischi è quello di fare attenzione a ciò che si posta, prestare attenzione all'analisi di quello che riguarda la persona, perché proprio quel magma di dati ed informazioni concorrerà a formare la sua reputazioni online.

A parere di esperti del settore, sarà la nuova generazione a pagare lo scotto maggiore dell'avvento digitale, a causa dei comportamenti, a volte anche troppo spregiudicati e disinibiti, verso le tecnologie in Rete, senza tener conto che il 70% dei 'recruiter', selezionatori del personale, valutano proprio i dati postati, prima di assumere[46], sull'errata convinzione che l'identità digitale che la persona offre di sé sia perfettamente coincidente con il suo prototipo reale.

Anche attraverso Facebook, piattaforma che si basa sul principio dell'identità reale, impiegando il proprio nome e cognome, ci si costruisce un'immagine digitale, dalla quale è possibile risalire al background culturale dell'individuo, alle sue convinzioni, alla sua eredità sociale ed intellettuale: è chiaro che i recruiters, prima ancora d'invitare al colloquio 'l'aspirante occupato', andranno a sbirciare la sua identità in Rete. E' pertanto indispensabile scegliere cosa condividere con la propria famiglia e con gli amici e cosa rendere pubblico a chi fa ricerche su Google e a chi, anche solo casualmente, rintracci il

[46] Nella vita professionale, la stretta di mano digitale ha via via assunto un'importanza sempre più pervasiva e condizionante per le relazioni umane, che si manifesta già dal momento della "ricerca del lavoro", per la quale non è più sufficiente essere in possesso di un buon curriculum, dal momento che i selezionatori, prima ancora di prenderlo in considerazione, effettuano la stretta di mano digitale, scartando tutti quei candidati che manifestino un risultato insoddisfacente. In tal modo, gli aspiranti in cerca di occupazione non saranno ammessi al colloquio, né mai saranno avvisati del reale motivo per il quale siano stati scartati.
E' una pervasività che dispiega, altresì, tutta la sua autorevolezza negli ulteriori e successivi aspetti della vita professionale: dal rapporto con i colleghi, in cui la stretta di mano digitale è mossa dalla curiosità, alle partnerships, in merito alle quali potrebbe determinare la rescissione di rapporti contrattuali, qualora il rappresentante dell'azienda presentasse di sé un'immagine digitale gravemente inadeguata e deficitaria; dalle relazioni con i clienti, il cui aspetto peculiare, costruito sulla fiducia, potrebbe essere gravemente condizionato, precludendo importanti opportunità, alle relazioni con i competitors, nelle quali, ove la stretta di mano dovesse presentare qualche punto di criticità o debolezza, l'immagine dell'azienda o del professionista potrebbe essere irrimediabilmente oscurata sul mercato.
Pervasività, che coinvolge anche altri settori, dal sociale, all'istituzionale, sino al parentale, sicché, non è un caso che negli USA siano già attivi servizi che consentono uno screening delle persone con le quali mantenere relazioni**.**
I motori di ricerca, pertanto, hanno un potere elevatissimo ed i risultati, associati ad una determinata ricerca, possono diventare un fattore determinante nelle scelte quotidiane di carattere economico e non. Una stretta di mano non adeguata può costituire una ragione 'silenziosa' che impedisce il contatto reale successivo.

profilo Facebook.[47] In alcuni Paesi sono circolate proposte per far sì che, compiuti i diciotto anni, si possano cancellare da Internet e dai social Network tutte le informazioni che i ragazzi minorenni hanno diffuso in Rete prima di quell'età: una restituzione di illibatezza digitale che eviterebbe problemi soprattutto in fase di ricerca del lavoro.

5.1) L'identità digitale: il nuovo biglietto da visita

Se la stretta di mano digitale è la nuova forma di presentazione, l'identità digitale è, a tutti gli effetti, il nuovo biglietto da visita, che contiene, non solo i dati anagrafici, ma uno spettro d'informazioni, sempre più pervasivo, del quotidiano, allarmante per la sua profondità e capillarità.

---

[47] I social potrebbero essere i più grandi nemici di chi cerca lavoro o di chi voglia solo conseguire miglioramenti nella propria attività professionale e, poiché la stretta di mano digitale non è soggetta a dialettica, la persona esclusa non sarà mai chiamata a chiarire cosa abbia inteso dire in quel particolare commento e se sia stata veramente lei l'autrice di un'esternazione. Semplicemente sarà esclusa, sia in forza della considerazione che bastano pochi secondi perché gli altri si formino un giudizio di te, sia perché le aziende hanno poco tempo da investire in colloqui.
Da qui la necessità di costruire delle regole, se non per annullare, quantomeno per ridurre i rischi della Rete, ripulendo il proprio profilo, cercando di renderlo attraente a chi andrà a visionarlo, in vista di eventuali e future selezioni professionali.
E' utile scegliere con cura le foto del profilo, quello è infatti il primo biglietto da visita, ma anche quelle successivamente postate all'interno della bacheca, associate al nome e cognome della persona. E' evidente la indispensabile coerenza tra le foto postate e l'immagine, corrispondente a quel nome e cognome, che si vuol dare. Bisogna selezionare il materiale, pubblicando tutto ciò che inerisca ai propri interessi o tutto ciò che si avvicini alla propria professionalità. Se si pubblicano video su ciò che si sa fare o se ne parla nei post, si avrà, tra l'altro, anche la possibilità di vincere 'il nemico nascosto', l'omonimo, il portatore dello stesso nome e cognome che, pubblicando contenuti inappropriati potrebbe, confondendo il selezionatore, produrre nocumento all'immagine del primo.
In forza di questo principio, se un contenuto non dovesse risultare perfettamente in linea con una posizione di lavoro, è preferibile scegliere l'opzione di restringere la cerchia della propria visibilità, anche se sarà necessario fare sempre i conti con le 'condivisioni'. Gli atteggiamenti difficili da spiegare, è preferibile cancellarli: "puoi essere un bravo studente 364 giorni all'anno, basta la bravata di un giorno per rovinarti la reputazione. Così come, "finalmente oggi è venerdì" potrebbe essere un post innocuo…ma così non è se a leggerlo è colui che dovrebbe dare fiducia, assegnando un ruolo di responsabilità a colui che l'ha postato. Sono sicuramente post da evitare anche perché sono proprio i post scomodi a costituire il "*curriculm vitae* digitale".
Per lo stesso motivo, i commenti devono essere equilibrati, privi d'insulti politici o razziali e soprattutto quantitativamente contenuti per non dare l'impressione di essere perennemente presenti in Rete, con gravi distorsioni nella vita privata e professionale. E' oggetto di attenzione anche l'originalità dei contenuti postati su Twitter. E' necessario, in conclusione, perché si abbia un utilizzo proficuo e non distorsivo della Rete, che ogni persona impari a sfruttare il web per creare la migliore proiezione pubblica e professionale di sé, diventando protagonista della propria identità, senza permettere che siano gli altri a definirla.
Non basta, in definitiva, la presenza di regole puntuali, né la previsione di forme di repressione, serve "l'educazione digitale", quale consapevolezza di ciò che si posta, e la comprensione delle insidie insite nel web, dal momento che Internet ha la grave colpa di moltiplicare un giudizio, di amplificare un grido, senza crearlo o accertarlo.

Non è la semplice trasposizione, nel mondo dei 'big data', dell'identità reale: la persona digitale è un modello di personalità basato su dati, qualcosa di più rispetto all'identità personale, perché non prevede tutte le espressioni di vita reale, ma solo quelle tracciate e modellate dalla Rete. E' qualcosa di più ampio perché riguarda, oltre che la proiezione nel web del patrimonio di idee ed azioni della persona, anche ulteriori aspetti specifici della dimensione informatica, quali l'identificazione di quella attraverso dati biometrici, abitudini di spostamento, di acquisto, di lettura, di reputazione, che forniscono una rappresentazione dell'individuo, non in quanto monade, ma immerso in un sistema di relazioni.

Informazioni, tra l'altro, il cui accesso è semplificato da una ricerca estremamente facile da effettuare, 'veloce', dal momento che i risultati sono in pochi secondi sotto gli occhi di chiunque lo voglia, 'economica', perché l'utilizzo di Internet non richiede grossi investimenti economici, e soprattutto 'profonda', considerato che le informazioni che si ricevono sono molto più estese di quelle richieste o anche solo immaginate.

Sono queste le ragioni per cui l'identità digitale dovrà essere priva di contenuti negativi legati al proprio nome o anche solo incompleti e inadeguati. E' il caso del dirigente d'azienda che presenti un profilo ricco di foto e video relativi al modo in cui trascorre il tempo libero, piuttosto che alla sua carriera. In questo caso, sebbene non si sia in presenza di contenuti negativi associati al nome, il biglietto da visita aziendale racconta ben poco d'interessante dal punto di vista professionale, anzi, al contrario, fornisce del professionista una figura sbiadita, ibrida. Ecco perché il problema che si è posto è stato anche quello di poter richiedere ai motori di ricerca la rimozione, non dei soli contenuti negativi, restituendo l'immagine o l'identità del soggetto interessato, depurata da quelle immagini o contenuti diffusi in Rete, che l'abbiano lesa, ma dell'intera identità digitale, per costruirne, in maniera razionale, una nuova, solida e ricca di informazioni interessanti, attraverso l'integrazione e l'interazione dei contenuti stessi. L'integrità della proiezione sociale della propria personalità, infatti, può risultare lesa anche solo dall'attribuzione di opinioni e idee che non sono di per sé offensive o illecite, ma semplicemente diverse da

quelle realmente professate dall'interessato[48]. Un'identità, quindi, tutta da ricostruire, che risulti vera e palesemente più utile alla persona[49].

Altro errore, gravemente sottovalutato, è rappresentato dallo 'spettro relazionale', ossia tutto l'insieme dei soggetti a cui l'individuo risulta correlato e che impedisce ad ogni identità di vivere in un'area perimetrata, circondata da alte mura, escludenti il contatto con gli altri. E' vero, infatti, il contrario, in quanto l'identità di ciascuno è soggetta a continue contaminazioni e scambi, più o meno culturali, con le altre identità con le quali va ad imbattersi, come immersa in un sistema di numerose identità, ognuna delle quali estende la sua influenza su quelle più prossime.

Non è chi non veda che, nell'effettuare la stretta di mano digitale con un altro individuo professionista, tra i vari contenuti presenti sul profilo di quest'ultimo, ci sono foto, video o altri commenti che lo citano e/o lo ritraggono insieme ad altri, per cui, qualora questi 'altri' fossero personaggi accademici, o comunque di spicco nella comunità, l'interrelazione con queste figure migliora enormemente l'identità del professionista e, come per osmosi, l'autorevolezza dell'identità degli altri si trasferisce sul primo. In caso contrario, su quest'ultimo verrebbe ad essere trasferito il rischio di un valore negativo, in relazione all'identità negativa dei personaggi che in quelle foto o video lo accompagnano. La morale è che lo spettro assai fluido delle identità impone di fare molta attenzione, non solo alla propria identità, ma anche a quella delle figure con cui s'intrecciano relazioni digitali. Essere associati a soggetti dalla reputazione negativa genera riflessi sconvenienti sul modo in cui l'individuo verrà percepito e profilato, con gravi distorsioni della propria identità, che potrebbero originare il rischio di far perdere importanti opportunità nella vita reale, in quanto è come se le caratteristiche negative della relazione digitale fossero in qualche misura traslate nell'individuo stesso, che ne diventerebbe, così, indiretto protagonista.

---

[48] G. PINO, *Il diritto all'identità personale ieri ed oggi. Informazione, mercati, dati personali, in* PANETTA R. (a cura di)*, Libera circolazione e protezione dei dati personali, Milano,* 2006, 620. Anche per l'Autore la tutela dell'identità personale non coincide con quella dell'onore e della reputazione, che presuppone invece l'attribuzione al diffamato di fatti offensivi.

[49] G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir.Inform.,* Anno XXIX, fascicolo 4 – 5 2014, 601. Valgono al riguardo le considerazioni di Finocchiaro, in riferimento al diritto all'identità personale e digitale: «*Il diritto alla protezione dei dati personali e i diritti della personalità ad esso limitrofi, quali i diritti all'identità personale, di rettifica, alla riservatezza, il diritto alla protezione dei dati personali, quelli alla reputazione, all'immagine, all'immagine, al nome, sono tutti diritti volti a tutelare un unico bene giuridico: l'identità*».

6) Dall'identità digitale alla reputazione in Rete

Il mondo digitale, fortemente pervasivo, che ha decretato la morte della privacy, ha fatto sorgere l'esigenza di mantenere e tutelare la reputazione on line di un individuo, di un'azienda e persino di un prodotto, consentendo contestualmente la possibilità di gestirne l'immagine proiettata in quel mondo.

Per la verità, la necessità di proteggere la propria reputazione è sempre esistita, solo che, mentre in passato le informazioni e i dati veicolavano attraverso il passaparola, per giungere ad un numero limitato di individui, oggi, invece, in un mondo iperconnesso, il problema si è notevolmente amplificato, essendo stato stravolto il meccanismo di veicolazione dei dati, per il quale non è più necessario il mero contatto fisico.

Oggi l'io digitale, forza invisibile che cerca informazioni, arrivando istantaneamente al portatore d'interesse, in quanto grandezza importante ed imponderabile, va governato. A questa specifica esigenza si deve la nascita dell'Ingegneria reputazionale, una vera e propria scienza informatica diretta ad analizzare e costruire la reputazione di un qualsiasi soggetto, azienda, prodotto, plasmando con dei criteri quasi fisici, e con delle regole strutturali, l'identità digitale di ciascuno.

E' una disciplina che, partendo dalla trasformazione dei contenuti in segnali matematici, è in grado di governare l'identità digitale attraverso un insieme di tecniche di trattamento dei segnali stessi, coniugando conoscenze avanzate d'informatica, data missing, comunicazione, marketing, pubbliche relazioni, al fine d'ingegnerizzare la reputazione di un soggetto.

La tecnologia, infatti, permette alle aziende di raccogliere, aggregare e analizzare i dati relativi a ciascun individuo, alle sue preferenze, opinioni, comportamenti e abitudini, con velocità, raffinatezza e precisione, attraverso operazioni matematiche, assegnando un punteggio ad ogni aspetto della sua vita[50]: dalle abilità di guida, alla salute, dall'affidabilità finanziaria, all'impegno politico, dalla predisposizione al matrimonio, al rispetto dell'ambiente. Punteggi basati su algoritmi elaborati da computers, privi di capacità di contestualizzazione, di compassione ed estremamente letterali ma estremamente pervasivi, dal momento che aziende e datori di lavoro fonderanno su questi punteggi le decisioni finalizzate a stabilire i rischi del credito, i premi delle assicurazioni, l'assunzione o il licenziamento del lavoratore.

[50] A. BARCHIESI, *La tentazione dell'oblio,* op.cit.

Una disciplina a metà tra precetti matematici e statistica dei risultati, oggi in grado di suggerire precise tecniche e punti di forza per costruire una buona reputazione, cercando di superare le selezioni operate da software e macchine.

Sono stati, altresì, elaborati dei precetti, cui la stessa ingegneria reputazionale deve sottostare, il primo dei quali è quello di: 'mai mentire'! La reputazione infatti, va costruita nel rispetto della verità, facendo emergere, attraverso i sofisticati mezzi d'ingegneria del web, i lati positivi che il soggetto possiede.

Inserendo una notizia falsa, la Rete avrà un meccanismo di reazione devastante: "mentire significa distruggere la propria credibilità e nessuno si avvarrà mai di una persona poco credibile. Il patto sociale si basa sull'affidabilità e sulla fiducia e la reputazione è un oggetto fondante della fiducia".

Quindi, prima regola: mai mentire!

Non è di secondaria importanza l'ultroneo principio che l'ingegneria reputazionale è tenuta ad osservare: "usare l'identità digitale per costruire, mai per distruggere[51]". Costruzione che va organizzata e pianificata attraverso un progetto e la sua successiva realizzazione, allo stesso modo che se si edificasse un edificio.

E' inoltre, indispensabile che ciascuno diventi un 'buon presentatore di se stesso', che impari a diffondere i propri contenuti, mettendoli a disposizione dei motori di ricerca. Il che non significa vivere continuamente in Rete, col rischio di produrre solo banalità, ma pubblicare commenti intelligenti, impegnarsi in conversazioni brillanti e socialmente edificanti.

E' anche consigliata la cura dello 'spettro relazionale', in quanto il collegamento con personaggi influenti farà maggiormente risplendere l'immagine di ciascuno, così come risulterà utile alla causa la costruzione di un profilo on line aggiornato e ricco di contenuti professionali, di post relativi agli ultimi sviluppi e tendenze, cancellando i post che potrebbero rivelarsi offensivi, oggetto di fraintendimento o quantomeno, rendendoli visibili solo agli amici più stretti, controllando costantemente la coerenza, e non contraddizione, tra il mondo on line e quello off line e facendo in modo che dal proprio profilo emerga qualcosa di unico e personale, che apporti valore all'azienda in cui si lavora, ai clienti, al pubblico.

[51] A. BARCHIESI, CEO di Reputation Manager, Intervista in *La Repubblica*, 14 febbraio 2016.

Come i motori di ricerca consentono agli utenti di trovare dati sul web, così i 'motori di reputazione' permetteranno sempre più alle aziende, ma anche alla gente comune, di cercare le tracce digitali di ciascun individuo, nel silenzio e nel segreto più assoluto sui fattori oggetto di valutazione presi in esame e sulle formule applicate per l'attribuzione dei punteggi.

Ecco perché è importante che la costruzione della reputazione avvenga ad opera di mani esperte, che sia fatta da professionisti con analitica scrupolosità e senza lasciare nulla al caso perché, a prescindere da quanto possano essere sofisticati i computer, essi non sono ancora in grado di discernere la finzione dalla realtà; la loro capacità a giudicare la veridicità delle informazioni deve ancora mettersi al passo con l'importanza delle decisioni che sono chiamati a prendere. Alle criticità dei meccanismi poco chiari e tutt'altro che intelligibili, fa però da contrappeso una miriade di opportunità e privilegi che una buona reputazione genera.

"Grazie alla capacità di Internet di trasmettere facilmente informazioni a chiunque nel mondo, come se si trovasse dietro l'angolo, l'occasione della vita può arrivare da qualunque luogo, anche da migliaia di chilometri di distanza[52]".

La web reputation, tuttavia, è efficace soprattutto nel lungo periodo e non opera nell'emergenza, in quanto è un'operazione diretta alla pubblicazione di contenuti premianti, volti a far scalare i risultati negativi sempre più in basso ed il lungo periodo sarà necessario per permettere la sedimentazione dei dati.

6.1) Reputation manager: come va costruita la reputazione online.

"Avere un'ottima reputazione e se manca costruirla! Con buone impronte digitali, il mondo è ai vostri piedi[53]". E' questa la parola d'ordine della reputation economy che introduce agli strumenti del mestiere, alle intuizioni ed ai segreti per gestirla, suggerendo come sfruttarne al meglio le dinamiche, per migliorare le prospettive professionali, finanziarie e sociali di ciascuno, ma anche creare carte false e cartine fumogene, per nascondere le informazioni negative.

[52] A. BARCHIESI, CEO di Reputation Manager, intervista alla *Repubblica*, op. cit.
[53] A. BARCHIESI, *La tentazione dell'oblio*, op. cit.

Nulla di nuovo se si pensa che già nel I Secolo a.c., lo scrittore romano Publio Siro annunciava che "una buona reputazione equivale ad un altro patrimonio, perché una buona reputazione ha più valore del denaro[54]".

Di nuovo, invece, c'è la tecnologia, che ha reso possibile la raccolta, la selezione, l'analisi e la distribuzione di ogni tipo d'informazione che ci riguardi, fino ad ottenere un elenco completo di tutte le attività, mettendo a dura prova l'immagine personale, oltre che la reputazione, tanto da richiedere come indispensabile, l'aiuto di professionisti specializzati nella gestione della reputazioni on line.

Società leader nel mercato della reputazione on line è 'Reputation manager', che ha all'attivo la gestione di centinaia di casi relativi a personaggi pubblici, istituzioni, aziende e prodotti, nei quali, applicando i principi di cui sopra, cerca di apportare dei correttivi alla web reputation dei suoi clienti.

Il punto di forza del servizio offerto dalla società è quello di definire, tutelare e promuovere sul web un'immagine professionale solida, sicura e ben posizionata. Spesso, infatti, capita che i dati presenti on line non riportino le informazioni realmente rilevanti per l'interessato e che andrebbero, invece, messe in evidenza. Il team di 'Reputation manager, dopo aver studiato i punti di forza, di debolezza e le lacune dell'immagine digitale, progetta una vera e propria strategia editoriale, per allineare l'identità on line a quella off line, attraverso l'elaborazione, l'organizzazione, la pubblicazione e soprattutto la valorizzazione di contenuti professionali di altissima qualità.

L'assenza di negatività, infatti, non significa avere una buona reputazione, perché questa potrebbe non essere negativa, ma essere molto debole, se non nulla. Una grande esperienza ma una scarsa visibilità sui motori di ricerca può essere fortemente penalizzante, per cui la società esperta in ricostruzione della reputazione, mettendo in luce tutto il potenziale positivo della persona, aiuta i suoi clienti ad individuarsi e differenziarsi in Rete, attraverso strategie di visibilità appropriate e personalizzate, creando profili on line di alto livello, costruendo un io adeguato al ruolo ed alle aspettative del cliente, accrescendo le potenzialità per moltiplicare le opportunità, attraverso l'utilizzo di canali di comunicazione specifici, ad elevato valore aggiunto. Si considerino due avvocati, entrambi con spiccate competenze nell'e-commerce: uno presente in Rete con una reputazione strutturata, l'altro no. Le aziende, molto probabilmente, si rivolgeranno al

[54] F. GIANNOTTI, *Ricerche sulla tradizione manoscritta delle sentenze di Publilio Siro*, Firenze, 1963.

primo; il secondo, pur avendo pari competenze e assenza di lesività, presentando, tuttavia, un'identità debole, difficilmente avrà l'opportunità di essere contattato. Della mancata opportunità non ne sarà nemmeno consapevole, perché la reputazione on line è una forza invisibile, che non accetta alcuna dialettica.

Sulla base di queste premesse, si osserva come l'ingegneria reputazionale è sicuramente in grado di porre riparo a situazioni personali gravemente compromesse, ma sarebbe erroneo affermare che assolva solo a questa funzione, perché altrimenti si dovrebbe giungere alla conclusione che chi non presenti alcuna lesività on line, non trarrebbe alcun giovamento dalla sua applicazione.

In quest'ottica, la soluzione alle problematiche legate alla gestione dell'ingegneria reputazionale non sarebbe l'esercizio del diritto all'oblio, quale forza sottrattiva in grado di escludere dalla Rete elementi dell'identità della persona, per ragioni tecnologiche o per espressa e formale richiesta della stessa, riducendo o eliminando tutto ciò che forze additive, interne o esterne al soggetto stesso, avevano inserito nei vari canali telematici e che andavano a costruire e irrobustire l'identità digitale della persona.

Agendo per sottrazione, l'esercizio del diritto all'oblio ottiene quale risultato, sicuramente quello di eliminare i contenuti lesivi, generando uno spostamento verso l'alto degli altri contenuti che si leggono digitando il nome e cognome dell'interessato, ma tra questi ultimi non è escluso che possano essercene di altrettanto lesivi e, in tal caso, la situazione non verrebbe a migliorare di molto. Tra l'altro, il suo esercizio, riducendo gravemente i contenuti, porterebbe il soggetto verso un'identità digitale poco robusta, poco credibile e, come tale, alquanto vulnerabile[55].

Serve, invece, adottare un metodo che riesca a coniugare le due forze, additive e sottrattive, allo scopo di costruire una reputazione digitale forte e robusta rispetto alle potenziali lesività, dal momento che l'obiettivo non è tanto quello di ridurre la propria presenza in Rete, se non addirittura azzerarla, ma avere un io digitale forte, adeguato alle proprie aspirazioni.

Secondo tale orientamento dottrinario, infatti, sarebbe opportuno utilizzare la leva delle forze additive che, se adeguatamente impiegate, potrebbero contribuire a costruire, in modo strutturato, l'identità digitale, anche attraverso il recupero dei trascorsi della

[55] A. BARCHIESI, *La tentazione dell'oblio,* op. cit., 190.

persona, passati sotto silenzio, per creare un meccanismo virtuoso che inneschi nuove relazioni con altri individui.

Forze additive interne, derivanti dai canali dello stesso interessato che, per rendere più robusta la propria identità, dovrà arricchirla con dati e informazioni inerenti aspetti positivi della sua vita professionale, sociale e familiare e forze additive esterne, comunque sempre controllate e controllabili dallo stesso.

Attraverso l'uso e l'operatività ben congegnata delle due forze, della loro intensità e intersezione, e quindi attraverso operazioni d'ingegneria reputazionale, sarebbe possibile non solo progettare e realizzare una precisa web reputation, ma anche indirizzare le sue possibili future evoluzioni.

6.2) Lo sportello Help Web Reputation Giovani del Co.Re.Com. Lombardia

Come le imprese si avvalgono ormai costantemente di professionisti per il cleaning della loro reputazione digitale, lo Sportello Help Web Reputation Giovani offre lo stesso tipo di servizi ai privati cittadini che, non solo non saprebbero a chi rivolgersi, ma non disporrebbero neanche delle risorse economiche e tecniche utili alla difesa della propria immagine in Rete.

Il Co.Re.Com della Regione Lombardia, primo nel settore in Italia e progetto pilota in Europa, ha realizzato un programma molto ambizioso, attivando uno 'Sportello Web Reputation', divenuto operativo dal 1° luglio 2014, al quale i cittadini, persone fisiche, imprese e soprattutto giovani, che si ritengano lesi nella propria reputazione attraverso un uso improprio della Rete, possano rivolgersi per ricevere assistenza ai fini della tutela della propria reputazione digitale, in maniera assolutamente gratuita[56].

E' possibile chiedere l'intervento dello 'Sportello' quando, imprudentemente o all'insaputa dell'interessato, siano stati immessi o diffusi immagini, scritti personali o corrispondenza, dati o informazioni oppure anche quando, in Rete, siano stati pubblicati articoli, commenti o immagini umilianti, discriminatorie (per orientamento sessuale, etnia o credo religioso dell'interessato), o offensive della reputazione, dignità e immagine della persona, al fine di ottenere la rimozione dei contenuti ritenuti lesivi, pur essendo,

[56] Il progetto presentato ufficialmente il 30 maggio 2014, anche sulla scia degli esiti della sentenza CGUE Google Spain, alla presenza, tra gli altri del Presidente dell'Agcom, Avv. Angelo Marcello Cardani, del Viceministro del Consiglio Antonio Catricalà e del Presidente del Comitato Media e Minori dott. Maurizio Mensi, lo *Sportello Help Web Reputation Giovani* è divenuto operativo dal 1° luglio del 2014.

l'interessato, comunque, libero, ove la pubblicazione comporti implicazioni giudiziarie, sia sotto il profilo penale che civile, di adire la via giudiziaria, non avendo lo sportello competenze in tal senso.

Al fine di facilitare il cittadino interessato, il Co.Re.Com Lombardia lavora in sinergia con il Compartimento di Polizia postale e delle Comunicazioni della Regione, sulla base di un Protocollo d'Intesa dagli stessi sottoscritto[57] che, da un lato, delimita i rispettivi ambiti d'intervento e, dall'altro, rende sinergica la loro collaborazione.

Per richiedere l'intervento, l'interessato non ha che da compilare il modello scaricabile dal sito della Co.Re.Com, completarlo in tutte le sue parti ed inviarlo, in via telematica, allo Sportello, i cui uffici, dopo una prima valutazione, mirata a distinguere ed eventualmente segnalare i casi di competenza dell'Autorità giudiziaria o di pubblica sicurezza, attraverso i propri operatori prenderanno in carico il caso sottoposto e, in tempi molto brevi, decideranno in merito alla richiesta di correzione o rimozione dei contenuti segnalati.

Le modalità attraverso cui ottenere la rimozione dei contenuti sono numerose e variano a seconda degli strumenti messi a disposizione dalle diverse piattaforme; la quasi totalità dei social network, infatti, presenta sistemi automatizzati di segnalazione di account per cui, una volta segnalati, i dati vengono rimossi in tempi piuttosto ristretti. Qualora invece, si tratti di blog, per cui è necessario fare riferimento ai gestori del servizio o ai titolari delle singole testate, la segnalazione avviene per via di comunicazione privata, al fine di tutelare la privacy del cittadino, parte lesa.

La segnalazione privata è comunque da preferire perché la visibilità della segnalazione di rimozione potrebbe avere l'effetto controproducente di dare maggiore visibilità al contenuto da rimuovere. In tal senso si è dimostrata di grande utilità la sentenza della CGUE 131 del 13 maggio 2014, sia come precedente specifico dell'applicazione delle leggi che tutelano la privacy e il diritto all'oblio dei cittadini europei nell'ambito dei nuovi media, che come origine di un processo di adeguamento, da parte dei colossi della Rete, rispetto alla procedure messe a disposizione degli utenti, per la tutela della propria reputazione.

[57] Progetto Co. Re. Com. Lombardia, *Protocollo per l'istituzione dello sportello Help Web Reputation e formazione alla tutela della riservatezza personale*, 1° ottobre 2014.

Lo ‘Sportello’, infine, svolge anche un’attività di prevenzione con l’Ufficio Scolastico regionale, organizzando corsi di formazione sul corretto uso della Rete da parte dei più giovani, allargando la partecipazione anche ai genitori, illustrando loro le caratteristiche dei singoli social networks, indicando ciò che è consentito fare o meno in Rete e chiarendo le modalità di inserimento e di rimozione delle informazioni dal web.

Gli esiti dell’attività svolta si sono rivelati, sin da subito, decisamente positivi, sia in termini di sensibilizzazione dei giovani e delle famiglie, che di quantità dei contenuti rimossi, ma il riscontro, al di là dei risultati conseguiti, è stato estremamente positivo anche sul fronte umano-psicologico, dal momento che tutti coloro che hanno partecipato al dialogo con queste istituzioni hanno manifestato apprezzamento per l’iniziativa; è altresì emerso dagli incontri un elevato uso del web e dei social media da parte degli adolescenti, cui corrisponde una scarsa consapevolezza dei rischi che, i sistemi messi a loro disposizione dalla Rete, comportano all’immagine e alla loro identità online e offline. Rischi sconosciuti, com’è risultato dagli incontri, agli stessi genitori, ed in generale agli adulti, che dovrebbero vigilare sui comportamenti dei figli.

7) Verso la reputation economy: lo scandalo Volkswagen

La reputazione è potere!

La capacità di condizionamento esercitata dalla reputazione è più potente che mai. Nell’economia della reputazione, in cui le tecnologie consentono ad aziende ed individui, non solo di raccogliere dati, ma anche di aggregarli ed analizzarli con una rapidità spaventosa, con precisione e in modo sofisticato, la reputazione digitale sta diventando la nostra moneta più preziosa.

Sebbene attenga alle regioni e alle ragioni dell’evoluzione tecnologica legata alla circolazione delle informazioni, la reputazione digitale non va, tuttavia, confusa con l’esposizione mediatica, dal momento che questa è un faro che si accende per brevi momenti dando luogo ad un’opportunità che può anche non essere colta; la prima, invece, è qualcosa che si sostanzia nel tempo ed è legata alla costruzione di un valore, quello della ‘fiducia’.

E’, infatti, proprio la fiducia a governare le relazioni on line e ad essere alla base dell’economia della reputazione: l’immagine di ciascuno dipende dalla percezione che gli

altri ricavano dai contenuti on line che lo riguardano e dalla fiducia o sfiducia che gli stessi generano.

La buona reputazione è la moneta giusta che consente all'individuo di accedere alle relazioni di valore professionale e non; una reputazione negativa equivale ad una moneta di pochissimo valore; una reputazione nulla equivale al mancato possesso di moneta.

Ancor peggio è una reputazione falsa, fondata su menzogne e costrutti artificiosi, che, presentando lo stesso valore di una moneta falsa, e quindi facilmente invalidabile, non può che generare una reputazione negativa.

E' di fine settembre lo scandalo reputazionale, di proporzioni mondiali senza precedenti, che ha travolto la società tedesca Volkswagen.

In seguito ad alcuni controlli effettuati negli USA, sui livelli di emissioni inquinanti dei veicoli diesel, è emerso che la casa automobilistica tedesca, per anni, abbia falsificato i test sull'impatto ambientale, utilizzando un software per truccare i risultati.

La conseguenza immediata è stata il crollo della fiducia che ha portato al crollo del titolo sul mercato di borsa e la perdita del 23% del valore di mercato.

Un danno economico spaventoso e un danno reputazionale, se è possibile, ancora più grande. A due giorni dall'assai difficile confessione al mondo, il CEO Martin Winterkorn, che si è dichiarato ignaro di quanto perpetrato per anni all'interno della sua azienda, e deciso ad accertarne tutte le responsabilità, ha rassegnato le dimissioni.

Su di lui e sul brand una pioggia di commenti negativi in Rete che, dopo qualche giorno, avevano raggiunto l'80% dei contenuti riferibili all'azienda in quel periodo. Lo scandalo è come se sia stato scolpito nella storia; immediatamente è esploso sulle pagine Wikipedia, su tutte le testate giornalistiche, su blog, nei forum e su tutte le prime pagine dei motori di ricerca.

Di fronte ad un clamore di tali dimensioni non è stato più possibile tornare indietro, neanche invocando l'intervento della macchina reputazionale. E' un caso in cui, tra l'altro, l'oblio non potrà mai essere concesso perché corrisponde al massimo livello d'interesse da parte della collettività, la conoscenza dell'operato di una figura mediaticamente e istituzionalmente tanto esposta.

Un caso che ha travolto non solo l'azienda ma l'intero settore automobilistico, l'industria e il governo tedeschi, con forti implicazioni sulle relazioni internazionali all'interno dell'UE e tra l'Unione europea e gli Stati Uniti d'America.

Prima dello scandalo, Winterkorn era ritenuto uno dei manager più capaci, con una solida reputazione, in Rete circolavano articoli che elogiavano le sue doti comunicative e la capacità di utilizzare in modo efficace i media digitali.
A un giorno dal suo coming out, su di lui, on line, restano solo le feroci critiche di chi non può credere che non sapesse e gli attacchi alla sua buonuscita milionaria.
In un caso del genere, la rimozione di milioni di contenuti, i tagli dei link, non pagano e, tra l'altro, non sarebbero neanche giusti, trattandosi di riferimenti ad un fatto storico molto grave, che tutti hanno il diritto di continuare a conoscere.
Certo lo scandalo della Volkswagen è un caso da manuale che fa comprendere come, di fronte ad eventi di tali proporzioni, sia necessario ridefinire tutte le priorità di business, di branding e di comunicazione e, lottando contro ciò che si è irrimediabilmente commesso agli occhi del mondo, ricostruire la reputazione della persona, dell'azienda, del prodotto.
L'esercizio del nuovo diritto all'oblio non è sufficiente, né utile alla causa.

SEZIONE II: Il trattamento dei dati personali nell'evoluzione normativa europea, dalla Convenzione di Strasburgo 108/1981: un lento affermarsi, nel quadro europeo, del diritto alla protezione dei dati personali

1) Il ruolo del ricordo e l'importanza dell'oblio: il diritto alla memoria e l'opposto diritto alla cancellazione dei dati non più necessari

L'uomo ha sempre fatto di tutto per non dimenticare, per tenersi stretto i ricordi, nonostante, in passato, dimenticare sia stato più facile e meno costoso che ricordare. Ha cercato di migliorare le sue capacità di trattenere i ricordi, aumentando la quantità d'informazioni da immagazzinare e richiamare alla memoria, perché ricordare aiutava ad affrontare la vita e prendere le decisioni, nella speranza che il ricordo del passato potesse sopperire alla mancanza d'informazioni sul presente e all'incertezza insita nel futuro.
Ricordi, che inizialmente veicolavano tra le genti attraverso il linguaggio, ma con il grosso limite che nel tempo, attraverso il racconto, i dettagli si perdevano, il ricordo intero sbiadiva, la storia veniva ad essere alterata.

Con l'invenzione della scrittura prima e le tecniche di conservazione delle conoscenze poi, si sono aperte nuove frontiere nella gestione del ricordo. La nascita delle biblioteche aperte al pubblico, anche nei centri minori, ha sicuramente favorito l'indelebilità dei fatti passati, anche se, a causa dell'analfabetismo assai diffuso e dell'alto costo, i libri, scritti a mano dagli amanuensi e perlopiù di proprietà dei governanti, di fatto erano consultati da pochi[58].

Complice l'invenzione della stampa a caratteri mobili di Gutemberg ed una riduzione drastica del prezzo della carta, a fine '800 la produzione di libri e giornali cresceva vertiginosamente, parallelamente all'aumento del numero dei lettori che, attraverso la lettura di massa, soprattutto dei giornali, riuscivano a definire i luoghi in cui si verificavano gli eventi, per cui, prescindendo dalle distanze, avevano la possibilità di sentirsi parte di una comunità in cui le persone si sentivano vicine, non per questioni geografiche, ma in quanto facenti parte della stessa comunità di appartenenza.

Nonostante la memoria prodotta nell'800 fosse di gran lunga superiore a quella precedente, per svariate ragioni, tuttavia, il ricordo a lungo termine continuava a conoscere limiti: la carta si disintegrava rapidamente e i documenti erano destinati all'autodistruzione. Contenevano in sé una scadenza automatica.

Il passaggio tecnologico successivo ha avuto un obiettivo chiaro, ambizioso e alternativo al precedente: quello di eliminare l'oblio, "credo sia questo il vero significato del personal computer: catturare tutta la vita di ognuno di noi[59]".

Con il passaggio dall'era tecnologica a quella digitale vengono a modificarsi in maniera sostanziale le tipologie di informazioni che possono essere ricordate, le modalità e il prezzo del ricordo.

Man mano, infatti, che sono venuti meno i vincoli economici, gli esseri umani hanno iniziato ad incrementare massivamente la quantità d'informazioni, affidandole alla memoria digitale, relativamente non solo ai settori economici, ma a tutti gli aspetti della

---

[58] D. V. MAYER-SCHONBERGER, *Delete. Il diritto all'oblio nell'era digitale,* Milano, 2013, 29: «*I Tolomei pagavano laute somme di denaro per prendere in prestito e copiare testi importanti custoditi all'estero. Tolomeo III, per esempio, versò una cauzione agli ateniesi per ottenere dei loro documenti importanti, ne fece delle copie meticolose e le mandò ad Atene, trattenendosi gli originali, perché riteneva che ogni copia comportasse inevitabilmente degli errori che riducevano il valore del documento*».

[59] G. SHARON, *Total recall: storing every life memory in a surrogate brain*, in *Computer world*, aprile, II, 2008.

vita dell'individuo, ribaltando il vecchio principio, sicchè oggi 'ricordare è la norma, non più l'eccezione'. Nel cyberspazio rimane traccia di tutto e di tutti.

L'informazione digitalizzata è 'a prova di futuro': una volta digitalizzato il segnale e salvato su memoria è come se fosse stato scolpito sulla pietra. I bassissimi costi di memorizzazione e diffusione delle informazioni hanno realizzato l'obsoleto desiderio umano di una sempre maggiore capacità di memoria: oggi dimenticare è diventato drammaticamente costoso e difficile.

La digitalizzazione, abbinata alla memorizzazione poco costosa e alla facilità delle tecniche di recupero e trasmissione delle informazioni online, fa sì che la stessa sia prontamente disponibile e per sempre.

Ovviamente l'operazione non è esente da rischi! Il più ricorrente è che l'informazione, una volta postata in Rete, attraverso il fenomeno della condivisione, cominci a vivere una vita propria, diversa e autonoma rispetto al suo autore che, in tal modo, ne verrà a perdere il controllo.

Difficilmente il suo titolare ne rientrerà in possesso, né potrà vietare agli altri di condividerla, dal momento che non è neanche in grado di sapere in quali mani i dati relativi alla sua persona siano finiti e per quali vie del cyberspazio stiano navigando.

Annullare questi default di memorizzazione è complesso, a volte impossibile; se ai tempi dell'analogico era già un'illusione pensare di esercitare un controllo assoluto sulla circolazione dei dati, con il passaggio al digitale, la possibilità di esercitare il diritto all'autodeterminazione informatica sui propri dati si è enormemente ridotta.

E' vero, d'altra parte, che la condivisione delle informazioni produce effetti anche positivi, offrendo "opportunità di continuità e conservazione che trascendono la condizione stessa dell'essere umano, lasciando tracce e facendo sì che la vita di una persona abbia significato, e non essere vissuti invano"[60].

"La conoscenza è potere", scriveva Bacon[61] e l'accesso alla memoria digitale, assecondando la sete di conoscenza, offre sicuramente vantaggi enormi, ma non si possono, d'altra parte, negare le conseguenze potenzialmente pericolose, cui i singoli, le società e la comunità intera sono esposti, in conseguenza del controllo sulle informazioni

[60] R. NOZICH, *Philosophical explanation*, in *Harvard University Press*, 1981, 584.
[61] F. BACONE, *Religious meditations of heresias*, Londra, XVI Sec.

loro riferibili e sulla loro veicolazione, fenomeni di fronte ai quali sono assolutamente inermi.

La consapevolezza che la perdita del controllo sui propri dati non sia affatto indolore ha indotto i governi di un po' tutti gli Stati, sin dalla metà del secolo scorso, a correre ai ripari, apprestando nuove regole dirette alla limitazione della circolazione delle informazioni, laddove non ne sia possibile il recupero.

2) Le prime leggi di protezione dei dati personali in Europa

Nessuna Carta costituzionale europea dei primi anni successivi alla Seconda Guerra Mondiale aveva provveduto ad inserire, tra i diritti fondamentali, quello alla protezione dei dati personali, quale diritto autonomo, distinto e separato dai diritti alla riservatezza e al rispetto della vita privata che, a differenza del primo, sono stati oggetto di riconoscimento di specifica tutela, a cominciare dalla CEDU[62].

Tanto, perché le Costituzioni dell'immediato dopoguerra, elaborate da una classe giuridica e politica di primissima qualità, che aveva sofferto le persecuzioni e gli abusi ad opera del precedente regime totalitario, hanno manifestato un interesse maggiore verso i valori della democrazia e un legame più profondo con la previsione di ogni possibile forma di tutela di quelli, sottovalutando o quanto meno non manifestando un'adeguata consapevolezza del ruolo e degli effetti, altamente dirompenti, che le nuove tecnologie legate all'informatica avrebbero avuto sui fondamentali diritti e libertà della persona[63].

Nel contesto europeo, pertanto, la consapevolezza della necessità di una normativa specifica a protezione dei dati personali, sganciata dal diritto alla riservatezza e da quello al rispetto della dignità umana, è mancata per lungo tempo anche perché la tecnologia, per altrettanto lungo periodo, è stata percepita come uno strumento, per alcuni versi anche utile e non come un elemento capace di condizionare le modalità di esercizio dei diritti o

[62] Convenzione europea dei Diritti dell'Uomo (CEDU), art. 8: «*Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. Non può esservi ingerenza di un'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 per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del Paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale o per la protezione dei diritti e delle libertà altrui*».

[63] Sul tema, uno degli autori che nella letteratura giuridica italiana ha manifestato particolare attenzione, è stato S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995; ID., *Tecnopolitica: la democrazia e le nuove tecnologie delle comunicazioni*, Bari, 2004. Più recente e con un approccio più filosofico: E. SEVERINO, *Democrazia, tecnica e capitalismo*, Brescia, 2009.

persino di comportare la nascita di nuovi diritti, idonei a regolamentare una pacifica ed equilibrata convivenza tra tecnica e democrazia.

Nella stessa direzione hanno operato i padri costituenti italiani, i quali, non avendo per tempo percepito la portata e le conseguenze che le innovazioni tecnologiche, in particolare quelle legate all'archiviazione e al trattamento automatizzato dei dati personali, avrebbero comportato, non hanno riportato nella Carta costituzionale alcun riferimento, diretto o indiretto, alla necessità di prevedere forme di tutela per i dati inerenti alla persona, limitandosi alla previsione espressa delle libertà d'informazione e di stampa.

Anche la Convenzione europea dei diritti dell'uomo, elaborata dal Consiglio d'Europa nel 1950 ed entrata in vigore nel 1953, non dedicava alla protezione dei dati personali una normativa specifica, facendo rientrare quell'esigenza nell'art. 8 che, garantendo il rispetto della vita privata e familiare, assorbiva il diritto alla protezione dei dati personali, prevedendo una serie di restrizioni.

La veloce evoluzione delle tecnologie applicate all'informazione ha determinato, intorno agli anni '60, un crescente bisogno di norme, più precise e dettagliate, finalizzate alla tutela delle persone e alla protezione dei loro dati, in assenza delle quali, il Comitato dei Ministri del Consiglio d'Europa, a metà degli anni '70, ha adottato varie risoluzioni, in quella materia, facendo riferimento proprio all'art. 8 CEDU.

La stessa giurisprudenza della Corte EDU, istituita nel 1959 con il compito di valutare e decidere sulle denunce presentate da singoli individui, gruppi, ONG o persone giuridiche che avessero lamentato violazioni della Convenzione, più volte si è trovata ad affrontare il tema della protezione dei dati, trattando per la maggior parte casi riguardanti presunte violazioni nel campo delle intercettazioni delle comunicazioni[64], forme di sorveglianza di massa[65], violazioni di norme inerenti la conservazione dei dati personali da parte delle autorità pubbliche[66].

---

[64] Corte eur. dir. uomo, sentenza del 6 settembre 1978, *Klass e altri c.Germania*, serie A nº 28, pp. 23-25, 50, 54 e 55, in *Quaderni eur*., 2015, 71; Corte eur. dir. uomo, sentenza 2 agosto 1984, *Malone c. Regno Unito* in *Riv. Dir. Internaz.*, 1986, 838; Corte eur. dir. uomo, sentenza, 3 aprile 2007 *Copland c. Regno Unito*.

[65]; Corte eur. dir. uomo, sentenza, 3 aprile 2007 *Copland c. Regno Unito*, in cui si tratta di dati raccolti attraverso la sorveglianza dell'uso che una persona fa di Internet, ivi compreso le e-mail; Corte eur. dir. uomo sentenza del 2 settembre 2010, *Uzun/Germania*, in www.osservatoriocedu.eu, in cui la Corte decide se la sorveglianza via GPS compiuta dalle autorità investigative interferisca o meno nel diritto del ricorrente al rispetto della propria vita privata.

[66] Corte eur. dir. uomo, sentenza del 26 marzo 1987, *Leander/Svezia* in *Rep. Giur. It*., 2008; Corte eur. dir. uomo, sentenza del 4 dicembre 2008, *S. & Marper/Regno Unito*, in www.biodiritto.org, in cui due cittadini inglesi, accusati di aver commesso alcune fattispecie di reato, venivano sottoposti a prelievo coattivo di

In tutte le sue pronunce, la Corte ha avuto modo di precisare che l'art. 8 CEDU, in assenza di altre e più specifiche norme, non solo obbliga gli Stati ad astenersi da qualsiasi azione che possa violare quel diritto espressamente previsto dalla Convenzione, ma impone loro l'obbligo di garantire attivamente l'effettivo rispetto della vita privata, proteggendo gli individui dagli abusi che possono accompagnare la raccolta e il trattamento dei dati personali, imponendo il rispetto dei principi di correttezza e liceità nella fase della raccolta e del successivo trattamento, la destinazione dei dati ad un uso compatibile con la raccolta, la loro archiviazione per scopi specifici e legittimi e la durata della conservazione, limitata al tempo necessario relativo alle finalità della raccolta stessa.
Precorrendo i tempi, vietava altresì il trattamento dei dati sensibili, come quelli inerenti la razza, le opinioni politiche, la salute, la religione, l'orientamento sessuale o i precedenti giudiziari dell'individuo e nel contempo riconosceva all'interessato il diritto ad essere informato del trattamento e della conservazione di informazioni e dati relativi alla sua persona, oltre a quello di chiederne, se del caso, la rettifica.
Quelle stesse esigenze che hanno giustificato gli interventi del Comitato dei Ministri del Consiglio d'Europa e della Corte EDU, hanno portato molti degli Stati nazionali a dotarsi di numerose leggi di protezione dei dati personali, in assenza dell'intervento univoco del Legislatore europeo, con un aggravio dei problemi causati dalla difficoltà di una reciproca compatibilità, o di vera e propria confliggenza, tra le varie legislazioni nazionali.
Spinto dalle necessità di cui sopra, agli inizi degli anni '80 del secolo scorso, si assisteva finalmente ad un nuovo intervento del Legislatore europeo, in particolare del Consiglio d'Europa, che il 28 gennaio 1981, a Strasburgo, adottava la Convenzione n. 108, relativa alla 'Protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale[67].

---

campioni biologici per la profilazione genetica, con conseguente storage permanente dei dati acquisiti nel database nazionale. A seguito del riconoscimento della loro innocenza i due chiedevano ripetutamente, con esito negativo, la cancellazione dei dati dai database nazionali. Adita la CEDU, questa si è pronunciata in merito ritenendo "incompatibili con l'art. 8 della Convenzione le modalità di conservazione di campioni e dati previste dal National DNA Database del Regno Unito" e condannando lo stato inglese in quanto la legislazione statale che ammette la conservazione illimitata di dati anche di cittadini innocenti "era lesiva del diritto alla vita privata dei ricorrenti e non rispettava lo standard di proporzionalità richiesto, superando il margine di apprezzamento statale ammesso".

[67] Convenzione 108/1981, art. 1: «*Scopo della presente Convenzione è quello di garantire, sul territorio di ogni Parte, ad ogni persona fisica, qualunque siano la sua cittadinanza o residenza, il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano ("protezione dei dati")*».

I tempi richiedevano una normativa europea che, in maniera uniforme, regolasse un fenomeno altamente pervasivo della vita privata, e la Convenzione 108, che sicuramente rappresenta un salto di qualità rispetto all'art. 8 CEDU, rispondeva perfettamente a quell'esigenza[68], avendo consentito la raccolta e il trattamento dei dati solo in presenza di basi giuridiche che lo avessero autorizzato, di scopi specifici e legittimi che lo giustificassero e della loro destinazione ad un uso compatibile con la finalità per la quale erano stati raccolti.

Richiedeva altresì, la necessità che i dati raccolti fossero corretti, pertinenti allo scopo e non eccessivi rispetto alla finalità perseguita, riconoscendo il diritto all'interessato di chiederne la rettifica se inesatti e di ottenere informazioni in merito a quali dati fossero conservati.

Vietava il trattamento dei dati sensibili.

In merito al trasferimento delle informazioni raccolte, conteneva un principio opposto a quello che poi sarebbe stato introdotto con la Direttiva 95/46 CE, ossia quello della loro circolazione senza necessità di autorizzazioni[69].

---

[68] Sul tema, particolarmente importanti sono gli art. 5 e 6 della Convenzione 108 del 1981.
Art 5:« *I dati a carattere personale oggetto di un'elaborazione automatizzata sono: a) ottenuti e elaborati in modo lecito e corretto; b) registrati per scopi determinati e legittimi ed impiegati in una maniera non incompatibile con detti fini; c) adeguati, pertinenti e non eccessivi riguardo ai fini per i quali vengono registrati; d) esatti e, se necessario, aggiornati; e) conservati in una forma che consenta l'identificazione delle persone interessate per una durata non superiore a quella necessaria ai fini per i quali sono registrati*».
Art 6: «*I dati di carattere personale indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altri credo, nonché i dati a carattere personale relativi allo stato di salute ed alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno non preveda garanzia adatte. Lo stesso dicasi dei dati di carattere personale relativi alle condanne penali*».

[69] Al contrario, l'art. 25 Dir. 95/46 CE, prevede che gli Stati membri devono assicurare che i trasferimenti di dati personali, che siano stati oggetto di trattamento o siano destinati ad esserlo, verso un Paese terzo, possano avere luogo solo se il Paese terzo garantisce un livello adeguato di protezione. Insomma, la Convenzione 108 del 1981 e la Direttiva 95/46 CE muovono da due principi opposti: la prima, che il trasferimento «*non può essere impedito salvo che…*», la seconda il trasferimento «*non può essere concesso salvo che…*». La cosa non è priva di interesse perché indica con tutta evidenza che la Convenzione 108 si collochi in una prospettiva che privilegia la libera circolazione dei dati e dei casellari, in coerenza con la lotta che essa fa (e si è ancora nel 1981) all'impostazione di altri Paesi che, considerando i casellari e gli archivi soprattutto come strumenti di controllo sui cittadini, ne vietavano la circolazione tra gli Stati. La Direttiva CE, invece, muove da una visione della Comunità europea come una "fortezza", caratterizzata anche dalla specifico alto livello di protezione dei dati personali e dunque vieta il loro trasferimento all'estero se non è garantito un analogo livello di protezione. Inoltre impone quest'obbligo a tutti gli Stati membri proprio perché si concepisce come una Comunità e dunque come un'area che garantisce a tutti i cittadini in essa residenti, un medesimo alto livello di protezione dei dati personali. In realtà la norma l'art. 25 della Direttiva CE è congegnato in modo da creare una sorta di barriera immateriale ai confini della Comunità, finalizzata di fatto anche a proteggere le sue attività economiche e produttive da ingerenze concorrenziali di imprese operanti in Paesi che non assicurino eguali tutele.

Nata dall'esigenza di una normativa europea autonoma e soprattutto uniforme, diretta a predisporre forme di tutela effettiva delle persone dalle aggressioni alla loro vita privata ad opera delle nuove tecnologie informatiche e, pur traendo ispirazione dall'art. 8 CEDU, rappresentava un salto di qualità rispetto a quello, tanto da aver portato, e non solo i giuristi, ad affermare che il lungo cammino, cominciato in Europa dagli Stati totalitari, che hanno usato le innovazioni tecnologiche per aumentare i controlli sui propri cittadini, si sia concluso proprio con questa Convenzione, adottata quando già alcuni Paesi si erano dotati di proprie leggi in materia di trattamento automatizzato dei dati personali.
Il valore della Convenzione, pertanto, era altissimo: chiudeva una fase storica, portando oltre ogni limite la sfida nei confronti di chi raccoglie e tratta informazioni archiviate in banche dati automatizzate, senza il rispetto delle garanzie definite dalla Convenzione, anticipando, per alcuni versi, il quadro concettuale che avrebbe caratterizzato la successiva legislazione europea.

3) La stigmatizzazione del diritto nella nuova normativa comunitaria: la centralità della Direttiva 95/46 CE ed il riconoscimento nel diritto positivo europeo del diritto all'oblio

Malgrado la Convenzione 108 sia stata approvata in ambito CEDU sin dal 1981, la Comunità europea, fino al 1995, non ha provveduto ad intervenire sulla materia, predisponendo forme di regolamentazione, né sotto la veste giuridica del Regolamento, che della Direttiva, accumulando un notevole ritardo anche rispetto alle normative interne degli Stati membri che, per la maggior parte, si erano munite di una legislazione, più o meno specifica, in materia di protezione dei dati personali.
Nel 1995, con la Direttiva 46 CE, l'Unione Europea finalmente elabora un articolato più dettagliato e specifico in quella materia, in qualche modo legato al Trattato di Maastricht[70] cha ha dato formalmente l'avvio a vari processi che, in qualche modo, sono direttamente e indirettamente legati alla necessità di una maggiore protezione dei dati personali.
Esigenza, avvertita come necessaria da tutti i Paesi dell'UE, conseguente all'entrata in vigore del Trattato di Maastricht e al successivo smantellamento delle dogane, è stata quella di superare le difficoltà rappresentate dalle 'frontiere immateriali', costituite dalle

[70] *Trattato sull'Unione europea* del 7 febbraio 1992, entrato in vigore il 1° novembre 1993, in *G.U.C.E.*, N. C 191/1.

diverse leggi nazionali in materia di protezione dei dati personali, per pervenire ad una normativa europea uniforme che fosse in grado di appianare ogni differenza di trattamento.

Le trattative, iniziate nel 1990, tra i Paesi membri hanno manifestato non poche difficoltà e battute d'arresto, tanto che, soltanto dopo cinque anni, nel 1995, con la Direttiva 46, anche detta Direttiva di armonizzazione, è stato possibile addivenire ad una normativa europea comune, contenente principi e regole non immediatamente vincolanti, ma ai quali tutti gli Stati membri avrebbero dovuto adeguare le loro normative nazionali: obiettivo cui tanto avevano lavorato i Paesi della Comunità, tuttavia, in gran parte ridimensionato dall'affermazione, tra i Paesi membri, del 'principio del mutuo riconoscimento', in forza del quale in ogni Stato dell'Unione si sarebbe applicata la legge di protezione dei dati del Paese in cui avrebbe avuto sede lo stabilimento principale del titolare del trattamento.

In tal modo si andava a vanificare gran parte della tutela giuridica apprestata all'interessato, considerato che i titolari del trattamento, avendo il loro stabilimento principale fuori dall'Europa, quasi tutti negli Stati Uniti d'America, non erano di conseguenza, obbligati all'applicazione della normativa comune europea.

La Direttiva inoltre, non solo non ha mutuato della Convenzione 108/81 il principio che un Paese membro potesse impedire il trasferimento dei dati dei propri cittadini ad altri Paesi che non avessero offerto adeguate garanzie, ma ne ha rovesciato l'impostazione laddove ha specificato che il trasferimento avrebbe potuto essere consentito solo qualora lo Stato terzo avesse assicurato il medesimo alto livello di protezione dei dati, alla pari di quello offerto dai Paesi comunitari.

In tal modo è vero che sono stati notevolmente elevati i sistemi di protezione dei dati personali all'interno della 'fortezza europea', ma, d'altra parte, si sono resi più difficili i rapporti con i Paesi Terzi, come gli Stati Uniti, che non assicuravano le medesime garanzie, avendo fatto della raccolta e trattamento dei dati personali un'attività libera, scevra da limiti e vincoli, in quanto utile e di supporto all'esplicazione dei fondamentali diritti di manifestazione del pensiero, di stampa e di cronaca[71].

[71] Vale la pena richiamare a questo proposito la sentenza della Corte di Giustizia (Grande Sezione) del 6 ottobre 2015, C-362/14, che ha annullato la decisione della Commissione UE, relativa ai cd. Accordi Safe habour. Alla luce delle carte svelate da Hedward Snowden sull'uso illegittimo della raccolta, trattamento e conservazione dei dati ad opera della NSA, la CGUE ha annullato la decisione della Commissione UE sul Safe harbour, con la sentenza C-362, Maximilian Schrems/Data Protection Commissioner, perché secondo

La tutela del diritto all'autodeterminazione informatica ha trovato una sua prima ed embrionale strutturazione nel quadro della Dir. 95/46, relativa alla "Tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione degli stessi"[72], che, per qualche decennio, ha avuto il monopolio della regolamentazione della materia e che, solo con l'entrata in vigore del nuovo Regolamento di protezione dei dati personali, ha visto svanire la sua centralità e quella dei principi e delle regole in essa contenuti, nel panorama giuridico europeo.

A quella normativa, in vigore ormai da quasi vent'anni, sono altresì vincolate le leggi nazionali di protezione dei dati, dal momento che tutti gli Accordi di adesione man mano stipulati, sulla base delle regole fissate dal Trattato di Amsterdam del 1997, hanno imposto l'obbligo ai Paesi entranti, di adeguarsi all'acquis communitair', del quale faceva parte anche la Dir. 95/46. Di conseguenza tutti Paesi, via via entrati nell'Unione, hanno dovuto adottare leggi di protezione dei dati armonizzate con la Direttiva[73], che continueranno ad esplicare i loro effetti, anche nella vigenza del Regolamento 2016/679, purché non confliggenti con i precetti nello stesso contenuti, essendo diversamente condannate alla disapplicazione ad opera del giudice nazionale, in assenza di forza abrogativa, da parte del Regolamento, nei confronti delle leggi nazionali, interne ai singoli Stati.

Anche l'Italia ha dato attuazione al lavoro del Legislatore comunitario, sebbene con significativo ritardo, cessato quando è stato chiaro che se avesse voluto entrare a pieno titolo nella Convenzione di Schengen, dal 1° gennaio 1998, avrebbe dovuto necessariamente adottare una normativa di protezione dati coerente con quella europea.

Normativa di cui il nostro Paese si è dotato con l'elaborazione della Legge 675/1996.

Sebbene in questi vent'anni, com'è stato più volte ribadito dai Garanti nazionali riuniti nel Gruppo Articolo 29, la Direttiva si sia dimostrata un'eccellente cassetta degli attrezzi', non sempre, tuttavia, si è palesata all'altezza di gestire le nuove sfide che la rapidità dell'evoluzione tecnologica ha lanciato al diritto alla protezione dei dati.

---

in giudici europei non c'erano sufficienti garanzie che la riservatezza dei dati degli europei venisse tutelata anche in America.

[72] Titolo della Direttiva, come pubblicata sulla GU della Comunità europea il 23 novembre 1995, numero 1, 281/31.

[73] Obbligo che è rimasto in vigore fino all'adozione del nuovo Regolamento di protezione dei dati personali, 2016/679.

La stessa, infatti, consacrava un 'modello statico' di trattamento dei dati personali, un modello fondamentalmente uno ad uno che vedeva le due parti, interessato e titolare del trattamento, ingessati in ruoli rigidi, mentre la realtà dei social networks impone un modello di uno a tutti, di condivisione dei dati destinati, fin dall'origine ad una circolazione globale. Di qui la difficoltà crescente di applicare quelle regole ai nuovi fenomeni e alle nuove modalità di trattamento e uso dei dati nel mondo digitale, senza aver preliminarmente spostato il baricentro delle responsabilità da chi fornisce il dato a chi lo fa circolare.

La sua inadeguatezza, quindi, a gestire le nuove modalità di trattamento, fornendo protezione a tutte le nuove figure ed esigenze giuridiche emerse, ha comportato, quale ovvia conseguenza, non solo interventi della Corte di Giustizia su questioni pregiudiziali, sollevate dalle Corti nazionali, aventi ad oggetto l'interpretazione di parti della Direttiva stessa, nell'intento di poterle adeguare, il più possibile, al nuovo scenario giuridico, quanto vere e proprie proposte legislative, da parte del Legislatore comunitario, alcune delle quali sono state assorbite nel nuovo Regolamento sulla protezione dei dati personali.

4) Il diritto alla protezione dei dati nel panorama normativo nazionale

Nel panorama normativo interno, il diritto all'autodeterminazione informatica ha trovato riconoscimento implicito nella Legge 675/96, emanata a ratifica della Direttiva 95/46, finalizzata oltre che all'adeguamento della normativa interna a quella comunitaria, a garantire che il trattamento dei dati personali si svolgesse nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla tutela della riservatezza e dell'identità personale[74].

Per parte della dottrina[75] la Legge 675/96 ha inaugurato una sorta di quarta fase nelle previsioni di forme di tutela della personalità, dopo una prima, caratterizzata da

[74] Così nell'art. 1 L. 31 dicembre 1996 n.675, cit., «*Gli Stati membri garantiscono conformemente alle disposizioni della presente Direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente della vita privata, con riguardo al trattamento dei dati personali. 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*».

[75] G. CASSANO - A. SORIANO, *I diritti della personalità dall'actio iniuriarum alle banche dati,* in *Vita not.*, 1998, 488. E questo perché, secondo gli Autori, il diritto di manifestare liberamente il proprio pensiero non può ritenersi avulso dal sistema dell'Ordinamento e, quindi, privo di limiti intrinseci, limite che non può non essere individuato nella tutela della persona rispetto alla quale anche i diritti contenuti nell'art. 21 Cost. sono strumentali, se è vero che tutto il sistema delle garanzie costituzionali è orientato verso la tutela della persona. Conferma ne è appunto l'art. 1 della L. 675/96.

un'estrema pochezza di disposizioni in materia, con il Codice civile; una seconda fase, caratterizzata dall'entrata in vigore della Carta costituzionale che, introducendo le locuzioni di 'diritti inviolabili dell'uomo' e di 'svolgimento della personalità', ha allargato le forme e le tipologie di tutele apprestate alla persona; una terza, caratterizzata dall'azione di dottrina e giurisprudenza, che hanno cercato spazi ulteriori di tutela dell'individuo, anche attraverso l'uso dello strumento processuale rappresentato dall'art. 700 c.p.c.; per approdare all'ultima, in cui il Legislatore, europeo e nazionale, preso atto delle nuove sfide lanciate ai fondamentali diritti di libertà della persona, è intervenuto con lo strumento legislativo, predisponendo regole più precise e raffinate, che i tempi ormai consideravano necessarie, ivi comprese sanzioni più rigide.

A parte la necessità dell'adeguamento della disciplina nazionale a quella europea, la Legge 675/96 è anche conosciuta come 'legge compromesso', poiché più che diretta alla soluzione dei problemi che si erano evidenziati, era frutto di un compromesso tra le varie ed opposte forze politiche, con l'aggravante che, essendo stata elaborata in modo piuttosto affrettato, ha da subito manifestato non poche criticità. Nonostante tutto era assolutamente indispensabile in quel momento storico caratterizzato dalla 'giungla dell'informatizzazione', nel quale, essendo stata sostituita la memoria cerebrale con quella magnetica, le tecniche informatiche erano in grado di trattare, conservare e diffondere l'intera esistenza di ciascuno, con serio rischio di aggressioni alla sfera privata. Anche il titolo con cui la legge era rubricata, 'Protezione dei dati personali', era un po' troppo ambizioso se rapportato ai suoi contenuti, perché di fatto, l'articolato ha semplicemente posto qualche paletto agli abusi dei titolari dei motori di ricerca, lungi dal contenere una normativa organica che disciplinasse il fenomeno.

Non era neanche di facile determinazione la fissazione di un limite temporale per la conservazione dei dati e non meno ibrida era la norma che, ad eccezione di quanto previsto per i dati sensibili, non richiedeva il consenso dell'interessato alla divulgazione delle informazioni, "quando il trattamento è effettuato nell'esercizio della professione giornalistica[76]". Balza agli occhi la difficoltà di stabilire fin dove possano spingersi le

[76] L. 31 dicembre 1996 n.675, art. 12: «*1. Il consenso non è richiesto quando il trattamento:*
a) riguarda dati raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per l'esecuzione di misure precontrattuali adottate su richiesta di quest'ultimo, ovvero per l'adempimento di un obbligo legale; c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da

finalità giornalistiche e di cronaca che hanno impedito di porre bavagli o freni ai giornalisti. E' un aspetto sul quale è caduto il silenzio della legge.

Norme piuttosto generiche ed elastiche, tanto da aver portato, in tanti in dottrina[77], ad affermare che la 'legge ha creato più problemi di quanti ne abbia risolti', per cui, a partire dal 1° gennaio 2004, la Legge 675/96 è stata sostituita dal D. Lgs. 196/2003, rubricato 'Codice in materia di protezione dei dati personali', nel quale il Legislatore ha riportato, non solo tutto quanto contenuto nel precedente testo normativo, ma anche i numerosi decreti legge e legislativi emanati in tempi successivi nonché le disposizioni di rango inferiore; un magma di norme che rendeva assai difficile e problematica l'interpretazione e l'applicazione della legge al caso concreto.

Il nuovo intervento del Legislatore è stato essenzialmente orientato, intanto all'eliminazione delle norme confliggenti tra loro, appartenenti alla numerose leggi che si erano susseguite, e al riordino di tutto il materiale legislativo, nell'intento di armonizzarlo con quello preesistente e con quanto richiesto dal Legislatore europeo.

Nella nuova legge nazionale, il diritto alla protezione dei dati personali non si esaurisce solo nella 'pretesa erga omnes' a mantenere riservata la sfera dell'individuo dalle altrui ingerenze, non giustificate da superiori interessi, ma viene ad acquistare una dimensione dinamica che si concretizza nella possibilità di mantenere il controllo sui propri dati[78], il

---

chiunque; d) è finalizzato unicamente a scopi di ricerca scientifica o di statistica ed è effettuato nel rispetto dei codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31; e) è effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità. In tale caso, si applica il codice di deontologia di cui all'articolo 25; f) riguarda dati relativi allo svolgimento di attività economiche raccolti anche ai fini indicati nell'articolo 13, comma 1, lettera e), nel rispetto della vigente normativa in materia di segreto aziendale e industriale; g) è necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere; h) è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; h-bis) è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato».

[77] A. LA TORRE, in A.A.V.V., *Il diritto all'oblio – atti del Convegno di Studi del 17 maggio 1997,* a cura di E. GABRIELLI, Napoli, 1999, 78.

[78] V. FRANCESCHINELLI, *La tutela della privacy informatica*, Milano, 1998, 57. Nella tutela del diritto all'oblio è insita la tutela all'identità personale, quale tutela della proiezione del soggetto nella realtà sociale, in funzione di ciò che egli è ed esprime, nell'attualità della sua presenza sociale. Consegue che, il passato della persona, quando non rappresenti la premessa necessaria per definirne l'attuale sua presenza sociale, deve restare nell'oblio, soprattutto quando l'evocazione di esso possa alterare la posizione presente del soggetto. T. E. FROSINI, *Il diritto all'oblio e la libertà informatica*, in *Dir. Inform.*, 2012, 918, argomentando sulla base di un'autorevole teoria della libertà informatica evidenzia che i dati personali costituiscono una parte dell'espressione della personalità dell'individuo ed allora deve essere consentito

c.d. diritto all'autodeterminazione informatica, esigenza avvertita come necessaria e non più derogabile.

5) La difficoltà di capire l'importanza della nuova normativa di protezione dei dati in molti Stati membri, in particolare in Italia

Nell'ambito di alcuni Paesi dell'Unione Europea, l'importanza della normativa sul diritto alla protezione dei dati personali, di cui alla Direttiva 95/46 CE, non è sempre stata capita e condivisa; tutt'oggi la previsione di quel diritto non sembra ancora essere scevra da problematiche, se è vero che il 1° giugno 2017 l'Autorità Antitrust, l'Autorità per le Garanzie nelle Comunicazioni e l'Autorità Garante per la Protezione dei dati personali hanno comunicato di "aver avviato un'indagine conoscitiva congiunta riguardante l'individuazione di alcune criticità connesse all'uso dei Big Data, per la definizione di un quadro di regole in grado di promuovere e tutelare la protezione dei dati personali, la concorrenza nei mercati dell'economia digitale, la tutela del consumatore ed i profili di promozione del pluralismo nell'ecosistema digitale[79]".

Si tratta di un'indagine a livello europeo prima nel suo genere, che coinvolge tre importanti Autorità Indipendenti, unite nell'affrontare in maniera multidisciplinare un tema di così forte attualità ed importanza strategica, sia per i suoi impatti sociali ed economici nell'odierna società che per l'influenza operata sulla sfera privata dei cittadini.

Nel 1981 la Convenzione 108 della CEDU fu salutata con grande favore dagli esperti che avevano visto in essa la conclusione di un lungo periodo storico e l'apertura di nuovi scenari per la protezione dei dati personali e per l'espansione dei diritti e delle libertà delle persone, a fronte delle valanghe di dati che le principali e le più profittevoli aziende della New Economy, Amazon – Google – Facebook, avevano incamerato, attraverso la

alla persona, a tutela della sua identità, l'esercizio del diritto di libertà informatica, che consiste nel potere di disporre dei propri dati e delle notizie che lo riguardano, nonché la contestualizzazione del dato e l'aggiornamento dello stesso.

[79] Le tre autorità hanno avviato il 30 maggio 2017 un'indagine conoscitiva congiunta sulle eventuali criticità circa la raccolta dei big data che si differenziano dagli altri dati per la particolare estensione della quantità delle notizie raccolte, la continua evoluzione delle stesse e la rapidità di analisi, in tempo reale, effettuata tramite l'utilizzo di complessi algoritmi. Dati che sono diventati essenziali per la crescita economica, per l'offerta di servizi innovativi, per la creazione di posti di lavoro ma il cui uso ha anche comportato potenziali rischi alla riservatezza delle persone.

creazione di nuove e potenti infrastrutture in grado di dominare i mercati, raggiungendo capitalizzazioni impressionanti[80].

La Direttiva 95/46, invece, al contrario della Convenzione 108, è stata avvertita da molti Paesi come una normativa a carattere prevalentemente burocratico, un'imposizione, tollerata con difficoltà dalla tecnocrazia di Bruxelles, piuttosto che come garanzia di tutela dei diritti e delle libertà fondamentali della persona, nonostante il contenuto dell'art. 1 Par. 1, secondo cui: 'Gli Stati membri garantiscono, conformemente alle disposizioni della presente Direttiva, la tutela dei diritti e delle libertà fondamentali', formula che riassumeva in sé tutto il percorso evolutivo del diritto alla protezione dei dati personali, che ha visto la sua origine nell'art. 8 CEDU e che, attraversando la Convenzione 108 e alcune Carte nazionali, era approdato nella nuova normativa comunitaria.

Norma dal chiaro contenuto, la locuzione di cui all'art. 1, Par. 1, ma che, tuttavia, ha creato non poche difficoltà interpretative: mentre i difensori del diritto alla protezione dei dati personali, tra i quali in particolare i Garanti di tutti i Paesi europei, hanno fondato su quella norma la ferma convinzione che la protezione dei dati costituisse diritto fondamentale già nella Direttiva 95/46, molti dei destinatari, le multinazionali della raccolta e del successivo trattamento, con altrettanta determinazione, hanno negato che la stessa, per il modo in cui era stata formulata, potesse essere sufficiente ad elevare la protezione dei dati personali a diritto fondamentale. Questa problematica che, più volte, ha fondato dibattiti molto accesi tra le parti in gioco, ha per anni richiesto l'intervento dei Garanti nazionali e di tutti gli operatori chiamati a dare attuazione al lavoro prodotto dal Legislatore europeo.

Discussioni ancora più accese quando gli operatori erano imprese abituate ad operare nel quadro normativo americano, che ha sempre negato che il diritto alla protezione dei dati potesse avere la stessa forza di altre libertà fondamentali elencate nel Bill of Rights; discussioni poi sedate dall'entrata in vigore della Carta di Nizza[81], nella quale l'Unione Europea ha espressamente riconosciuto il diritto alla protezione dei dati, come un diritto fondamentale.

---

[80] Esemplare il fatto che Facebook Inc., nata nel 2004, è capitalizzata con circa 450 miliardi di dollari al 2016, mentre la General Electric, fondata nel 1982, capitalizza circa 240 miliardi di dollari.

[81] La *Carta di Nizza*, solennemente proclamata una prima volta il 7 dicembre 2000 a Nizza ed una seconda volta, in una versione adattata, il 12 dicembre 2007 a Strasburgo da Parlamento, Consiglio e Commissione è in realtà definita come *Carta dei diritti fondamentali dell'Unione europea*.

La Direttiva madre, altresì, come precisato dall'Agenzia dell'Unione Europea per i diritti fondamentali[82], se da una parte ha dato attuazione, all'interno dell'Unione, a quanto previsto dalla Convenzione 108, e da una lettura evolutiva dell'art. 8 CEDU in materia di protezione dei dati, dall'altra è andata molto oltre, avendo previsto, rispetto ai precedenti lavori legislativi, ulteriori strumenti di tutela, quali le Autorità nazionali di controllo[83], preposte a presidio di garanzie aggiuntive alla tutela dei dati, dando nel contempo, legittimazione giuridica a quel diritto, altrimenti frutto di mera interpretazione estensiva. Il limite significativo della normativa europea era rappresentato dal momento storico nel quale era stata pensata ed adottata: un momento nel quale tutto il sistema delle comunicazioni elettroniche era alle soglie di un cambiamento di portata epocale, per cui, mentre da un lato il nuovo strumento normativo europeo ha continuato ad essere considerato la 'madre' di tutta la normativa di protezione dei dati dell'Unione, dall'altra gli operatori giuridici si sono da subito resi conto che la tutela di quel diritto richiedeva nuovi e ulteriori interventi normativi, diretti ad affinare, regolamentandole, tutte quelle nuove, e particolarmente avanzate, applicazioni tecnologiche legate alla raccolta di massa delle informazioni personali, al loro trattamento e circolazione.

6) La Carta di Nizza e il Trattato sul Funzionamento dell'Unione Europea

Il panorama normativo europeo, in materia di protezione dei dati personali, si è ulteriormente arricchito con la proclamazione della Carta di Nizza e con la successiva approvazione del Trattato sul Funzionamento dell'Unione Europea[84].

L'art. 8 della Carta di Nizza, oggi incorporato nel Trattato di Lisbona[85], è dedicato al diritto alla protezione dei dati personali, considerato come diritto fondamentale a se stante

---

[82] Cfr. su questo punto, Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dei dati*, pubblicato dall'Ufficio delle pubblicazione dell'Unione europea, 2014, 18. Come avverte l'editore, il Manuale è stato redatto in lingua inglese e poi tradotto in tutte le lingue dell'Unione.

[83] Il sistema delle Autorità di controllo e dei gruppi di lavoro comune è stato, infatti, ripreso anche nell'ambito del Consiglio d'Europa (CED), col *Protocollo aggiuntivo alla Convenzione 108*, approvato nel 2001.

[84] Il Trattato sul funzionamento dell'Unione europea (TFUE), da ultimo modificato dall'articolo 2 del trattato di Lisbona del 13 dicembre 2007 e ratificato dall'Italia con legge 2 agosto 2008, n. 130, su G.U. n. 185 dell'8-8-2008.

[85] Trattato di Lisbona**,** firmato a Lisbona il 13 dicembre 2007 dagli allora 27 Stati membri dell'Unione Europea (Austria, Belgio, Bulgaria, Cipro, Danimarca, Estonia, Finlandia, Francia, Germania, Gran Bretagna, Grecia, Irlanda, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia, Portogallo, Repubblica Ceca, Romania, Slovacchia, Slovenia, Spagna, Svezia, Ungheria) ed entrato in vigore il 1° dicembre 2009.

ed autonomo rispetto al diritto alla riservatezza e a quello alla tutela della vita familiare. Allo stesso modo il TFUE, all'art. 16[86], prevede specificamente l'obbligo di tutela dei dati personali, fornendo alla Direttiva 95/46 CE, e in generale a quella materia, una solida copertura che potrebbe definirsi costituzionale, ancorché contenuta in un Trattato[87].

Dopo la Carta di Nizza, le Istituzioni europee si sono definitivamente vincolate a considerarlo come diritto fondamentale dell'Unione, con base normativa fondata direttamente sul Trattato dell'Unione.

L'avvenuta costituzionalizzazione del diritto alla protezione dei dati ha costituito uno stimolo, per la Corte di Giustizia, ad elaborare una giurisprudenza sempre più incisiva e coraggiosa, sia rispetto alle leggi nazionali, armonizzate con la Direttiva, che agli Accordi stipulati dalla Commissione con i Paesi terzi[88].

Tutto questo ha portato alla formazione di un importante 'Corpus' di pareri, decisioni e raccomandazioni in materia di protezione dei dati, che ormai fa parte, a pieno titolo, del diritto europeo in materia.

In tal modo, sia pure attraverso una via tortuosa e impervia, l'Unione Europea è giunta a considerare la protezione dei dati personali come una garanzia essenziale per la libertà delle persone contro i controlli indebiti, quanto illegittimi, degli Stati sui cittadini e di chiunque possa avvalersi dei trattamenti automatizzati.

Tutti gli Stati membri, nell'ottica dell'armonizzazione, sono stati obbligati ad adottare leggi di protezione dei dati personali armonizzate, dalle quali sarebbe dovuta emergere l'autonoma valenza costituzionale di quel diritto, oggi in grado di coesistere con gli altri diritti e le altre libertà, nella consapevolezza che soprattutto nell'epoca delle

---

[86]Trattato sul funzionamento dell'Unione europea (TFUE), art. 16: «*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 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*».

[87] Ovviamente, nell'ambito dell'Unione non si può parlare di "Costituzione", ma solo di diritti fondamentali, oggi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, riconosciuta con valore di trattato, da parte del Trattato di Lisbona. L'uso del termine "costituzionalizzazione" nel testo è volutamente atecnico, ma utile a far comprendere il rango che questo diritto ha avuto anche formalmente nell'ambito dell'ordinamento europeo.

[88] Così come è avvenuto con il *Safe harbour* e con la Decisione del 6 ottobre 2015 CGUE (Grande sezione), causa C-326/14, *Maximilian Schrems/ Data Protection Commissioner*.

comunicazioni elettroniche e del digitale, i diritti e le libertà delle persone, devono essere rafforzati ed amplificati.

7) Gli esiti dirompenti della Sentenza CGUE, C- 131/12 del 13 maggio 2014 in materia di trattamento dati ed oblio

La sentenza in esame ha prodotto una svolta giurisprudenziale innegabile, aprendo una breccia importante nell'ambito della tutela dei diritti in Rete. Nel suo provvedimento la Corte di Giustizia, nel riconoscere all'avvocato Costeja Gonzales il diritto all'oblio, ha obbligato i motori di ricerca a rimuovere alcune informazioni a lui relative. Nel 1998 Gonzales, cittadino spagnolo, aveva subito un rovescio finanziario, che aveva comportato la messa all'asta della sua proprietà per mancato pagamento di debiti verso il fisco. La notizia finì sui giornali e, nonostante il debitore avesse successivamente appianato il suo debito, continuava ad essere riportata in bell'evidenza, intrappolando l'Avv. Gonzales nel suo passato digitale.

Dopo aver percorso tutti i gradi della giustizia amministrativa e giudiziaria spagnola, con alterne pronunce, il caso è approdato innanzi alla Corte di Giustizia che, nella succitata sentenza, ha riconosciuto al ricorrente il diritto di ottenere la rimozione del link dal motore di ricerca, su semplice digitazione del suo nome e cognome.

E' una sentenza spartiacque in materia di protezione dei dati e diritto all'oblio, innanzitutto perché ha attribuito a Google ed ai gestori dei motori di ricerca la qualifica di responsabili del trattamento dei dati personali, con il conseguente obbligo di deindicizzare i link contenuti nella relativa pagina web, a richiesta del titolare di quei dati. Pertanto, l'interessato, che, a seguito di ricerca effettuata inserendo semplicemente il suo nome e cognome, dovesse ottenere dall'elenco dei risultati un link contenente informazioni sul suo conto, obsolete e lesive della sua sfera privata, potrebbe rivolgersi direttamente al gestore del motore di ricerca, per chiederne la rimozione e, qualora questi non dovesse dar seguito alla sua domanda, adire le Autorità amministrativa e/o giudiziaria competenti, per ottenere la soppressione del link dall'elenco dei risultati ed eventualmente il risarcimento dei danni.

Il punto cruciale della decisione europea è rappresentato dal fatto che la rimozione dei link dal motore di ricerca non viene a comportare alcun obbligo per i siti-sorgente, cui i

links rimandano, che potranno pertanto decidere come gestire i dati personali in loro possesso, senza il consenso del titolare. La relativa pagina, pertanto, potrà essere mantenuta visibile sui singoli siti d'informazione, conservando la sua attualità, anche se il motore di ricerca, accogliendo l'istanza del titolare dei dati, avesse deciso di rimuoverla. Gli interessati potranno eventualmente agire in parallelo per ottenere anche dagli editori dei siti web la cancellazione delle informazioni che li riguardino.

La sentenza Google/Spain è stata ritenuta una rivoluzione copernicana[89] anche per aver rimodulato le responsabilità degli operatori della Rete, stabilendo che le norme europee trovassero applicazione anche nei confronti dei motori di ricerca, che avessero la loro sede sorgente fuori dall'Europa ma che, in uno Stato membro, avessero una stabile organizzazione, filiale o succursale, presso la quale si svolgesse attività di trattamento dei dati.

Anche questi operatori della Rete, a parere dei giudici europei, sono obbligati al rispetto della normativa europea, con l'obbligo di rimuovere dall'elenco dei risultati i links di collegamento con le pagine web, contenenti informazioni lesive della sfera privata delle persone, anche nell'ipotesi in cui tali informazioni fossero lecite.

Sulla questione fa fede altresì, il punto 7 delle Linee Guida del 26 novembre 2014 dei Garanti europei, che perentoriamente sancisce: "dev'essere garantita in ogni modo un'effettiva e completa protezione del diritto dell'interessato e la legislazione europea dev'essere rispettata in modo tassativo e puntuale". Non risulta dunque sufficiente e conforme ai vigenti obblighi normativi l'applicazione della de-indicizzazione ai soli domini nazionali o europei; anche le versioni ".com" dei motori di ricerca devono applicare eventuali decisioni in tal senso.

---

[89] CGUE, sentenza 131/12 del 13 maggio 2014, comunicato stampa n. 70/14, Lussemburgo, *Google Spain SL, Google Inc./ Agencia espanola del protection de datos, Mario Costeja Gonzales*. G. BUSIA, *Una vera rivoluzione copernicana*, in *Il Sole 24 Ore*, 10 maggio 2014. E' una vera rivoluzione copernicana, per l'Autore, quella emersa dalla sentenza con la quale la Corte di Giustizia ha definito la controversia tra Google e l'Agenzia spagnola per la protezione dei dati: «*Una rivoluzione che fa intravedere nuove frontiere per la tutela dei diritti della personalità sul web e forse nuovi spazi per la costruzione di un rapporto egualitario tra i produttori di contenuti dei siti web e coloro che, come Google, ne facilitano il raggiungimento da parte degli utenti. Tutto questo perché i motori di ricerca non sono macchine impersonali, mosse da algoritmi imparziali, ma soggetti che, analogamente agli editori delle pagine web, devono farsi carico delle operazioni che compiono e delle conseguenze che possono comportare sulla vita delle persone. Ecco perché per i giudici di Lussemburgo, i motori di ricerca sono stati considerati come autori autonomi del trattamento, quindi obbligati a rispettare la normativa sulla protezione dei dati personali*».

Ovviamente il ricorrente dovrà provare che, la permanenza in Rete del link ad una notizia che lo riguardi, gli crei un pregiudizio sociale o professionale, attestando, altresì, che l'eventuale rimozione del link non crei un vulnus alla completezza delle informazioni di interesse pubblico su di lui.

Il motore di ricerca, attraverso una valutazione operata caso per caso, dovrà accertare se le informazioni, delle quali l'utente chiede la rimozione, siano effettivamente obsolete o se siano ancora di pubblico interesse, impedendo che l'esercizio del diritto all'oblio possa trasformarsi nel diritto dei potenti a cancellare il proprio passato scomodo, sartorializzando la propria identità digitale, ripulendola dalle informazioni ingombranti.

Al rifiuto dell'istanza da parte del motore di ricerca, al ricorrente è stata riconosciuta la possibilità di rivolgersi alle Autorità Amministrative e/o giudiziarie per far valere le sue ragioni.

Una decisione intransigente, ma anche una risposta necessaria e non più dilazionabile, dal momento che la forza delle multinazionali americane dell'informazione si era fino ad allora fondata sulla costante negazione dell'applicabilità, nei loro confronti, della legislazione europea, in quanto i trattamenti dalle stesse posti in essere erano effettuati fuori dal territorio UE', nonostante avessero istituito sedi nei Paesi dell'UE, nelle quali era regolarmente svolta attività di trattamento dati.

Per anni, prima della pronuncia CGUE, è stato un gioco per i colossi americani dell'informazione online, sottrarsi ai restrittivi vincoli normativi europei, accumulando una montagna di dati sulle abitudini di ciascuno.

I giudici europei, avendo precisato il principio di stabilimento, li hanno compresi e costretti in quei vincoli, la cui violazione avrebbe comportato forme di responsabilità.

8) Il diritto all'oblio e al trattamento dei dati personali nelle Linee Guida del WP29

Il provvedimento della CGUE, del 13 maggio 2014, relativamente alla causa C-131/12, sebbene particolarmente articolato e puntuale, aveva dato origine a non pochi dubbi e perplessità nelle successive applicazioni dei principi che imponeva.

La necessità di superare le difficoltà che si erano manifestate e soprattutto l'importanza di procedere in maniera uniforme in tutti gli Stati membri, ha portato i Garanti europei per la protezione dei dati personali, riuniti nell'Article 29 Working Party, a pubblicare il 26 novembre 2014, immediatamente dopo la pronuncia della CGUE, delle 'Linee Guida'

contenenti un'interpretazione univoca della pronuncia, che aveva sollevato non pochi dubbi interpretativi soprattutto laddove aveva previsto l'obbligo per il motore di ricerca (nel caso di specie Google), di deindicizzare, ai propri risultati, quei links, che dagli interessati fossero stati ritenuti lesivi del loro diritto all'oblio. Più precisamente il provvedimento giudiziario aveva riconosciuto agli interessati la possibilità di avanzare la pretesa ad ottenere la cancellazione dei contenuti delle pagine web che, a loro parere, avessero offerto una rappresentazione non più attuale della loro persona.

Le Linee Guida hanno avuto il merito di stabilire una serie di criteri comuni diretti ad orientare e uniformare l'attività amministrativa dei singoli garanti nazionali.

Il documento, approntato dall'Article 29 Working Party, nel confermare l'applicabilità della Direttiva 95/46 CE ai motori di ricerca, anche qualora il trattamento dei dati personali fosse stato da loro compiuto attraverso un'azienda sussidiaria diretta alla promozione e vendita di spazi pubblicitari, purché residente in uno Stato europeo, ha precisato che la decisione della Corte di Giustizia sancisce espressamente il diritto alla rimozione dei dati scaturenti dalla semplice digitazione del nome e cognome del privato, con il limite, tuttavia, che la soppressione avrebbe dovuto riguardare solo i risultati dei motori di ricerca e non le informazioni originarie contenute nei siti-sorgente.

L'informazione, pertanto, avrebbe potuto essere sempre accessibile attraverso ricerche effettuate con altri termini (e non con il nome e cognome).

Hanno precisato, altresì, che la de-indicizzazione sarebbe potuta essere richiesta dagli interessati con qualunque mezzo e che, in caso di rifiuto da parte del motore di ricerca, regolarmente motivato e tempestivamente comunicato, l'interessato avrebbe potuto rivolgersi all'Autorità nazionale o agli Organi giudiziari, al fine di ottenere una protezione effettiva e completa della sua sfera privata.

A tal fine non sarebbe stato sufficiente, a parere dei Garanti europei, delimitare la rimozione ai soli risultati dei motori di ricerca con domini europei, ma sarebbe stato utile e necessario filtrare tutti i domini internazionali, compreso: 'com'.

Il Documento specificava altresì che i motori di ricerca non sarebbero stati tenuti a comunicare, al webmaster delle pagine deindicizzate, l'esclusione dei risultati collegati al nome del privato e formalizzava una serie di criteri comuni che le Authority nazionali, avrebbero dovuto applicare nei casi in cui i motori di ricerca si fossero rifiutati di esaudire

le richieste di rimozione provenienti dai cittadini. Criteri da applicare relativamente ai singoli casi e in concordanza con le leggi nazionali rilevanti.

A seguito della pronuncia dei giudici europei, Google ha costituito un Consiglio di esperti per redigere Linee Guida interne alla Compagnia e il 6 febbraio 2015 ha pubblicato il rapporto 'The Advisory Council to Google on the Right to be Forgotten', contenente le Best Practices, nettamente differenti da quelle contenute nel Lavoro prodotto dai Garanti europei. Anzi trattasi di due Ordinamenti che si scontrano: la visione americana più aperta e garantista della libertà e del diritto di accesso alle informazioni, quella europea più sensibile nel prevedere tutte le forme di tutala possibili della sfera privata delle persone. Il Rapporto Google individuava una serie di eccezioni in cui l'interesse pubblico sarebbe stato privilegiato rispetto al diritto all'autodeterminazione informatica, mentre per i Garanti UE la regola sarebbe rappresentata dalla prevalenza dei 'Data Protection', cui l'Azienda non avrebbe potuto derogare, se non per interessi superiori, comunque trascendenti la tutela della sfera intima dell'individuo.

Le Linee Guida elaborate da Google, tra l'altro, offrivano soluzioni standardizzate che, nella maggior parte dei casi, vedevano il 'no index', a seconda che l'interessato fosse stato o meno una persona pubblica e a seconda della natura della notizia da deindicizzare: le notizie a forte impatto privacy venivano distinte dalle notizie a forte impatto pubblico. Le Linee Guida europee invece rifuggivano dalla logica delle soluzioni precostituite secondo protocolli statici, assumendo quale principio fondamentale, il bilanciamento degli interessi comparativi in gioco, dopo una disamina caso per caso. Bilanciamento operato secondo il criterio della potenziale gravità dell'impatto privacy negativo e considerando il criterio della proporzionalità, pertinenza e non eccedenza, per giungere ad una soluzione accurata per ciascun caso.

In Italia il Garante della Privacy, a partire dal novembre 2014, ha adottato i primi provvedimenti, relativi a casi di presunta violazione del diritto all'oblio e conseguente lesione della sfera privata, con i quali ha respinto il ricorso degli interessati, in quanto, nella maggior parte dei casi[90], aveva ad oggetto la richiesta di cancellazione di URL relative ad articoli contenenti vicende processuali recenti o non ancora concluse.

Laddove, invece, il Garante nazionale, nel caso sottopostogli, ha riscontrato la presenza di connotazioni negative, idonee ad incidere sulla sfera privata dell'interessato, in

[90] Uno per tutti, Garante per la protezione dei dati personali, *Doc. Web*, n. 5690378, 6 ottobre 2016.

coerenza con le indicazioni suggerite dalle Linee Guida, ha prescritto a Google Inc., la de-indicizzazione dell'URL segnalato[91].

SEZIONE III: Le difficoltà nel garantire il diritto alla protezione dei dati a seguito dell'affermazione delle più recenti innovazioni tecnologiche ed informatiche

1) Il diritto alla protezione dei dati nella dialettica e interazione con i social network

La crescente diffusione dei social networks, se da un lato ha moltiplicato l'interattività tra gli utenti, dall'altro ha messo a nudo gli elementi di vulnerabilità delle comunicazioni elettroniche in ordine alla tutela dei tradizionali diritti alla sicurezza e riservatezza dei dati personali.

In un contesto fluido, dinamico e illimitato, come quello della Rete, il problema non può essere risolto con la persecuzione e repressione delle condotte: la difesa più efficace della privacy passa anche attraverso l'autoresponsabilizzazione dell'utente, chiamato a gestire in maniera attenta i propri dati personali, secondo l'opinione ormai diffusa delle istituzioni preposte alla regolamentazione della Rete, tra le quali va sottolineata quella del Garante della Privacy che, in più occasioni ha messo in guardia la comunità degli utenti circa i rischi connessi all'uso dei social networks, fornendo consigli utili per un loro utilizzo consapevole.

Social networks come Facebook, Myspace, LinkedIn, Badoo.Com., Twitter danno agli utenti l'impressione di coltivare uno spazio personale (del resto era proprio questa la finalità che ha visto la nascita di Facebook - Libro delle fotografie: la creazione di una bacheca dei ricordi che favorisse la condivisione di immagini, video e opinioni, tra universitari che volevano restare in contatto anche dopo il loro ingresso nel mondo del lavoro), ma in realtà accolgono informazioni personali destinate a diventare di dominio pubblico, che difficilmente potranno essere eliminate dalla Rete.

[91] Da ultimo Doc. Web n. 6692214 del 15 giugno 2017 in cui il Garante nazionale, in presenza delle indicazioni suggerite dalle Linee Guida e verificato che all'URL si giunge a seguito di una ricerca effettuata a patire dal nome dell'interessato, che il trascorrere del tempo ha reso obsoleta e non più utile alla collettività la conoscenza dell'informazione, con l'ulteriore aggravante della violazione del principio dell'esattezza dell'informazione di cui al Punto 4 delle Linee Guida, ha accolto il ricorso dell'interessato, ordinando a Google la rimozione dell'URL indicato dai risultati di ricerca, a partire dal nome dell'interessato, in tempi contingentati.

I dati personali inseriti nei social network, entrati nel mare magnum del web, diventano ingovernabili e ingestibili; la loro circolazione non è più controllabile dal titolare degli stessi, il quale, anche se dovesse decidere di uscire dal sito, disattivando il proprio profilo, non ne potrebbe impedire né la permanenza, né la circolazione, dal momento che gli stessi potrebbero essere comunque conservati nei server e negli archivi informatici dell'azienda che offre il servizio.

Le aziende che gestiscono i social networks, d'altra parte, hanno tutto l'interesse ad accumulare dati e informazioni perché, vendendo pubblicità mirate, sartorializzate sui singoli utenti, dei quali analizzano in dettaglio il profilo, le abitudini, gli interessi, a chi ne ha bisogno, incrementano i profitti[92].

Alla luce di tali considerazioni il Garante suggerisce di pubblicare con accortezza i propri dati personali, in particolare quelli che rendono la persona rintracciabile, di non accettare con disinvoltura richieste di contatti e di amicizia, di meditare a lungo prima d'inserire in Rete opinioni o informazioni che potranno riemergere a distanza di anni, grazie all'opera dei motori di ricerca, di utilizzare impostazioni orientate alla privacy e di verificare continuamente il rispetto delle condizioni d'uso da parte del fornitore del servizio[93].

Una delle prime pronunce[94] del Garante della Privacy nei confronti di Facebook è del 2016 e riguarda un ricorso relativo al caso della creazione di un profilo falso. L'interessato aveva già sporto denunzia, circa il falso profilo, al social e, avendo ritenuto insoddisfacente la risposta, si è visto costretto ad adire la via amministrativa, proponendo ricorso all'Autorità Garante e lamentando di essere stato vittima di minacce, insulti tentativi di estorsione e sostituzione di persona da parte di altro iscritto che, dopo aver chiesto ed ottenuto la sua 'amicizia', avrebbe inizialmente intrattenuto una

[92] E' il tema della pubblicità comportamentale, basato sulla raccolta di dati on-line, relativi al comportamento degli utenti su Internet ed ai loro percorsi di navigazione. Essa utilizza le informazioni relative all'attività in Rete del singolo utente, come le pagine visitate o le ricerche effettuate su un motore di ricerca, per identificare la tipologia di contenuti pubblicitari da proporgli. Questo tipo di attività è generalmente condotta attraverso i cookie, i quali tengono traccia delle attività dell'utente e associano tali informazioni ad un determinato computer o altro dispositivo. Negli Stati Uniti, le aziende hanno sottoscritto codici di autoregolamentazione nei quali si impegnano a chiedere il previo consenso degli utenti prima di utilizzare i loro dati a fini pubblicitari ed a garantire ai consumatori massima trasparenza mediante chiare comunicazioni e informative circa la raccolta e l'utilizzo dei dati. Le informazioni si predispongono ad essere utilizzate per studiare i loro gusti e le loro abitudini e sullo sfondo c'è sempre il grande tema Big Data, l'immensa mole di dati digitali che gli utenti lasciano ogni giorno in Rete, immense scie elettroniche che possono essere analizzate e utilizzate per le più diverse finalità.

[93] Garante nazionale per la Protezione dei Dati Personali, *Social network: attenzione gli effetti collaterali,* in *www.garanteprivacy.it,* 2009.

[94] Garante nazionale per la Protezione dei Dati personali, *Doc. Web*, *n. 4833448*, 11 febbraio 2016.

corrispondenza confidenziale, poi sfociata in tentativi di reato. Il ricorrente, recriminando che il 'nuovo amico', a causa del suo rifiuto di sottostare alle richieste di denaro, avrebbe creato un falso account, utilizzando i suoi dati personali e la fotografia del profilo, attraverso il quale avrebbe inviato a tutti i suoi contatti facebook fotomontaggi di fotografie e video gravemente lesivi dell'onore e del decoro, oltre che della sua immagine pubblica e privata, chiedeva la cancellazione e il blocco del falso account nonché la comunicazione dei suoi dati, da parte del social, in forma chiara, anche di quelli, presenti nel profilo 'fake'.

L'Autorità amministrativa, nell'accogliere in pieno le lamentele del ricorrente, ha obbligato il 'social' ad adempiere a tutto quanto dallo stesso richiesto.

E' un caso sintomatico dei gravi rischi nei quali il cybernauta può incorrere, in maniera del tutto inconsapevole, nell'uso delle piattaforme proposte dalla Rete. I rimedi tecnici e giuridici per tutelare la sfera più intima della persona esistono, ma non bastano perché spesso il danno è fatto! Senza considerare i patemi d'animo, nonché, talvolta, anche gli oneri economici e i tempi, non sempre contingentati, necessari per consentire all'incauto 'navigatore' di ottenere piena giustizia.

L'evoluzione delle tecnologie, rapidissima quanto pericolosa per i numerosi servizi creati e messi a disposizione degli utenti, che facilmente possono trasformarsi in forme di raccolta dati, controllo e profilazione degli individui, aveva reso i tempi maturi per un nuovo intervento del legislatore europeo, finalizzato alla produzione di una normativa in grado di governare le nuove tecniche informatiche, uniforme per tutti i Paesi europei e volta ad armonizzare definitivamente le legislazioni, superando le precedenti frammentazioni.

Lo sforzo del legislatore europeo si è materializzato con l'entrata in vigore del Regolamento europeo, nel maggio 2018, resosi quanto mai necessario anche per normare le numerose opportunità offerte da Internet, che 'prendono' dall'utente, molto più di quanto effettivamente gli diano, nonostante l'apparente gratuità dei servizi offerti.

2) La tutela dei dati e delle informazioni personali in Google

Con provvedimento web del 2014, n. 3283078, il Garante nazionale della Privacy, nel diagnosticare una serie di falle nel sistema di gestione dei dati personali da parte di Google, ne ha previsto e indicato la cura.

Per la verità, già negli anni precedenti, l'Autorità garante nazionale ed altri Garanti europei, si sono visti costretti ad intervenire, a causa delle assai numerose lamentele dei cittadini che avevano denunziato palesi violazioni alla loro sfera intima da parte del colosso di Mountain View.

A titolo meramente esemplificativo, il 21 settembre 2010, con provvedimento n. 1759972, a proposito di comunicazioni 'captate' su reti wi-fi, il Garante ha ordinato a Google Street View il blocco di qualsiasi trattamento sui cosiddetti 'payload data, captati dalle vetture di Street View, inviando gli atti all'Autorità Giudiziaria affinché valutasse gli eventuali profili penali, derivanti dalla raccolta di quel tipo di dati.

L'Autorità aveva avviato l'istruttoria nei confronti di Google nel maggio 2010, quando era venuta a conoscenza della circostanza che le Google cars, girando sul territorio italiano, oltre a raccogliere immagini, avevano anche catturato, a partire dall'aprile 2008, tramite appositi software, frammenti di comunicazioni elettroniche – i payload data – trasmessi da utenti che utilizzavano reti wi-fi non protette. Nel corso del procedimento, Google, fornendo i riscontri richiesti dal Garante, ha confermato la raccolta dei dati durante il passaggio delle vetture Street View e, pur ammettendone l'errore, aveva aggiunto che i dati raccolti erano così frammentati, da non poter essere considerati informazioni personali, tanto da non essere mai stati utilizzati, né comunicati a terzi, ma solo conservati nei suoi server, negli Stati Uniti.

Ad avviso del Garante, invece, il motore di ricerca avrebbe violato il Codice Privacy ed anche alcune norme del Codice penale[95], poiché una tale raccolta d'informazioni, effettuata in modo sistematico e per lungo periodo di tempo, aveva comportato la concreta possibilità che alcune delle informazioni 'catturate', avendo natura di dati personali, avrebbero potuto consentire di risalire a persone identificate o identificabili.

Alla luce di quanto riscontrato, il Garante ha ritenuto necessario trasmettere gli atti all'Autorità giudiziaria, ai fini dell'accertamento di eventuali profili penali dell'accaduto,

[95] L'art. 617 *quater* c.p. punisce le intercettazioni fraudolente di comunicazioni effettuate su un sistema informatico o telematico e l'art. 617 *quinquies* c.p. punisce l'installazione, fuori dei casi previsti dalla legge, di «*apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico*».

e, imponendo al colosso dell'informazione la sospensione di qualunque trattamento, ha deliberato che i cittadini avrebbero dovuto essere informati della presenza delle Google Cars, al fine di poter decidere, in piena libertà, i loro comportamenti ed eventualmente scegliere di sottrarsi alla 'cattura' delle immagini, allontanandosi dai luoghi ripresi. I veicoli del servizio Street View, da parte loro, avrebbero dovuto essere facilmente individuabili, attraverso cartelli o adesivi ben visibili, che indicassero, in modo inequivocabile, l'acquisizione di immagini fotografiche per quella finalità. Alla società californiana è stato inoltre ordinato di pubblicare sul proprio sito web, tre giorni prima dell'inizio delle riprese, le località visitate dalle vetture Street View.

Altrettanto, il Garante per la Privacy francese, il 21 marzo 2011 ha sanzionato Google per il servizio di mappe on-line, per aver violato dati sensibili dei cittadini, a causa dei collegamenti alle reti wi-fi che avevano catturato password, indirizzi e-mail e informazioni private: il motore di ricerca, nonostante la promessa di cancellare tutti i dati privati, aveva continuato ad usare gli identificativi dei punti di accesso wi-fi all'insaputa dei titolari.

Viepiù, la quarta sezione penale del Tribunale di Milano[96], nel febbraio 2010, ha condannato tre dirigenti di Google per non aver impedito la pubblicazione di un video che mostrava un minore affetto da sindrome di down, picchiato e insultato da quattro studenti in un Istituto tecnico di Torino. Il video girato con un videofonino era poi stato caricato su Google Video, piattaforma di hosting per la condivisione dei video[97].

I tre dirigenti, a parere dei giudici milanesi, avevano violato il Codice della Privacy in materia di trattamento dei dati, visto che l'informazione alla privacy "era talmente

---

[96] Trib. Milano, sentenza del 24 febbraio 2010, n. 1972, in *Giur. Merito,* 2011, 1, 159 con nota di F.G. CATULLO.

[97] Verdetto poi ribaltato da App. Milano, sentenza del 27 febbraio 2013, n. 8611, in *Giur. merito* 2013, 7-8, 1577 che, nell'assolvere i tre manager 'perché il fatto non sussiste', ha riconosciuto «*l'impossibilità effettiva e concreta di esercitare un pieno ed efficace controllo sulla massa dei video caricati da terzi, visto l'enorme afflusso dei dati' e ravvisando in un controllo preventivo da parte del provider, un restringimento ella libertà di espressione*». Le conclusioni dei giudici di appello sono state poi confermate anche dai giudici di legittimità, Cass. Pen., Sez. III, sentenza del 3 febbraio 2014, n. 5107, in *Dir. giust.*, 2, 2014, i quali hanno ribadito che Google è «*solo virtuale di un contenitore virtuale dove gli internauti possono liberamente caricare i loro video, fornendo un mero servizio di Internet host provider, non essendo pertanto, titolare di alcun trattamento e che gli unici titolari del trattamento dei dati sensibili eventualmente contenuti nei video sono gli stessi utenti che li hanno caricati, ai quali soli possono essere applicate le sanzioni amministrative e penali previste per il titolare del trattamento dal Codice della Privacy*». Per approfondimenti sulla sentenza definitiva Google-Vividown: M. IASELLI, *Video offensivo on-line: nessuna responsabilità per l'Internet provider*, in *www.altalex.com*, 26 marzo 2014; P. ZARZACA, *Vividown, La fine ella caccia alle streghe*, in *www.leggioggi.it,*11 febbraio 2014.

nascosta nelle condizioni generali di contratto, da risultare assolutamente inefficace per i fini previsti dalla legge": si insinuava, così, il dubbio che Google, nascondendo le limitazioni legate alla privacy in un lunghissimo testo (che pochi leggono), in realtà puntasse ad allargare indiscriminatamente l'utenza, perseguendo un interesse commerciale prioritario rispetto a quello di fornire tutela ad un principio di libertà di espressione in Rete[98].

Ancora, nella sentenza n. 40356 dell'8 ottobre 2015, la terza sezione penale della Corte di Cassazione ha condannato per trattamento illecito di dati personali colui che aveva pubblicato su You Tube un video che ritraeva le pose oscene della vittima.

Inoltre, in materia di profilazione, il Garante (con provvedimento n. 161 del 19 marzo 2015 "Linee Guida in materia di trattamento di dati personali per profilazione on-line") ha ribadito che il consenso dell'interessato, per ogni attività di profilazione on-line è obbligatorio e revocabile in ogni momento.

I numerosi e reiterati casi nei quali il primo colosso dell'informazione, Google, non solo a livello nazionale, è stato oggetto di lamentele e, come abbiamo visto di denunce sia in sede civile, che penale, hanno sollecitato il WP29 ad inviare, il 16 ottobre 2012, a Mister Page (Fondatore e CEO di Google),una missiva contenente contestazioni circa "l'omessa conformità dei trattamenti effettuati ai requisiti imposti dalla disciplina europea", invitandolo all'adozione di misure idonee ad assicurare il rispetto di alcuni specifici principi e deliberando nel contempo, un'apposita task force, di cui sono state chiamate a far parte alcune delle Autorità di protezione dei dati personali degli Stati membri, tra cui l'Italia", finalizzata a creare forme di controllo più penetranti sulle modalità di trattamento e conservazione dei dati.

Successivamente a tale missiva, il Garante italiano ha informato il colosso di Mountain View dell'avvio del procedimento amministrativo nei suoi confronti, finalizzato alla verifica della liceità e correttezza dei trattamenti effettuati, alla luce della nuova Privacy Policy che, dal 1° marzo 2012, ha unificato oltre 70 diverse Privacy Policy in un unico documento.

[98] La sentenza Google-Vividown è importante anche in materia di responsabilità del provider, com'è spiegato nel paragrafo 6.3. Per un approfondimento della sentenza, G. CAMERA- O. POLLICNO, *La legge è uguale anche sul web*, Milano 2010; E. MAGGIO, *Sentenza Google – Vividown, Non esiste la sconfinata prateria di Interne dove tutto è permesso e niente può essere vietato*, in *www.dmt.it*.

La società aveva infatti unificato in un unico documento le regole di gestione dei dati relativi alle numerosissime funzionalità offerte, dalla posta elettronica (G.Mail), ai social (Google Plus), alla gestione dei pagamenti on-line (Google Vallett), alla diffusione di filmati (You Tube), alle mappe on-line (Street View), all'analisi statistica (Google Analytics), procedendo all'integrazione e interoperabilità anche dei diversi protocolli e dunque all'utilizzo di più servizi.

Nonostante nel corso dell'istruttoria il motore di ricerca abbia adottato una serie di misure per rendere la propria Privacy Policy più conforme ai dettami della normativa, il Garante ha riscontrato diverse criticità riferibili al trattamento dei dati da parte di Big Google, relative soprattutto al contenuto dell'informativa resa agli interessati, all'omessa richiesta del loro consenso per trattamenti con finalità di profilazione e ai tempi di conservazione, tutte analiticamente descritte nel provvedimento del 10 luglio 2014, n. 3283078: documento di natura prescrittiva, nel quale l'Autorità amministrativa nazionale, oltre ad aver puntualmente individuato le criticità nel trattamento, ha suggerito direttamente al motore di ricerca quali accorgimenti adottare per potersi adeguare efficacemente ai dettami normativi vigenti.

Google è stata, quindi, invitata a predisporre un'informativa in modo chiaro, completo ed esaustivo, facilmente accessibile con un solo clic dalla pagina del dominio da cui l'utente accede, formulata in modo da consentire agli utenti di raffrontare le diverse Privacy Policy susseguitesi nel tempo e strutturata su più livelli (informativa per minori, adulti, imprese, professionisti, società), nel rispetto dell'opinione 10/2004 dei Garanti europei della privacy.

Richieste fin troppo puntuali ma ragionevoli, dal momento che tutto il mondo dei dati e del loro trattamento ruota intorno a Google e circola attraverso le app e i servizi che il colosso di Mountain View mette 'generosamente' a disposizione degli utenti. Lo stesso Internet quasi s'identifica con Google per cui, se da un lato oggi pensare al web senza quel motore di ricerca è impossibile, non per questo gli si deve consentire di potersi sottrarre alle norme che le Istituzioni europee e i diversi Stati membri hanno sottoscritto, a tutela di un patrimonio tanto prezioso, quanto sfuggente, quale quello dei nostri dati personali.

Il Garante nazionale ha svolto lodevolmente il suo compito, prima nel garantire e tutelare la sfera più intima dell'io dematerializzato che la persona evidentemente non è stata in

grado di proteggere da sola e, successivamente, nell'obbligare il motore di ricerca al rispetto delle indicazioni contenute nel provvedimento del luglio 2014 e disciplinate nel protocollo di verifica dallo stesso, sottoscritto nei primi mesi del 2015[99], contenente l'implementazione di una serie di misure atte a garantire la tutela dei dati personali degli utenti dei circa settanta diversi servizi offerti.

3) La sfida lanciata al diritto alla protezione dei dati dai nuovi servizi offerti dalla Rete

3.1) Il Cloud Computing

Il cloud computing, ossia quell'insieme di tecnologie informatiche che consente l'impiego di risorse e di servizi hardware e software residenti prevalentemente nei server web, piuttosto che essere sparsi sui singoli computers connessi in Rete[100], consente all'utente, che dispone di un qualunque 'device' (come ad es. un palmare, un pc o uno smartphone), di un browser e di una connessione a Internet, di accedere alla 'nuvola giusta' che gli può fornire i servizi e/o i dati che gli necessitano[101].

Modello ibrido di sfruttamento delle risorse offerte dalle Reti di computer, in primis Internet, che superando il vecchio modello cliente/server, che lo ha da sempre caratterizzato e dominato, è oggi impiegato in differenti contesti quali: il SaaS – Software as a Service, applicazioni erogate da un remoto provider esterno all'azienda utente; il PaaS – Platform as a Service, simile al SaaS costituito da più programmi, consistente in una piattaforma software, della quale fanno parte diversi servizi e programmi e l'IaaS – Infrastructures a Service, ossia nell'utilizzo di risorse hardware.

L'idea e la relativa filosofia del Cloud Computing nasce dalla difficoltà di trovare le giuste soluzioni di fronte ad un improvviso upgrade o downgrade di un sistema informativo: con questa funzione, invece, non ci si trova di fronte ad un unico fornitore di servizi e ad un solo committente, così come viene ad essere modificato il paradigma

[99] Approvazione del protocollo di verifica che disciplina le attività di controllo da parte del Garante sulle prescrizioni impartite a Google il 10 luglio 2014 - 22 gennaio 2015, *Doc. Web n. 3738244*.

[100] A tale riguardo è opportuno ricordare che l'utilità propria di ogni computer è quella di eseguire programmi o applicazioni; le parti immateriali del computer, che consentono l'esecuzione dei programmi sono definite software e si contrappongono a quella che è la parte cosiddetta fisica o elettronica degli elaboratori di programmi, ossia l'hardware.

[101] Questi servizi potranno essere composti a piacimento dall'utente nel contesto dei suoi bisogni. In questo modo l'utente potrà creare uno strumento personalizzato composto da un moltitudine di funzionalità derivanti dalla somma dei singoli servizi web.

dei soggetti attori, che sono essenzialmente tre, il fornitore di servizi, ossia i server virtuali, il cliente amministratore, colui che sceglie e configura i servizi messi a disposizione dal fornitore e il cliente finale, colui che utilizza i servizi configurati dal cliente amministratore[102].

L'aspetto decisamente innovativo del sistema, per l'utente finale, è dato dalla possibilità di spostare i dati dal proprio device su una 'nuvola', con il risultato di ottenere tutto ciò che serve all'utilizzatore in ogni posto e in qualunque momento, così che, ovunque l'utente acceda ad Internet, disponga dei dati, dei software e dei relativi servizi, come se si trovasse in casa propria o nel suo ufficio, realizzando una vera e propria delocalizzazione delle proprie risorse.

Se oggi il 'cloud computing' consente di gestire archivi, foto e video, posta elettronica e agenda appuntamenti, testi e documenti vari, l'offerta dei servizi è in progressiva e costante crescita, favorita anche da ragioni economiche, quali la possibilità di riduzione degli investimenti in hardware, da parte dell'azienda che, grazie a quel sistema, può affidare, al solo fornitore di cloud, l'erogazione dei servizi d'informatica.

Le applicazioni aziendali tradizionali, infatti, sono sempre state molto complicate e costose: la quantità molto elevata di hardware e software necessari per la loro esecuzione richiedeva un intero team di esperti per istallarle, configurarle, testarle, eseguirle, proteggerle e aggiornarle; moltiplicando tutto questo per decine e centinaia di applicazioni, è facile intuire perché anche le più grandi aziende, con i migliori reparti IT, non siano riuscite ad ottenere tutte le applicazioni di cui avrebbero avuto bisogno, mentre le piccole e medie sono andate letteralmente fuori dal mercato.

Il Cloud computing ha permesso di eliminare, o comunque di ridurre al minimo, tutti questi problemi non richiedendo al cliente la gestione di hardware e software, dal momento che ad occuparsene è un fornitore esperto: è sufficiente aprire un browser, personalizzare l'applicazione ed iniziare ad usarla, usufruendo di una serie di servizi, dalla gestione delle relazioni con i clienti, a quella delle risorse umane, ai servizi di contabilità e molto altro ancora. L'infrastruttura offre un funzionamento simile a quello di servizi pubblici: l'utente paga solo le funzionalità necessarie, gli aggiornamenti sono automatici e i costi abbastanza contenuti.

[102] Da sottolineare come in determinate circostanze, il cliente amministratore e il cliente finale possano coincidere. Così un cliente può utilizzare un servizio di 'storage' per effettuare il 'backup' dei propri dati. In questo caso il cliente provvede sia a configurare che ad utilizzare il servizio.

I maggiori player di questa nuova sfida tecnologica sono grandi ed importanti società come Microsoft, Google, Oracle, IBM ed Amazon. Anche la NATO ha recentemente messo in funzione un proprio sistema privato di server remoti, utile a consolidare i vari flussi d'informazioni e facilitare il compito di comando negli scenari operativi. Così come Telecom Italia ha deciso di lanciarsi nel cloud computing, consentendo alle grandi imprese e alla Pubblica Amministrazione di usufruire d'infrastrutture e servizi costantemente aggiornati, ottimizzandone i costi e le prestazioni e proponendosi come principale player nazionale nel settore[103].

3.1.1) Vantaggi e criticità del Cloud Computing in materia di protezione dei dati personali

Evidenti sono i vantaggi apportati dal Cloud Computing, primo fra tutti quello di ridurre al minimo, grazie al suo potenziale, il tempo necessario per recuperare danni cagionati da guasti o da calamità naturali, senza dimenticare il beneficio, consistente nella possibilità che le infrastrutture Cloud possano gestire efficacemente gli eventuali picchi di domanda da parte di singoli clienti, dal momento che le risorse vengono condivise tra più servizi e clienti.

Considerato che il crescente potenziale di queste nuove tecnologie favorirà lo sviluppo di una mole impressionante di dati di vario genere, accessibili nelle varie 'nuvole' ed i rispettivi gestori saranno depositari di una quantità sterminata d'informazioni, sorge spontaneo il timore, che coloro che accederanno a questo servizio, potranno essere fortemente penalizzati nella loro sfera privata e nella possibilità di poter tutelare e proteggere i loro dati.

Il Garante per la Privacy nel 2012[104] si è espresso con una serie di indicazioni, rivolte ad imprese private e pubblica amministrazione, nelle quali ha avuto modo di sottolineare che

[103] I servizi previsti sono: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS), quest'ultimo in collaborazione con i partner di Telecomitalia, attivi nel settore IT. Nei segmenti IaaS e PaaS saranno disponibili soluzioni di storage, desktop virtuali e soluzioni di collaboration, oltre al servizio già siaponibile di hosting evoluto, che consente l'utilizzo da remoto di risorse hardware, distribuite e di videocomunicazione in alta definizione, erogabile su apparati eterogenei e tra aziende diverse. All'interno del segmento SaaS sono comprese soluzioni di infomobilità, gestione documentale ed Enterprise resource planning (Erp), dedicati alle imprese e soluzioni indirizzate alla PA, come l'Energy Management o gli Smart Service per la gestione intelligente del territorio, l'informatizzazione della scuola, l'inclusione sociale negli ospedali.

[104] Garante per la Protezione dei dati personali, *Cloud Computing, Proteggere i dati per non cadere dalle nuvole*, in *www.garanteprivacy.it.*

"Chi è titolare del trattamento dei dati personali, che trasferisce, del tutto o in parte, il trattamento sulle 'nuvole', deve designare il fornitore dei servizi cloud, 'responsabile del trattamento". Questo significa che il cliente dovrà comunque prestare attenzione a come saranno utilizzati e conservati i dati caricati sulla 'nuvola: in caso di violazioni commesse dal fornitore, anche il titolare sarà chiamato a rispondere dell'eventuale illecito. In tal caso anche le piccole aziende, quelle con minore capacità di contrattazione con i Cloud Provider, saranno in ogni modo chiamate a chiedere clausole contrattuali o modalità di controllo più stringenti.

I rischi derivanti dall'utilizzo di un sistema di Cloud Computing attengono, infatti, in primo luogo, agli aspetti legati alla sicurezza e alla continuità del servizio: l'utilizzo del servizio di Cloud Computing, nel memorizzare dati personali, espone l'utente a seri rischi di violazione della sua privacy. I suoi dati, che risultano in possesso dell'azienda, qualora quest'ultima volesse tenere un comportamento scorretto, o comunque dare priorità a forme d'investimento economico piuttosto che di tutela della privacy, potrebbero essere resi, da quella, facilmente accessibili per indagini di mercato o di profilazione dell'utente. Rischi che potrebbero essere in parte neutralizzati crittografando le informazioni sul server, al fine d'impedire alla società l'accesso alle stesse. La soluzione, tuttavia, non risolve del tutto il problema, dal momento che il servizio Cloud Computing potrebbe passare a monitorare le attività degli utenti ed effettuare comunque una loro profilazione per fini pubblicitari.

Il controllo sui dati, quindi, è ancora decisamente molto scarso, anche considerato che questi risiedono in server di cui l'utente finale non conosce nemmeno la dislocazione o il numero delle replicazioni, così come sussiste il problema che lega il trasferimento dei dati on-line con la possibile violazione del diritto alla riservatezza. E', pertanto, indispensabile che il titolare del trattamento debba assicurarsi che siano adottate misure tecniche ed organizzative, volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, di modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole, così come il cliente dovrebbe poter, in ogni momento, accertarsi che i dati siano sempre per lui disponibili e 'riservati', nel senso che ne sia consentito l'accesso solo a chi ne abbia il diritto.

Per garantire, tuttavia, la sicurezza delle informazioni non è importante solo il modo in cui il dato sia conservato, ma anche quello in cui venga trasmesso, se ad esempio siano utilizzate tecniche di cifratura delle informazioni.

Il Codice nazionale della Privacy, così come il Regolamento 2016/679 UE, che ha abrogato la Direttiva 95/46 CE, attribuiscono agli interessati, titolari dei dati, una serie di diritti, (conoscere quali e quanti dei suoi dati siano in possesso dell'Amministrazione pubblica o delle imprese private, chiederne copie, aggiornamenti, rettifiche o integrazioni) la cui violazione potrebbe anche portare al blocco, alla cancellazione e alla trasformazione in forma anonima delle informazioni. Da parte sua il cliente del servizio Cloud, in qualità del titolare del trattamento dati, per soddisfare queste richieste, deve poter mantenere un adeguato controllo, non solo sulle attività del fornitore, ma anche su quelle degli eventuali subfornitori dei quali il Cloud Provider potrebbe avvalersi.

Se il Cloud Computing[105], pertanto, permette l'accesso agevole a documenti, informazioni, e-mail e contatti, anche quando si è lontani dalla postazione abituale**,** è, tuttavia, necessario adottare delle precauzioni nel momento in cui si decide di appoggiarsi a siffatte risorse esterne sulle quali, inevitabilmente, il controllo dell'utente finale è vicino allo zero.

Tale accortezza è tanto più necessaria se, come è opinione largamente diffusa, il Cloud Computing, e in particolare la tipologia IaaS, che consente alle aziende di innovare con maggiore facilità, a rischi e costi sempre minori, nei prossimi anni è destinata a giocare un ruolo determinante nelle attività IT Aziendali.

Le promesse dei Cloud Computing sono, infatti, palesemente allettanti: pagare quanto si consuma, trasformare i costi fissi in costi variabili, eliminare i grandi investimenti, sostituendoli con costi operativi diluiti nel tempo. Sull'altro piatto della bilancia va messo tuttavia, il rischio di perdite in termini di controllo sui propri dati e di sicurezza degli stessi, rischi a tal punto fondati che una serie di applicazioni, in particolare nei settori finanziario e sanitario, non possono e non devono fare ricorso al Cloud computing proprio per ragioni normative e rischi per la privacy.

3.2) L'IOT: Internet of Things

[105] Con riferimento alle aziende, il ricorso al Cloud Computing permette alle banche dati aziendali di poter lasciare i locali dell'impresa, per essere ospitate presso reti di 'data center' gestite da soggetti terzi.

L'IOT[106], l'Internet degli oggetti, neologismo riferito all'estensione di Internet al mondo degli oggetti e dei luoghi concreti, è utilizzato, da ormai qualche anno, per definire la rete delle apparecchiature e dei dispositivi, diversi dai computer, connessi a Internet, quali sensori per il fitness, automobili, radio, impianti di climatizzazione, ma anche elettrodomestici, lampadine, telecamere, container per il trasporto delle merci, qualunque dispositivo elettronico dotato di un indirizzo IP, che ne consenta l'identificazione univoca sulla Rete e la capacità di scambiare dati attraverso la Rete, senza necessità dell'intervento umano.

Obiettivo degli 'oggetti connessi' è quello di semplificare la vita, automatizzando i processi, come, ad esempio, per i 'termostati intelligenti', che essendo in grado di imparare orari ed esigenze e di scegliere la temperatura adatta ad ogni momento, consentono risparmi, anche in termini di energia, non solo di tempo, potendo essere azionati a distanza attraverso smartphone.

Secondo un rapporto del 2015 della Commissione europea[107], nel 2020 saranno più di sei miliardi gli oggetti intelligenti interconnessi su piattaforme 'Internet of Things', mentre la protezione delle informazioni, derivate dall'uso degli oggetti interconnessi, è ancor lontana dall'essere garantita.

L'IoT, infatti, fa parte del nostro quotidiano: i dispositivi connessi entrano nelle nostre case, alberghi e uffici e non è fantascienza immaginare uno scenario in cui malintenzionati, o anche solo individui spinti da interessi economici, possano tenere in scacco strutture sensibili.

Il problema relativo ai rischi connessi all'uso di quella piattaforma è stato sollevato dal Garante nazionale nel marzo del 2015[108] e, nel settembre dello stesso anno, anche l'FBI ha diramato bollettini di sensibilizzazione alle criticità in materia di protezione dei dati personali.

---

[106] Neologismo introdotto da Kevin Ashton, ricercatore presso il Mit, nel 1999. Anche K ASHTON, *That 'Internet of Things'*, in *RFID Journal*, 22 luglio 2009.

[107] Commissione europea, *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination*, Framework Programme for Research and Innovation 2014-2020.

[108] Il Garante per la protezione dei dati personali, con il *Documento n. 3898704* del 26 marzo 2015, ha dato l'avvio ad una consultazione pubblica sull'IoT, volta all'acquisizione di osservazioni e proposte riguardo gli aspetti di protezione dei dati personali connessi alle nuove tecnologie classificabili come Internet of Things, con specifico riguardo ai risvolti implementativi delle criticità riscontrabili o già riscontrate nel settore di riferimento)

A dare ulteriore spessore al dibattito è intervenuta anche l'Azienda di analisi e consulenza Gartner, sempre nel 2015, con l'affermazione secondo cui "L'IoT ridisegna il concetto di sicurezza, ampliandone i campi di applicazione e aggiungendo responsabilità che derivano dalle nuove piattaforme, dai nuovi servizi e dalle strategie future. Le imprese devono rimodellare i propri reparti IT e la sicurezza informatica[109]."

L'attenzione al problema e le preoccupazioni derivano proprio dalla facilità con cui la Rete viene scandagliata alla ricerca di dispositivi, non solo da parte di malintenzionati ma anche da marketer, aziende ed esperti di profilazione, per sferrare attacchi mirati e, ancor prima, dalla semplicità con cui le informazioni che produciamo e rilasciamo, possano essere intercettate e utilizzate da varie categorie di persone e classi professionali.

Secondo Jay Coley, Global Enterprise Sercurity architects di Akamay, i "Cloud sono importanti; diventa altrettanto importante mettere in sicurezza piattaforme e dispositivi, perché le botnet non sono il solo problema che può minarne lo sviluppo e la diffusione[110]", per cui, secondo la sua esperienza, la tutela e la protezione dei dati tendenzialmente si potrebbe avere prima di tutto minimizzandone l'acquisizione: gli sviluppatori dovrebbero raccogliere i dati limitatamente a quelli strettamente necessari e con una frequenza giustificata. Il prelievo di informazioni non influenti e con eccessiva ciclicità aumenterebbe, infatti, il rischio di violazioni e la possibilità d'intercettare anche quelle sensibili. Il secondo e conseguenziale paletto sarebbe rappresentato dalla riduzione dei tempi di conservazione degli stessi: i dati, una volta analizzati, andrebbero distrutti, evitando il rischio del deposito degli stessi su server che potrebbero essere esposti a infiltrazioni e violazioni. Archiviare le informazioni permetterebbe, tra l'altro, in caso di violazioni, la ricostruzione di una situazione storica inutile e dannosa. Per lo stesso motivo sarebbe opportuno che le informazioni raccolte fossero sempre crittografate.

I rischi di aggressione alla sfera privata potrebbero essere contenuti anche attraverso la riduzione della granularità delle informazioni raccolte. I dispositivi e le applicazioni, infatti, dovrebbero richiedere dati molto aggregati, così da renderli difficilmente decifrabili e, come tali, potenzialmente meno lesivi della sfera intima personale. A parte il diritto al controllo sugli stessi, che il global Enterprise Sercurity Architects di Akamay

---

[109] R. MERCANTALLI, *Gartner Trends 2017: un'analisi di dettaglio su IA, Things e App Intelligenti*, in *http://www.zerounoweb.it,* 18 aprile 2017.

[110] Affermazione resa durante l'Akamay Edge, a Las Vegas nel 2017. L'apporto di Coley è particolarmente interessante perché, oltre ad una carriera ventennale nella sicurezza IT, ha trascorso beni undici anni nelle fila dell'esercito americano ed ha un approccio globale ai temi della prevenzione e della riservatezza.

riconosce ai titolari dei dati stessi, un ruolo fondamentale, in termini di tutela, è anche quello svolto da Organismi di supervisione indipendenti che andrebbero assolutamente creati, affinché, con verifiche mirate, possano opportunamente intervenire.
Anche per l'IoT vale quanto detto a proposito di tutti gli altri sistemi idonei a mettere in sicurezza i dati relativi al singolo e cioè che, al di là delle soluzioni tecniche e normative, sono in definitiva gli utenti a dover fare la loro parte, dimostrando un'elevata sensibilità e attenzione quando acquistano i prodotti, così da indirizzare la scelta verso quelli che più di altri soddisfino i canoni della sicurezza, pur presentando costi più elevati, ed operando uno sforzo di fantasia ulteriore quando impostano password per l'accesso a portali, dispositivi e applicazioni.

3.3) La smart grid e la tutela dei dati personali

Con la locuzione 'smart grid' – Rete intelligente - si fa riferimento ad una progettazione, sempre più diffusa in tutta Europa, che mira a sfruttare al meglio la rete di distribuzione dell'energia elettrica, in modo da migliorare le condizioni di trasferimento dell'energia, dalle unità di produzione al consumatore finale, per la cui realizzazione è necessaria la raccolta di una moltitudine d'informazioni, sia dal lato della produzione, che da quello dell'utilizzo.
La disponibilità di un sistema intelligente finalizzato ad ottimizzare la distribuzione dell'energia elettrica, evitando sovraccarichi di rete ed individuando percorsi alternativi ove si verifichi un'interruzione nelle linee principali di trasmissione, presenta un prezzo da pagare in termini di dati ed informazioni sulle abitudini e comportamenti che, dagli utenti, trasmigrano verso le società energetiche per essere archiviati e immagazzinati, nella più totale inconsapevolezza dei titolari dei dati stessi.
Per questa ragione, a livello europeo, è stato fondato un gruppo di lavoro, cui è stato affidato l'incarico di analizzare in dettaglio i risvolti della nuova attività di raccolta ed utilizzo dei dati, in relazione ai principi di cui alla Convenzione dei diritti dell'uomo ed alla nuova normativa europea sulla protezione dei dati personali, a tutela degli stessi. Dagli studi condotti dal Gruppo di lavoro circa la conformità della rete intelligente alle disposizioni normative richieste in materia di protezione dei dati, è emersa la carenza della legislazione, nazionale ed europea, nella regolamentazione del nuovo fenomeno, per cui i lavori si sono chiusi con una precisa raccomandazione da parte del Gruppo,

strettamente legata all'insufficienza della normativa in atto, rivolta agli organismi legislativi dell'Unione Europea affinchè producessero documenti a livello europeo (perché il problema è europeo, non solo nazionale), che regolamentassero la nuova frontiera di trattamento e di protezione dei dati legati alla realizzazione di reti intelligenti. Quindi, in nome della sicurezza delle informazioni, sarebbe auspicabile l'introduzione di nuove normative, a livello europeo, ivi compresi eventuali sistemi di sicurezza, come la possibilità di applicare eventuali algoritmi criptografici per trasferire i dati dal contatore intelligente al gestore della rete, applicabili a tutti i progetti di reti intelligenti.
Modello di protezione criptografica che ovviamente dev'essere omogeneo a livello europeo, dal momento che le reti intelligenti hanno dimensione europea.

3.4) I contatori intelligenti

L'art.13 della Direttiva 2006/32 CE, sull'uso efficiente dell'energia, ha obbligato gli Stati europei ad installare progressivamente contatori intelligenti, in modo da raggiungere gli obiettivi di energia sostenibile fissati dall'Unione Europea entro il 2020.
Ma un contatore intelligente, a differenza di uno tradizionale, può acquisire informazioni circa il consumo energetico dell'utente e archiviarle, oppure, ad intervalli più o meno regolari, o su richiesta, inviarle al gestore energetico.
Poiché questa raccolta di dati rientra appieno nella categoria dei dati personali, occorre valutare quale possa essere l'impatto di questo nuovo dispositivo sulla raccolta e gestione degli stessi e quali risvolti potrebbero esserci, per la loro tutela, qualora non fossero sufficientemente protetti.
Lo studio del problema è stato affidato al Gruppo dei garanti europei, Art. 29 Working Party, che, dopo un'attenta analisi del fenomeno, è giunto alla determinazione che la raccolta dei dati, da parte dei nuovi e intelligenti dispositivi di misurazione energetica, è massiccia, potendo arrivare perfino a profilare l'utente e le sue abitudini, attraverso la quantità di energia consumata: informazioni che possono essere archiviate o inviate al gestore su sua mera richiesta, anche all'insaputa dell'utente.
Se da una lato questi dispositivi facilitano le forme di controllo sugli usi e abusi nell'ambito del servizio energetico, come eventuali allacci abusivi con conseguente sottrazione di energia, dall'altro manifestano tutta la loro potenziale pericolosità allorquando, dalla lettura in tempo reale dei dati di consumo, si arrivasse ad ipotizzare

che nessuno sia presente in casa, qualora il contatore non denunciasse alcun assorbimento energetico.

Se a questo, che è solo uno dei tanti pericoli cui contatori intelligenti espongono l'utente, si aggiunge il fatto che in Italia nascono continuamente nuovi enti che offrono servizi energetici, il rischio dell'accumulo e dispersione dei propri dati personali non è affatto remoto.

Tale preoccupazione ha portato il Gruppo di Lavoro dei Garanti europei, in attesa di una normativa comunitaria utile ad affrontare il problema e valutata la situazione non dissimile da quella già vista per gli operatori telefonici, a richiedere in sede di raccolta dei dati il consenso esplicito da parte dell'interessato. Occorre, pertanto, che in fase di firma del contratto di fornitura di energia elettrica, un apposito spazio sia dedicato all'informativa circa i dati che vengono generati dai contatori intelligenti, la durata della conservazione ed informazioni relative alla loro destinazione e/o trasmigrazione verso il gestore o parti terze.

E' anche vero che il D. Lgs. 196/2003[111] ricorda che il consenso non è necessario quando l'elaborazione del dato è indispensabile per la fornitura dei servizi specificati nel contratto: di talché l'utente non potrebbe impedire la raccolta dei dati afferenti l'assorbimento energetico, altrimenti non potrebbe essere emessa la bolletta. Tuttavia, una cosa è l'informazione afferente l'assorbimento complessivo, altra è quella relativa al consumo giorno per giorno o addirittura ora per ora[112].

3.5) Reperimento dei dati in Rete e comunicazioni indesiderate: lo Spam

Con il dilagare della pratica del web marketing si sono poste complesse questioni in ordine al corretto sfruttamento delle potenzialità offerte dalle reti telematiche. Una delle

---

[111] D.Lgs 30 giugno 2003 n.196, art. 24, comma 1, lett b): Casi nei quali può essere effettuato il trattamento senza consenso

«*1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:*

b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato».

[112] A. BIASOTTI, *Il nuovo regolamento europeo sulla protezione dei dati*, op. cit, 600. Avendo qualche analista sostenuto che il problema del consenso non è poi così importante perché in fondo i contattori vengono installati per soddisfare una direttiva europea in tema di risparmio energetico, e quindi la raccolta del dato avverrebbe per soddisfare un interesse pubblico, l'Autore in decisa antitesi, ha precisato che ciò che dovrebbe indurre a porre un freno, arginando il fenomeno, non è la raccolta in sé che sarebbe legittimata dal fine pubblico, quanto il modo e gli altri fini per cui potrebbero essere utilizzate le informazioni raccolte, che potrebbero non essere altrettanto legittimi e per cui abbisognerebbero del consenso espresso dell'interessato.

pratiche più diffuse consiste nell'inoltro di e-mail in quantità massicce agli indirizzi di posta elettronica di una pluralità di soggetti, senza che questi ne abbiano fatto esplicita richiesta.

"Lo spam – a parere di Maria Beatrice Magro - può essere definito come la pratica di spedire a mezzo e-mail corrispondenza non richiesta, normalmente di natura commercial, a soggetti con cui non si è avuto alcun rapporto in precedenza. L'attività di spamming, quindi, presuppone il reperimento di indirizzi e-mail forniti in modo diretto dai visitatori del sito con il consenso di questi, o raccolti in modo occulto attraverso registri elettronici, all'insaputa dell'utente destinatario. Non è estranea anche la possibilità di avvalersi di elenchi preparati e venduti da terzi che raccolgono indirizzi di spazi internet pubblici, quali newsgroup o chat-room, per destinarli alle aziende[113]".

L'art. 130 Codice Privacy richiede l'obbligo del consenso dell'interessato per l'invio di comunicazioni indesiderate, messaggi di posta elettronica, comunicazioni telefoniche a fini pubblicitari o di vendita o di ricerche di mercato, messaggi via telefax, sms, mms o comunicazioni di altro tipo, comunque non richiesti dal soggetto ricevente. Tale invio, inoltre, deve conformarsi ad una serie di altri requisiti, primo fra tutti quello relativo ad una chiara indicazione del mittente e dell'indirizzo a cui il destinatario possa rivolgersi, per ottenere l'eventuale cessazione delle comunicazioni e la cancellazione dei propri dati dalle liste utilizzate per l'inoltro dei contenuti pubblicitari. E' tuttavia consentita la deroga al principio del consenso, in forza del quarto comma dell'art. 130 Cod. Privacy[114], qualora il titolare del trattamento utilizzi, a fini di vendita diretta di prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio: potrebbe non richiedersi il consenso, a condizione che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, da parte sua, adeguatamente informato, non rifiuti tale uso, anche in occasione delle successive comunicazioni.

---

[113] M.B. MAGRO, *Internet e riservatezza: profili di tutela penale dell'utente telematico*, in www.dirittoegiustizia.it, 30 luglio 2005. In questo scritto si fa anche riferimento, tra le altre cose, ai modelli di tutela della privacy, al delitto di trattamento illecito dei dati – art. 167 d.lgs. 196/2003 – e alla tutela della riserbatezza informatica.

[114] La disposizione di cui al quarto comma art. 130 Cod. Privacy era stata implicitamente abrogata dal primo comma dell'art.58 d.lgs. 6 settembre 2005, n. 206, Codice del Consumo, in *G.U. Suppl. ord.,* 162, 2005, ma è tornata pienamente in vigore in forza dell'art. 1 primo comma del d.l. 21 febbraio 2014 n.21 in *G.U.*, 58, 2014, emanato in attuazione della Direttiva 83/2011/UE.

E' evidente che l'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per tali finalità, dovrà essere informato della possibilità di opporsi, in maniera agevole e gratuita al trattamento.

Senza dubbio lo spamming rappresenta uno strumento efficace di diffusione per gli operatori del mercato, che intendano pianificare operazioni di marketing nei confronti degli internauti, essendo una modalità di promozione economica, idonea a raggiungere un grande bacino di utenti, con costi praticamente pari a zero. Non può, tuttavia, sottovalutarsi l'attitudine del fenomeno in questione ad incidere in maniera negativa nella sfera privata dei destinatari: nella gran parte dei casi gli stessi ignorano che la propria e-mail sia stata carpita indebitamente dagli spammers, i quali intanto avranno già inverosimilmente provveduto ad intasare le loro caselle di posta elettronica con del materiale indesiderato.

Il fatto che gli indirizzi e-mail e gli altri dati personali degli utenti siano facilmente reperibili sul web non autorizza a servirsene liberamente e a qualsiasi scopo, dal momento che un loro utilizzo massivo potrebbe comportare una lesione ingiustificata dei diritti dei destinatari, costretti ad impiegare tempi più lunghi per mantenere il collegamento in Rete al fine di ricevere, esaminare, selezionare i diversi messaggi, senza trascurare i costi sostenuti per il collegamento telefonico (incrementati dai messaggi di dimensioni rilevanti che rallentano le operazioni) e per la predisposizione di filtri idonei a verificare la presenza di eventuali virus nei messaggi.

La questione giuridica sottesa a tale fattispecie, pertanto, consiste nella ricerca di un equilibrio tra il diritto delle imprese all'informazione commerciale sui prodotti e sui servizi offerti, quale manifestazione della più ampia libertà d'iniziativa economica privata, sancita dall'art. 41 della Costituzione, e il diritto del cittadino alla tutela e sicurezza e riservatezza dei propri dati personali.

A fronte dell'insufficienza degli strumenti normativi classici a circoscrivere e regolare questo nuovo fenomeno, nonché in virtù del crescente numero di ricorsi, reclami e segnalazioni pervenuti, il Garante della Privacy ha sempre invitato a non abbassare la guardia contro la continua pioggia di posta elettronica indesiderata.

Già l'8 febbraio 2005, le Autorità per la tutela della privacy di 13 Stati europei hanno siglato una sorta di patto anti-spamming per intensificare la lotta al flusso inarrestabile di posta elettronica, istruendo procedimenti comuni di contrasto al fenomeno: da tempo,

anche l'International Telecommunication Union (ITU), organizzazione che opera nell'ambito dell'ONU, avendo dichiarato guerra allo spam, ha varato una strategia d'intervento fondata su alcuni punti chiave, quali il rafforzamento delle leggi in materia, la messa a punto di strumenti tecnici più sofisticati come i filtri anti-spam, la sensibilizzazione di consumatori e imprese rispetto allo spam e alla sicurezza in Internet e, più in generale il potenziamento della cooperazione internazionale attraverso il coinvolgimento dei governi, dei gestori e di tutte le parti in causa.

In Italia si è aperto un dibattito molto acceso sullo spamming in materia elettorale, in occasione delle elezioni amministrative ed europee del 12 e 13 giugno 2004, allorchè la Presidenza del Consiglio dei Ministri ha inviato a tutti gli italiani, possessori di un cellulare, un sms non richiesto dagli utenti che, pertanto, hanno lamentato la violazione della loro privacy.

Di fronte alle montanti proteste sollevate da numerosissimi cittadini, il Garante, nel richiamare i contenuti di un suo documento del 12 marzo 2003, nel quale aveva consentito l'invio di sms, senza il consenso dell'interessato, se alla base giuridica dell'invio vi fossero state 'ragioni di ordine pubblico, igiene e sanità pubblica', ha ritenuto l'esistenza, nel caso di specie, delle ragioni di ordine pubblico, dal momento che, qualche giorno prima dell'invio degli sms, il Ministro degli Interni aveva varato un decreto urgente sulla necessità dell'invio 'dell'sms elettorale' a causa della non sufficiente conoscenza da parte degli elettori, delle novità circa le giornate e gli orari di voto.

Un anno più tardi l'Autorità è tornata sull'argomento in occasione delle primarie del centrosinistra, con un provvedimento *ad hoc* del 7 settembre 2005[115], nel quale ha chiarito dettagliatamente come avrebbero potuto essere utilizzati i dati personali dei cittadini nel rispetto dei diritti fissati dal Codice della privacy, precisando altresì i casi nei quali non era indispensabile la richiesta del consenso dell'interessato/elettore, come quelli per l'invio del materiale di propaganda o di materiali di scarso rilievo dimensionale, come i 'santini' di candidati.

Anche in occasione delle politiche del 2006, con provvedimento del 24 maggio[116], il Garante, nel richiamare le forze politiche al rispetto delle norme contenute in un suo documento dell'anno precedente e nel ribadire i vincoli previsti per partiti, liste e

[115] Garante per la protezione dei dati personali, *Il decalogo del Garante*, Doc. Web n. 1165613, 7 settembre 2005, in *G.U.*, 212, 2005.

[116] Garante per la protezione dei dati personali, Doc. Web n. 1298743, 24 maggio 2006.

candidati, ha respinto il ricorso di tutti quanti avevano lamentato la ricezione di messaggi indesiderati, pur avendo sottoscritto contratti che ne prevedevano la ricezione, in cambio di ricariche telefoniche.

Così, nel febbraio 2010[117], in vista delle consultazioni elettorali, il Garante ha esonerato dall'obbligo d'informativa, partiti, movimenti politici, comitati organizzatori, sostenitori e singoli candidati, che trattavano dati personali per esclusiva finalità di selezione dei candidati alle elezioni, di comunicazione politica e di propaganda elettorale.

Ancora: con provvedimento pubblicato sulla Gazzetta Ufficiale del 14 gennaio 2013, in vista delle elezioni politiche del 24 e 25 febbraio dello stesso anno, il Garante ha distinto i dati che partiti, organismi politici, comitati promotori sostenitori e singoli candidati avrebbero potuto usare a fini di propaganda senza il consenso dell'interessato, da quelli che non avrebbero potuto utilizzare in assenza di quel consenso, ossia quelli attinenti a particolari modalità di comunicazione elettronica (sms, e-mail, mms, telefonate preregistrate) e quelli raccolti automaticamente su internet, o ricavati da forum o newsgroup.

Fuori dalla materia elettorale, il 2 marzo 2006[118] l'Autorità ha disposto il blocco di alcuni archivi di un'agenzia che, in violazione delle norme sulla privacy, inviava sistematicamente fax pubblicitari, senza il consenso dei destinatari, al fine di offrire servizi di direct marketing, precisando che la necessità di un consenso esplicito da parte dei destinatari è una previsione del Codice della Privacy, che fissa tale procedura per poter inviare materiali pubblicitari e promozionali attraverso mezzi tecnici espressamente elencati (posta elettronica – fax – sms – mms). In mancanza di tale consenso, si concretizza la fattispecie di trattamento illecito dei dati, sicuramente sanzionabile.

Con altra decisione del 20 aprile 2006[119] l'Autorità Garante ha ordinato ad una società operante in Internet la cancellazione dei dati personali di un cittadino che lamentava di aver ricevuto posta elettronica indesiderata, anche se la convenuta si era difesa, affermando che si era trattato solo di un 'primo invio' mirato a richiedere il consenso per l'inoltro di ulteriori comunicazioni professionali.

---

[117] Garante per la Protezione dei dati personali, *Misure in materia di propaganda elettorale- esonero dall'informativa*, *Doc. Web n. 1694531,* 11 febbraio 2010, in *G.U.* 22 febbraio 2010, n. 43.

[118] Garante per la Protezione dei dati personali, *Telecomunicazioni – stop all'invio di materiale pubblicitario indesiderato*, *Doc. Web n. 1376148*, 2 marzo 2006.

[119] Garante per la Protezione dei dati personali, *Doc. Web, n. 1289884*, 20 aprile 2006.

Il 22 maggio 2009[120] il Garante ha adottato un provvedimento inibitorio e prescrittivo nei confronti di una società che, presumendo di poter inviare comunicazioni pubblicitarie in ragione dell'acquisto da terzi di un database, non è stata in grado di documentare il consenso del segnalante al trattamento dei suoi dati personali e, in diversi provvedimenti successivi,[121] ha continuato a vietare l'invio, mediante posta elettronica, di comunicazioni promozionali a terzi, senza il consenso specifico, preventivo ed informato degli interessati, ai sensi dell'art. 130 Cod. Privacy.

Anche nella decisione 175 del 5 giugno 2012, il Garante si è pronunciato sulle comunicazioni commerciali indesiderate, ribadendo il principio, enunciato il 29 maggio 2003, secondo cui, preventivamente all'invio di comunicazioni commerciali, debba essere recepito in forma scritta il consenso del destinatario della comunicazione, precisando che "tale disciplina non può essere elusa inviando una prima e-mail che, nel chiedere un consenso, abbia comunque un contenuto promozionale o pubblicitario".

Il numero esponenzialmente crescente di ricorsi, reclami e segnalazioni, pervenuti all'Autorità Garante, ha sollecitato quest'ultima a realizzare delle Linee Guida in materia di attività promozionale e contrasto alle comunicazioni non sollecitate – spam[122], definendo in un quadro unitario misure ed accorgimenti per combattere il marketing selvaggio e favorire pratiche commerciali corrette, alla luce del mutato quadro normativo nazionale e comunitario e dello scenario tecnologico.

Per poter inviare comunicazioni promozionali e materiale pubblicitario, tramite sistemi automatizzati, è necessario acquisire prima il consenso dell'interessato, che dev'essere specifico, libero, informato e reso in forma scritta. Per contro, lecito è il soft- spam, ossia l'invio di messaggi promozionali tramite e-mail ai propri clienti su beni o servizi analoghi a quelli già acquistati; così come un'impresa o una società potrà inviare offerte commerciali ai propri 'follower' sui social network, quando dalla loro iscrizione alla pagina commerciale si evinca chiaramente l'interesse o il consenso a ricevere messaggi pubblicitari concernenti il marchio, il prodotto o il servizio offerto.

---

[120] Garante per la Protezione dei dati personali, *Doc. Web n. 1622647*, 22 maggio 2009.

[121] Garante per la Protezione dei dati personali, *Doc. Web n. 1601674*, 19 febbraio 2009; *Prescrizioni per la videosorveglianza in un supermercato*, *Doc. Web n. 1601522*, 26 febbraio 2009; *Doc. Web n. 1624716*, 22 maggio 2009.

[122] Garante per la Protezione dei dati personali, *Linee guida in materia di attività promozionale e contrasto alla spam*, *Doc. Web n. 2542348*, 4 luglio 2013.

Sul versante della giustizia ordinaria, la prima sentenza di condanna al risarcimento danni da spamming è stata pronunciata il 10 giugno 2004 dal Giudice di Pace di Napoli, che ha condannato una società di articoli sportivi, la Nencini sport Srl, al risarcimento di danni materiali e morali, per responsabilità extracontrattuale da fatto illecito, ai sensi dell'art. 2043 c.c, per violazione della normativa sulla privacy. "Pertanto – si legge nella sentenza - l'invio di posta elettronica indesiderata è illegittimo sotto due profili: da un lato per la scorrettezza ed l'illeceità del trattamento dei dati personali della persona interessata, dall'altra perché provoca una legittima intrusione e invasione nella sfera di riservatezza della stessa".

Baypassando altri procedimenti penali[123],che hanno visto la condanna di società, al risarcimento dei danni in sede civile, e a mesi di reclusione in sede penale, per trattamento illecito di dati personali, avendo inviato, senza l'adeguato consenso da parte degli utenti iscritti alla newsletter, e-mail contenenti messaggi pubblicitari, in materia si è altresì pronunciata anche la Suprema Corte di Cassazione[124], che ha ravvisato la configurabilità del reato di trattamento illecito di dati, previsto e punito dall'art. 167 d.lgs.196/2003, essendo stati realizzati invii non richiesti di materiale pubblicitario nella casella e-mail di destinatari finali. In quell'occasione, i giudici di legittimità hanno precisato che il trattamento illecito di dati personali si viene a configurare qualora la condotta illecita, indipendentemente dal fatto che sia stata posta in essere al fine di trarne un profitto personale per sé o per altri, determini necessariamente un nocumento ai danni della persona offesa. A parere della Suprema Corte, tra l'altro, il nocumento non dev'essere necessariamente di tipo economico, potendo anche consistere "nella perdita di tempo nel vagliare e-mail indesiderate e nelle procedure da eseguire per evitare ulteriori invii". Quindi non necessariamente deve sostanziarsi in una *deminutio patrimonii*, potendo identificarsi anche nel semplice fastidio, ravvisabile nell'inutile dispendio di tempo dedicato alla cancellazione della pubblicità spamming.

[123] Trib. Milano, con sentenza del 17 dicembre 2010, in ha condannato due manager di Buongiorno Vitaminic S.p.A. per aver spammato gli indirizzi e-mail di 180.000 utenti via news-letter. E' una sentenza apripista perché è la prima volta che un'azione di spamming subisce una condanna penale.

[124] Cass. Pen., Sez. III, sentenza del 15 giugno 2012, n. 23798, in *D&G*, 2012, 18 giugno con nota di FERRETTI.

Anche il Tribunale di Brescia[125], tornando sull'argomento spamming a mezzo fax, ha condannato la società Wind Telecomunicazioni S.p.a. al risarcimento dei danni patrimoniali, ai sensi degli articoli 15 Cod. Priv. e 1226 c.c., per illecito trattamento di dati personali, in considerazione del particolare patimento e disagio conseguente al continuo invio di fax, da parte della società, ai ricorrenti, nonostante la diffida di questi ultimi contenente l'espressa richiesta di cessazione dell'invio.

Di tenore analogo la sentenza n. 14326 del 24 giugno 2014 della Seconda Sezione Civile della Corte di Cassazione: "L'invio di una fax promozionale ad un numero estratto dagli elenchi telefonici, se non preceduto dall'informativa sul trattamento del dato personale e dall'acquisizione del consenso del titolare, integra due illeciti amministrativi, consistenti nell'omessa informativa ex articoli 13 e 161 del Codice Privacy e nella non assentita comunicazione automatizzata ex articoli 23,130,162 e 167 del medesimo Codice della Privacy".

A fronte dei numerosissimi casi discussi in sede amministrativa e giudiziaria, non c'è alcun dubbio sull'attitudine dello spamming a ledere in maniera sempre più incisiva diversi diritti tutelati dal nostro Ordinamento, tra i quali spicca la protezione dei dati personali. Non è una caso dunque che tale fenomeno sia stato, sempre più spesso, oggetto di attenzione da parte degli operatori del diritto e che, in virtù della mancanza di una disciplina *ad hoc*, si sia cercato di colmare il vuoto normativo, attraverso il richiamo del Codice in materia di protezione dei dati personali e all'apparato sanzionatorio ivi previsto.

Il fenomeno dello spamming nasce e si sviluppa in modo esponenziale negli States, prima di diffondersi nel resto del mondo, poiché proprio in America era nata Internet e proprio gli Stati Uniti, che in passato si caratterizzavano per un complesso sistema di leggi statali che disciplinavano in modo autonomo la protezione contro lo spamming, sono giunti alla creazione di un'unica legge federale, il cd. 'Can-Spam Act of 2003", che ne ha uniformato il trattamento giuridico in tutti gli Stati. In Europa, invece, le soluzioni sono sempre state frammentate ed inidonee alla risoluzione del problema. Le direttive che si sono seguite hanno in qualche modo ridotto, ma non annullato, le differenti scelte operate dai legislatori nazionali che, diversamente dalla normativa americana, che non proibisce di per sé l'invio di email indesiderate ma prevede che gli operatori commerciali rimuovano

[125] Il Tribunale Brescia, Sez. I, con sentenza del 4 marzo 2013, ha condannato Wind al risarcimento del danno sia patrimoniale che morale per trattamento illecito dei dati, consistente nell'invio di fax pubblicitari.

dalle proprie liste i consumatori che ne facciano espressamente richiesta, hanno scelto il principio dell'opt-in, consistente nella richiesta preventiva del consenso per le comunicazioni indesiderate.
In ragione del fatto che statistiche ufficiali provano che una rilevante percentuale di spam viene prodotta proprio negli USA, l'inefficienza della normativa americana in materia si ripercuote in modo sfavorevole anche nel resto del mondo, Italia compresa.

3.6) Il fenomeno del Telemarketing

Il rapporto tra diritto alla protezione dei dati personali e il telemarketing, pratica di direct marketing consistente nel contatto telefonico diretto, svolto con l'ausilio di operatori commerciali, tra l'azienda ed il cliente potenziale o attuale, per promuovere, pubblicizzare e vendere, attraverso il canale telefonico, le attività, i servizi e i prodotti dell'azienda stessa, è di quelli conflittuali di lunga durata. In Italia, in particolare, la difficile opera di bilanciamento fra il diritto a non essere disturbati nella propria sfera privata, a non essere assillati da promozioni telefoniche indesiderate e il diritto di promuovere liberamente prodotti e servizi è, da almeno vent'anni, oggetto d'interventi ondivaghi, discussioni e provvedimenti, talvolta tesi a rafforzare la privacy dei cittadini, talaltra a sacrificare quest'ultima, in nome del rilancio dell'iniziativa economica.
L'attività di telemarketing, che non si esaurisce nell'uso della comunicazione telefonica, ma può attingere ad altri canali, che sono andati via via diffondendosi sul mercato, come il telefono cellulare (sms), la posta elettronica, si avvale di due tipologie di contatto: l'outbound e l'inbound.
Nella prima, maggiormente invasiva rispetto alla seconda, è l'operatore che decide di mettersi in contatto con il cliente potenziale al fine di rivolgergli una specifica offerta e fargli conoscere l'azienda, coltivando scopi esclusivamente commerciali; la seconda rispecchia la volontà del consumatore di attingere informazioni commerciali di suo interesse.
L'outbound ha da sempre destato dubbi e perplessità riguardo alla tutela della privacy dei consumatori e per questo motivo, negli anni, è stata oggetto di diversi tipi di regolamentazione. Anche perché, per agevolare le aziende nella ricerca di contatti utili, sono nate società dedicate esclusivamente al reperimento dei dati dei cittadini, quindi specializzate nella creazione e vendita di banche dati, che raccolgono informazioni

personali attraverso elenchi del telefono, censimento, indagini territoriali, dividendo la popolazione per reddito, stile di vita, età, aspetti demografici e sociologici.

Proprio a queste società specializzate nella creazione e nella vendita di banche dati (Ammiro Partners, Telextra, Consodata) era indirizzato il provvedimento del settembre 2008[126] del Garante della Privacy, sollecitato da una serie di segnalazioni di telefonate promozionali indesiderate, nel quale aveva loro vietato l'ulteriore trattamento dei numeri di telefono di 15.000.000 di utenti, poiché raccolti in modo illecito, senza che i diretti interessati fossero stati informati o avessero manifestato il loro consenso. Identico divieto era scattato anche per quelle aziende, come Wind, Fastweb, Tiscali e Sky, che avevano acquistato i database da quelle società, per contattare i potenziali clienti.

L'anno successivo, il 12 marzo 2009[127], il Garante ha emanato una serie di Linee Guida, da rispettare durante tutto l'anno, atte ad impedire, o quantomeno a ridurre il fenomeno del telemarketing selvaggio, prorogate poi per altri sei mesi, fino a che, il 25 maggio 2010, è entrato in vigore il c.d. 'Decreto Ronchi'[128], che ha nuovamente cambiato il rapporto tra 'call center' e cittadini, avendo reso contattabili tutte le utenze, comprese quelle che non avevano manifestato il loro consenso, ed avendo introdotto la novità sostanziale del passaggio da un sistema opt-in, in base al quale ogni abbonato poteva ricevere chiamate promozionali, sottoporsi a ricerche di mercato, accettare vendite dirette solo nel caso in cui avesse fornito un consenso esplicito in tal senso, ad un sistema opt-out in cui l'utente può essere contattato al telefono, a meno che non sia iscritto nel Registro delle opposizioni per escludere una tale possibilità.

Registro delle opposizioni[129] che permette, infatti, agli utenti, attraverso l'iscrizione, di formalizzare il rifiuto di ricevere telefonate promozionali da parte delle aziende, anche se

---

[126] Garante per la Protezione dei dati personali, *Doc. Web n. 7592090*, 30 novembre 2017; *Marketing telefonico: scattano i divieti del Garante alle chiamate indesiderate*, *Doc. Web n. 1544315*, 2 settembre 2008; *Doc. Web 1544326*; *Doc. Web n. 1544338*.

[127] Garante per la Protezione dei dati personali, *Prescrizioni ai titolari di banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005 a seguito della deroga introdotta dall'art. 44 d.l. n. 207/2008*- 12 marzo 2009, *Doc. Web n. 1598808*, 12 marzo 2009, in *G.U.* 20 marzo 2009, n. 66.

[128] Legge 20 novembre 2009 n. 166 di conversione in legge del D.L. 25 settembre 2009 n. 135, recante disposizioni urgenti per l'attuazione di obblighi comunitari e per l'esecuzione di sentenze della Corte di Giustizia della Comunità europea, che ha modificato l'art. 130 del Codice in materia di protezione dei dati personali.

[129] Il Registro è stato istituito con D.P.R. 7 settembre 2010 n. 178, in *G.U.* 2010, 256. Il Ministero dello Sviluppo Economico ha affidato alla Fondazione Ugo Bordoni, con la delibera a contrarre del Capo Dipartimento delle Comunicazioni del 3 novembre 2020, la realizzazione e gestione del Registro, al quale devono iscriversi gli abbonati che non desiderano essere più contattati telefonicamente per scopi

in modo reversibile, dal momento che l'utente può sempre decidere, in qualsiasi momento, di prestare il proprio consenso alle telefonate promozionali e commerciali.

Per tutti gli utenti che non si siano iscritti nel Registro, il Codice di Autoregolamentazione[130], intitolato "Norme per la regolamentazione del trattamento dei dati estratti dagli elenchi abbonati per fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale mediante l'impiego del telefono", ha previsto precise garanzie, avendo stabilito fasce orarie molto rigide durante le quali è espressamente vietato il contatto: oltre che di domenica e nei festivi, gli utenti non possono essere disturbati dalle 21,30 alle 9, dal lunedì al venerdì. Il sabato le telefonate pubblicitarie sono vietate prima delle 10 e dopo le 19.

Il garante per la Privacy, con successivo provvedimento del 31 gennaio 2011,[131] nel precisare i limiti entro i quali gli operatori del settore avrebbero potuto utilizzare i dati personali presenti negli elenchi telefonici per effettuare chiamate finalizzate all'invio di materiale pubblicitario, ha imposto alle società telefoniche l'obbligo d'informare i vecchi e i nuovi abbonati circa le modalità d'iscrizione nel Registro delle opposizioni.

Così, con altro provvedimento del 29 settembre 2011[132], la medesima Autorità ha chiarito che i dati contenuti negli albi professionali possono essere utilizzati per chiamate commerciali solo se il promotore abbia acquisito il consenso dell'interessato o presenti offerte strettamente attinenti all'attività svolta dal professionista contattato. In quella circostanza l'Autorità ha vietato ad una società di utilizzare per scopi commerciali i dati personali di un avvocato, che si era lamentato di essere stato disturbato in ufficio con offerte di servizi di telefonia destinati all'utenza business.

Con ulteriore e successivo provvedimento, n. 262 del 20 settembre 2012, il Garante alla luce dell'art. 40 della legge 214 /2011, ha previsto che le persone giuridiche non possano essere contattate se iscritte nel Registro delle opposizioni, né possano ricevere senza

---

promozionali, commerciali o per i, compimento di ricerche di mercato. L'iscrizione può avvenire attraverso cinque modalità: web, via e-mail, numero verde, fax e raccomandata.

[130] Promosso da Asstel, Confindustria, e varato il 21 dicembre 2010, con l'adesione di tutte le più importanti aziende di telecomunicazioni.

[131] Garante per la Protezione dei dati personali, *Telemarketing: le regole del Garante per l'uso dei dati degli abbonati*, *Doc. Web n. 1785597*, 31 gennaio 2011.

[132] Garante per la Protezione dei dati personali, *Vietate le telefonate professionali a fini di marketing verso numeri tratti da albi professionali senza il consenso preventivo dell'interessato*, *Doc. Web n.1851415,* 29 settembre 2011.

consenso telefonate da sistemi automatizzati, fax ed sms. I dati delle persone giuridiche possono però essere utilizzati per finalità commerciali, se estratti, anziché dagli elenchi telefonici, da siti Internet, albi, atti o documenti pubblici. In questo caso, anche la telefonata commerciale con operatore potrebbe risultare estranea alla normativa sulla privacy, lasciando di conseguenza, le persone giuridiche senza tutela. Ciò in quanto, spiega il Garante nel suo Provvedimento, il trattamento dei dati, che costituisce il presupposto di quei contatti promozionali, se effettuato nei confronti di persone giuridiche, enti o associazioni, non risulta più soggetto agli obblighi del preventivo rilascio dell'informativa e acquisizione del consenso, mancando la possibilità di ricondurlo alla disciplina generale di cui agli articoli 23 e 24 del Testo Unico, applicabili esclusivamente agli interessati/persone fisiche. Tuttavia, continua a trovare applicazione, per le persone giuridiche, la normativa del Capo I del Titolo X del testo Unico, che consente loro di richiedere tutela dinanzi l''Autorità Giudiziaria, se lesi, o anche solo infastiditi, da forme di telemarketing selvaggio.

Con provvedimento 503 del 1 ottobre 2015, il Garante della Privacy ha altresì chiarito, aprendo un nuovo canale di discussione che avrebbe poi visto l'intervento del legislatore, che le società di marketing non avrebbero potuto contattare un'utenza riservata, senza aver prima acquisito il consenso dell'intestatario della linea. Un numero riservato, infatti, non può essere iscritto nel Registro pubblico e quindi la regola è che possa essere selezionato dal call center e dalle compagnie telefoniche solo se l'utente abbia già espresso il suo consenso al trattamento dei dati personali per finalità di marketing.

Su quest'ultimo punto è anche intervenuto il legislatore nazionale che, il 22 dicembre 2017, ha definitivamente approvato il disegno di legge n. 2603, che estende la possibilità di iscrizione nel Registro delle opposizioni ai numeri di cellulare e a tutti i numeri riservati non presenti negli elenchi pubblici telefonici. La nuova legge, tuttavia, sarà operativa dopo l'emanazione del Regolamento attuativo (ovvero dopo l'aggiornamento del D.P.R. 178/2010), nel quale saranno definite le modalità tecniche di iscrizione nel nuovo Registro e gli obblighi di consultazione degli operatori di telemarketing. Il Disegno di legge ha introdotto ulteriori ed importanti novità a tutela della privacy dei cittadini, finalizzate al tentativo di arginare il fenomeno del telemarketing selvaggio, prima fra tutte l'annullamento dei consensi precedentemente prestati dai cittadini per finalità pubblicitarie, dal momento in cui sarà diventata operativa l'iscrizione nel Registro. Ciò

non esclude la possibilità di poter sempre successivamente autorizzare i singoli soggetti commerciali alle chiamate pubblicitarie, ma quantomeno in modo consapevole.

Anche l'Autorità Giudiziaria[133] è recentemente intervenuta in materia, condannando un noto gestore telefonico per aver proceduto, nel corso del 2015, a contattare circa 2 milioni di ex clienti che avevano esplicitamente negato o che comunque, non avevano espresso il consenso, ad essere contattati per finalità promozionali. Un'interpretazione costituzionalmente orientata, quella dei giudici milanesi, che, nel conflitto tra il diritto personalissimo alla protezione della propria vita privata, ex art. 2 della Costituzione, e quello alla libertà d'iniziativa economica, ex art. 41 della Costituzione, nel caso di specie ha visto la prevalenza del primo, con conseguente obbligo di inibizione, a carico della società, a contattare gli ex clienti per finalità, anche mediate, di natura promozionale e commerciali.

Corollario di tale conclusione è che i consensi ottenuti attraverso una procedura da qualificarsi illecita alla luce dei principi generali in tema di trattamento dei dati in genere, e in particolare di quelli trattati dalle utenze telefoniche, debbano qualificarsi come illegittimamente acquisiti con conseguente inibitoria alla loro utilizzazione.

Il passaggio dall'opt-in all'opt-out ha senza dubbio agevolato il cittadino nell'esercizio dei suoi diritti, avendo imposto agli operatori nuovi obblighi d'informativa e trasparenza allorché, al momento della chiamata, devono: garantire la propria identificazione, in forza agli art. 9 del D.P.R. 178/2010[134], mostrando il loro numero telefonico, indicare con precisione agli abbonati che i loro dati personali sono estratti dagli elenchi telefonici pubblici e ad informarli e metterli al corrente della possibilità di iscrizione al Registro pubblico delle Opposizioni al fine di non essere più contattati.

La nuova regolamentazione del telemarketing, oltre ad aver permesso la chiusura del procedimento d'infrazione contro l'Italia da parte della Commissione europea, avviato nel gennaio 2010 e dovuto al fatto che le banche dati istituite in passato per creare elenchi telefonici erano accessibili a società esterne che praticavano telemarketing senza che gli

[133] Tribunale Milano, sentenza 5 maggio 2017, n. 5022 Con la sentenza il Tribunale di Milano ha irrogato una sanzione pecuniaria a Telecom Italia per aver ricontattato gli ex utenti senza il consenso degli stessi.

[134] D.P.R. 178/2010, art. 9: Obbligo di presentazione dell'identificazione della linea chiamante
«*Gli operatori che effettuano trattamenti di dati ai sensi del presente regolamento sono tenuti, quando effettuano chiamate nei confronti degli abbonati, a garantire la presentazione dell'identificazione della linea chiamante e a non modificarla*».

abbonati interessati ne fossero al corrente, ha allineato la regolamentazione nazionale alla normativa prevalente europea, dove l'out-put è ormai adottato dalla maggior parte dei Paesi e a quella vigente nel sistema giuridico statunitense che, infatti, è molto simile a quello europeo, avendo, le Autorità locali, la Federal Communications e la Federal Trade Commission, istituito un elenco nazionale "do not call list", che garantisce a coloro che si iscrivono il diritto a non essere più disturbati dagli operatori telefonici.

3.7) La regolamentazione in materia di Cookie

I Cookies, piccoli file di testi creati all'interno di un sito web, allo scopo di registrare alcune informazioni relative alla visita, nonché di elaborare un sistema per riconoscere l'utente anche in momenti successivi, rappresentano uno strumento tecnico essenziale per il buono e corretto funzionamento di quasi tutti i siti web. Alcune operazioni, infatti, non potrebbero essere compiute senza il loro uso, in quanto necessari ed utili a rendere più rapida la navigazione e fruizione del web, intervenendo a facilitare alcune procedure, come gli acquisti on-line, l'accesso all'home banking e alle attività che possono essere svolte sul proprio conto corrente on-line. Tutte operazioni che sarebbero molto più complesse da svolgere, e meno sicure, senza la loro presenza.

Una sorta di memoria attraverso la quale un sito web, grazie all'impostazione di un cookie sul browser dell'utente, riesce a riconoscere uno specifico utente e ad associargli delle informazioni di varia natura e per differenti finalità, a condizione che le preferenze configurate da quest'ultimo lo consentano. In tal caso il browser potrà consentire ad un determinato sito web l'accesso solo ed esclusivamente ai cookies da esso impostati, non a quelli impostati da altri siti web.

Sebbene alcuni cookies potrebbero rivelarsi estremamente invasivi della sfera privata dell'utente, non tutti sono 'cattivi', e di questo se ne è reso conto l'Autorità Garante allorché, nel suo provvedimento dell'8 maggio 2014[135], ha identificato due macrocategorie: i 'cookie tecnici', trasmessi dal gestore del sito per il buono e corretto funzionamento dello stesso e per effettuare la trasmissione di comunicazioni su una rete di elettronica, nella misura strettamente necessaria, al fornitore di un servizio della società dell'informazione, espressamente richiesto dall'abbonato o dall'utente**[136]**, per quali il

[135] Garante per la Protezione dei dati personali, *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie*, *Doc Web n. 3118884*, 8 maggio 2014.
[136] T.U. Privacy, art. 122, comma 1: Informazioni raccolte nei riguardi del contraente o dell'utente

Legislatore non ha richiesto alcun consenso preventivo da parte dell'utente; ed i cookie di profilazione, utilizzati al fine d'inviare messaggi pubblicitari all'utente, in linea con le preferenze dallo stesso manifestate nell'ambito della navigazione in Rete, come accade quando, nell'accedere alla propria pagina su un social network, si visualizzano dei banner pubblicitari legati alle ultime ricerche sul web o agli ultimi acquisti fatti in Internet.

Anche se la capacità d'identificare un utente, associandogli delle informazioni, è stata concepita per finalità tecniche molto importanti, e non solo per tracciare un profilo della personalità e delle abitudini dell'utente in Internet, in ragione della particolare invasività che tali dispositivi[137] potrebbero avere nell'ambito della sfera privata dei singoli, soprattutto quelli di terze parti, provenienti da altri siti e contenuti in vari elementi ospitati dalla pagina stessa (come ad es. immagini, banner pubblicitari, video), tanto la normativa europea, che quella italiana, hanno previsto che l'utente sia adeguatamente informato sull'uso degli stessi ed esprima un proprio valido consenso.

La disciplina relativa ai cookie è stata modificata con l'entrata in vigore della 'Cookie Law'[138], provvedimento nato a livello comunitario, a seguito della Direttiva 2009/136 CE, finalizzata ad arginare la diffusione dei cookie di profilazione ed i connessi rischi per la privacy degli utenti in Rete.

Direttiva che, a sua volta, aveva modificato la precedente, 2002/58, avendo introdotto il principio dell'opt-in in tutti i casi in cui si acceda o si registrino 'informazioni' (compresi quindi i cookie) sul terminale dell'utente o dell'abbonato. E', pertanto, necessario che l'utente esprima un valido consenso preliminare al trattamento, sulla base di

---

«*1. L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con le modalità semplificate di cui all'articolo 13, comma 3. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio. Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente*».

[137] A questi ultimi si riferisce l'art. 122 comma 1 T.U. sulla Privacy laddove prevede che l'archiviazione delle informazioni nell'apparecchio terminale di un utente o l'accesso ad informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbiano espresso il loro consenso, dopo essere stato informato con le modalità semplificate di cui all'art. 13 comma 3, oggi art. 122 comma 1 T.U.

[138] La normativa Cookie Law, in vigore dal 3 giugno 2015, obbliga all'adeguamento alla normativa sui Cookies; non pubblicare le informative potrebbe esporre il titolare del sito a pesanti sanzioni pecuniarie.

un'informativa chiara e completa, in merito alle modalità e alle finalità della manipolazione dei suoi dati.

Inoltre, mentre nel passato erano consentiti soltanto 'cookie tecnici', per i quali era necessario il consenso preventivo, ed ogni altro accesso o registrazione non autorizzati sul terminale dell'utente erano vietati, oggi la nuova normativa (il nuovo art. 122, comma 1, della 'Cookie Law'), prevede che i cookie tecnici possano essere utilizzati anche in assenza del consenso, ferma restando naturalmente l'informativa, semplificando, in tal modo, notevolmente l'attività degli operatori on-line, non più obbligati a chiedere ed ottenere il consenso preventivo.

Sulla base della recente normativa comunitaria, l'Autorità Garante, nel suo provvedimento dell'8 maggio 2014, ha avuto modo di precisare che quando l'interessato accede alla home page o ad altra pagina di sito web che usa cookie per finalità di profilazione e marketing, deve immediatamente comparire un banner ben visibile, che indichi chiaramente: l'uso dei cookies di profilazione da parte del sito, il consenso prestato dal sito all'invio di 'cookie di terze parti', ossia installati da un sito diverso, il rinvio ad un'informativa più ampia che contenga, oltre alle indicazioni sull'uso dei cookie, anche la possibilità di negare il consenso alla loro installazione, nonché l'espressa previsione che la continuazione della navigazione potrebbe avere valenza di consenso all'uso dei cookie.

All'interno dell'informativa, quindi, dev'essere indicata la possibilità per l'utente di rifiutare per default quel dispositivo, attraverso l'attivazione della opzione 'Do not track', che comporta automaticamente la dismissione della raccolta delle informazioni, o mediante la modalità di 'navigazione anonima', che consente la navigazione senza lasciar traccia nel browser dei dati di navigazione. I siti, in questo caso, non si ricorderanno dell'utente e le pagine da questo visitate non saranno memorizzate, ma non sarà, tuttavia, garantito l'anonimato in Internet, data la mera finalità perseguita, consistente nel non mantenere i dati di navigazione nel browser, che, invece, continueranno a rimanere nella disponibilità dei gestori dei siti web e dei provider di connettività.

Esistono, infine, apposite funzioni dirette all'eliminazione dei cookie senza, tuttavia, risolvere il problema, poiché ad ogni collegamento Internet la Rete provvederà a scaricarne dei nuovi, con la conseguenza che l'operazione di cancellazione dovrà essere ripetuta periodicamente.

3.8) La tecnica dello screenshot e il difficile controllo sui dati personali

Il rapporto tra l'interessato e il titolare di un social o chi, attraverso di esso, ha diffuso un'informazione senza consenso, è oggi reso ancora più complicato dall'esistenza degli screenshots, che possono conservare l'informazione e renderla accessibile attraverso i siti più diversi, anche dopo che l'autore o il provider l'abbiano cancellata dal social sul quale è stata inizialmente postata.

Una notizia, infatti, postata sulla Rete e connotata da uno specifico URL, può essere fotografata con la tecnica dello screenshot, diventando così un altro e diverso oggetto, che a sua volta può essere diffuso in Rete con un proprio URL, che nulla ha a che vedere con quello della notizia originale.

Si viene così a creare una catena quasi infinita di riproduzioni della medesima informazione originaria, ciascuna delle quali però non solo può avere nomi diversi ed essere collocata su siti differenti, ma soprattutto non è rintracciabile in Rete, anche inserendo nel motore di ricerca il nome e cognome della persona alla quale l'informazione di riferisca o che in essa è citata e coinvolta.

Per tutelare l'informazione oggetto di screenshot, consistente essenzialmente in una fotografia, a nulla vale il ricorso alla de-indicizzazione sul motore della notizia originaria, così come molto poco potrà fare la previsione di una normativa più severa perché, nelle more, quella si sarà moltiplicata e diffusa in maniera massiccia su altri e sconosciuti siti, sottratta al controllo di tutti, non solo dell'interessato.

La tecnica dello screenshot è la prova provata che tanto ciò che vogliamo cancellare, quanto ciò che vogliamo conservare, sia per motivi quantitativi che tecnici, sta ormai uscendo sempre più dalle maglie di controllo degli interessati, ma anche degli operatori della Rete, quasi come si vivesse in una Rete a trame fittissime, dalla quale i dati personali non possano più uscire[139].

[139] Lo scenario è ampiamente descritto da E. ZACCONE, *Social Media e permanenza dei contenuti*, Palermo, 2015.

CAPITOLO SECONDO

LA LIBERTA' DI INFORMAZIONE, QUALE DIRITTO FONDAMENTALE SPETTANTE ALLA COLLETTIVITA', ALLA LUCE DEL REGOLAMENTO EUROPEO 2016/679

SEZIONE I: Il nuovo Regolamento europeo sulla protezione dei dati personali: un ponte tra presente e futuro

1) Il diritto europeo all'oblio e, nella sua accezione dinamica, alla protezione dei dati personali: un work in progress

Il diritto all'oblio è, senza dubbio, una delle grandi innovazioni che il Reg. UE 2016/679 abbia codificato, consentendogli di entrare a far parte, definitivamente, all'interno del sistema normativo del diritto alla protezione dei dati personali.

Dal 1995, con l'introduzione della Direttiva madre, ad oggi, il tema del diritto all'oblio e della cancellazione dei dati personali è stato al centro di vari interventi di grandissimo impulso creativo, ad opera di Autorità giudiziarie e amministrative europee e nazionali, appartenenti ai vari Stati membri.

Va detto, tuttavia, che chi attendeva con trepidazione la costituzionalizzazione dell'istituto, all'interno di un atto normativo europeo vincolante, generale e direttamente applicabile, come il Regolamento, è rimasto non poco deluso dall'approssimazione minimalista del Legislatore europeo che, perdendo un'importante opportunità, nella previsione normativa, non ha tenuto conto di tutte quelle sfaccettature che l'istituto ha assunto nel tempo, appiattendolo fin troppo sul concetto di '*erasure*', tanto da farlo quasi coincidere, così che il diritto alla cancellazione dei dati personali e il diritto all'oblio si traducono inevitabilmente nella volontà da parte del soggetto interessato alla cessazione del trattamento relativo ai suoi dati personali, confondendosi, come in un gioco di ombre, operazione materiale e finalità[140].

[140] Come analizza G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, op. cit., 596: «*volendo meglio delineare i confini dei termini dal significato limitrofo, quali cancellazione dei dati e oblio, si può definire la cancellazione, come un'operazione sui dati, che esclude ogni conservazione degli stessi, mentre l'oblio sembra piuttosto essere una finalità che si può raggiungere con la cancellazione, ma anche con il blocco*».

D'altra parte, ma questa non vuole essere una giustificazione, l'aumento esponenziale dei dati immessi sulla piattaforma telematica dai fruitori della stessa, dei servizi offerti dalla Rete in cambio di forme massicce di immagazzinamento degli stessi, coniugati con i crescenti problemi di sicurezza, che rendono ineludibile l'accesso ai dati per fini di polizia e di prevenzione, richiedevano un intervento urgente e ormai non più differibile, diretto ad un ripensamento radicale dell'intero impianto normativo a protezione dei dati, sfociato poi, nella riforma del 2016, Regolamento UE 2016/679, rubricato "Regolamento sulla protezione dei dati" (GDPR, General Data Protection Regulation), la cui adozione ha mandato in cantiere la Direttiva madre 95/46 CE.

In verità, in un momento immediatamente precedente, il 2 febbraio 2016, l'Unione Europea e gli Stati Uniti, recependo l'orientamento sposato dalla Corte di Giustizia europea, nella sentenza del 6 ottobre 2016[141], avevano raggiunto un accordo politico, Scudo UE/USA per la Privacy, relativo alla regolamentazione dei flussi transatlantici dei dati, avente lo scopo primario di proteggere i diritti fondamentali dei cittadini europei, i cui dati erano continuamente oggetto di trasferimento negli USA, al fine di garantire la certezza del diritto per operatori e utenti della Rete. In forza dell'Accordo, le imprese che operavano negli Stati Uniti, obbligate a rispettare, in sede di trattamento, precisi parametri normativi, sanciti per meglio proteggere i dati personali dei cittadini europei, vedevano la loro azione sottoposta a poteri di controllo rafforzati ad opera del Dipartimento del Commercio degli Stati Uniti nonché della *Federal Trade Commission*, operanti in stretta collaborazione con le Autorità europee di protezione dei dati.

Interventi caratterizzati da un'affannosa rincorsa, da parte del Legislatore nazionale ed europeo, che, cercavano, per quanto possibile, di rispettare i ritmi dell'evoluzione tecnologica, per seguirne le orme e adeguarsi. Un work in progress, sia quando la sua evoluzione è stata caratterizzata da una frattura rivoluzionaria rispetto al passato, sia allorché si è delineata come frutto di una gestione ordinata del presente per preparare la sua metamorfosi da proiettare nel futuro. Questa seconda forma di cambiamento è particolarmente evidente nel settore del diritto alla protezione dei dati personali: di fronte a realtà in profondissimo e veloce cambiamento, le norme pensate anche solo poco tempo prima, rivelatesi obsolete, sono state costrette a cedere il passo a nuove forme di

[141]Corte di Giustizia dell'Unione europea (CGUE), sentenza 6 ottobre 2016, *causa C-218, 2015*.

regolamentazione più sensibili alle problematiche emergenti, con un legislatore in affanno.

La Convenzione 108/1981, le Direttive 95/46 e 2002/58, sicuramente pensate per un mondo che già conosceva le problematiche relative ai nuovi trattamenti automatizzati dei dati, non avevano, tuttavia, ancora assistito all'esplosione del web 2.0, ai trattamenti, massicci quanto invasivi, operati per fini di polizia di sicurezza, nonché alle problematiche connesse al trasferimento dei dati senza frontiere.

Il problema della sicurezza in particolare, nato all'indomani dell'11 settembre 2001, e mai cessato, da una parte, ha amplificato in maniera esponenziale l'uso della Rete per migliorare le capacità di controllo e di prevenzione da qualsiasi forma di attacco, ma, dall'altra, ha visto, per lungo tempo, la Direttiva madre, 95/46 CE, per quanto ritenuta 'utile cassetta degli attrezzi'[142], manifestare tutta la sua inadeguatezza nel gestire la difficoltà, sempre crescente, nell'assicurare un'effettiva protezione ai dati personali. Dell'immobilismo normativo, successivo alla sua emanazione, si sono a lungo avvantaggiate le multinazionali operanti nel settore della fornitura dei servizi digitali, che hanno visto moltiplicare il loro business con l'affermarsi di un web 2.0 sempre più pervasivo. La preoccupazione di offrire nuove forme di tutela ai diritti inerenti la sfera privata, seriamente minacciati dall'uso del cloud, dalla nuova realtà dei 'big data', dall'analytics, dall'IOT e da tutte le altre app, che, in cambio di servizi apparentemente gratuiti, di fatto immagazzinano e trattano dati personali, ha fatto avvertire nel legislatore europeo la necessità di un ripensamento legislativo, questa volta orientato ad alzare barriere, quanto più solide possibili, contro l'indebito uso dei dati, ivi compreso quello per finalità di polizia e sicurezza, con un occhio piuttosto attento soprattutto a quelle attività compiute al di fuori dell'UE.

Com'è facile immaginare, il percorso che ha portato all'adozione del nuovo Regolamento europeo non è stato affatto lineare, a causa dei fortissimi interessi in gioco che hanno cercato di condizionarne il cammino: da un lato, il sistema economico multinazionale spingeva ad una nuova normativa europea, coltivando la speranza di sciogliersi dai vincoli

[142] Risale al 2009 la prima grande fase di pubblica riflessione, a livello anche delle Istituzioni europee, circa la necessità di rivedere la regolazione in materia di dati personali. Così Working Party 29, *The Future of Privacy: Joint contribution to the Consultation in the European Commission on the legal framework for the fundamental right to protection of personal data,* 1° dicembre 2009 (WP n. 159). Anche conferenza organizzata dalla Commissione europea, *Personal Data: more use, more protection*, dedicata ad una consultazione pubblica sullo stato di attuazione della direttiva 9546/CE, Bruxelles, maggio 2009.

posti dalla precedente, soprattutto relativamente agli scambi dei dati tra UE e USA[143]; dall'altro, la nuova regolamentazione era vista con timore dagli stessi apparati di sicurezza, che vedevano incisa la loro opera d'azione[144].

Questo spiega il 'vivace confronto', durato ben cinque anni[145], tra i parlamentari, esponenti d'interessi confliggenti, sia in sede di Parlamento europeo che di Consiglio d'Europa.

2) Breve storia del diritto all'oblio

All'alba della nascita della nozione di oblio, quando nel panorama giuridico e sociale ancora non aveva irrotto con tutta la sua forza invasiva il web, la ricostruzione tradizionale della dottrina e della giurisprudenza si era consolidata prevalentemente su una concezione di oblio, come divieto di reiterazione della pubblicazione di una notizia, ormai datata nel tempo e per la quale l'interesse pubblico alla conoscenza era svanito[146], collegando, in tal modo, quel diritto, in stretta connessione con l'attività giornalistica e la riproposizione di fatti di cronaca, con il diritto della stampa ad informare e dei cittadini ad essere informati[147].

Questa primigenia concezione del diritto all'oblio, quale divieto di reiterazione di una notizia nel tempo, si colloca in una dimensione 'off-line', che differisce da quella 'on-line' per il ruolo che assume, all'interno della dinamica 'pubblicazione-violazione privacy', il fattore tempo[148], con la precisazione che tale concezione solo *de relato* sia

---

[143] Questo si è verificato sin dalla prima fase, legata alla consultazione di Bruxelles, di maggio 2009, organizzata dalla Commissione europea. In questo senso anche Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al comitato economico e sociale europeo ed al Comitato delle regioni*, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, Bruxelles, 4 novembre 2010.

[144] Anche la Dichiarazione n. 20, allegata al Trattato di Lisbona e specificamente riferita all'art. 16 del Trattato sul Funzionamento dell'unione europea, precisa che «*ogni qual volta le norme in materia di protezione dei dati personali, da adottare in base all'art. 16, possano avere implicazioni dirette per la sicurezza nazionale, si dovrà tener debito conto delle caratteristiche specifiche della questione*».

[145] I lavori per la redazione del Regolamento si sono infatti aperti nel 2010 e solo il 17 dicembre 2015 la Commissione ha presentato il primo testo di legge.

[146] Così: Cass. Civ., Sez. I, sentenza 18 ottobre 1984, n. 5259, in *Giur. It.*, 1985, 762 ss; Trib. Roma, sentenza 15 maggio 1995, in *Dir. Inform*., 1996, 424 ss; Trib. Roma, ordinanza 27 novembre 1996, in *Dir. Aut*., 1997. 372 ss.

[147] V. D'ANTONIO - S. VIGLIAR, *Studi di diritto della comunicazione*. *Persone, società e tecnologie dell'informazione*, Padova, 2009, 1 ss.

[148] Come ritenuto da V. D'ANTONIO, che analizza l'evoluzione storica del diritto all'oblio da una dimensione off-line ad una dimensione on-line, *Oltre la cancellazione dei dati personali: l'originaria concezione del diritto all'oblio offline, Oblio e cancellazione dei dati nel diritto europeo, in* S. SICA, V. D'ANTONIO, G.M. RICCIO, (a cura di)*, La nuova disciplina europea della Privacy,* Padova*,* 2016, 203 ss.

riconducibile al diritto alla riservatezza, in quanto non è trascurabile il fatto che *in primis* la pubblicazione della notizia era legittima, giacché relativa a fatti di cronaca di pubblico interesse che non fuoriuscivano dalla sfera di riservatezza dell'individuo e, dunque, non violavano la sua privacy.

L'oblio, secondo tale accezione, toccava il diritto alla riservatezza allorquando nell'equazione subentrava il fattore tempo: ciò perché la reiterazione della pubblicazione di una notizia, in precedenza legittimamente pubblicata, con il trascorrere del tempo, perdendo di attualità ed utilità informativa per la collettività, sarebbe andata a scalfire, violandolo, il diritto all'identità personale. Pertanto, stante la legittimità dell'originaria pubblicazione, il diritto all'oblio non coincideva con la cancellazione della notizia, ma andava ad incidere esclusivamente sulla reiterazione di quest'ultima in un arco temporale differito, senza che potesse configurarsi un'ipotesi di cessazione del trattamento.

Lo scenario muta completamente nella dimensione on-line, nella quale il fattore temporale perde del tutto la funzione discriminante tra il momento di pubblicazione della notizia e quello di riproposizione della stessa. Qui il dato temporale, infatti, risulta appiattito su di un'unica linea di contesto, quella del web, in cui non si ha più la presenza di momenti temporali separati e distinti, ma di uno spazio temporale unico e continuo, dove la notizia permane in Rete dal momento dell'upload, rendendosi consultabile da chiunque e in qualunque momento. E' chiaro che in una situazione di questo genere, in cui manca la 'riproposizione della notizia', il diritto all'oblio non possa più essere interpretato come la pretesa dell'interessato a che il fatto che lo riguardi, ormai coperto dal tempo, non sia soggetto ad ingiustificate ripubblicazioni da parte di una testata giornalistica[149].

Variato il contesto, è variata anche l'interpretazione e il contenuto di quel diritto, di modo che la tutela dell'identità personale del soggetto interessato possa essere efficacemente salvaguardata all'interno delle nuove trame delineate dalla Rete.

In questo modo la vecchia concezione del diritto all'oblio si è trasformata nella pretesa dello stesso soggetto a che il fatto che lo riguardi sia 'contestualizzato' e l'informazione

[149] Come sottolineato da G. FINOCCHIARO, *La memoria della Rete ed il diritto all'oblio,* op. cit., 593 «*In Rete la ripubblicazione non è più necessaria, dal momento che per la stessa organizzazione dell'informazione, nella rete l'informazione non è cancellata, ma permane disponibile o quantomeno astrattamente disponibile. In altri termini non si tratta solo o necessariamente di una ripubblicazione dell'informazione, quanto piuttosto della sua permanenza in Rete. Muta dunque il ruolo che gioca il temo e muta l'esigenza che si vuole soddisfare*».

relativa alla sua persona sia aggiornata, vera ed utile alla conoscenza, con un appiattimento del fattore temporale che, tuttavia, non scompare del tutto: è infatti proprio lo strumento dell'aggiornamento, obbligo posto in capo al responsabile della pubblicazione di mutare sul web ciò che è mutato nella realtà, che dà una nuova dimensione al fattore tempo.

Questa nuova accezione del diritto all'oblio, quale contestualizzazione del dato online, è stata recepita con successo, tanto dal Garante Privacy italiano, che più volte ha preteso che gli archivi dei quotidiani online fossero aggiornati[150], che dalla giurisprudenza italiana[151].

Il significato del diritto all'oblio viene ad assumere un'ulteriore sfaccettatura esegetica a seguito dell'ormai nota sentenza Google Spain, C-131/12 del 13 maggio 2014[152], ad opera dei giudici europei, emessa a seguito del ricorso presentato dal Sig. Gonzales, diretto ad ottenere il taglio dei link alla notizia relativa ad una sua vicenda personale, che comparivano su semplice digitazione dei suoi dati, dal momento che le informazioni che lo riguardavano erano relative ad una vicenda datata, ormai relegata ad un momento passato e risultavano altamente lesive per la sua immagine, non essendo i contenuti aggiornati. Un quotidiano spagnolo, La Vanguardia, infatti, aveva pubblicato un elenco di proprietà che erano state sequestrate dal dipartimento di sicurezza sociale per procedimenti correlati al recupero di crediti. Tra le proprietà elencate, c'era una piccola proprietà in Catalogna: prima dell'asta i proprietari erano Mario Costeja Gonzales e la moglie. Nel 2009 il quotidiano cominciava le pubblicazioni anche online e, da quel momento in avanti, i lettori avrebbero potuto fare gratuitamente ricerche sul sito del quotidiano sino al 1981. Gonzales, che dieci anni dopo era divorziato ed aveva onorato i suoi debiti, effettuando un banalissimo *ego search* in Google, mediante l'inserimento del proprio nome e cognome nel box del motore di ricerca, notava che uno dei primi risultati a comparire era proprio la pagina del quotidiano che annunciava una sua proprietà

[150] Si veda Garante per la protezione dei dati personali, *Doc. Web n. 2286820*, 24 gennaio 2013; *Doc. Web n. 1617673*, 8 aprile 2009; *Doc. Web n. 1583162*, 11 dicembre 2008, in *www.garanteprivacy.it*.

[151] Cass. Civ., Sez. III, sentenza 5 aprile 2012, n. 5525, in *D&G*, 2012, 5 aprile: sentenza storica in tema di aggiornamento in cui i giudici di legittimità hanno imposto alla testata giornalistica on line la necessità della contestualizzazione dell'informazione e l'obbligo del suo aggiornamento perché "*la notizia non può continuare a risultare isolatamente trattata e non contestualizzata in relazione ai successivi sviluppi, giacché altrimenti la notizia, originariamente completa e vera, non aggiornata, diviene quindi parziale e non esatta e pertanto, sostanzialmente non vera*".

[152] Corte di Giustizia dell'Unione Europea, C-131/2012 Google Spain SL, *Google Inc. vs Agencia Espanola de Protection de Datos, Mario Costeja Gonzales*.

all'asta. Gonzales iniziò a domandare al quotidiano la rimozione, ma ricevette risposta negativa e contattò Google, facendo presente che il primo risultato che lo riguardava era un'informazione non più rilevante, né tantomeno aggiornata. Dopo le due prime risposte negative, decise di rivolgersi all'Autorità garante per la protezione dei dati in Spagna, che respinse la domanda nei confronti del quotidiano, ma accolse quella diretta a Google, in qualità di intermediario: Google avrebbe avuto il dovere di rimuovere quei contenuti, in quanto non più attuali e rilevanti, essendo l'asta avvenuta dieci anni addietro e non riscuotendo, la notizia, alcun interesse attuale. Google decise allora di appellarsi all'Autorità superiore, in Spagna, che decise di rinviare la decisione alla Corte di Giustizia dell'Unione europea. Il ricorso è stato integralmente accolto dalla Corte di Giustizia europea, che ha riconosciuto, senza ombra di dubbio, come il trascorrere del tempo fosse da solo idoneo a rendere illecito un trattamento originariamente lecito. Con quella pronuncia i giudici europei hanno obbligato il gestore del motore di ricerca alla cancellazione dei collegamenti alle pagine elettroniche, su semplice digitazione dei dati del ricorrente, ritenendo in tal modo il 'diritto ad essere dimenticati' prevalente sia sul diritto all'informazione che sugli interessi economici del motore di ricerca.

I giudici europei hanno così contribuito ad aggiungere un'ulteriore sfumatura del diritto all'oblio, passando dal diritto ad essere dimenticati, alla pretesa a 'non essere trovati facilmente', tecnicamente intesa come diritto alla de-indicizzazione delle informazioni[153]. Secondo questa interpretazione, ciò che si persegue non è la totale eliminazione del dato personale dal web, quanto piuttosto un'operazione di linkaggio che vede la dissociazione del nome dell'interessato da un determinato risultato di ricerca, rendendo impossibile per il motore di ricerca ricollegare nuovamente le due informazioni, riunendole attraverso un nuovo link. Il dato conservato continuerà comunque a vivere all'interno di archivi on-line di pagine web, risultando sempre accessibile con altre e differenti chiavi di accesso, seppur con maggiori difficoltà.

In questa ulteriore specificazione il diritto all'oblio si traduce nella sottrazione al pubblico di una modalità di accesso semplificata e generalizzata ad informazioni sul proprio

[153] Sul tema si rinvia a G. RESTA-V. ZENO-ZENCOVICH, *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015 e a F. PIZZETI, *La decisione della Corte di Giustizia sul caso Google Spain: più problemi che soluzioni*, Roma, 2014.

conto[154], con la conseguenza che saranno difficilmente ipotizzabili istanze di rimozione di risultati di ricerca che vadano oltre la dissociazione di una determinata pagina del sito sorgente collegata ad un particolare nome, sino a coprire tutte le possibilità di accesso alla pagina stessa mediante differenti modalità di interrogazione del motore di ricerca[155].

A differenza delle precedenti interpretazioni di quella pretesa, che non avevano come target finale quello della cessazione del rapporto di trattamento, anzi al contrario ne era consentivano la continuazione al fine dalla concreta operabilità dell'oblio, nel caso, invece, dell'oblio inteso come 'de-indicizzazione', anche se non è prevista la cancellazione del dato, come invece richiesto dall'art. 17 del nuovo Reg. UE, la finalità è pur sempre coincidente con quella della disposizione regolamentare, ossia la cessazione del trattamento imposta al titolare/ responsabile dello stesso.

Non a caso questa concezione è quella che più si avvicina all'interpretazione datane dal Legislatore europeo, che ha appiattito il diritto all'oblio sulla concezione di 'erasure', cioè della cancellazione del dato personale da parte del titolare del trattamento, con la conseguente cessazione del trattamento stesso.

La sentenza della Corte (Grande Sezione), pertanto, ha rappresentato l'alba di un nuovo concetto di oblio, facendo entrare nel vivo il dibattito su quell'istituito. E' stato affermato, infatti, un diritto all'oblio dai confini differenti da quelli fino ad allora teorizzati dalla giurisprudenza italiana, strettamente legato al diritto all'autodeterminazione informativa, che ha visto i motori di ricerca divenire attori principali del processo di de-indicizzazione, preceduto in ogni caso da un'operazione di bilanciamento tra la pretesa ad essere dimenticati e quella contraria al permanere dei dati nei canali del web.

Non è, d'altra parte, la prima occasione in cui la Corte di Giustizia ha dovuto affrontare problematiche riguardanti il bilanciamento tra tutela dei diritti fondamentali ed accertamento e prevenzione di attività illecite e reati. In alcuni precedenti, la Corte[156] ha valorizzato i diritti previsti dagli articoli 8 e 11 della Carta dei Diritti Fondamentali dell'Unione Europea, oltre alla libertà di impresa, ai sensi dell'art. 16, per garantire la

---

[154] Così V. D'ANTONIO, *Il diritto all'oblio on line come diritto alla de-indicizzazione del dato. Oblio e cancellazione dei dati nel diritto europeo*, in S. SICA - V. D'ANTONIO - G.M. RICCIO (a cura di), *La Nuova Disciplina Europea della Privacy*, Milano, 2016, 212 ss.

[155] Si veda inoltre S. SICA- V. D'ANTONIO, *La procedura di de-indicizzazione*, in *Dir. Inform.*, 2014, fasc. 4-5

[156] La Corte di Giustizia dell'Unione Europea, sentenza 24 novembre 2011 (*C-70/10*) e sentenza 16 febbraio 2012 (*C-360/10*), nonché in termini parzialmente diversi, Corte di Giustizia dell'Unione Europea, sentenza 27 marzo 2014 (*C-314/12*).

loro prevalenza nel bilanciamento con le esigenze di tutela della proprietà intellettuale in Internet, le cui violazioni costituiscono, in molti Stati, un illecito penale[157].

Questa volta al centro della questione è stata la configurabilità del diritto all'oblio inteso in una particolare accezione: ottenere direttamente da un motore di ricerca la cancellazione, dai risultati generati dal sistema, dei collegamenti a notizie relative a circostanze dalle quali un soggetto si è nel tempo allontanato.

3) Il diritto all'oblio

L'evoluzione rapida e profonda dell'istituto ha fatto sì che dello stesso non possa essere fornita una definizione univoca, così come non è semplice affermare che l'oblio, fino a qualche tempo fa, abbia potuto rappresentare realmente un diritto, nonostante già dal 2004 l'Autorità Garante italiana[158], allora presieduta da Stefano Rodotà, si sia occupata proprio di questo argomento, adottando un provvedimento ben articolato e motivato. Il ricorrente, in quell'occasione, aveva lamentato la pubblicazione di un provvedimento amministrativo obsoleto, relativo alla sua persona, sul sito dell'Autorità garante, che avrebbe arrecato grave pregiudizio alla sua sfera privata e professionale. Utilizzando, infatti, un normale motore di ricerca, la decisione dell'Autorità sarebbe stata costantemente affiancata al nome del ricorrente ed, avendo, questa modalità di pubblicazione, un carattere pressoché perpetuo, avrebbe potuto provocare conseguenze ben più gravi della pubblicazione a mezzo stampa, che pure costituiva una precisa sanzione accessoria, limitata però nel tempo. Istanza avversata da controparte, sul presupposto che la pubblicazione dei provvedimenti era mera ottemperanza ad un obbligo di legge.

Il problema dei dati personali, captati dai canali del web e destinati alla reperibilità eterna, è di gran lunga precedente alla pronuncia della Corte di Giustizia europea, la C-131/2014: quest'ultima, infatti, ha solo espressamente riconosciuto alcuni diritti all'interessato,

---

[157] Cercando di sintetizzare, in due casi (*C-70/10* e *C-360/10*), la Corte ha affermato che il giudice nazionale non può imporre ad un service provider l'adozione di specifici sistemi di filtro per impedire agli utenti di usare tecnologie di file sharing in violazione delle norme in materia di diritto d'autore. Un sistema di filtraggio attivo e preventivo, senza limiti di tempo, a totale carico economico del provider richiederebbe un controllo sistematico ed attivo sulla totalità delle comunicazioni elettroniche e, indistintamente, sugli utenti che si avvalgono del servizio, indipendentemente dalla natura dei contenuti trasmessi. Sul rapporto tra libertà in Rete ed operazioni di monitoraggio del Web, finalizzate alla repressione di possibili reati, si rinvia all'analisi di R. FLOR, *Tutela penale ed autotutela tecnologica dei diritti d'autore nell'epoca di Internet*, Cedam, Padova, 2010.

[158] Garante per la protezione dei dati personali, *Doc. Web n. 141911*, 10 novembre 2004

titolare dei dati personali trattati, a tutela della sua sfera privata, in assenza di "un interesse pubblico che giustifichi la violazione di quell'aspetto della dignità/riservatezza, definito 'diritto all'oblio[159]". In tal modo si è espressa la Suprema Corte di recente, richiamando l'impostazione classica, che tende a collocare il diritto entro i confini di concetti noti ed affermati, come la dignità e la riservatezza e, più in generale, nell'alveo dei diritti della personalità, dovendosi riconoscere all'individuo la possibilità di cambiare, trasformarsi e crescere, lasciandosi alle spalle un passato, a volte anche pesante[160].

Ed in questi termini è anche un segno di civiltà, espressione della funzione rieducativa della pena, di cui all'art. 27, comma 3, Cost., volta non solo a punire il condannato, ma anche a favorirne il reinserimento sociale e la sua restituzione alla società civile.

E' certamente difficile accettare l'idea di una rieducazione in assenza del silenzio della memoria: se nella società rimanesse ben saldo il ricordo di quanto commesso dal condannato e se questo fosse rinsaldato proprio dalla permanenza in Rete dell'informazione o dalla ripubblicazione, a distanza di tempo, della notizia, di sicuro verrebbe ad essere annientata la funzione rieducativa della pena e non si favorirebbe il reinserimento del reo nella comunità sociale, dalla quale si era estraniato, attraverso la pedagogica correzione della sua antisocialità e l'adeguamento del suo comportamento alle regole giuridiche e sociali.

E' un diritto particolarmente fluido, dinamico e in continua evoluzione[161]; così è stato, infatti, negli anni, potendosi riassumere, nell'espressione, più significati: la pretesa, del soggetto interessato, alla cancellazione dei propri dati (e di 'diritto alla cancellazione' parla il nuovo Regolamento europeo in tema di dati personali) nonché, da un'altra angolazione, il desiderio, espresso da un soggetto, di non vedere riproposte notizie attinenti al suo passato ormai superate[162] ed in grado di arrecargli pregiudizio[163].

---

[159] Cass. Pen., Sez I, 8 gennaio 2015, n. 13941, in *Ced. Cass*., 2015.

[160] Così anche per L. RATTIN, *Il diritto all'oblio*, in *Arch. Civ*, 2000, 1069.

[161] In particolare, sul punto si rinvia a G. FINOCCHIARO, *La memoria della Rete ed il diritto all'oblio*, op. cit., 392; F. DI CIOMMO- R. PARDOLESI, *Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. E' la rete, bellezza!*, in *Danno e resp*., 2012, fascicolo 7, 703.

[162] G. MARCHETTI, *Diritto di cronaca online diritto all'oblio*, in *AA.VV*., *Da internet ai social network*, Rimini, 2013, 71.

[163] Un'attenta voce ha ritenuto che il diritto all'oblio può essere indicato come "*il diritto a non essere esposti a tempo indeterminato ai pregiudizi che può comportare la reiterata pubblicazione di una notizia; si tratta del diritto a non vedere più associato il proprio nome a vicende che, pur avendo avuto una rilevanza pubblicistica in un certo momento, si ritiene non ne abbiano più per essere trascorso un lasso di tempo significativo dalla relativa divulgazione, tale da far ritenere che l'interesse alla conoscenza della notizia sia venuto meno*" (L. CAPUTO, *Il diritto all'oblio, Dylan Dog e il desiderio di dimenticare,* in

Dalla giurisprudenza, e nemmeno tanto obsoleta, il diritto all'oblio è stato trattato come un istituto strettamente connesso al diritto alla riservatezza, tanto da esserne considerato una sua declinazione. Allocare, tuttavia, l'istituto nell'alveo della riservatezza non può che essere riduttivo: il diritto all'oblio non è una costola della disciplina della privacy ma, rientrandovi la pretesa alla tutela dei dati personali[164], sarebbe più corretto considerarlo come estrinsecazione dei diritti della persona, in particolare come risposta alla necessità di porre un freno al diritto alla libertà di pensiero e d'informazione, laddove queste, senza arrecare alcuna utilità informativa alla collettività, si rivelassero lesive, adombrando ingiustamente l'identità dell'individuo. E', infatti, utile precisare che il diritto all'informazione debba essere considerato sovrano e che, solo in presenza di alcune condizioni (una notizia obsoleta o di scarso interesse pubblico o ancora, non aggiornata), la pretesa alla de-indicizzazione o cancellazione dei dati dovrà essere oggetto di bilanciamento con il diritto di cronaca e con l'interesse pubblico alla conoscenza delle informazioni acquisibili attraverso la Rete.

Il diritto all'oblio, al più, in quanto strettamente legato al controllo dei propri dati, potrebbe rappresentare una declinazione del 'diritto all'autodeterminazione informativa', recuperando un'impostazione tradizionale relativa ai diritti del soggetto all'onore e soprattutto alla reputazione[165]: in effetti, come chiarito dalla Suprema Corte nel 2012[166], "il diritto all'oblio, pur apparendo legato alla nozione di riservatezza, salvaguarda la proiezione sociale dell'identità personale, l'esigenza del soggetto di essere tutelato dalla divulgazione d'informazioni potenzialmente lesive, in ragione della perdita di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della sua personalità". Il tutto naturalmente in una logica di bilanciamento tra il diritto del soggetto a fornire un'immagine sociale il più possibile compatibile con la propria percezione del sé e il diritto della collettività di conoscere eventi d'interesse pubblico.

In forza di queste premesse, la giurisprudenza nazionale ha tendenzialmente riportato il diritto ad essere dimenticati entro i confini dell'ampia disciplina della protezione dei dati personali che impone il corretto uso degli stessi in sede di trattamento, sino a legittimarne

---

Iurisprudentia.it). Tale diritto, secondo l'Autore, costituisce una sorta di rovescio della medaglia dell'interesse pubblico all'informazione.

[164] Si veda G. SCIULLI, *Il diritto all'oblio e l'identità digitale*, *Narcissus*, Milano 2014.

[165] Così, A. DE CUPIS, *Condizioni morali e tutela dell'onore*, in *Foro Pad.*, 1960, Vol. I., 677.

[166] Cass. Civ., Sez III, sentenza 5 aprile 2012, n. 5525, cit.

la richiesta di cancellazione qualora quei dati non fossero più attuali, risultando quindi lesivi dell'identità.

3.1) Il 'diritto all'oblio nelle pronunce dei giudici nazionali, successivamente alla 'Google Spain'

La sentenza della Corte di Giustizia dell'Unione europea, C-131/12 del 13 maggio 2014, che, nell'operazione di bilanciamento tra l'istanza del ricorrente alla de-indicizzazione dei dati che comparivano su digitazione del suo nome e cognome e il diritto alla conoscenza di quei dati, ha ritenuto la prevalenza della prima rispetto all'interesse economico del motore di ricerca ed all'interesse pubblico ad accedere a quelle informazioni, costituisce tutt'oggi uno spartiacque nel panorama giuridico, non solo europeo, riferimento imprescindibile, qualora ricorrano i presupposti delineati dai giudici europei, per i giudici nazionali.

Così è stato, sia pure con alterne vicende!

Poco dopo la pubblicazione della sentenza della CGUE, un interessato si è rivolto al Tribunale di Roma[167] per vedersi accolta la sua richiesta di 'oblio' nei confronti di un motore di ricerca. I giudici aditi, pur avendo seguito l'orientamento della Corte di Giustizia nel riconoscere il diritto del soggetto a non rimanere indeterminatamente esposto ad una rappresentazione non più attuale della propria persona, a causa della presenza in Rete di notizie liberamente accessibili a chiunque e, dopo un'approfondita disamina della situazione, sono giunti alla conclusione opposta, ossia di non accogliere la richiesta dell'istante. Nell'operazione di bilanciamento, infatti, essendo ancora la notizia di pubblico dominio ed avendo un valore attuale, in quanto il caso giudiziario che vedeva coinvolto l'interessato non si era concluso, è risultato prevalente l'interesse alla conoscenza dell'informazione da parte della collettività.

Decisione differente è stata di recente assunta dal Tribunale di Milano[168], che ha "riconosciuto il diritto dell'interessato di rivolgersi al gestore del motore di ricerca al fine di ottenere la rimozione dei risultati ottenuti inserendo, come criterio d'indagine, il nome del soggetto cui si riferiscono le informazioni, quando le stesse risultino inadeguate, non

[167] Trib. Civ. Roma, sentenza 3 dicembre 2015, n. 23771.
[168] Trib. Milano, Sez I, sentenza 4 gennaio 2017, n. 12623.

pertinenti o non più pertinenti ovvero eccessive, in rapporto alle finalità per le quali sono state trattate e al tempo trascorso".

Orientamento ribadito dai giudici di legittimità[169], i quali hanno affermato che "l'illecito protrarsi del trattamento dati giustifica l'accoglimento della pretesa risarcitoria quando – secondo una valutazione bilanciata del diritto di cronaca e del diritto all'oblio – il mantenimento del diretto ed agevole accesso sul web alla risalente notizia di cronaca esorbita dal fine del lecito trattamento di archiviazione online, ledendo i diritti all'identità ed alla reputazione dell'interessato".

Ancora la Suprema Corte[170], accogliendo in parte il ricorso del cantautore romano Antonello Venditti contro Rai 1, per la messa in onda, 13 anni fa, di un servizio da parte della trasmissione 'La vita in diretta', senza il suo consenso, offensivo e denigratorio per le affermazioni a commento, gli ha riconosciuto il diritto a che i suoi dati non fossero più oggetto di trattamento, con la precisazione che in tema di riservatezza, dal quadro normativo e giurisprudenziale nazionale ed europeo, si ricava che il diritto all'oblio può subire una compressione in favore dell'ugualmente fondamentale diritto di cronaca, solo in presenza di taluni presupposti, tra i quali verrebbe ad emergere l'interesse pubblico alla conoscenza della notizia, e non la mera diffusione della stessa per ragioni divulgative o, ancor peggio, commerciali, come individuate dai giudici nel caso loro sottoposto.

Pronunce giudiziali assai distanti tra loro, nonostante i presupposti invocati dai ricorrenti fossero gli stessi e, ciò che è ancor più grave, pronunce opposte, relative allo stesso caso giudiziario, destinate a ripetersi nel tempo, anche a causa dell'assenza di criteri precisi ed oggettivi, uniformemente validi per tutti. Le leggi europee e nazionali che si sono susseguite, ivi compreso il recente Regolamento UE, pur avendo individuato la soluzione nella tecnica del bilanciamento laddove si fosse profilata un'ipotesi di conflitto tra il diritto ad essere dimenticati e l'antagonista diritto all'informazione, si sono ben guardate dall'indicare modalità e/o parametri in forza dei quali operare la tecnica risolutrice, perdendo un'utile occasione per perimetrare la discrezionalità dei motori di ricerca, che avessero voluto tagliare in maniera generosa, e dei giudici successivamente chiamati a decidere, anche per limitare il rischio di pronunce tra loro confliggenti, seppur relative allo stesso caso giudiziario.

---

[169] Cass. Civ., Sez. I, sentenza 24 giugno 2016, n.13161, in *www.ridare.it,*19 ottobre 2016 con nota di D. BIANCHI.

[170] Cass. Civ., ordinanza 20 marzo 2018, n. 6919.

4) Il diritto all'oblio e la tutela dei diritti fondamentali della persona nel Regolamento europeo 2016/679

Con il nuovo Regolamento, adottato il 27 aprile 2016 ed in vigore dal 25 maggio 2018[171], il Legislatore dell'Unione ha codificato il diritto all'oblio, rafforzando, nel contempo, il diritto alla protezione dei dati personali, entro e fuori i confini dell'Unione europea, con l'indubbio pregio, stante l'uso dello strumento regolamentare, di agevolare il processo di armonizzazione delle varie legislazioni nazionali sulla protezione dei dati.

L'intento primario del Legislatore comunitario, elemento di novità rispetto alla precedente normativa europea, è stato quello di regolamentare il 'diritto di stabilimento', (tema particolarmente caro alla Corte di Giustizia Europea, affrontato nella CGUE 131/2014), prescrivendo la vigenza della nuova normativa per tutte le imprese aventi la loro sede nell'UE e per quelle situate fuori dall'UE che, tuttavia, gestiscano i dati dei residenti nell'Unione europea o offrano servizi o prodotti a persone che si trovano nel territorio dell'Unione europea[172].

Da un punto di vista oggettivo, il 'nuovo corpus', nel definire i limiti al trattamento automatizzato dei dati personali e nel porre le basi per l'esercizio di nuovi diritti, ha previsto criteri rigorosi in materia d'informativa e trasferimento dei dati al di fuori dell'UE. La previsione di un obbligo dell'informativa, quale strumento di trasparenza, impone che gli interessati debbano essere a conoscenza della circolazione dei loro dati, dell'eventuale loro trasmissione al di fuori dell'UE e delle relative garanzie, così come debbano avere consapevolezza del diritto di poter revocare il consenso, relativamente a

---

[171] L'art. 99 del Reg. 2016/679 stabilisce che esso entrerà in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale dell'UE e al secondo paragrafo, sancisce che si applicherà a decorrere dal 25 maggio 2018 realizzando, in tal modo, una scissione temporale, uno *spatium deliberandi* tra validità ed efficacia del corpo normativo, finalizzata a garantire a tutti i soggetti obbligati (enti pubblici e privati, associazioni, imprese e liberi professionisti), un tempo congruo per riprogrammare e riorganizzare le loro attività in maniera conforme alle nuove previsioni.

[172] E' questo un elemento di novità rispetto alla Direttiva madre: per questa vincolati alle norme ivi contenute erano il titolare e il responsabile del trattamento, stabiliti nel territorio di uno Stato membro o, se aventi stabilimento fuori dall'UE, qualora avessero fatto ricorso a strumenti presenti in uno Stato UE. Era richiesto quindi, un aggancio oggettivo al luogo (intra/extra UE) per l'applicazione del diritto interno di uno Stato europeo. Con il Regolamento si 'apre la porta' all'applicazione del diritto interno di uno Stato europeo ai trattamenti eseguiti al di fuori dell'UE per cui s'interviene anche laddove i responsabili dei trattamenti siano stabiliti extra UE ma si rivolgano ad interessati comunitari. Il parametro oggettivo del 'principio di stabilimento' è altresì integrato da parametri soggettivi oggettivantesi nell'appartenenza all'UE del titolare/responsabile o degli interessati, con un conseguente ampliamento dell'ambito di applicazione territoriale della nuova legislazione europea, la cui ratio sembra puntare ad una tutela che non lasci vuoti di copertura.

determinati trattamenti. Quanto al 'trasferimento dei dati', il Regolamento ha introdotto il diritto alla 'portabilità' dei propri dati personali, ossia la possibilità di poterli trasferire da un titolare del trattamento ad un altro (ad eccezione di quelli contenuti in archivi pubblici) o di cambiare il provider, senza perdere i contatti ed i messaggi salvati. Il trasferimento dei dati al di fuori dell'Unione europea è stato sottoposto a limiti più stringenti, essendo stato imposto il divieto di trasferimento di dati personali verso Paesi situati al di fuori dell'UE o verso Organizzazioni internazionali che non rispondano agli standard minimi di tutela e sicurezza: i dati potranno essere trasferiti solo con il consenso espresso dell'interessato, a meno che non ricorrano particolari condizioni, quali il rispetto di obblighi contrattuali o motivi d'interesse pubblico o giudiziario.

Sempre nell'ottica d'incrementare le forme di protezione della sfera privata dell'individuo, il Legislatore comunitario ha posto numerosi obblighi in capo al titolare/responsabile del trattamento, come quelli, a titolo meramente esemplificativo, di comunicare eventuali violazioni dei dati personali (data breach) all'Autorità di protezione degli stessi e, nell'ipotesi in cui la violazione dovesse rappresentare una minaccia per i diritti e le libertà, il dovere d'informare, senza indugio, i diretti interessati, indicando le eventuali soluzioni per limitarne i danni; di assolvere all'obbligo dell'informativa da sottoporre all'interessato, il cui adempimento potrebbe comportare uno sforzo, e non solo economico, sproporzionato; di assumere e di provare l'adozione di idonee misure di sicurezza a protezione dei dati, la cui presenza dev'essere garantita fin dalla fase dell'ideazione e progettazione del trattamento, effettuando, se del caso, 'valutazioni d'impatto' prima di procedervi, qualora lo stesso presenti rischi elevati per le persone e consultando, in ultima analisi, l'Autorità di protezione'[173].

Il Legislatore regolamentare ha, tra gli altri, espressamente riconosciuto il 'diritto all'oblio', azionando il quale, gli interessati potranno ottenere la cancellazione dei propri dati personali, da parte dei soggetti attivi del trattamento, ricorrendo le condizioni ivi prescritte ed in assenza di altre situazioni giuridiche espressamente indicate nel lavoro legislativo, che riconoscono la prevalenza del diritto alla conservazione dei dati.

---

[173] S. BONGIOVANNI- C. MOTTINO, *Il vademecum sul Regolamento europeo 2016/679*, Frosinone, 2017, 66. Nel confronto con il Codice, nel Regolamento emerge che la tutela dei diritti dell'interessato, che pure occupa un posto di assoluto rilievo, per certi aspetti sembra essere strumentale rispetto all'obbiettivo principale che pare più quello d'impedire o porre fine a trattamenti illeciti o illegittimi, che quello di proteggere prima di tutto i dati e i connessi diritti dell'interessato.

Nuove, rispetto alle abrogate normative, ed efficaci, sono le sanzioni amministrative e pecuniarie, a carico dei responsabili, per la mancata osservanza della normativa regolamentare che, nei casi di acclarata e reiterata inadempienza, potranno raggiungere tetti piuttosto elevati.

4.1) Lo strumento del Regolamento al posto della Direttiva: obbligatorietà della normativa senza oneri di recepimento

Spinto dalla necessità di assicurare una maggiore uniformità normativa, armonizzazione e, per alcuni versi, anche chiarezza, il Legislatore europeo, al posto della Direttiva, è ricorso all'uso dello strumento del Regolamento, obbligatorio in tutti i suoi elementi, le cui norme producono effetti vincolanti nei confronti di tutti coloro che, autorità pubbliche o soggetti privati, siano obbligati al rispetto del diritto dell'Unione.

Il Regolamento è legge dello Stato a tutti gli effetti, per di più con la forza sovraordinata, che gli deriva dall'essere disciplina uniforme dell'Unione europea.

Questo significa che uno Stato membro non può adottare unilateralmente provvedimenti interni volti a limitare l'applicazione delle norme regolamentari, né può farne applicazione selettiva. Le disposizioni contenute nel Regolamento, infatti, entrano in vigore e cominciano a produrre immediatamente i loro effetti giuridici, senza necessità di forme d'intermediazione legislativa e misure di recepimento all'interno degli Ordinamenti giuridici interni, da parte degli Stati membri, vincolandoli al rispetto delle finalità in esso contenute.

E' d'altra parte evidente, tuttavia, che molte disposizioni, per il modo in cui sono state elaborate, prestino il fianco ad interpretazioni differenti ed altre, a causa dell'astrattezza con cui sono state formulate, si prestino ad essere più affermazioni di principio, che dettato normativo.

Alcune norme, per il modo in cui sono state scritte, appaiono addirittura più limitative delle corrispondenti contenute nella Direttiva madre, cosicché le forme di tutela che intendono assicurare sembrano indebolite[174], altre presentano poca chiarezza e forme di disallineamento: il caso che immediatamente salta agli occhi è contenuto nei paragrafi 1

[174] Si pensi all'art. 2, comma 1, che pare restringere molto il campo di applicazione del Regolamento. La Direttiva invece, all'art. 3 paragrafo 1, prevedeva che le disposizioni in essa contenute dovessero trovare applicazione per i trattamenti interamente o parzialmente automatizzati – e fin qui la coincidenza con la direttiva è perfetta - nonché ai trattamenti non automatizzati di dati personali contenuti o destinati a figurare in archivi, tutela, quest'ultima, che sembra essere esclusa nel nuovo Regolamento.

e 2 dell'art. 1, entrambi aventi ad oggetto la protezione dei dati personali, con la differenza che mentre il paragrafo 1 mette al centro la protezione dei dati personali fine a se stessa e le regole sulla loro circolazione, il successivo, per alcuni aspetti ripetizione del contenuto del par. 1, art. 1 della Direttiva – madre, sembra privilegiare la tutela dei diritti e delle libertà fondamentali, sebbene con la precisazione che "tale finalità è pur sempre con riferimento alla protezione dei dati[175]".

Il nuovo Regolamento, pertanto, se da un lato risente in maniera grave del peso della Direttiva 95/46, tanto da averne riprodotto al suo interno alcune norme, dall'altro ne rappresenta il rovesciamento[176], soprattutto per la terminologia adoperata: sintetica e compatta, quella della Direttiva, dettagliata ed estremamente particolareggiata, quella adoperata dal Legislatore regolamentare. Anche nell'enucleare i principi relativi al trattamento dei dati, il legislatore europeo, in numerose norme (relative al consenso, ivi compreso quello espresso per conto dei minori da chi ne fa le veci, ai dati sensibili, alle attività di polizia e sicurezza), in maniera quasi maniacale, si è soffermato a definire principi e concetti in maniera estremamente dettagliata, con consequenziali irrigidimento del testo normativo e problemi interpretativi. Se da una parte, pertanto, la vocazione al dettaglio è stata una precisa scelta diretta, attraverso definizioni puntuali, a dare una risposta chiara, evitando le problematiche nelle quali era incorsa la precedente esperienza normativa, dall'altra, la pregevole ricerca di precisione e dettaglio ha ingessato le norme, impedendo, nella fase della loro interpretazione, quell'elasticità che la Direttiva ha dimostrato di avere, manifestandosi all'altezza, anche a distanza di anni dalla sua entrata in vigore, di fornire soluzioni a vicende e problematiche via via più poderose.

---

[175] Il comma 1 dell'art. 1 della Direttiva 45/96 recita: "*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*".

[176] Si veda, ad esempio, quanto dispongono l'art. 1, paragrafo 3 del Regolamento e l'art. 1, paragrafo 2 della Direttiva. Pare proprio che l'uno sia la ripetizione dell'altro, anche se, in realtà, una differenza esiste: nel Regolamento la libertà di circolazione dei dati non può essere limitata "with regard to the processing of personal data", cosicché al centro del divieto di limite è il trattamento. Diversamente, invece, il comma 2 dell'art. 1 della Direttiva afferma che la libertà di circolazione dei dati non può essere limitata per ragioni relative alla loro tutela, così come garantita al paragrafo precedente. Dunque, al centro della norma della Direttiva sta il divieto a che la tutela (e non il trattamento) dei dati sia assunta come un limite alla loro circolazione. La differenza si spiega agevolmente: la Direttiva è una normativa di armonizzazione, che ha l'intento di evitare che leggi nazionali, relative a forme diverse di tutela di dati personali, possano essere di ostacolo alla libera circolazione dei dati. Il Regolamento, invece, essendo applicabile direttamente, non ha più ragione di evitare discrepanze tra le leggi nazionali, mettendo al centro della sua attenzione il divieto di limitare la libertà di circolazione dei dati, ma può, come infatti fa, mettere al centro della sua regolazione, i trattamenti.

4.2) Il nuovo Regolamento e il suo impatto sulle normative nazionali degli Stati membri

L'art. 189 del Trattato Istitutivo della Comunità europea, qualificando il Regolamento come un "atto di portata generale, obbligatorio in tutti i suoi elementi e direttamente applicabile in tutti gli Stati membri", non richiede, per la sua applicazione, un atto di recepimento negli ordinamenti interni dei singoli Stati, ad opera dei Legislatori nazionali e, dato il primato del diritto comunitario su quello interno, il giudice nazionale sarà tenuto a disapplicare la norma statale, confliggente con quella comunitaria, a prescindere dal fatto che sia anteriore o successiva a quella. Le modifiche all'acquis communautaire sono, pertanto, dotate di un impatto diretto negli ordinamenti degli Stati membri, fatti salvi margini di flessibilità, per le legislazioni nazionali, su specifiche disposizioni di attuazione, per cui, mentre la Direttiva è stata completamente travolta dal nuovo lavoro legislativo europeo[177], le norme contenute nel Codice della Privacy nazionale, il D. Lgs. 196/2003, non avendo il Regolamento la forza d'inciderle, travolgendole, gli sopravviveranno, anche se dovranno essere disapplicate, dai giudici nazionali, nel rendere giustizia al caso concreto, qualora in contrasto con le previsioni regolamentari sulla protezione dei dati personali.

Nelle more, lo *spatium deliberandi* di due anni perché la nuova normativa fosse applicabile, secondo l'intenzione del legislatore, sarebbe stato utile alle Autorità per attrezzarsi, governando la transizione ed una non sempre pacifica convivenza del nuovo lavoro con la normativa interna, anche se la soluzione al problema è stata quella di auspicare, *rectius* sollecitare, l'intervento del Legislatore nazionale, eliminando ogni problema o equivoco derivante dal rapporto non sempre compatibile tra disciplina comunitaria e nazionale[178].

[177] Il travolgimento ha riguardato non solo la Direttiva madre, ma anche le successive Dir. 2002/58 e 2009/136 CE. Nella disposizione finale del Regolamento, infatti, si legge a far data da maggio 2018, le norme contenute nella Direttiva madre risulteranno abrogate e i riferimenti alla Direttiva s'intenderanno come riferimenti al Regolamento stesso.

[178] Voci contrarie, P. MARINI, *Web and Tech Privacy,* 5 maggio 2016, secondo il quale non sono pochi i rischi che una nuova legge, nel nostro Ordinamento comporterebbe, data la scadentissima tecnica legislativa che spesso complica quello che dovrebbe semplificare.

4.3) Il rovesciamento di prospettiva tra Direttiva e Regolamento: da un apparato normativo incentrato sui diritti dell'interessato al suo opposto fondato sui doveri del titolare/responsabile

Con l'entrata in vigore del Regolamento sulla protezione dei dati personali, le aziende dell'informazione online hanno subito una vera e propria svolta culturale in materia di privacy: dal vecchio concetto di privacy si passa a quello di 'data protection risk based', fatto di processi. L'obiettivo della nuova normativa europea non è stato tanto quello di aggiornare i contenuti della vecchia Direttiva 95/46, quanto stravolgerne completamente il significato, passando da una 'data protection one size fits all', fatta di policy, ad una 'data protection risk based', fatta di processi. Tale previsione comporta che le aziende oggi devono prestare particolare attenzione all'analisi dei trattamenti, valutare in anticipo l'impatto che potrebbero avere sulla privacy, identificare i rischi e le relative contromisure, quantomeno per mitigarli.

Con la grande novità che queste norme, molto più stringenti rispetto alle precedenti, si applicheranno non solo alle aziende nazionali ma anche a tutte quelle che, pur avendo sede negli USA o in altri Paesi extraeuropei, trattino dati di cittadini appartenenti all'UE, come del resto avevano stabilito i giudici europei nella 131/2012.

Il regolamento, pertanto, ha rovesciato la prospettiva della direttiva laddove ha prestato molta più attenzione agli obblighi e alle misure di sicurezza imposte ai soggetti attivi del trattamento, controller e processor, al fine di garantire una tutela effettiva della sfera privata degli interessati. Sia da un punto di vista quantitativo che qualitativo, infatti, le norme sui doveri del controller e del processor sono molto più numerose rispetto al passato: mentre la Direttiva 95/46 CE vi dedicava solo gli articoli 16 e 17[179], il

[179] Direttiva 95/46 CE, articolo 16: Riservatezza dei trattamenti
«L'incaricato del trattamento o chiunque agisca sotto la sua autorità o sotto quella del responsabile del trattamento non deve elaborare i dati personali ai quali ha accesso, se non dietro istruzione del responsabile del trattamento oppure in virtù di obblighi legali».
Articolo 17: Sicurezza dei trattamenti
«1. Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali.
Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere.
2. Gli Stati membri dispongono che il responsabile del trattamento, quando quest'ultimo sia eseguito per suo conto, deve scegliere un incaricato del trattamento che presenti garanzie sufficienti in merito alle

Regolamento dedica ben quattro delle cinque sezioni del Capitolo IV alla definizione degli obblighi delle due figure giuridiche, sancendo in modo estremamente dettagliato i criteri da osservare nella valutazione, i doveri in materia di data protection impact assessment e di prior consultation, limitando fortemente la loro sovranità nell'attività di trattamento dati, onde ridurre fortemente i rischi di attività illecite ed assicurare un elevato livello di sicurezza nel trattamento dei dati, anche al fine di garantire una solida credibilità dei titolari/responsabili nei confronti degli utenti.

Sempre nella stessa ottica, e difformemente dalla Direttiva, il Regolamento ha dato vita ad una figura nuova nel diritto europeo di protezione dei dati, quella del 'Data Protection Officer', figura obbligatoria, preposta a garantire la liceità dei trattamenti, per uffici ed enti pubblici, mentre per i privati solo qualora siano presenti alcune condizioni-presupposto di cui all'art. 35 GDPR 2016/679. Figura autonoma e indipendente sia nei confronti del titolare/responsabile, che della struttura tutta, dotato di autonomi mezzi, ma anche responsabile di eventuali illegittimità dei trattamenti operati e referente unico delle autorità di controllo.

Il regolamento, pertanto, ha notevolmente elevato il livello di protezione dei dati trattati, moltiplicando gli oneri, le responsabilità e le sanzioni a carico delle aziende operanti nel settore dell'informazione online, facendo emergere forti conflitti soprattutto da parte dei colossi dell'informazione abituati a realtà giuridiche molto più flessibili e più garantiste del diritto all'informazione.

4.4) Forme di tensione USA – UE: le reazioni alla proposta del Regolamento europeo

Il rafforzamento delle tutele giuridiche offerte ai cittadini europei nella gestione dei dati ha comportato la nascita di un vivace dibattito sui possibili conflitti tra il nuovo diritto all'oblio e la speculare pretesa all'informazione. Il problema si è posto in particolare nei

---

misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare e deve assicurarsi del rispetto di tali misure.

3. L'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente:

- che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento;

- che gli obblighi di cui al paragrafo 1, quali sono definiti dalla legislazione dello Stato membro nel quale è stabilito l'incaricato del trattamento, vincolino anche quest'ultimo.

4. A fini di conservazione delle prove, gli elementi del contratto o dell'atto giuridico relativi alla protezione dei dati e i requisiti concernenti le misure di cui al paragrafo 1 sono stipulati per iscritto o in altra forma equivalente».

rapporti dell'Unione europea con gli USA per la forte asimmetria giuridica tra l'Ordinamento statunitense, improntato alla prevalenza del diritto all'informazione, riconosciuto come fondamentale già nel First Emendament della Carta costituzionale statunitense, e quello europeo, improntato ad un maggior rigore, che porta a tutele effettive del diritto alla protezione dei dati.

Il punto di massima tensione è sicuramente rappresentato dall'articolato relativo alla "raccolta, trattamento e uso delle informazioni relative agli utenti" da parte dei fornitori dei servizi, ossia il modo in cui debbono essere raccolti e trattati i dati e il grado d'informazione e consenso assicurato agli utenti circa il loro uso[180].

Il tema assume un rilievo particolare perché i dati oggi rappresentano il 'nuovo petrolio', la vera remunerazione di chi fornisce servizi online, solo apparentemente gratuiti, ma di fatto retribuiti con pezzi di privacy, trattati e manipolati dalle multinazionali per trarre informazioni da informazioni, per operare profilazioni di massa finalizzate ad orientare gli utenti nelle loro scelte, con guadagni rilevanti. E le aziende di profilazione, le multinazionali, sono tutte, guarda caso, d'oltreoceano.

Di fronte a questo scenario è evidente che l'imposizione alle aziende USA di regole europee assai più stringenti e rispettose del profilo privato dell'individuo, in materia di raccolta e trattamento dati, rispetto a quelle statunitensi, propense a sacrificarlo in nome del business che ruota intorno al traffico delle informazioni, ha prodotto effetti dirompenti, anche in considerazione del fatto che il legislatore comunitario, nel suo ultimo lavoro, ha spostato il peso degli obblighi e delle garanzie sulle spalle dei grandi colossi dell'informazione, quasi tutti statunitensi.

E' facile immaginare quali siano state le reazioni: i Commentatori[181], non solo non hanno ritenuto il diritto all'oblio meritevole di tutela giuridica, in quanto privo di fondamento normativo/costituzionale, ma hanno paventato che il riconoscimento all'interessato del

---

[180] In particolare, G. D'ACQUISTO, *Diritto all'oblio tra tecnologia e diritto*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, 97, ha ritenuto che una «*cancellazione del dato dai sistemi del titolare, ne avrebbe compromesso la stessa esistenza come soggetto economico e avrebbe potuto nuocere anche all'interessato. In linea di principio, la realizzazione del diritto ad essere dimenticati dovrebbe avere, come presupposto tecnologico, l'introduzione di una forma di opt-in su ogni dato immesso su Internet: ogni post su un forum, ogni commento all'interno di un blog, ogni dato personale citato all'interno di un testo, ogni fotografia o video caricato su un social network, dovrebbero richiedere uno specifico consenso da parte del soggetto cui i dati si riferiscono, rispetto ai vari tipi di trattamento cui il dato può essere sottoposto*».

[181] L. DETERMAN, *Social media Privacy*: *a dozen myths and fact*, in *Stanford Technology Law Review*, 2012, 7.

diritto alla cancellazione dei dati potesse comportare conseguenze assai pregiudizievoli alla libertà di espressione, a causa dei costi che il provider avrebbe dovuto sopportare per procedere alla rimozione sia di quanto pubblicato dall'utente, che del materiale successivamente copiato e pubblicato, attraverso le 'condivisioni' da altri utilizzatori della Rete[182]. Tali oneri, non solo economici, ma anche di organizzazione, ufficialmente avrebbero scoraggiato i provider che, pertanto, sarebbero stati molto cauti nell'operare il trattamento, con serie compromissioni delle libertà di espressione e d'informazione, ed avrebbero fortemente leso le multinazionali, danneggiandole, nelle relazioni economiche che s'intrecciano all'ombra del trattamento e della circolazione dei dati.

Di parere contrario, e più orientato all'intransigenza verso trattamenti liberi da regole, l'ex Garante nazionale per la protezione dei dati, Stefano Rodotà, che, in qualità di Presidente della Commissione costituita dalla Dott.ssa Boldrini per la predisposizione della 'Dichiarazione dei diritti in Internet'[183], ebbe ad affermare che " la predisposizione di diritti e doveri in Internet è condizione necessaria perché sia assicurato il funzionamento delle Istituzioni, evitando il prevalere di poteri pubblici e privati, che potrebbero portare ad una società della sorveglianza, del controllo e della selezione sociale."

5) Il Regolamento sulla Data Protection: una naturale evoluzione del Codice della Privacy

Il Codice nazionale della Privacy, D.Lgs 196/2003, elaborato in recepimento ed attuazione della Direttiva 95/46 CE, dopo oltre dieci anni di operatività, ancora ritenuto completo e organico, pressoché integralmente applicabile ed in armonia con l'Ordinamento giuridico, (nonostante le novità procedurali degli ultimi anni), già prevedeva il diritto alla cancellazione dei dati personali in casi particolari, disponendo che "l'interessato ha il diritto di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è

[182] E' questa l'opinione anche di A. MANTELERO*, U.S. Concern about the Eupean Right to Be Forgotten and Free Speech*, in *Contemporary Private Law/Sylvia Kirkegaard International Association of it lawyers*, 88.

[183] Il 28 luglio 2015, ad un anno esatto dall'insediamento, la Commissione, voluta dall'allora Presidente della Camera, Laura Boldrini, e presieduta dal giurista Stefano Rodotà, ha presentato un documento unico nel suo genere in Europa, la '*Dichiarazione dei diritti in Internet'*, utile strumento per contribuire a costruire una cittadinanza nell'era di Internet.

necessaria la conservazione in relazione agli scopi per i quali i dati siano stati raccolti o successivamente trattati, vietando altresì la comunicazione e la diffusione di quei dati per i quali era stata ordinata la cancellazione o per i quali sia decorso il tempo indicato[184]".

Nonostante un po' tutte le legislazioni nazionali degli Stati membri, allo stesso modo dell'Ordinamento italiano, contenessero previsioni normative a protezione e tutela dei dati della persona, il Legislatore europeo ha ritenuto indispensabile ed indifferibile il suo intervento per perimetrare ulteriormente gli spazi entro i quali i soggetti attivi del trattamento avrebbero potuto operare, consolidando definitivamente un diritto, relativamente nuovo, quale il diritto all'oblio, cui ha dedicato particolari attenzioni, non solo per ragioni squisitamente giuridiche, ma anche per gli 'effetti negativi' che informazioni non più attuali e prive d'interesse avrebbero potuto generare nel campo della 'business information' e, più ancora, nella sfera intima del titolare di tali informazioni.

Da un punto di vista strettamente giuridico, d'altra parte, una regolamentazione uniforme della materia non poteva che giovare agli interessi di tutti, non solo delle parti direttamente coinvolte.

La pronuncia 131/2014 della CGUE, intransigente, quanto dirompente, in materia di oblio, aveva sicuramente moltiplicato le problematiche piuttosto che semplificarle, lasciando molti interrogativi inevasi e costringendo le Corti nazionali, in sede di decisione, ad allargare o restringere le maglie di quel diritto, talvolta con modalità decisamente discrezionali. Prova ne è in Italia una pronuncia della Suprema Corte che[185], allargando un po' troppo le maglie del diritto all'oblio, ha colpito il giornale online PrimaDaNoi.it, con un'interpretazione inedita, quanto pericolosa di quella pretesa.

Nella sentenza i giudici di legittimità, in nome della Google Spain, hanno stabilito che un articolo di cronaca relativo ad un accoltellamento in un ristorante dovesse essere 'rimosso dall'archivio digitale' perché, pur corretto e vero, aveva prodotto danni ai ricorrenti, soggetti attivi della vicenda giudiziaria, garantendo le loro istanze oltre ogni limite. Con l'aggravate che la vicenda giudiziaria relativa all'accoltellamento, ai tempi della richiesta di rimozione, non si era ancora conclusa.

Non pare che nella fattispecie sia stato operato un equo bilanciamento tra i due diritti fondamentali, quello di cronaca e il diritto all'oblio, perché con l'accoglimento della

[184] D.Lgs 196/2003, art. 7 comma 3 lett. b).
[185] Cass. Civ., Sez. I, 24 giugno 2016, n. 13161.

richiesta di rimozione dell'articolo dall'archivio online, il diritto della collettività all'informazione ne è sicuramente risultato fortemente indebolito. Né è invocabile, a supporto di una decisione così tanto generosa, la pronuncia CGUE n. 131/2014, dal momento che i giudici europei hanno riconosciuto al ricorrente il solo diritto alla de-indicizzazione dal motore di ricerca della notizia su digitazione del suo nome, consentendole di continuare a vivere negli archivi delle testate giornalistiche e più in generale nei canali del web, accessibile sempre e comunque, attraverso l'uso di altre chiavi di accesso che non fossero i dati dell'interessato.

Critiche che hanno trovato ulteriore conferma nelle Linee Guida del WP Articolo 29, che, al paragrafo 18, hanno stabilito che la de-indicizzazione (e non la rimozione dagli archivi come voluta dai giudici di legittimità) non dovesse riguardare i motori di ricerca di piccola portata, come quelli dei giornali online. Ergo, nel caso di specie, per la testata on-line non vi sarebbe stato l'obbligo di rimuovere l'articolo e tantomeno di deindicizzarlo dal proprio motore di ricerca.

Per fortuna, in un maggior numero di casi, altre Autorità giudiziarie e lo stesso Garante per la protezione dei dati personali, più volte sollecitato dagli interessati ad intervenire, molto raramente hanno riconosciuto, nell'operazione di bilanciamento la prevalenza del diritto all'oblio, rigettando i ricorsi che, per la verità, erano pervenuti a migliaia dopo la pronuncia della CGUE, tanto da aver indotto Google.com a predisporre un modulo per la presentazione delle richieste di de-indicizzazione, spinta dal timore di evitare elevate sanzioni pecuniarie.

La situazione di grande caos, anche a causa dell'assenza di parametri oggettivi in base ai quali operare il bilanciamento del diritto all'oblio dell'interessato con l'interesse pubblico alla conoscenza delle informazioni che, a meno che non infierisca pesantemente sulla sfera personale dell'interessato, dovrebbe essere prevalente, ha portato le Autorità Garanti per la privacy ad attivarsi nell'elaborazione di criteri comuni per gestire i ricorsi ed i reclami presentati dagli interessati che si erano visti respingere le istanze da parte del motore di ricerca, sollecitando, nel contempo, l'intervento del legislatore europeo al fine di elaborare una disciplina armonica, contenente criteri, procedurali e sostanziali, in forza dei quali operare un equo bilanciamento.

6) Genesi del 'diritto alla cancellazione («diritto all'oblio»)' di cui all'art. 17 Reg. 2016/679 UE

La Commissione europea, in data 25 gennaio 2012, ha adottato la proposta concernente un regolamento generale sulla protezione dei dati, destinato a sostituire la Direttiva 95/46, animato dal duplice scopo di rafforzare i diritti in materia di protezione dei dati delle persone fisiche e migliorare le opportunità per le imprese, agevolando la libera circolazione dei dati personali nel mercato unico digitale.

Parallelamente alla proposta di Regolamento, la Commissione europea adottava una comunicazione strategica[186], contenente gli obiettivi, ed una direttiva sul trattamento dei dati[187] a fini di attività di contrasto, volte a sostituire la decisione quadro del 2008 sulla protezione dei dati.

Il Consiglio europeo invitava così la Commissione a valutare il funzionamento degli strumenti giuridici dell'Unione europea in tema di protezione dei dati e a presentare, se necessario, nuove iniziative legislative e non.

Sul punto il Parlamento europeo, nella risoluzione sul Programma di Stoccolma, rubricata "Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini[188]", aveva già accolto la proposta relativa ad un quadro giuridico completo in materia di protezione dei dati in Unione europea, chiedendo, tra l'altro, la revisione della decisione quadro. Nel piano d'azione per l'attuazione del programma di Stoccolma, la Commissione europea aveva a sua volta evidenziato la necessità di assicurare l'applicazione sistematica di quello che era stato ritenuto il diritto fondamentale alla protezione dei dati personali nel contesto di tutte le politiche europee. Il piano d'azione sottolineava che: "In una società globalizzata, caratterizzata da un rapido progresso tecnologico, in cui lo scambio d'informazioni non conosce confini, è quanto mai importante garantire il rispetto della vita privata. L'Unione deve assicurare l'applicazione sistematica del diritto fondamentale alla protezione dei dati. Occorre rafforzare la posizione dell'UE in relazione alla protezione dei dati personali

---

[186] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni per salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XI Sec*., 27 gennaio 2012, n 5852.

[187] Commissione europea, *Proposta di Direttiva del Parlamento europeo e del Consiglio, concernente la tutela 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 libera circolazione di tali dati*, 27 gennaio 2012, n. 5833.

[188] Testo disponibile all'indirizzo http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//TEXT+TA+P7-TA-2009-0090+0+DOC+XML+V0//IT.

in tutte le politiche europee, anche nel contrastare e prevenire la criminalità e nelle relazioni internazionali".

La proposta concernente un regolamento generale sulla protezione dei dati conteneva, già nella versione del 25 gennaio 2012, una previsione esplicita della volontà di disciplinare un diritto all'oblio ed alla cancellazione, in forza del quale l'interessato avrebbe avuto il diritto di ottenere, dal responsabile del trattamento, la cancellazione di dati personali che lo riguardavano e la rinuncia ad una ulteriore diffusione di tali dati, in particolare in relazione a quelli resi pubblici quando lo stesso era minore[189].

[189] Il testo di tale articolo era il seguente:
«*1. L'interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati, in particolare in relazione ai dati personali resi pubblici quando l'interessato era un minore, se sussiste uno dei motivi seguenti:*
a) i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si fonda il trattamento, di cui all'articolo 6, paragrafo 1, lettera a), oppure il periodo di conservazione dei dati autorizzato è scaduto e non sussiste altro motivo legittimo per trattare i dati;
c) l'interessato si oppone al trattamento di dati personali ai sensi dell'articolo 19; 252
d) il trattamento dei dati non è conforme al presente regolamento per altri motivi;
2. Quando ha reso pubblici dati personali, il responsabile del trattamento di cui al paragrafo 1 prende tutte le misure ragionevoli, anche tecniche, in relazione ai dati della cui pubblicazione è responsabile per informare i terzi che stanno trattando tali dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Se ha autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento è ritenuto responsabile di tale pubblicazione.
3. Il responsabile del trattamento provvede senza ritardo alla cancellazione, a meno che conservare i dati personali non sia necessario:
a) per l'esercizio del diritto alla libertà di espressione in conformità dell'articolo 80;
b) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 81;
c) per finalità storiche, statistiche e di ricerca scientifica in conformità dell'articolo 83;
d) per adempiere un obbligo legale di conservazione di dati personali previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento; il diritto dello Stato membro deve perseguire un obiettivo di interesse pubblico, rispettare il contenuto essenziale del diritto alla protezione dei dati personali ed essere proporzionato all'obiettivo legittimo;
e) nei casi di cui al paragrafo 4.
4. Invece di provvedere alla cancellazione, il responsabile del trattamento limita il trattamento dei dati personali:
a) quando l'interessato ne contesta l'esattezza, per il periodo necessario ad effettuare le opportune verifiche;
b) quando, benché non ne abbia più bisogno per l'esercizio dei suoi compiti, i dati devono essere conservati a fini probatori;
c) quando il trattamento è illecito e l'interessato si oppone alla loro cancellazione e chiede invece che ne sia limitato l'utilizzo;
d) quando l'interessato chiede di trasmettere i dati personali a un altro sistema di trattamento automatizzato, in conformità dell'articolo 18, paragrafo 2. 5. I dati personali di cui al paragrafo 4 possono essere trattati, salvo che per la conservazione, soltanto a fini probatori o con il consenso dell'interessato oppure per tutelare i diritti di un'altra persona fisica o giuridica o per un obiettivo di pubblico interesse.
6. Quando il trattamento dei dati personali è limitato a norma del paragrafo 4, il responsabile del trattamento informa l'interessato prima di eliminare la limitazione al trattamento.
7. Il responsabile del trattamento predispone i meccanismi per assicurare il rispetto dei termini fissati per la cancellazione dei dati personali e/o per un esame periodico della necessità di conservare tali dati.

Il testo veniva successivamente emendato, con l'esclusione del diritto all'oblio ed alla cancellazione in favore di un 'diritto alla cancellazione', che prevedeva il diritto dell'interessato ad ottenere, dal responsabile del trattamento, la cancellazione di dati personali che lo riguardassero, la rinuncia ad un'ulteriore diffusione di tali dati nonché la possibilità di ottenere da terzi la cancellazione di qualsiasi link, copia o riproduzione di dati, al sussistere di determinate condizioni.

Il tema connesso alla possibilità di disciplinare il diritto all'oblio mediante una norma positiva ha altresì attirato le attenzioni della dottrina[190].

L'iniziativa legislativa del Parlamento europeo si concretizzava poco tempo dopo, il 25 gennaio 2012: in tale sede, il Comitato per le libertà civili, la giustizia e gli Affari interni auspicava un nuovo regolamento che avrebbe dovuto, tra l'altro, tutelare il diritto all'oblio ed alla cancellazione. Il Comitato per l'Energia, venendo migliorate le informazioni sui diritti e sulla protezione dei dati e auspicando l'introduzione del diritto di rettifica, di oblio e di cancellazione, nonché di quelli di opposizione ed alla portabilità dei dati, manifestava parere positivo, nell'intento di vedere rafforzata la fiducia dei consumatori nei confronti dei servizi on-line.[191]

Dello stesso avviso appariva il Comitato giuridico, il quale, per bocca di Marielle Gallo[192], chiariva come fosse necessario rafforzare anche il diritto all'oblio, proponendo d'introdurre un obbligo, a carico del responsabile del trattamento, di informare l'interessato della risposta data dai terzi alla richiesta.

---

8. Quando provvede alla cancellazione, il responsabile del trattamento si astiene da altri trattamenti di tali dati personali.
9. Alla Commissione è conferito il potere di adottare atti delegati in conformità all'articolo 86 al fine di precisare:
a) i criteri e i requisiti per l'applicazione del paragrafo 1 per specifici settori e situazioni di trattamento dei dati;
b) le condizioni per la cancellazione di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico, come previsto al paragrafo 2;
c) i criteri e le condizioni per limitare il trattamento dei dati personali, di cui al paragrafo 4».

[190] In senso critico G. HORNUNG, *Eine Datenschutz-Grundverordnung fur Europa, in Licht und Schatten im kommissionsentwurf vom*, ZD, 2012, vol. 25, 99-106.

[191] L'iniziativa 2012/0011 (COD) prevedeva la necessità di «*provides the data subject's right to be forgotten and to erasure»*. Curiosamente la versione francese dello stesso documento diversamente indicava «*un droit a l'oublì numerique tout en precisant le droit d'effacement prevu a la directive 95/46 CE*», prevedendo così un diritto alla cancellazione valido unicamente nell'ambiente digitale.

[192] MARIELLE GALLO, Relatore del *Progetto di parere della Commissione giuridica destinato alla Commissione per le libertà civili, la giustizia e gli affari interni sulla proposta di regolamento del Parlamento europeo e del Consiglio, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati*. (COM (2012)0011- C7-0025/2012-2012/0011(COD)).

Il 12 marzo 2014 il Parlamento europeo approvava il testo definitivo, cancellandovi la menzione del diritto all'oblio in favore di un diritto alla cancellazione, che avrebbe consentito all'interessato "di ottenere da terzi la cancellazione di qualsiasi link, copia o riproduzione di tali dati[193]".

[193] Il testo di tale articolo è il seguente:
«*1. L'interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati e di ottenere da terzi la cancellazione di qualsiasi link, copia o riproduzione di tali dati, se sussiste uno dei motivi seguenti:*
a) i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si fonda il trattamento, di cui all'articolo 6, paragrafo 1, lettera a), oppure il periodo di conservazione dei dati autorizzato è scaduto e non sussiste altro motivo legittimo per trattare i dati;
c) l'interessato si oppone al trattamento di dati personali ai sensi dell'articolo 19; c bis) un tribunale o autorità di regolamentazione dell'Unione ha deliberato in maniera definitiva e assoluta che i dati in questione devono essere cancellati;
d) i dati sono stati trattati illecitamente. 1 bis. L'applicazione del paragrafo 1 dipende dalla capacità del responsabile del trattamento di verificare che la persona che richiede la cancellazione sia l'interessato.
2. Quando ha reso pubblici dati personali ingiustificatamente conformemente all'articolo 6, paragrafo1, il responsabile del trattamento prende tutte le misure ragionevoli per far cancellare i dati, anche da parte di terzi, fatto salvo l'articolo 77. Il responsabile del trattamento informa l'interessato, ove possibile, dell'azione intrapresa da parte dei terzi interessati.
3. Il responsabile del trattamento e, se del caso, i terzi provvedono senza ritardo alla cancellazione, a meno che conservare i dati personali non sia necessario:
a) per l'esercizio del diritto alla libertà di espressione in conformità dell'articolo 80;
b) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 81;
c) per finalità storiche, statistiche e di ricerca scientifica in conformità dell'articolo 83;
d) per adempiere un obbligo legale di conservazione di dati personali previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento; il diritto dello Stato membro deve perseguire un obiettivo di interesse pubblico, rispettare il contenuto essenziale del diritto alla protezione dei dati personali ed essere proporzionato all'obiettivo legittimo;
e) nei casi di cui al paragrafo 4.
4. Invece di provvedere alla cancellazione, il responsabile del trattamento limita il trattamento dei dati personali in modo tale che non siano sottoposti al normale accesso ai dati e alle operazioni di trattamento e che non possano più essere modificati:
a) quando l'interessato ne contesta l'esattezza, per il periodo necessario ad effettuare le opportune verifiche;
b) quando, benché non ne abbia più bisogno per l'esercizio dei suoi compiti, i dati devono essere conservati a fini probatori;
c) quando il trattamento è illecito e l'interessato si oppone alla loro cancellazione e chiede invece che ne sia limitato l'utilizzo;
c bis) quando un tribunale o autorità di regolamentazione dell'Unione ha deliberato in maniera definitiva e assoluta che i dati in questione devono essere limitati;
d) quando l'interessato chiede di trasmettere i dati personali a un altro sistema di trattamento automatizzato, in conformità dell'articolo 15, paragrafo 2 bis.
d bis) quando la particolare tecnologia di memorizzazione non consente la cancellazione ed è stata installata prima dell'entrata in vigore del presente regolamento.
5. I dati personali di cui al paragrafo 4 possono essere trattati, salvo che per la conservazione, soltanto a fini probatori o con il consenso dell'interessato oppure per tutelare i diritti di un'altra persona fisica o giuridica o per un obiettivo di pubblico interesse.
6. Quando il trattamento dei dati personali è limitato a norma del paragrafo 4, il responsabile del trattamento informa l'interessato prima di eliminare la limitazione al trattamento.
7. Soppresso
8. Quando provvede alla cancellazione, il responsabile del trattamento si astiene da altri trattamenti di tali dati personali.

Giunto in sede di Consiglio dell'Unione Europea, i diversi orientamenti dei componenti ivi presenti consentivano una convergenza di vedute che si traduceva nell'approvazione di numerosi[194] emendamenti, contenuti poi nel testo definitivo. Tale testo veniva poi pubblicato il 4 maggio 2016 sulla Gazzetta Ufficiale dell'Unione europea, insieme alla Direttiva che regola il trattamento dei dati personali nei settori di prevenzione, contrasto e repressione dei crimini. Il Regolamento sarebbe stato vigente, in via diretta in tutti gli Stati europei, a partire dal 25 maggio 2018.

7) Il diritto all'oblio secondo l'art. 17 del Regolamento 2016/679 UE

Il Nuovo Regolamento sulla protezione dei dati personali, all'art. 17, rubricato «'Diritto alla cancellazione' ('diritto all'oblio')», disciplina espressamente l'istituto paladino della dignità della persona, accomunando, in un'unica disposizione, due differenti posizioni giuridiche, il diritto alla cancellazione e il diritto all'oblio, per trattarle in maniera congiunta, tanto in sede di determinazione del contenuto, che della disciplina[195].

Diritto alla cancellazione e diritto all'oblio, quindi, si sovrappongono, arrivando a coincidere quasi alla perfezione in termini sostanziali[196], prevedendo entrambi la cessazione del trattamento dei dati personali ogni qualvolta risultino violati i principi di finalità, di liceità del trattamento e quello del consenso; sovrapposizione quanto mai impropria, considerato che si tratta di due istituti distinti: per parte della dottrina[197], la cancellazione, infatti, non può che porsi in rapporto di conseguenza rispetto alla pretesa

---

8 bis. Il responsabile del trattamento predispone i meccanismi per assicurare il rispetto dei termini fissati per la cancellazione dei dati personali e/o per un esame periodico della necessità di conservare tali dati.
9. Alla Commissione è conferito il potere di adottare, previa richiesta di parere al comitato europeo per la protezione dei dati, atti delegati in conformità all'articolo 86 al fine di precisare:
a) i criteri e i requisiti per l'applicazione del paragrafo 1 per specifici settori e situazioni di trattamento dei dati;
b) le condizioni per la cancellazione di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico, come previsto al paragrafo 2;
c) i criteri e le condizioni per limitare il trattamento dei dati personali, di cui al paragrafo 4».

[194] Cfr. C. BURTON- L. DE VOEL- C. KUNER -A. PATERAKI, *The Proposed EU Data Protection Regulation Three Years Laters: The Council Position*, in *BNA Privacy e Security Law Report*, 29 giugno 2015, in *Internet*, https://www.wsgr.com/eudataregulation/pdf/BNA-0615.pdf.

[195] Si veda F. PIZZETTI, *Il prisma del diritto all'oblio,* in ID., *Il caso del diritto all'oblio*, Torino, 2013, 21 e ss.

[196] Si veda V. D'ANTONIO, *Oblio e cancellazione dei dati nel diritto europeo*, op. cit., 220, dove afferma che "*la codificazione del diritto all'oblio proposta dal Regolamento europeo non rappresenta affatto lo stato dell'arte della materia ed anzi induce a ritenere che la storia di questa posizione giuridica, lungi dall'aver raggiunto un punto d'arrivo, continuerà ad essere affidata più alle parole di corti e studiosi, che a quelle dei legislatori nazionali e sovranazionali*".

[197] G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, op. cit., 596; C. DI COCCO - G. SARTOR, *Temi di diritto dell'informatica*, Torino, 2017, 137.

all'oblio, per cui seguirà, quale ovvia conseguenza, l'istanza di oblio qualora, ricorrendone i presupposti, questa sia stata positivamente valutata. I due termini, pertanto, non vanno letti come sinonimi ma vedono esistente tra loro un rapporto di causa ed effetto.

Questa tendenza si riscontra già in alcuni Considerando[198] introduttivi al testo normativo. Nel Considerando 65, infatti, è precisato che all'interessato debba essere garantito "il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali non più necessari per le finalità per le quali siano stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardino, quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente Regolamento". Il Considerando prosegue prevedendo dei limiti al diritto dell'interessato, qualora si dovesse riscontrare la necessità della conservazione dei dati trattati, per cui, riprendendo integralmente il terzo paragrafo dell'art. 17 GDPR, e ponendo limiti all'esercizio del diritto alla cancellazione/oblio, statuisce che non potrà essere azionato quel diritto, prevalendo la pretesa alla conservazione, "per esercitare il diritto alla libertà di espressione e d'informazione, per adempiere ad un obbligo legale, per eseguire un compito d'interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi d'interesse pubblico nel settore della sanità pubblica, a fini d'archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria".

Il riscontro positivo alla pretesa a che i propri dati personali siano cancellati e non più sottoposti a trattamento, pertanto, l'interessato potrà ottenerlo qualora ricorrano precise situazioni-presupposto che obbligheranno il titolare/responsabile del trattamento, su richiesta del primo, alla cancellazione dei dati. Il Legislatore europeo, quindi, ha riconosciuto alla persona fisica il diritto di esercitare la propria pretesa all'oblio se la conservazione dei dati non è conforme al Regolamento, al diritto dell'Unione ma anche qualora il trattamento avvenga in violazione della normativa dello Stato membro, cui è soggetto il titolare/responsabile dello stesso.

[198] Ci si riferisce ai Considerando 65, 66 e 67 del Regolamento citato.

In conformità ai propositi espressi da Viviane Redig[199], il Regolamento evidenzia l'importanza di tale diritto qualora l'interessato abbia prestato il consenso quando era minore, quindi presumibilmente non pienamente consapevole dei rischi derivanti dal trattamento, ed intenda successivamente negarlo, con particolare riferimento al consenso al trattamento operato in Internet.

La pretesa dell'interessato alla cancellazione dei dati, operata dal Legislatore europeo, come si evidenzia, è contenuta in spazi puntualmente perimetrati ed è configurata come conseguenza di situazioni-presupposto che coprono una casistica di carenze del trattamento, originarie o sopravvenute, tali da determinare, quale effetto, l'obbligo del titolare/responsabile di attendere all'istanza di cancellazione dei dati[200].

Quanto ai 'tempi' della procedura, in forza del considerando 59[201], il titolare è tenuto a rispondere alle richieste dell'interessato "senza ingiustificato ritardo e al più tardi, entro un mese e a motivare la sua eventuale intenzione di non accogliere la richiesta". I tempi, "al più tardi entro un mese", in cui il titolare dovrà rispondere alla richiesta dell'interessato, sia nel caso in cui proceda alla soddisfazione totale o parziale, che nell'ipotesi di rigetto della stessa, sono piuttosto stringenti, al fine di garantire all'interessato una giustizia effettiva alle sue ragioni.

Non è previsto alcun obbligo di rimozione a carico di titolare del trattamento qualora ricorrano le ipotesi di cui al paragrafo 3 dell'art. 17, che espressamente sancisce il divieto di procedere alla cancellazione dei dati, nonostante l'eventuale istanza contraria dell'interessato.[202]

---

[199] L'eurodeputato ha più volte sottolineato la necessità di offrire adeguata tutela ai dati dei minori trattati in rete. Cfr. il comunicato stampa disponibile in Internet all'indirizzo *http://europa.eu/rapid/press-release-IP-10-63-it.htm*.

[200] Considerando 65: "*Un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che lo riguardano ed il diritto all'oblio, se la conservazione dei dati violi il presente Regolamento o il diritto dell'Unione o degli stati membri cui è soggetto il titolare del trattamento…*".
Considerando 66: "*Per rafforzare il diritto all'oblio nell'ambiente online è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali ad informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link, verso tali dati, o copia o riproduzione di detti dati personali…*".

[201] Considerando 59, Regolamento 2016/679 UE: «*E' opportuno preveder modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei diritti di cui al presente regolamento, compresi i meccanismi per richiedere e, se del caso, ottenere gratuitamente, in particolare l'accesso ai dati, la loro rettifica e la cancellazione e per esercitare il diritto di opposizione. Il titolare del trattamento dovrebbe predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici*».

[202] Considerando 156: "*Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fin statistici dovrebbe essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente Regolamento. Tali garanzie dovrebbero assicurare che*

In tutte queste ipotesi, tra le quali primeggia l'affermazione del diritto alla libertà di espressione e d'informazione rispetto alla pretesa all'oblio, quest'ultima, ove non supportata da una serie di connotazioni che la fondino e la giustifichino, sarà destinata a soccombere rispetto al prevalente diritto all'informazione.

Il metro di valutazione, da attendere in sede di bilanciamento, per assumere la deliberazione di un eventuale cancellazione o meno dei dati, non è solo di carattere cronologico, non essendo sufficiente, affinché la notizia perda d'interesse, il mero trascorrere del tempo, (come appare talvolta da semplificazioni concettuali), ma di tipo logico-funzionale, dal momento che dovrà tenersi conto di una serie di altri fattori, quali la gravità dell'informazione, il peso sociale degli eventi, il pregio informativo, l'attualità residua[203], il ruolo e la posizione pubblica dell'interessato[204].

Potrebbe risultare una maturazione della pretesa di oblio in tempi assai brevi, come anche una diluizione particolarmente lenta e perfino un riaffioramento dell'interesse pubblico, che verrebbe ad escluderla del tutto, come sottolineato dalle molteplici pronunce giurisprudenziali in materia, appellatesi ad una serie di criteri, che purtroppo non hanno trovato alcuna formalizzazione nell'art. 17, essendosi, quest'ultimo, limitato a riprodurre, con qualche precisazione e puntualizzazione in più, i contorni del diritto alla cancellazione dei dati, come disciplinato nella Direttiva 95/46, avendo determinato, così, per il Legislatore, la perdita di una fondamentale opportunità di intervento a precisazione.

Neppure in merito al bilanciamento con il diritto di cronaca, e più in generale con l'attività giornalistica, in funzione antagonista rispetto alla pretesa all'oblio dell'interessato, il

---

siano state predisposte misure tecniche ed organizzative al fine di garantire, in particolare, il principio della *minimizzazione dei dati. L'ulteriore trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è da effettuarsi quando il titolare del trattamento ha valutato la fattibilità di conseguire tali finalità, trattando dati personali che non consentono o non consentono più di identificare l'interessato, purché esistano garanzie adeguate*."

[203] Cass. Civ., Sez. III, sentenza 26 giugno 2013, n. 16111. La vicenda riguardava la pubblicazione di una notizia di cronaca che rievocava la passata militanza di un soggetto in un'associazione terroristica, in relazione al recente ritrovamento di un arsenale di armi nella sua zona di residenza, evento, quest'ultimo, ritenuto dalla Corte generico ed insufficiente a giustificare la rievocazione di vicende ormai remote nel tempo e superate dal reinserimento sociale della persona.

[204] In materia di riconoscimento dell'oblio rispetto ai dati personali pubblicati da un motore di ricerca, cfr. CGUE, *Google Spain SL e Google Inc*., C-131/12: «*Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli artt. 7 e 8 della Carta, chiedere che l'informazione non venga più messa a disposizione del grande pubblico […], i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico ad accedere all'informazione […]. Tuttavia, così non sarebbe qualora risultasse, a causa del ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso all'informazione di cui trattasi*».

Legislatore europeo ha fornito criteri e previsioni oggettive, indispensabili per sottrarre quella tecnica all'opera, spesso discrezionale, dei motori di ricerca, in prima battuta, e delle autorità nazionali, amministrative o giudiziarie, successivamente, nonostante la giurisprudenza, in passato, abbia lavorato con finezza per individuare delle connotazioni oggettive, utili a sottrarre le decisioni, circa la presenza dell'oblio, da possibili connotazioni soggettive e, in quanto tali, discrezionali.

Nessuno schema giuridico maturato dal pensiero degli operatori della giustizia, infatti, ha trovato formalizzazione nell'art. 17 GDPR che, in effetti, si è limitato a riprodurre, con qualche lieve precisazione, il diritto alla cancellazione dei dati di cui alla Direttiva 95/46, per cui appare condivisibile l'opinione di coloro che sostengono la perdita di una grande occasione per il Legislatore europeo, che non ha dato soluzione ad una serie di problematiche, fatte accuratamente emergere dalla giurisprudenza europea e nazionale, in sede di applicazione delle norme vigenti.

Per altra parte della dottrina[205], la singolare scelta stilistica adottata dal Legislatore UE, verrebbe a rappresentare la mera cancellazione dei dati, impropriamente chiamata "diritto all'oblio", differentemente da quanto da altri affermato[206], secondo cui si sarebbe di fronte ad un tortuoso processo di composizione negoziale, sfociata in un compromesso lessicale. Ancora, c'è chi, in dottrina[207], sostiene che, con quella formulazione il Legislatore europeo abbia voluto forzatamente dare un segnale a chi chiedeva una reazione politica alla sentenza Google Spain e chi[208] legge l'espressione "diritto all'oblio" come equivalente (o al massimo specificazione) di "diritto alla cancellazione".

---

[205] Sostengono che il diritto all'oblio, così come formulato nel testo del Regolamento, sia in realtà diritto alla cancellazione, F. PIZZETTI, *Il prisma del diritto all'oblio*, op. cit., 62; A. MANTELERO, *Il futuro regolamento EU sui dati personali e la valenza 'politica' del caso Google: ricordare e dimenticare nella digital economy*, in G. RESTA - V. ZENO - ZENCOVICH (a cura di), *Il diritto all'oblio su Internet*, op. cit.,125 e ss.

[206] Nella proposta iniziale di Regolamento, l'art. 17 era rubricato «Right to be forgotten («diritto ad essere dimenticato», che in lingua italiana è stato - forse frettolosamente - tradotto in "diritto all'oblio") and to erasure (diritto alla cancellazione)». Tale testo veniva successivamente modificato, escludendo l'oblio in forza di un solo «diritto alla cancellazione», che prevedeva il diritto dell'interessato ad ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia ad un'ulteriore diffusione degli stessi e di ottenere da terzi la cancellazione di qualsiasi link, copia o riproduzione di tali dati, al sussistere di determinate condizioni.

[207] Tesi sposata da F. PIZZETTI, *Il prisma del diritto all'oblio*, op. ult cit., 21 ss., e A. MANTELERO, Il futuro regolamento, in G. RESTA - V. ZENO - ZENCOVICH (a cura di), *Il diritto all'oblio su Internet*, op. ult. cit., che, commentando la sentenza Google Spain, la definisce una «*decisione di politica del diritto», sottolineando lo «stile argomentativo della sentenza che, specie per quanto concerne il diritto all'oblio, mostra in taluni punti carenze che svelano la chiara intenzione politica della pronuncia*», 126.

[208] *Ex multis*, E. STRADELLA, *Cancellazione e oblio*: *come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella Rete, quali anticorpi si possono*

Interpretazione, quest'ultima, non condivisa da altra autorevole dottrina[209], che non vede nella 'cancellazione' e nell' 'oblio', nonostante la rubrica legis, due sinonimi giuridici.
Orientamento suffragato dallo stesso Legislatore europeo, che ha inteso mantenere distinti i due concetti, e che si desumerebbe, altresì, dalla formulazione degli stessi Considerando 66 e 156 del Regolamento UE[210], che manterrebbero ben distinti i due concetti.
Una misura alternativa di contemperamento tra diritto alla cancellazione e diritto al mantenimento dei dati è rappresentata dall'opzione, pure contemplata nel Regolamento, in forza della quale il titolare, evitando il taglio, potrà 'limitare' il trattamento dei dati personali, in modo da sottrarli al normale accesso, qualora l'interessato ne contesti l'esattezza, e limitatamente al periodo necessario per effettuare le opportune verifiche, i dati debbano essere conservati per fini probatori, il trattamento sia illecito ma l'interessato si oppone alla loro cancellazione, chiedendo che ne sia solo limitato l'utilizzo, la limitazione del trattamento dei dati sia stata deliberata, in maniera definitiva, dall'Autorità giudiziaria, la particolare tecnologia di memorizzazione non consenta la cancellazione e sia stata installata prima dell'entrata in vigore del Regolamento.

---

sviluppare, e, infine, cui prodest?, in AIC, n. 4, 12 dicembre 2016; G. GARDINI, *Le regole dell'informazione. L'era della postverità*, Torino, 2017, 331; M. MEGALE, *ICT e diritto nella società dell'informazione*, Torino, 2017, 135; F. POLITI, *Diritto pubblico*, Torino, 2017, 446.

[209]Così per S. ZANINI, *Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?*, in Federalismi.it, Rivista di diritto pubblico italiano, comparato, europeo, 18 luglio 2018, secondo cui: «A ben vedere, cancellazione e oblio non sono sinonimi giuridici, nonostante la *rubrica legis* esaminata possa indurre in errore. Il legislatore europeo, dal canto suo, ha espresso più volte la volontà di mantenere distinti i due concetti. Nella Carta dei diritti fondamentali di internet del 2015, l'art. 11, rubricato «Diritto all'oblio», fa riferimento esclusivamente al rapporto tra utente e motore di ricerca, mentre l'art. 6 della stessa Carta, rubricato «Diritto all'autodeterminazione informativa», sancisce il diritto di accedere ai propri dati e di chiederne l'integrazione, la rettifica e la cancellazione: pare quindi che il legislatore abbia deciso di ricondurre al diritto all'oblio una situazione giuridica che non ha ad oggetto la cancellazione definitiva del dato, ma l'eliminazione del link riferito al dato stesso. Il diritto alla cancellazione vantato nei confronti di soggetti diversi dal gestore del motore di ricerca (in primis, il gestore del sito web) non determinerebbe quindi alcun diritto all'oblio. Anche dalla formulazione degli stessi Considerando del Reg. UE 679/16 precedentemente esaminati si desume la volontà del legislatore di tenere distinti i concetti di cancellazione e oblio (mai usati, infatti, come sinonimi). Nello specifico, nella parte in cui si afferma che «per rafforzare il "diritto all'oblio" nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso […]» (Considerando 66), o ancora quando, prevedendo la possibilità per gli Stati di derogare a determinate discipline, vengono inseriti nell'elenco sia il diritto alla cancellazione che il diritto all'oblio (Considerando 156)».

[210] Nel Considerando 66 si afferma che «per rafforzare il "diritto all'oblio" nell'ambiente *online*, è opportuno che il diritto di cancellazione sia esteso […]», pertanto i due concetti sono tenuti ben distinti, senza che vi sia assimilazione alcuna, o ancora, nel Considerando 156 si prevede la possibilità per gli Stati di derogare a determinate discipline e si inseriscono nell'elenco sia il diritto alla cancellazione che il diritto all'oblio, mantenendoli così debitamente distinti.

8) Paragrafo 2 dell'art. 17 GDPR: la vera rivoluzione copernicana del Legislatore europeo

Superando le posizioni discordanti espresse dalla dottrina in merito alla *rubrica legis* dell'art. 17 Regolamento 2016/679, a serbare le maggiori sorprese è il paragrafo 2 di quella norma, che si riferisce ai dati personali pubblicati, stabilendo che il titolare del trattamento, se ha reso pubblici i dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto delle tecnologie disponibili e dei costi di attuazione, adotti le misure ragionevoli, anche tecniche, per informare i titolari del trattamento, che stanno trattando quei dati personali, della richiesta, avanzata dall'interessato, di cancellare qualsiasi link, copia o riproduzione degli stessi.

Il modello classico 'bipolare' di rapporto intercorrente tra titolare ed interessato, come definito dalla direttiva 95/46 CE, viene ad essere superato dal coinvolgimento di soggetti ulteriori, i quali, disponendo dei dati, sono tenuti a loro volta a procedere alla cancellazione.

Da qui la portata innovativa celata nel dettato in analisi.

Secondo autorevole dottrina[211], leggendo tale prescrizione, in combinato disposto con il già citato Considerando 66, emerge una rappresentazione che a ben vedere si pone in contrasto con le determine della Google Spain.

Circa la questione centrale relativa alla qualificazione del gestore del motore di ricerca come responsabile del trattamento dei dati resi disponibili a terzi, questione che ha fatto emergere il concetto di oblio come de-indicizzazione, il Considerando rende manifesto come il Regolamento consideri responsabile del trattamento solo il soggetto che ha inserito i dati personali nel circuito della Rete, tramite il sito fonte, imponendo solo nei suoi riguardi l'onere, di cui al paragrafo 2, di comunicare ai terzi che trattino tali dati, la richiesta di cancellazione formulata dal soggetto interessato.

Il gestore del motore di ricerca rientra chiaramente tra i suddetti terzi: nonostante cataloghi, memorizzi, indicizzi e diffonda i dati non sarebbe stato considerato dal Legislatore europeo titolare del trattamento e sarebbe stata esclusa, pertanto, la possibilità per l'interessato di esercitare nei suoi confronti il diritto alla cancellazione. Solo a seguito della comunicazione dell'informativa sulla richiesta di cancellazione, da parte del sito

[211] Così per S. ZANINI, *Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?,* op. cit.

fonte, verrà attribuita la titolarità del trattamento anche al gestore del motore di ricerca[212]. Tale comunicazione, infatti, farebbe sorgere nello stesso la consapevolezza di trattare dati di natura personale, proprio in quanto oggetto di legittima richiesta di cancellazione.

Il gestore del motore di ricerca si limiterebbe ad offrire, infatti, uno strumento di mera organizzazione delle informazioni, senza esercitare alcun controllo sui dati personali contenuti in pagine *web* di terzi e senza conoscerne la natura; solo la decisione cosciente di non ottemperare alla comunicazione della richiesta di cancellazione avanzata

---

[212] Ancora così per S. ZANINI, *Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?,* op. ult. cit., secondo cui: «Tale Considerando*,* infatti, ricalca l'impronta della sentenza della Corte di Giustizia solo per quanto concerne la volontà di base di riconoscere il diritto in oggetto.
Viceversa, circa la questione centrale relativa alla qualificazione del gestore di motore di ricerca come responsabile del trattamento dei dati resi disponibili ai terzi (questione che ha fatto emergere il concetto di "oblio" come "de-indicizzazione"), il Considerando rende manifesto come il Regolamento consideri responsabile del trattamento solo il soggetto che ha inserito i dati personali nel circuito della rete (tramite il sito fonte), e come solo su tale soggetto incomba l'obbligo, *ex* par. 2, di comunicare ai terzi che trattano tali dati la richiesta di cancellazione formulata dal soggetto interessato.
Il gestore del motore di ricerca, che rientra chiaramente tra i suddetti «terzi» (affermazione confermata dal richiamo espresso a concetti quali «*link, copia o riproduzione dei dati»* nel par. 253), cataloga, memorizza, indicizza e diffonde i dati, ma ciò non pare sufficiente per permettere che si eserciti *direttamente* nei suoi confronti il diritto alla cancellazione».
L'autrice, a sostegno della sua tesi richiama anche quanto affermato dal W.P. 29, nel parere n. 1/2010: «il principio di proporzionalità comporta che, nella misura in cui interviene esclusivamente come intermediario, il *provider* di motori di ricerca non deve essere considerato il responsabile principale del trattamento con riguardo al trattamento di dati personali in questione. In questo caso, i responsabili principali del trattamento sono i fornitori di informazioni».
Pertanto, secondo la Zanini: «Solo a seguito della comunicazione dell'informativa sulla richiesta di cancellazione da parte del sito fonte verrà attribuita la titolarità del trattamento *anche* al gestore del motore di ricerca: tale comunicazione, infatti, fa sorgere nello stesso la *consapevolezza* di trattare dati che sono (anche potenzialmente) di natura personale, proprio in quanto oggetto di legittima richiesta di cancellazione (prima di questo momento il fornitore del servizio non conosce la natura dei dati che tratta)».
Dello stesso avviso anche O. POLLICINO e M. BASSINI, *Il diritto all'oblio*, in *http://www.academia.edu/33139336/Il_diritto_alloblio*, secondo i quali: «a norma del par. 2 dell'art. 17, il titolare che ha reso pubblici dati personali (supponiamo il titolare di una testata giornalistica online o comunque di un sito di informazione) è tenuto ad adottare, «tenendo conto della tecnologia disponibile e dei costi di attuazione», le misure ragionevoli, anche di natura tecnica, per assicurare la cessazione del trattamento dei dati da parte di terzi. Dette misure occorrono, così, ad «informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali» Il caso di specie è dato proprio dall'ipotesi in cui a trattare i dati resi pubblici da una testata giornalistica telematica sia un motore di ricerca: poiché quest'ultimo ricade, secondo quanto stabilito nella sentenza Google Spain, nella categoria del titolare del trattamento, e i dati da questi trattati sono stati resi pubblici dal proprietario di un sito terzo, ove l'interessato faccia valere i suoi diritti nei confronti di quest'ultimo, di riflesso anche il provider dovrà ottemperare alla richiesta di cessare il trattamento. Il meccanismo introdotto dal Regolamento prevede dunque un raccordo tra il gestore di un sito e il gestore di un motore di ricerca finalizzato ad evitare un'asimmetria nella divulgazione di dati personali. Appare curiosa la connotazione che traspare da questa norma rispetto al ruolo del motore di ricerca, che appare dipinto come un "titolare di secondo grado": questa circostanza tradisce evidentemente le difficoltà di riconciliare una visione olistica dello scenario, assai complesso, dei diversi attori che si agitano sullo scenario dell'informazione in rete, con le conclusioni della Corte di giustizia nel caso Google Spain».

dall'interessato al sito fonte, sempre a parere di questa dottrina, potrebbe comportare la responsabilità del *provider*.[213]

Premesse che hanno condotto quella stessa dottrina[214] ad affermare che nel paragrafo 2 dell'art. 17, si parlerebbe anche di de-indicizzazione dei dati da parte dei motori di ricerca, ma non negli stessi termini ed alle stesse condizioni enunciate dalla Corte di Giustizia.

Il soggetto interessato, infatti, non potrebbe rivolgersi direttamente al motore di ricerca né per chiedere la de-indicizzazione, né per richiedere la cancellazione dei dati. La sua richiesta potrà essere rivolta esclusivamente al sito fonte: sarà quest'ultimo che dovrà provvedere a comunicare al gestore del motore di ricerca l'istanza di cancellazione ed il suo accoglimento, ai sensi del paragrafo 1. Il motore di ricerca, da parte sua, in tal caso, per non incorrere in responsabilità, dovrà procedere alla de-indicizzazione dei dati nel momento in cui ne riceverà notizia da parte del sito sorgente. Pertanto, a parere di tale dottrina, il motore di ricerca potrebbe intervenire, de-indicizzando i link alla notizia, solo in seconda battuta, non essendo possibile per l'interessato rivolgersi direttamente allo stesso.

Posizione, quest'ultima, invero, solo parzialmente condivisibile! Il sito fonte, infatti, è obbligato ad assolvere all'obbligo di comunicazione al gestore del motore di ricerca,

---

[213] Così sempre per S. ZANINI, *Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?* cit., che, nel richiamare una decisione della Corte tedesca sulla funzione *auto-complete* di *Google* (*BGH Case* VI ZR 269/12, del maggio 2013), nella quale si affermava l'obbligo del *provider* di reagire e attivarsi non appena avesse appreso di star fornendo informazioni in conflitto con i diritti della personalità, afferma: «È proprio tale elemento soggettivo, che può essere racchiuso nel concetto di "trattamento consapevole", a far sorgere la responsabilità in capo al *provider*, il quale, ricevuta la comunicazione (attraverso, ad esempio, i c.d. *codici di esclusione*), sarà tenuto ad assicurare la deindicizzazione dei *link* interessati, come fosse una sorta di titolare del trattamento "di secondo grado"».

[214] Ancora, S. ZANINI, *Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?,* op. cit.*,* secondo cui: «Al paragrafo 2 si parla (anche) di de-indicizzazione dei dati da parte dei motori di ricerca, ma non nei termini usati dalla Corte di Giustizia. Il regolamento UE 679/16, all'art. 17, non sta positivizzando *quel* diritto all'oblio, ma qualcosa di parzialmente diverso.

Il soggetto interessato, infatti, non può rivolgersi *direttamente* al motore di ricerca, né per richiedere la de-indicizzazione, né per ottenere la cancellazione dei dati (d'altronde, per il *provider* sarebbe tecnicamente impossibile cancellare *dati,* come previsto al par. 1; può solo cancellare - *rectius* deindecizzare - *link*): il motore di ricerca, per non incorrere in responsabilità, dovrà procedere alla de-indicizzazione dei dati (o all'aggiornamento della memoria *cache*) nel momento in cui riceverà notizia della richiesta di cancellazione dei dati personali da parte del sito fonte.

La richiesta di cancellazione formulata dall'interessato, quindi, è rivolta anche ai titolari "secondari", ma giunge loro tramite il primo titolare.

Ciò traspare con ancora maggiore chiarezza nella versione inglese del par. 2: «*Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of those personal data».*

limitatamente e nel rispetto della tecnologia disponibile e dei mezzi a sua disposizione, ai sensi del paragrafo 2, art. 17 Regolamento europeo 2016/679. Le possibilità di deroga a tale onere non sono poche infatti: il sito fonte potrebbe, in ogni momento, non adempiervi, adducendo, quali motivazioni, i costi eccessivamente elevati, nonché la penuria di misure tecniche e figure professionali idonee a traghettare sui vari motori di ricerca l'istanza di cancellazione pervenuta dall'interessato e, quand'anche dovesse adempiervi, l'obbligo sarebbe limitato dal fatto che non tocchi a lui verificare quale comportamento adotteranno gli altri titolari del trattamento, anche tenendo conto del fatto che la richiesta dell'interessato dovrà essere oggetto di valutazione da parte di ciascun titolare, al fine di valutare se per lui sussista o meno il dovere di accoglienza. Il titolare del trattamento, quindi, non dovrà accertarsi del comportamento degli altri titolari, dovendo limitarsi alla mera comunicazione, della quale peraltro non vi sarebbe neppure certezza, se si considera che trattasi di un obbligo sprovvisto di sanzione, per cui il sito sorgente che non volesse far perdere visibilità a dati ed informazioni di cui fosse fornitore, potrebbe non ottemperare all'obbligo di comunicazione, senza incorrere in alcuna responsabilità e/o sanzione pecuniaria. Il sito fonte, infatti, ove costretto a cancellare ricorrendo i presupposti di cui al paragrafo 1, art. 17 GDPR, sarebbe comunque orientato a non perdere visibilità tra i risultati forniti dal motore di ricerca. La conseguenza sarebbe un vero e proprio paradosso: i dati personali relativi alle informazioni sarebbero cancellati sul sito fonte, continuando a vivere nei canali del Web, in quanto indicizzate dai motori di ricerca, vanificando per giunta le motivazioni che avrebbero indotto l'utente ad inoltrare la richiesta di cancellazione dei suoi dati personali. Il danno sarebbe ulteriormente amplificato se si tenesse conto del fatto che oggi gli utenti, affamati di informazioni, aggrediscono in prima battuta il motore di ricerca, quale contenitore di qualunque informazione cui i link rinviano, più che i siti sorgente. I rischi paventati rendono quanto mai necessaria la coesistenza delle procedure di de-indicizzazione e cancellazione dei dati, lasciando l'utente libero di optare per l'una o per l'altra, o per entrambe, escludendo qualsiasi forma di assorbimento della prima nella seconda. Solo in questo modo l'interessato, desideroso di essere dimenticato, potrà ottenere una tutela veramente completa: questi, infatti, potrebbe adire direttamente il gestore del motore di ricerca, chiedendo la de-indicizzazione, allorquando volesse esclusivamente ottenere la recisione dei link alla notizia; viceversa, potrebbe formulare istanza di cancellazione dei

dati al titolare del sito sorgente, ove fosse interessato alla rimozione di quei dati a lui relativi dalle pagine Web del sito fonte, ottenendo, altresì, suo tramite, la de-indicizzazione da parte del motore di ricerca, laddove il sito sorgente ottemperasse all'obbligo di comunicazione previsto dal paragrafo 2 dell'art. 17 GDPR. In assenza di tale comunicazione, al fine di ottenere una tutela completa, l'interessato potrebbe azionare contemporaneamente entrambe le procedure, adendo contestualmente il motore di ricerca ed il titolare del sito sorgente. Solo in questo modo il diritto all'oblio non rimarrebbe una mera enunciazione di principio!

9) Un'analisi critica: l'ambiguità del testo e i problemi applicativi

Come sottolineato dalla dottrina americana[215], nei primi commenti, la versione definitiva del testo non ha risolto i dubbi già sollevati in sede di analisi delle precedenti versioni, non solo dagli operatori della materia, ma anche dall'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)[216], titolata ad assistere la Commissione europea nella redazione dei testi di legge afferenti la sicurezza informatica e le reti di comunicazione.

Il testo finale risulta, infatti, foriero di una serie di ambiguità, che, invece di essere definite in sede legislativa, continueranno ad essere risolte dall'autorità giudiziaria. A parte alcune problematiche irrisolte relative all'applicazione territoriale[217], è proprio il punto inerente al diritto all'oblio, e più in generale ad ogni operazione di trattamento dati, ad essere ancora controverso.

A livello generale il diritto all'oblio, più volte espunto e reinserito all'interno delle varie proposte di legge ed ora menzionato nel titolo dell'articolo, tra parentesi, assume

---

[215] Per una prima analisi, si rinvia a D. KELLER, *The final draft of europe's right to be forgotten law*, in *Internet, all'indirizzo* http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europe's-right-be-forgotten-law .

[216] Cfr. P. DRUSHEL- M. BACKES- R. TIRTEA, *Impossible, the right to be forgotten between expectations and practice: report by Eupean Network and Security Agency*, in *Internet* http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten. A pag. 14 gli Autori sottolineano come «*una volta che vengono pubblicate le informazioni personali, è impossibile prevenire ed osservare, per mezzo di misure tecnologiche, la creazione di copie non autorizzate di questa informazione. In un sistema aperto come Internet, il diritto ad essere dimenticato non può essere fatto rispettare solamente tramite mezzi tecnici […], ma deve derivare da una combinazione di disposizioni tecniche e di norme di diritto internazionale*».

[217] Il trattamento trova applicazione anche con riferimento ai trattamenti effettuati fuori dai confini dell'Unione a condizione che sia effettuato nei confronti di cittadini comunitari e che abbia ad oggetto l'offerta di beni o servizi o il monitoraggio del comportamento degli utenti. Tale formulazione di per sé molto ampia è in idonea a racchiudere tutti i servizi della società dell'informazione.

un'accezione del tutto diversa da quella di cui alla pronuncia CGUE 131/2012, configurandosi piuttosto come un 'diritto alla cancellazione', in assenza, nel testo della norma, di un esplicito riconoscimento del diritto alla de-indicizzazione dei dati personali dal motore di ricerca. I responsabili del trattamento[218], categoria nella quale potrebbero rientrare alcuni intermediari della società dell'informazione, dovrebbero – e qui l'uso del condizionale appare d'obbligo – cancellare i dati personali sulla base dell'esercizio di un diritto all'oblio, solo a seguito della relativa richiesta. La norma tace sulla possibilità che soggetti terzi, che abbiano in gestione parti di sistemi informativi – più semplicemente soggetti che gestiscano profili sociali – debbano o meno adempiere a tale obbligo.

Tale circostanza potrebbe essere esclusa sulla base del Considerando 15[219], che tuttavia potrebbe riferirsi agli utilizzi dei social network effettuati per finalità personali, tra le quali appare dubbia l'inclusione della finalità di diffusione dei dati in reti telematiche. D'altro canto il Regolamento non chiarisce neppure la posizione di chi le piattaforme social le gestisce, non specificando se questi siano o meno responsabili del trattamento ovvero, come osservato da autorevole dottrina olandese[220] in relazione alle precedenti proposte di regolamento del Parlamento europeo, se debbano o meno disporre non solo del potere di cancellare i dati dei propri utenti dai loro sistemi ovvero, ancor più, anche dai sistemi di terzi soggetti che dispongano di piattaforme di pubblicità online alle quali siano soliti trasferire i dati.

Non è indicata neppure la posizione dei motori di ricerca e la condotta che questi dovranno tenere; se è pur vero che il motore di ricerca, dalla pronuncia CGUE 131/12, è stato riconosciuto titolare del trattamento, tuttavia il Regolamento nulla specifica in merito a come questi debba assicurare il diritto all'oblio degli interessati. Tale scelta appare discutibile soprattutto se paragonata ad analoghe decisioni assunte dai Legislatori

---

[218] L'art. 4 definisce i responsabili come «*la persona fisica o giuridica, l'autorità pubblica, le agenzie o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento dei dati personali*».

[219] Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati ad essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine.

[220] G. J. ZWENNE, *Nog veel onzekerheden over het recht om te worden vergeten, in Tijdschrift voor Internetrecht*, 2012, vol. 9, 68-76. A pag. 69, l'Autore dichiara «*Se si assume che il responsabile sia tenuto ad eliminare i dati nel rispetto degli altri utenti dei social network, allora si ritiene che egli debba richiederne la cancellazione anche alle aziende pubblicitarie alle quali li ha forniti*».

non europei, che, seppur criticate da una parte della dottrina[221], hanno disciplinato chiaramente il concetto di motore di ricerca, definendone il ruolo e gli ambiti di operatività.

In questo contesto è così ipotizzabile che gli intermediari – ed in generale chiunque abbia un seppur minimo potere d'imperio sui dati personali presenti in Rete – decidano di procedere ad assecondare ogni richiesta, non potendo contare su uno spazio netto di esenzione di responsabilità per i contenuti veicolati. A sostegno di questa visione depone il fatto che non siano state previste sanzioni[222] nel caso di una ultrattività del responsabile del trattamento finalizzata alla rimozione eccessiva dei contenuti, mentre è prevista una sanzione particolarmente gravosa nel caso di mancato rispetto della richiesta di de-indicizzazione, che potrebbe raggiungere una somma pari al 4% del fatturato annuo mondiale del responsabile.

Quanto alla procedura di de-indicizzazione, viene da chiedersi, in questo contesto, quale sarà la posizione dei principali motori di ricerca non eccessivamente diffusi, Bing – Yahoo, posto che questi con riferimento alle richieste avanzate nel territorio dell'Unione europea, hanno respinto ad oggi circa la metà delle istanze di de-indicizzazione, esponendosi al rischio di sanzioni rigorose, sia pure d'importo minore rispetto a quelle previste dal regolamento.

Il rafforzamento di tutela della sfera privata del cittadino, consentito dal Legislatore europeo, è particolarmente evidente laddove il Regolamento ha previsto il diritto ad ottenere la 'cancellazione' dei dati, in presenza di determinati presupposti, al posto della de-indicizzazione, che, all'indomani della Google Spain, aveva già fatto registrare la tendenza dei titolari dei diritti ad incrementare esponenzialmente le proprie richieste, causando una perdita di qualità delle valutazioni su di esse effettuate ed una disponibilità dei motori di ricerca, sia pure di piccole dimensioni, a procedere alla rimozione dei

[221] In senso critico, M. BELLEZZA, *L'oblio è legge in Russia*, in *Medialaw*, 16 novembre 2016. L'Autore ritiene che la legge è stata aspramente criticata perché, diversamente dalla decisione della Corte di Giustizia, introduce la possibilità, anche per le figure di rilevanza pubblica, di rivolgersi ai motori di ricerca, per chiedere la rimozione dei contenuti, spostando pericolosamente l'ago della bilancia a favore del diritto alla riservatezza a discapito della libertà di informazione.

[222] L'art. 83, par. 5, Reg. 2016/679 UE prevede che «*La violazione delle disposizioni seguenti, in conformità al paragrafo 2 bis, può essere oggetto di sanzioni amministrative fino a 20.000.000 Euro, o in caso di un'impresa fino al 4% del fatturato mondiale totale dell'esercizio precedente*».

contenuti, anche qualora vi fossero stati dubbi sulla correttezza delle relative richieste, al fine di evitare il rischio di sanzioni[223].

Altro elemento destinato a sollevare perplessità è il coordinamento tra il Regolamento e la Direttiva sul commercio elettronico: il testo del Regolamento, infatti, prevede che questo debba essere attuato senza pregiudizio della Direttiva, omettendo, tuttavia, di definire la portata di tale affermazione[224]. Con riferimento al diritto all'oblio non è chiaro, segnatamente, se il Regolamento trovi o meno applicazione con riferimento all'attività del provider. E' pur vero che il Regolamento non dovrebbe trovare applicazione nei confronti dell'intermediario che tratti dati di terzi, da parte della dottrina qualificato come titolare del trattamento "di secondo grado"[225], ma, essendo la definizione stessa d'intermediario divenuta molto labile, appare difficile assumere una posizione risolutoria. In ogni caso i titolari del trattamento devono tempestivamente rimuovere il contenuto non in linea qualora ricevano una richiesta di cancellazione, mantenendolo offline, fino a quando non abbiano effettuato una valutazione in merito alla validità della stessa; valutazione rimessa ad algoritmi che, operando meccanicamente, prescindono da valutazioni fattuali da operare caso per caso. Il Legislatore europeo, infatti, si è guardato bene dal fornire criteri mediante i quali i titolari/responsabili debbano decidere se gettare o meno nell'oblio un dato, prevedendo unicamente criteri ricavabili dall'intero complesso normativo e, ancora una volta, rimessi a valutazioni discrezionali dei motori di ricerca (sebbene non siano predisposti a 'dimenticare' facilmente), o delle autorità amministrative o giudiziarie. Qualora, conseguentemente, l'interessato affermi che

---

[223] D. SENG, *The state of Discordant Union: An Empirical Analysis of DMCA Take down Notices*, in *Virginia Journal of Law and Techonology*, 2014, vol. 18. A pag. 56 dello scritto, l'Autore evidenzia che «*l'unica cosa statica in Internet è il cambiamento. Siamo giunti ad avere titolari individuali del copyright ed i loro avvocati, responsabili del marketing e soggetti che rilevano tali violazioni e che operano nell'eliminazione di contenuti online. Siamo giunti all'invio di comunicazioni con un/due richieste di rimozione all'invio di migliaia di richieste ai service provider. Siamo passati da un sistema manuale con la presa in carico individuale delle comunicazioni ad un sistema automatico nel quale sia chi rileva le violazioni che i service provider, utilizzano i computer per prendere in gestione un gran numero di comunicazioni e richieste con i tempi di evasione molto brevi. E con il cambiamento arrivano anche le inevitabile conseguenze dei titolari dei diritti ed i soggetti che segnalano le violazioni devono lottare con forme elettroniche di non facile utilizzo, di comunicazioni sintetiche di soggetti che rilevano le violazione dei diritti, che sono schiacciate dalle immense comunicazioni con migliaia di richieste di rimozioni di male informati titolari dei diritti e di soggetti che inviino le segnalazioni che inviano richieste di rimozione abusive, vaghe ed ambiziose […]*».

[224] L'articolo 2, comma 3 del Regolamento prevede infatti che «*questa norma deve essere senza pregiudizio nell'applicazione della direttiva 2000/31, in particolare della legge sulla responsabilità del service provider disciplinata negli articoli dal 12 al 15 della direttiva*».

[225] Così per S. ZANINI, *Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?,* op. cit. e O. POLLICINO E M. BASSINI, *Il diritto all'oblio,* op. cit.

un'informazione online sia corredata dei presupposti perché possa operare l'oblio, l'intermediario dovrà limitare l'accesso all'informazione per un tempo tale a consentirne il controllo, in ogni caso non superiore ad un mese, elevabile a due in presenza di specifiche circostanze, un tempo per certi aspetti breve se riferito ad aziende non strutturate[226].

Questo tipo d'indagine fattuale sui contenuti generati dagli utenti, tra l'altro, è una funzione in palese contrasto ideologico con il principio di neutralità del provider ed, in ogni caso, difficilmente esigibile da parte di ogni responsabile, che si troverebbe a fronteggiare una presunzione di colpevolezza in merito ai contenuti segnalati.

Ancora una volta, e con amarezza, ci si trova a constatare come l'attesa normativizzazione del diritto all'oblio ad opera del Legislatore europeo ha lasciato irrisolte numerose problematiche già evidenziate e denunciate nei decenni precedenti dagli operatori della giustizia, dagli interessati all'oblio e da coloro che intendevano tutelare la 'memoria'. Nella redazione di un qualsiasi testo normativo, normalmente intervengono svariate componenti, anche di ordine politico, cosicché le disposizioni legislative finiscono con l'essere espressione di un compromesso tra le diverse componenti sociali. Nel caso del 'diritto all'oblio', probabilmente, le carenze risolutive riscontrate e la superficialità con cui è stato trattato un istituto particolarmente sensibile sono state volute; il Legislatore ha avuto tempo e modo per poter affrontare l'argomento in maniera più dettagliata, anche sulla base delle problematiche emerse nei decenni precedenti di applicazione dell'istituto. Non lo ha fatto! Sembra quasi che abbia volutamente omesso di assumere posizioni definite, piegandosi ad una flessibilità quanto mai inopportuna e rimettendo le soluzioni del caso concreto alle valutazioni degli operatori, ancora una volta in assenza di criteri operativi.

---

[226] Regolamento europeo 2016/679, art. 18: Diritto di limitazione del trattamento
«*L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:*
a) l'interessato contesta l'esattezza dei dati personali per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento, ai sensi dell'art. 21 par. 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato […]»

In una società come la nostra, gli interessi del singolo utilizzatore della Rete devono, senza dubbio, essere contemperati con altri e, non ultimo, con quelli della società, intenta a trarre vantaggio dall'accessibilità ai dati ed alle informazioni. E' vero che la legge mai avrebbe potuto fornire una cassetta degli attrezzi utile a risolvere le problematiche più disparate che il trattamento dei dati potrebbe evidenziare, dovendosi comunque cercare nel 'bilanciamento' la soluzione, ma non sarebbe certamente risultata superflua la previsione di criteri oggettivi e uniformemente applicabili in forza dei quali operare il bilanciamento, se non altro per evitare, o quanto meno ridurre, il rischio di pronunce giudiziarie tra loro confliggenti, relative allo stesso caso giudiziario, emesse da tribunali di diversi livelli.

Per aiutare l'utente comune ad orientarsi in questo quadro a tinte fosche di pronunce, interventi normativi incompleti e poco soddisfacenti, all'indomani dell'epocale sentenza della Corte di Giustizia dell'Unione europea, Google ha comunicato in un report[227], tramite il suo neonato "Advisory Council on the Right to be Forgotten", talune determine, che potrebbero chiarire il panorama attuale ed essere utili alle giurisdizioni locali in caso di contestazioni. Quattro sono i criteri, in presenza dei quali, il colosso americano ritiene meritevole di apprezzamento la possibilità di de-indicizzazione di taluni dati, su richiesta dell'interessato: il ruolo dell'interessato nella vita pubblica, la tipologia di informazione oggetto della richiesta, la fonte dell'informazione, il trascorrere del tempo. In merito al primo criterio, è operata una differenziazione tra soggetti che rivestono un 'preciso ruolo nella dimensione pubblica', per i quali minore sarà la possibilità di accoglimento di una richiesta di de-indicizzazione di informazioni, 'soggetti privi di rilievo nella vita pubblica', le cui richieste di rimozione verosimilmente potrebbero incontrare più facilmente la disponibilità del motore di ricerca, 'soggetti con un ruolo pubblico limitato a specifici ambiti', le cui istanze necessiterebbero di una valutazione più accurata, affrontata in relazione alle peculiarità delle singole esigenze prospettate.

In merito, invece, al tipo di informazione oggetto del caso, l'Advisory Council ha ritenuto opportuno definire due categorie di "notizie tipo". La prima categoria, comprendente immagini o i filmati riguardanti l'interessato, informazioni relative alla sua situazione economica e sessuale, dati sensibili, contatti, informazioni relative a minori, credenziali di autenticazione ed autorizzazione, vede la prevalenza dell'interesse alla riservatezza

[227] Report of the Advisory Commitee to Google on the Right to be Forgotten, 6 febbraio 2015.

rispetto all'interesse pubblico, trattandosi di dati particolarmente confinanti con la sfera privata.

Nella seconda categoria rientrerebbero, invece, tutte le informazioni che generalmente rivestono un pubblico interesse, relative a temi politici, dibattiti religiosi, sociali, questioni attinenti alla salute pubblica, notizie relative a fatti penalmente rilevanti, di interesse storico o riguardanti ricerche scientifiche o forme di espressione artistica. In merito a queste informazioni, l'interesse pubblico alla notizia si presume prevalente rispetto al diritto all'oblio.

Con riferimento, poi, alla fonte dell'informazione, il motore di ricerca sostiene che per verificare la sussistenza di un pubblico interesse alla conoscenza della notizia contestata, si debba far riferimento alla fonte dell'informazione ed alla sua finalità: la pubblica rilevanza potrebbe riguardare, senza dubbio, le notizie divulgate nell'ambito dell'attività giornalistica o diffuse da siti d'informazione.

In ultimo, ma non per importanza, andrebbe considerato il fattore temporale: l'unità di tempo trascorsa dalla verificazione del fatto, oggetto dell'informazione, all'istanza di de-indicizzazione, potrebbe aver mutato il ruolo e la dimensione pubblica dell'interessato all'oblio.

I criteri forniti dall'Advisory Council del più grande motore di ricerca oggi esistente, seppur fondamentali, sono deputati a lasciare un ampio margine di discrezionalità nella valutazione delle singole istanze, senza dubbio utile per consentire l'adattamento della decisione alle peculiarità delle singole esigenze, ma, al contempo, pericoloso, in quanto idoneo a danneggiare i diritti della personalità, laddove si ravvisasse la prevalenza del pubblico interesse, o creare vulnus nella memoria collettiva, se si adoperassero rimozioni piuttosto generose, in ottemperanza al desiderio di rimozione del ricordo, vantato dal richiedente l'oblio.

10) Il Consiglio d'Europa, nell'ottica del Regolamento 2016/679 UE, aggiorna la Convenzione 108/1981

Con lo scopo di rafforzare la protezione dei dati personali oggetto di elaborazione automatizzata su scala globale, e anche alla luce della nuova normativa regolamentare europea, il Consiglio d'Europa ha adottato un protocollo di modifica che migliora e aggiorna alle nuove minacce del mercato digitale, la Convenzione sulla tutela delle

persone rispetto al trattamento dei dati, meglio nota come 'Convenzione 108', per continuare a meglio proteggere i dati personali e affrontare con più sicurezza le nuove sfide digitali e i nuovi pericoli che si presentano quotidianamente a livello globale.

Nel 1981 il Consiglio d'Europa ha adottato il primo, e tuttora unico, Trattato internazionale sul diritto delle persone alla protezione dei propri dati personali: la Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati personali, nota come 'Convenzione 108'. Un protocollo aggiuntivo imponeva a ciascuno Stato parte del Trattato di istituire un'Autorità indipendente per garantire il rispetto dei principi di protezione dei dati, stabilendo regole sui flussi transfrontalieri dei dati.

La Convenzione 108 è stata oggetto di un processo di modernizzazione iniziato nel 2011, continuato, in quanto necessario per l'adeguamento di quella normativa a quella più evoluta contenuta nel Regolamento 2016/679, e portato a termine dal Consiglio d'Europa il 18 maggio 2018.

L'entrata in vigore del GDPR, che uniforma la legislazione dell'Unione europea in materia di trattamento dei dati personali, le nuove tecnologie, l'espansione dei flussi transfrontalieri di dati, l'aumento delle violazioni al diritto dei dati personali richiedevano una risposta forte e coordinata a livello internazionale. In questa logica si è inserito il Protocollo di aggiornamento della Convenzione, unico Trattato internazionale esistente, giuridicamente vincolante con rilevanza globale nel settore della tutela della privacy.

Il testo modernizzato, nel mantenere le disposizioni della Convenzione a livello di principio (rimanendo tecnologicamente neutrale e consentendo alle Parti un margine di discrezionalità nell'attuare tali norme attraverso la propria legislazione) e nel richiedere che il trattamento dei dati personali applichi il principio della 'privacy by design', introduce maggiori tutele in favore degli interessati in un contesto in cui le decisioni vengono prese da un decisore automatizzato e prevede il diritto di avere conoscenza della logica e delle finalità che stanno alla base del trattamento dei dati.

Il Protocollo contiene altre innovazioni rilevanti come l'obbligo di notificare le violazioni dei dati e richiede con maggiore forza che il trattamento dei dati sia effettuato in modo proporzionato, secondo i principi di 'minimizzazione' e di *'accountability'*. Rafforza le responsabilità dei titolari del trattamento dei dati e la trasparenza dell'iter del trattamento stesso, elemento essenziale per mantenere la fiducia nell'ambiente digitale. Ha, altresì, previsto l'inserimento, tra i dati sensibili, di quelli biometrici e genetici, assenti nella

precedente formulazione, ampliando i diritti degli interessati che ora comprendono anche il diritto a non essere soggetto a decisioni puramente automatizzate e a conoscere la logica sottesa al trattamento.

Il Protocollo fornisce un quadro giuridico multilaterale solido e flessibile per facilitare il flusso di dati a livello transfrontaliero e nel contempo offre garanzie efficaci e concrete nell'ambito dei trattamenti dei dati personali, contribuendo ad assicurare il rispetto dei diritti e delle libertà fondamentali di ogni individuo, indipendentemente dalla propria nazionalità o luogo di residenza. E' espressione del forte impegno che le diverse regioni del mondo, nel quadro del trattamento dei dati personali, hanno deciso di assumere e, riprendendo molti dei principi contenuti nel GDPR, ha inteso garantire il libero flusso dei dati a livello transfrontaliero in un sistema protetto da standard e principi condivisi.

La Convenzione, così aggiornata, è stata adottata dal Comitato dei Ministri del Consiglio d'Europa in occasione della sua 128^ sessione svoltasi a Elsinore. Partendo dalla Convenzione 108, sottoscritta da più di 50 Stati, anche il Protocollo di modernizzazione continuerà ad essere aperto a qualsiasi Paese del mondo come unico standard riconosciuto a livello globale.

Ricorda il Garante che "la modernizzazione della Convenzione 108, che è tuttora l'unico strumento sulla protezione dei dati vincolante a livello internazionale, risponde alle molte sfide intervenute negli anni per l'avvento delle nuove tecnologie, assicurando la tenuta dei principi della Convenzione, rafforzando i meccanismi per la sua effettiva implementazione. Il Protocollo ha lo scopo di garantire gli standard elevati in una cornice normativa flessibile che facilita la loro adozione da parte di un ampio numero di Paesi, inclusi quelli che non fanno parte del Consiglio d'Europa e costituisce un ponte tra i diversi approcci regionali, incluso il Regolamento UE 2016/679[228]".

Il Regolamento UE, infatti, entrato in vigore il 25 maggio 2018, colloca l'adesione da parte di Paesi terzi alla Convenzione 108 tra i criteri da considerare nella valutazione di adeguatezza di tali Paesi, nel contesto dei trasferimenti dei dati.

[228] Garante della Protezione dei dati personali, *Relazione del 23 maggio 2018*, in *Dir. giust.,*, maggio 2018.

SEZIONE II: Il diritto all'esercizio delle libertà fondamentali spettante alla collettività e il diritto all'oblio: forme di tensione

1) Le tensioni tra il diritto alla protezione dei dati personali e la libertà di espressione e di informazione

L'art. 8 della Convenzione europea dei diritti dell'uomo e delle libertà fondamentali[229], nel sancire il diritto di ciascun individuo al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza, pur evidenziando una dimensione piuttosto debole della riservatezza, non prevedeva espressamente il diritto alla libertà di espressione ed informazione.

La norma, invece, va fatta oggetto di una lettura combinata con il contenuto dell'art. 10 della medesima Convenzione, che dispone il riconoscimento ad ogni persona della libertà di espressione, includendo nella locuzione tanto la libertà di opinione, che quella di ricevere o comunicare informazioni o idee, senza ingerenze da parte dell'autorità pubblica e senza considerazioni di frontiera.

Diritto alla protezione dei dati personali e libertà di espressione: due interessi co-primari, entrambi previsti e sanciti dalla medesima Convenzione e riconosciuti come tali da tutti gli interventi legislativi successivi, ivi compreso il Regolamento europeo 2016/679.

Il diritto alla cancellazione dei dati personali, previsto dal Legislatore europeo nell'art. 17 del Regolamento europeo, non è, infatti, un diritto assoluto: costituisce, piuttosto, un limite esterno al diritto di cronaca ed alla libertà di stampa ed, in tal senso, va opportunamente bilanciato con il diritto in competizione.

Tale pretesa, pertanto, non deve essere indiscriminatamente riconosciuta e concessa, essendo opportuno, meglio doveroso, il confronto con altri diritti della società civile, tra i quali spicca, appunto, il diritto all'informazione, sancito dall'art. 21 della Costituzione.

Lo spirito del nuovo Regolamento consiste, infatti, nel consentire agli interessati di gestire i loro dati personali, preservando, al contempo, il diritto d'informazione e la libertà di espressione.

Sicché l'art. 17, nel suo terzo paragrafo, consente, ai titolari, la prosecuzione del trattamento e della elaborazione dei dati, allorquando siano necessari al perseguimento

[229]La Convenzione dei diritti dell'Uomo e delle libertà fondamentali è stata firmata a Roma il 4 novembre 1950 e ratificata dall'Italia con legge del 4 agosto 1955 n. 848. E' entrata in vigore il 26 ottobre dello stesso anno, previo deposito dello strumento di ratifica a Strasburgo.

degli scopi per i quali siano stati raccolti ed esista ancora una base giuridica che giustifichi il trattamento degli stessi, identificabile anche con l'esercizio del diritto alla libertà di espressione e di informazione.

Pertanto, non è obbligatorio l'accoglimento dell'istanza di cancellazione dei dati avanzata dall'interessato, residuando sempre un margine di discrezionalità nei confronti del motore di ricerca, chiamato a valutare e considerare esigenze di rilievo costituzionale e sociale non subalterne.

Viepiù, la misura a protezione dell'istanza dell'interessato non può e non deve essere la cancellazione totale delle informazioni online, quanto, piuttosto soluzioni dai risvolti chirurgici meno invasivi, purché in grado di riequilibrare i diritti in contrapposizione, riducendo la portata del trattamento, quali, la cancellazione dei soli dati personali legati alla notizia o la mera de-indicizzazione da parte del motore di ricerca, che consente in ogni caso la permanenza dell'informazione nel sito sorgente, rendendone esclusivamente più impervio l'accesso.

D'altronde, non stupisce che il più poderoso e spregiudicato intervento legislativo a protezione dei dati personali, volto a contenere lo strapotere detenuto dall'esiguo numero di aziende che possiedono un patrimonio di conoscenze gigantesco e dispongono di potenti mezzi per indirizzare la loro influenza nei nostri riguardi, contempli il limite del diritto all'informazione e della libertà di espressione, quali contrapposti presidi costituzionali.

Ad ulteriore riprova dell'attenzione prestata dal Legislatore regolamentare alla libertà di informazione, nella sua duplice accezione, attiva, quale diritto del giornalista di informare, e passiva, quale diritto del cittadino di essere informato, precondizioni per la salvaguardia della democraticità delle società contemporanee, l'art. 85 del Regolamento europeo prevede esenzioni e deroghe, in favore dell'attività giornalistica, ma anche in favore dell'espressione accademica, artistica e letteraria. Sicché le norme derogatorie previste per i giornalisti si applicano a chiunque eserciti la libertà di manifestazione del pensiero, anche attraverso espressioni artistiche e letterarie.

Il Legislatore europeo prevede, altresì, che spetti agli Stati Membri l'onere di conciliare la protezione dei dati personali con il diritto alla libertà di espressione e di informazione, incluso il trattamento a scopi giornalistici e di espressione accademica, artistica e letteraria, consentendo altresì agli Stati Membri l'adozione di esenzioni e deroghe ai

principi imposti dall'UE, allorquando necessari per la conciliazione delle opposte necessità. Nonostante siano decorsi due anni dalla pubblicazione del Regolamento europeo per la protezione dei dati personali, nessuno si è premurato di promuovere un'iniziativa legislativa in Italia, volta a prevedere quelle deroghe ed esenzioni previste dall'art. 85, con grave pregiudizio non solo dell'attività giornalistica, ma anche di quella accademica, artistica e letteraria.

2) Applicabilità ai motori di ricerca della 'eccezione giornalistica'

Il tema dell'eventuale applicabilità a un motore di ricerca come Google della cosiddetta journalistic exemption, di cui all'art. 9 della Direttiva 95/46 CE, in base alla quale gli Stati membri possono prevedere deroghe alle regole sul trattamento dei dati personali nei confronti di chi effettua il trattamento "esclusivamente a scopi giornalistici o di espressione artistica o letteraria", al fine di "conciliare il diritto alla vita privata con le norme sulla libertà di espressione", è stato recentemente affrontato dalla giurisprudenza inglese che, in mancanza di operatività del Regolamento 2016/679, non ha potuto basare il giudizio sulle norme in esso contenute, ma solo su quelle della previgente Direttiva 95/46 CE e della legislazione nazionale di recepimento e attuazione della stessa.

Posto che una delle attività dei motori di ricerca è quella di aggregare e rendere visibili le informazioni prodotte da fonti giornalistiche e, in forza di un'interpretazione piuttosto lata della locuzione 'scopi giornalistici', considerato che in effetti il ruolo dei motori di ricerca è anche quello di 'facilitatori' della pubblicazione di informazioni giornalistiche prodotte da terze parti, i giudici inglesi sono pervenuti alla conclusione che anche quello effettuato dai motori di ricerca possa essere considerato un trattamento di dati a scopi giornalistici.

Interpretazione estensiva del concetto di 'scopi giornalistici', anche suffragata da una sentenza della Corte di Giustizia del dicembre 2008[230], in risposta a una domanda di pronuncia pregiudiziale, con la quale si è affermato il principio per cui anche un'attività di pubblicazione e diffusione, con qualsiasi mezzo, di dati fiscali riferiti a cittadini finlandesi, che la legge nazionale considera pubblici, corrisponde alla nozione di scopi giornalistici, di cui alla Direttiva 95/46 CE, qualora abbia come unica finalità – la cui

[230] Corte di Giustizia dell'Unione Europea, Grande Sezione, ricorso C-72/07 Tietosuojavaltuutettu c. Satakunnan Markkinaorssi Oy e Satamediaoy, sentenza 16 dicembre 2008.

valutazione è rimessa al giudice nazionale - quella di "divulgare al pubblico informazioni, opinioni o idee".

Secondo il ragionamento della High Court, anche attività ancillari e di supporto all'attività giornalistica potrebbero rientrare in una nozione ampia di 'scopi giornalistici', beneficiando della journalistic exemption ma a condizione, stando alla lettera dell'art. 9 Dir. 95/46, che ciò avvenga in modo esclusivo, mentre le attività del motore di ricerca "are not exclusively subsidiary, subservient or ancillary to those of any publisher".

Il ragionamento è corretto stando al testo letterale dell'art. 9 Dir. 95/46 CE. L'entrata in vigore del Regolamento 2016/679 UE, il cui articolo 85 nel riprodurre il principio della journalistic exemption ha eliminato l'avverbio 'esclusivamente', provoca un mutamento di scenario. Eliminazione sicuramente opportuna se si considera che ben raramente oggi chi pubblica notizie via Internet lo fa esclusivamente per scopi giornalistici: lo scopo giornalistico può essere preponderante ma non esclusivo, in quanto può essere accompagnato da altre attività, fra cui, ad esempio, la raccolta di inserzioni pubblicitarie, la profilazione degli utenti del servizio a fini di pubblicità comportamentale ecc.

Persino i social network stanno gradualmente sviluppando sinergie con il settore dell'editoria tradizionale, per sfruttare, a loro vantaggio, l'affidabilità e la credibilità di cui gode la stampa: alcuni di essi, ad esempio, possiedono una piccola redazione formata da giornalisti e professionisti che producono contenuti, curano e selezionano le notizie e colmano le lacune del materiale prodotto dagli utenti.

Anche un motore di ricerca come Google persegue, più o meno direttamente, finalità d'informazione (eventualmente qualificabili come giornalistiche) nel momento in cui, in risposta alle query formulate dagli utenti, presenta un elenco di link correlati tra loro per via della presenza di comuni parole-chiave. Ovviamente il servizio Google News, che si autodefinisce 'copertura giornalistica completa e aggiornata ottenuta combinando fonti di notizie in tutto il mondo' persegue scopi giornalistici.

Pertanto, se con l'entrata in vigore del GDPR è venuto meno il requisito dell'esclusività degli scopi giornalistici, sul quale la Corte inglese aveva fondato la decisione della non applicabilità a Google della journalistic exemption, per il futuro si aprono nuovi scenari interpretativi che potrebbero arrivare a ricomprendere varie categorie d'intermediari digitali, tra cui i social network e i motori di ricerca, all'interno di una nozione estesa di attività giornalistica.

Inoltre, poiché il comma 2 dell'art. 85 GDPR rimette alla discrezionalità degli Stati membri l'ampiezza e la qualità delle deroghe applicabili al trattamento dei dati effettuato per scopi giornalistici rispetto alla normativa generale, non è escluso che le discipline nazionali possano divergere tra loro in ordine alla qualificazione degli scopi giornalistici, ai soggetti cui le esenzioni si riferiscono e alla tipologia delle stesse. Da questo punto di vista, il Regolamento sembra contravvenire alla finalità, più volte ribadita nei suoi Considerando, di prevenire ed eliminare le disparità che possano ostacolare la libera circolazione dei dati personali nel mercato interno, assicurando 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.

3) La libertà di stampa e il diritto all'oblio: premessa

Il fulcro del dibattito, in tema di diritto all'oblio, ruota sul difficile equilibrio, da un lato, delle finalità giornalistiche e documentaristiche, che legittimano l'ulteriore conservazione per fini storici e, dall'altro, delle esigenze di tutela di persone, che potrebbero legittimamente invocare, in certi casi e a determinate condizioni, l'oblio su vicende ormai non più attuali e lontane e spesso confliggenti con il proprio attuale percorso di vita.

Gli interessi fatti valere, pertanto, da chi invoca il diritto all'oblio sono legati al bilanciamento tra i diritti della personalità dei soggetti, i cui dati vengono trattati, e gli operatori dell'informazione, il cui lavoro è svolto all'ombra della libertà di espressione del proprio pensiero e in particolare della libertà di stampa.

4) La libertà di stampa nelle sue estrinsecazioni del diritto ad informare e ad essere informati

a) Il diritto ad informare

L'attività d'informazione, indipendentemente dai mezzi di diffusione, rappresenta un fenomeno unitario, espressione della caratterizzazione democratica di un sistema che, in quanto afferente ai profili di partecipazione dei singoli all'organizzazione sociale e politica della comunità, trova il suo fondamento nella Dichiarazione Universale dei Diritti dell'Uomo, il cui art. 19 riconosce ad ogni individuo il diritto alla libertà di opinione e di espressione, ivi compreso il diritto di cercare, ricevere e diffondere informazioni e idee con ogni mezzo e indipendentemente dalle frontiere.

Similmente, l'art. 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali sancisce per ogni persona il diritto alla libertà di espressione, che comprende la libertà di opinione e quella di ricevere e comunicare informazioni o idee, senza che vi possa essere interferenza delle pubbliche autorità: principio integralmente riportato nella Carta costituzionale italiana, all'art. 21.

E', tuttavia, convinzione diffusa in dottrina che la ricostruzione normativa della disciplina giuridica della 'comunicazione sociale' non possa essere limitata alla disposizione direttamente regolante l'attività d'informazione, esistendo nell'Ordinamento giuridico altre norme di riferimento riconducibili alla previsione di tutele di tutte quelle libertà che si concretizzano in una scelta, essendo necessario 'conoscere' per deliberare ed informare. La tutela costituzionale del diritto all'informazione, pertanto, sarebbe rinvenibile anche in tutte quelle norme che garantiscono il pieno sviluppo della persona umana, in forza degli articoli 2 e 3, comma 2 Cost., del principio di sovranità popolare, di cui all'art. 1 Cost., della partecipazione effettiva all'organizzazione politica, economica e sociale in quanto solo un'esatta informazione costituisce l'essenza della democrazia, consentendo un'effettiva e consapevole partecipazione dell'individuo alla vita di relazione.

In tal senso, anche quanto posto in luce dalla Corte Costituzionale[231], secondo cui "in un ordinamento democratico il ruolo della stampa e dell'informazione è inteso al soddisfacimento di un interesse generale, individuabile nella formazione di un'opinione avvertita e consapevole".

Secondo passate modalità, l'informazione era intesa come un rapporto bilaterale in cui un soggetto attivo la trasmetteva ad un soggetto passivo, che era, pertanto, il recettore della stessa: si trattava, più che altro, di un'informazione interindividuale, che avveniva mediante corrispondenza, telegrafo o telefono. Nell'era della comunicazione sociale, invece, il rapporto è diventato di uno a tanti, per cui l'unilateralità del messaggio si oppone alla pluralità e indeterminatezza dei destinatari, che, grazie alla veloce circolazione dei dati, consentita dalle nuove tecnologie dell'informazione, sono in grado di pervenire in tempo reale alle notizie, con l'ulteriore novità rappresentata dal ribaltamento dei ruoli che ha visto il polo passivo della dialettica del rapporto d'informazione svolgere un ruolo attivo, atteggiandosi ad attore della diffusione dei dati

[231]Corte Cost., sentenza del 9 giugno 1972, n. 105, in *CED Cassaz.*, 1972.

relativi alla sua sfera personale e, in via mediata, anche di quelli inerenti la privacy di terzi ignari della cosa.

Per quanto il diritto all'informazione abbia un solido riconoscimento costituzionale, deve comunque misurarsi con limiti di natura pubblica, laddove andasse a confliggere con disposizioni di legge, con la morale, il buon costume e l'ordine pubblico, ma soprattutto di natura privatistica, nel caso in cui andasse a violare quei paletti predisposti per apprestare forme di tutela alla personalità dei singoli, ai loro dati personali, più in generale alla loro sfera di riservatezza. Limiti di fronte ai quali il diritto all'informazione è destinato a soccombere, a meno che non riguardi fatti e accadimenti assolutamente indispensabili da conoscere per una crescita culturale della persona, consapevole e completa.

Anche se in dottrina[232], secondo una visione ottimistica, i due diritti sono stati definiti come 'terreni confinanti', il rapporto tra il diritto all'informazione e quello alla tutela della sfera privata è, normalmente, un rapporto conflittuale intercorrente tra pretese, che, se dilatate, potrebbero entrare in collisione: come il diritto all'informazione, se eccessivamente dilatato, potrebbe interferire e violare la sfera privata, allo stesso modo, la estremizzazione del diritto alla protezione dei dati potrebbe esondare, mettendo nell'angolo il primo. Nonostante tutto, la libertà di informazione ed il rispetto della privacy non vanno intese come libertà contrapposte, al più come due diritti che, alternativamente, potrebbero emergere, facendo soccombere l'antagonista, in forza delle circostanze del caso concreto ed all'esito di un'operazione di bilanciamento, resa oggi particolarmente ardua a causa della transnazionalità degli strumenti attraverso i quali si attua la libertà di manifestazione del pensiero che, sia per il massiccio immagazzinamento dei dati, che, per la facilità con cui ne consentono la circolazione, potrebbero rivelarsi gravemente lesivi della sfera di riservatezza dei singoli.

La difficoltà più grande oggi è quella di classificare i nuovi mezzi di comunicazione per definire quale sia l'attesa di privacy- il tasso di consapevolezza rispetto al potenziale di invadenza- che gli stessi pongono.

---

[232]M. MEZZANOTTE, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli 2009, 230-231. Tanto il diritto all'informazione, quanto quello alla tutela della sfera intima, a parere dell'Autore, non possono confliggere in quanto entrambi convergono verso una medesima finalità, quella appunto, di consentire «*il pieno sviluppo della persona e, pertanto, devono integrarsi reciprocamente. Tutto deve convergere al fine dello sviluppo della persona umana. L'unico limite che l'Ordinamento pone al concreto esercizio e godimento di queste libertà e di queste posizioni fondamentali è costituito dal rispetto delle libertà altrui e dalla confliggente presenza di un interesse pubblico che può rendere necessario, in specifiche circostanze, il sacrificio di singoli diritti e di singole libertà*».

Gli strumenti di telecomunicazione satellitare, le reti telematiche, i mezzi interattivi, avendo rivoluzionato le comunicazioni e facilitato il potere di accesso alle stesse, relativamente al rapporto tra il diritto alla privacy e la libertà di stampa, hanno aperto due ordini di problemi: in primo luogo, hanno reso difficile la definizione di "sfera privata", dal momento che i dati residenti nel computer di una persona si confondono con quelli delle reti, cui la comunicazione satellitare rinvia per scrutare immagini e spostamenti in tempo reale. Di non secondaria importanza, i problemi posti da Internet, come nuovo giornale globale, in cui lettori e giornalisti si fondono e confondono in un mix che potrebbe anche realizzare quel diritto alla libera manifestazione del pensiero, quale possibilità concreta di comunicare al mondo ciò che si pensa, sancito dalla Carta costituzionale. Da questo punto di vista la realtà statunitense può risultare illuminante, avendo elaborato una serie di ipotesi che definiscono differenti livelli di attesa di riservatezza: dalla pubblica via, un'attesa di privacy minima, alla casa privata, un livello di attesa massimo. Parlare al telefono non è come parlare per strada e scrivere una lettera non è come postare su un social. In forza di tanto la giurisprudenza americana, senza rinunciare alla valutazione di altri requisiti nella operazione di bilanciamento, quali l'utilità sociale a conoscere l'accadimento, il fatto storico o le connotazioni di un individuo, in quanto soggetto pubblico o soggetto che rivesta un ruolo istituzionale, ha elaborato il concetto di "expectation of privacy", in base al quale ha ritenuto di considerare, per determinare se vi sia stata una violazione del diritto alla riservatezza di una persona, tra gli altri, il livello di privacy che la persona si sarebbe ragionevolmente dovuta aspettare in quel contesto.

b) Il diritto ad essere informati e il diritto di accesso alle informazioni

Il diritto ad essere informati non è solo il riflesso passivo del correlativo diritto ad informare, ma è anche espressione manifesta dell'obbligo della Repubblica di eliminare ogni ostacolo che possa impedire al cittadino l'accesso all'informazione e quindi la partecipazione all'organizzazione economica, politica e sociale del Paese. Inizialmente il diritto ad essere informati non è stato ritenuto un'esplicazione dei diritti della personalità meritevole di protezione giuridica, al contrario, non potendo la notizia essere assimilata ad un qualsiasi bene giuridico, è stato visto piuttosto come una tipologia ambigua di

diritto[233], in quanto privo di contenuto reale e di un qualsiasi riferimento oggettivo sul quale poter esercitare una signoria esclusiva, impossibilitato a far valere correlativamente *erga omnes* un dovere di astensione.

Un diritto oltretutto carente di un solido fondamento costituzionale, non potendo, a parere di buona parte della dottrina[234], costituire, l'art. 21 Cost., il riferimento legislativo del diritto ad essere informati: il contenuto della norma costituzionale[235], infatti, non sarebbe stata la libertà di informazione, quanto piuttosto la libertà di manifestazione del pensiero, dalla quale si sarebbe anche potuta evincere l'idea di una libertà di informazione, ma solo in quanto "strumento di manifestazione del pensiero".

L'orientamento di quella dottrina piuttosto obsoleta, intendendo la notizia come "possibilità di conoscenza", ossia come un bene che avrebbe potuto concorrere a formare la personalità, con una precisa influenza nel condizionarne gli svolgimenti, ha ricavato la tutela da apprestare al diritto ad essere informati da una lettura costituzionalmente orientata del combinato disposto degli articoli 2, 3, 21 e 41 Cost., dalla quale sola sarebbe

---

[233]G. B. FERRI, *Diritto all'informazione e diritto all'oblio*, op. cit., 803. Un rilievo centrale svolge «*l'interesse pubblico alla conoscenza, sia come fattore legittimante l'iniziale diffusione della notizia, sia come elemento persistente nel tempo, tale da escludere l'illiceità della successiva rievocazione. E' pertanto necessaria la presenza di un interesse pubblico che giustifichi l'attenzione dei Media nell'immediatezza della loro pubblicazione, ma lo stesso interesse dovrà essere presente anche nelle successive rievocazioni degli accadimenti. Un interesse pubblico nuovo ed attuale e soprattutto prevalente rispetto alla pretesa del singolo a che il proprio passato venga dimenticato*».

[234]N. LIPARI, *Libertà di informazione o diritto ad essere informati*, in *Dir. Radiodiff*, 1978, 5. «*Diritto ad essere informati di 'che e da chi' e soprattutto chi sono gli eventuali titolari di questo diritto*»: difficilmente, per l'Autore, «*le due domande possono trovare una risposta adeguata in chiave di diritto soggettivo della personalità, perché siffatta prospettazione del diritto ad essere informati sembra essere il frutto di troppo facili scorciatoie e disinvolte opzioni di politica del diritto. Anche se nel linguaggio giornalistico si parla di acquisto e vendita di notizie, l'informazione non può essere considerata un 'bene' in senso giuridico, in quanto il bene in senso giuridico non sembra essere tanto la notizia, quanto piuttosto il valore economico dell'esclusività della sua utilizzazione*».

[235]A. PACE, *Replica (XXVIII Congresso nazionale di studio dell'UGC)*, I, Roma, 9-11 dicembre 1977, pag. 178. Per l'Autore, l'art. 21 della Costituzione non garantirebbe la copertura costituzionale esclusivamente al lato attivo della libertà d'informazione, ma anche al profilo passivo (quale libertà ad essere informati). *Contra*: LOIODICE A., *Le radici nella Costituzione*, in JACOBELLI J. (a cura di), *Verso il diritto all'informazione*, Bari, 1991, pag. 95, per il quale, l'art. 21 non può, da solo, essere in grado di sorreggere tale diritto che, pertanto, almeno parzialmente, è sganciato da quella norma. Il diritto all'informazione andrebbe desunto da tutte quelle disposizioni che garantiscono il pieno sviluppo della persona umana, ossia dagli articoli 2, 3 e 21 della Costituzione. Altri ancora, tra cui R. ZACCARIA, *Diritto dell'informazione e della comunicazione*, Padova, 2013, 81, sostengono che: «*il 'diritto ad essere informati' vada ricercato non solo nell'art. 21, ma anche in altre disposizioni costituzionali, configurandolo come un 'diritto sociale fondamentale' che trae il proprio fondamento dalla Costituzione, per la cui realizzazione il legislatore deve intervenire in virtù degli articoli 2 e 3 della Costituzione*». P. BARILE, *Libertà di manifestazione del pensiero*, in *Enciclopedia del diritto*, XXIV, Milano, 1974, 424, il diritto ad essere informati è completamente sganciato dall'art. 21 della Costituzione, la sua base costituzionale sarebbe rappresentata non solo dall'art. 21, bensì da tutte le norme costituzionali che presuppongano che le scelte che il cittadino è chiamato ad effettuare, siano precedute da un'informazione sufficiente.

emersa la protezione costituzionale del diritto all'informazione, quale diritto ad acquisire una serie di notizie, che sono elementi costitutivi del modo di espressione e di realizzazione della personalità all'interno del sistema giuridico.

Che possa trovare copertura costituzionale nell'art. 21 Cost., piuttosto che in una lettura costituzionalmente orientata del combinato disposto degli artt. 2, 3, 21, 41 Cost., il diritto ad essere informati trova comunque il suo fondamento nella Carta costituzionale, assumendo il medesimo rango dell'antagonista diritto alla protezione dei dati personali, nel quale potrebbe impattarsi, svuotandosi di contenuto, ove quello dovesse prevalere, all'esito di un'opera di bilanciamento tra i due. Il legittimo esercizio del diritto alla protezione dei dati personali da parte del suo titolare, infatti, potrebbe vanificare quello all'informazione, così come l'impedimento alla circolazione della notizia, anche solo per il mero decorso del tempo, potrebbe avere pesanti ripercussioni sul legittimo interesse della collettività a conoscere.

Il diritto ad essere informati, a seguito dell'evoluzione tecnologica applicata alla circolazione delle informazioni, ha subito il mutamento della veste giuridica, mutuandosi in 'diritto di accesso' alle informazioni, che verrebbe a trovare la sua base giuridica comunitaria nell'art. 11 della Carta dei diritti dell'Unione[236], che espressamente include nella libertà di espressione, le libertà di opinione e di ricevere o comunicare idee ed informazioni.

Ogni individuo, pertanto, ha diritto di ricevere informazioni o idee, che in tempi relativamente recenti, nel quadro europeo come in quello nazionale, ha avuto un ulteriore *upgrade* che ne ha ampliato il significato, fino a ricomprendervi anche il diritto di accesso ai documenti, ivi compresi quelli delle autorità pubbliche[237].

---

[236]Carta dei Diritti dell'Unione europea, art. 11: «*Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee, senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiere*».

[237]In realtà il tema del diritto ad essere informati, come diritto di accesso a documenti e dati in possesso della P.A. ha una storia e tradizione ormai lunga. Lasciando da parte la diversa tematica del diritto di accesso agli atti del procedimento amministrativo da parte di chi abbia un interesse legittimo, in Italia disciplinato per la prima volta dalla L. 17 agosto 1990 n.241, successivamente modificata a più riprese, il diritto di accesso ai dati e alle informazioni in possesso dell'Amministrazione, ha avuto la sua nascita essenzialmente nel *Freedom Information Act (FOIA)*, emanato negli USA durante la presidenza Johnson e più volte modificato. Nel 1996, poi, dopo che l'amministrazione Clinton ebbe aperto all'uso commerciale di Internet, fu emanato anche l'*Electronic Freedom Informatiion Act (E-FOIA)*. In Italia la richiesta di una normativa che assicuri il diritto di accesso alle informazioni pubbliche, che vada oltre la già ampia legislazione in materia di trasparenza pubblica, non ha ancora trovato piena soddisfazione, anche se forma oggetto di delega al governo nell'ambito della Riforma Madia, approvata con Legge di delega n. 124 del 2015 e dei conseguenti Decreti delegati. Anche l'Autorità italiana di Protezione dei Dati personali ha avuto modo di

Tanto il diritto ad essere informati, quanto la sua recente estrinsecazione, il diritto di accesso alle informazioni e ai dati, potrebbero entrare in collisione con il diritto alla protezione dei dati personali: collisione, che non può non trovare la sua soluzione nel raggiungimento di un giusto e ragionevole equilibrio alla luce della più volte richiamata operazione di ponderazione tra l'interesse della collettività a conoscere, anche attraverso l'accesso alle informazioni, e il correlativo diritto della persona interessata al rispetto della vita privata e alla protezione dei dati relativi alla sua persona.

Nella scelta tra la tutela del cittadino 'a conoscere' e la tutela dell'antagonista diritto dell'interessato a che le informazioni inerenti la sua sfera privata non siano divulgate, o quanto meno a che la loro circolazione non sia eterna, occorrerà tener conto di diversi criteri di valutazione, quali la natura dell'informazione, il suo carattere sensibile per la vita privata, l'interesse del pubblico a riceverla[238], che potrà anche variare a seconda del ruolo che la persona rivesta nella vita pubblica. L'operazione di bilanciamento, pertanto, dovrà consistere nella valutazione di tutti gli elementi a favore e contro le parti in gioco e non potrà che estrinsecarsi in un giudizio *ex post*, che vedrà di volta in volta, a seconda delle circostanze del caso concreto, la prevalenza dell'uno o del contrapposto interesse.

Orientamento ormai consolidato nella prassi delle autorità giudiziarie ed amministrative ed oggetto di ulteriore recente conferma da parte dei giudici di legittimità[239], i quali hanno ritenuto che anche rispetto ad un fatto accaduto più di trent'anni fa, considerata la 'notorietà' del protagonista, sia possibile la permanenza dell'interesse pubblico alla sua rievocazione, prevalendo il diritto alla conoscenza dello stesso, sul correlativo diritto all'oblio.

---

intervenire numerose volte su questi temi, soprattutto con riguardo ai casi in cui la legge impone la pubblicazione online di delibere o altri documenti della P.A., o prevede che forme di comunicazione al pubblico, stabilite dalla legge, debbano essere oggetto anche di comunicazione digitale.

[238]Un *uomo pubblico* ha meno diritto alla tutela dei dati; al contrario, soprattutto se riveste ruoli istituzionali, è necessario che le sue referenze e i suoi trascorsi siano noti. E' quanto anche sottolineato nella *Dichiarazione del Consiglio dei Ministri del Consiglio d'Europa*, approvata a Strasburgo il 12 febbraio 2004 – *Dichiarazione sulle libertà del discorso politico nei media* – laddove ha evidenziato che i particolari della vita privata delle figure pubbliche e dei loro familiari non devono essere rivelati, a meno che tali informazioni non siano direttamente pertinenti, in quanto «*gettano luce sulle modalità con cui tali figure pubbliche svolgano le funzioni alle quali sono state chiamate, o comunque quelle informazioni risultino importanti ai fini della conoscenza storica*».

[239]Cass. Pen., Sez. V, sentenza del 3 agosto 2017, n. 38747, in *Corr. giur*., 2018, 8-9, 1105 con nota di SIROTTI GAUDENZI. Nel caso specifico si è trattato della regolamentazione del diritto di stampa (diffusione di notizie), in contrapposizione al diritto all'oblio esercitato dal Principe di Savoia per la notizia riguardante i fatti risalenti all'uccisione di circa 39 anni fa, del giovane tedesco Dirk Hamer.

In particolare si trattava di un articolo, pubblicato nel 2007 su un noto quotidiano nazionale, relativo ad un fatto di cronaca nell'ambito del quale vi era la rievocazione di un altro accadimento verificatosi tre decenni prima.

Si trattava dell'oscura vicenda, verificatasi nel 1987, in cui perse la vita un giovane cittadino tedesco, Dirk Hamer, a causa di un colpo di fucile esploso da Vittorio Emanuele di Savoia. Nel commentare con tono critico la partecipazione del principe alla riapertura di una ex residenza sabauda – la reggia di Venaria Reale – l'articolista si riferiva all'erede degli ex monarchi, apostrofandolo come "quello che usò con disinvoltura il fucile all'isola di Cavallo, uccidendo un uomo".

Ne scaturiva un defatigante processo penale a carico dell'articolista e del direttore del giornale per il reato di diffamazione a mezzo stampa, correlato anche alla gratuità della riproposizione della notizia a distanza di moltissimo tempo e quindi alla lesione del diritto all'oblio del Savoia. La Suprema Corte, nel confermare la sentenza assolutoria d'Appello, ha avuto modo di precisare come preliminarmente dovessero essere rispettati i canoni di verità (e il fatto storico si era verificato in quei termini, a prescindere dall'assenza di responsabilità penale per il Savoia) e continenza espressiva, trattandosi di un giudizio critico e non di un attacco smodato. Per quel che più interessa ai nostri fini, i giudici di legittimità hanno ritenuto la rievocazione sicuramente assistita da un 'interesse pubblico', giacchè l'informazione era stata pubblicata in occasione di un fatto di cronaca, cui partecipò Vittorio Emanuele, la cui storia, in quanto figlio dell'ultimo re d'Italia, rivestiva senz'altro rilievo pubblico, a parere di quei giudici, sia in considerazione delle vicissitudini giudiziarie, che in quegli anni lo avevano interessato, sia per le anacronistiche rivendicazioni reali, che lo stesso aveva fatto.

I giudici di legittimità hanno concluso, precisando che: "...il diritto all'oblio sulle proprie vicende personali […] si deve confrontare, invero, col diritto della collettività ad essere informata e aggiornata sui fatti da cui dipende la formazione dei propri convincimenti, anche quando da essi derivi discredito alla persona che è titolare di quel diritto. Sicché non può dolersi Savoia della riesumazione di un fatto certamente idoneo alla formazione della pubblica opinione"[240].

Il diritto di sapere e la libertà di comunicare non possono, pertanto, cancellare il bisogno d'intimità, il diritto di sviluppare liberamente la personalità, di costruire la propria sfera

[240]Cass. Pen., Sez. V, sentenza del 3 agosto 2017, n. 38747, cit..

privata e di veder rispettata la propria dignità, ma solo a condizione che dall'opera di bilanciamento il diritto della collettività ad essere informata, considerando la specificità soggettiva e fattuale della vicenda, la sua valenza storica e la notorietà del protagonista, non risulti essere prevalente.

5) Il diritto di cronaca ed il diritto all'oblio: i confini ridisegnati dalla sentenza CEDU 'AFFAIRE M.L. ET W.W. c. ALLEMAGNE del 28 giugno 2018 e la palese distorsione del diritto all'oblio operata dalla Corte di Cassazione con la pronuncia 24 giugno 2016, n. 13161

Il diritto di cronaca, che rientra nella più vasta categoria delle libertà di manifestazione del pensiero e di stampa, riconosciute dall'art. 21 della Costituzione, si estrinseca nel potere/dovere del giornalista di portare a conoscenza del lettore fatti d'interesse pubblico, con la precisazione che il diritto di manifestare il proprio pensiero, solo entro certi limiti può identificarsi con il diritto di cronaca, in quanto, viceversa, quest'ultimo, nel limitarsi ad una rappresentazione oggettiva della realtà, della quale il soggetto narrante ha avuto cognizione, priva di qualsivoglia considerazione personale critica, rappresenta sicuramente un *minus* rispetto alla più ampia categoria del diritto a poter manifestare il proprio pensiero e ad informare[241].

Anche l'esercizio del diritto di cronaca, che negli ordinamenti democratici assolve alla funzione d'informare, riportando fedelmente i fatti e prescindendo dai personalismi del giornalista, affinché ciascuno possa liberamente orientarsi rispetto ad avvenimenti di rilevanza pubblica, è, infatti, un'estrinsecazione del più ampio diritto di manifestazione del pensiero e d'informazione e, come questi, viene a trovare un limite nell'esigenza di tutela della reputazione e dell'identità personale del protagonista del fatto oggetto di cronaca e, più in generale, nell'esigenza di tutela della sua privacy[242].

---

[241]Così per G. GIACOBBE, *Il diritto all'oblio (Atti del Convegno di studi, 17 maggio 1977)*, op. cit., 22: «*Il riconoscimento del diritto di manifestazione del proprio pensiero non si indentifica con il diritto di cronaca, il quale, solo entro certi limiti, può essere rappresentato come espressione del diritto di manifestare il pensiero. Infatti la manifestazione del pensiero si può configurare come un apporto critico di colui che si esprime, mentre la cronaca costituisce soltanto rappresentazione di una realtà della quale si è avuta cognizione e che si porta a conoscenza del pubblico*».

[242]Cass. Civ., Sez. III, sentenza del 25 giugno 1967, n. 1959, in *Rep. Giur. It.*, 1959. L'esercizio legittimo del diritto di cronaca comporta, quali oneri per il giornalista, oltre alla necessità di riportare i farri in maniera oggettiva, privi di qualsiasi connotazione critica, anche quella di garantire, quale connotato essenziale e caratteristico di un regime democratico, l'accesso del pubblico a tutte le fonti di informazione idonee ad incidere sullo sviluppo culturale e morale dei singoli e dei gruppi e ad assicurare la libera formazione del loro orientamento politico e sociale.

La qual cosa determina che, nell'esercizio del diritto di cronaca, l'intromissione nella sfera privata degli individui sia giustificata solo dalla presenza di "un interesse pubblico alla conoscenza di fatti oggettivamente rilevanti per la collettività[243]", con la precisazione che, talvolta, anche la narrazione di fatti privati potrebbe risultare di pubblico interesse, qualora dagli stessi possano desumersi elementi di valutazione sulla personalità e sulla moralità di un uomo pubblico, che proprio per il fatto di essere pubblico, deve godere della fiducia dei cittadini[244].

Il diritto di sapere, la libertà di comunicare, la trasparenza, non possono in ogni caso cancellare il bisogno d'intimità, il diritto di sviluppare liberamente la personalità, di non veder lesa la propria sfera privata, nella sua nuova dimensione, faticosamente ricostruita con la complicità del decorso del tempo trascorso rispetto ad una vicenda obliata, soprattutto quando la conoscenza degli aspetti personalissimi della vita delle persone nulla aggiunge alla comprensione dei fatti narrati, servendo solo ad alimentare un insano pettegolezzo.

Lo sviluppo tecnologico, tra l'altro, i motori di ricerca e soprattutto Internet, offrendo al giornalista l'accesso a molte più informazioni con la possibilità di divulgarle, hanno contribuito alla nascita di problemi ulteriori per le persone interessate, le cui vicende potrebbero essere lette ovunque e per un tempo indefinito, con gravi compromissioni della sfera privata dell'individuo.

Nonostante tutto, i due diritti non possono e non devono entrare in collisione tra loro, rappresentando l'uno la demarcazione ed il confine dell'altro. Due diritti che vanno resi compatibili, attraverso una costante, spesso non facile, opera di bilanciamento finalizzata alla ricerca di un giusto equilibrio che vedrà il prevalere ora dell'uno, ora dell'altro, sempre tenendo presente, come ha ribadito recentemente la Suprema Corte di

---

[243]Cass. Pen., 6 dicembre 1998, n. 1473, in *Giust. Pen.*, 1999, pag. 687. Non è sufficiente la sola curiosità del pubblico a giustificare la diffusione di notizie sulla vita privata altrui, occorrendo, invece, che quelle notizie siano di oggettivo interesse per la collettività. Il limite dell'utilità sociale della notizia, che è piuttosto elevato nell'ipotesi di conflitto fra il diritto di cronaca e di critica cin aspetti concernenti la vita privata dell'individuo, si abbassa notevolmente ove si tratti di fatti di natura non privata, relativamente ai quali va tenuto conto della notorietà della persona alla quale i fatti si riferiscano.

[244]UBALDI, *Diffusione e diritto di cronaca: più spazio alla libertà di stampa, a patto che le dichiarazioni siano d'interesse pubblico*, in *Dir. giustizia*, 2003, pag. 16. Per i giudici la valutazione della violazione della sfera privata dell'individuo, a mezzo l'esercizio del diritto di cronaca, non è per l'uomo pubblico la stessa che per il privato cittadino. Come nel sistema americano, l'uomo pubblico, più degli altri, deve sottostare alle esigenze della cronaca ed anche alla curiosità dell'informazione, mentre il privato cittadino vanta un diritto maggiore ad essere tutelato nella sua intimità. Grosso modo tutti i giudici si regolano alla stessa maniera, anche se con la nuova legge qualcosa è cambiato.

Cassazione[245], la prevalenza dell'attività d'informazione rispetto ai diritti personali della reputazione e riservatezza.

A parere dei giudici di legittimità, infatti, se è vero che l'art. 1 della Costituzione assegna al popolo la sovranità perché sia esercitata nei limiti della 'Carta', il presupposto per un "pieno, legittimo e corretto esercizio di questa sovranità è che essa si realizzi mediante tutti gli strumenti democratici a tal fine predisposti dall'ordinamento, tra i quali un posto e una funzione preminenti spettano all'attività d'informazione[246]".

In una pronuncia del 2014[247] i giudici di legittimità, in tema di rapporto tra diritto all'informazione e tutela della privacy, sono giunti alla conclusione che giornalisti ed editori sono tenuti a risarcire i danni morali ed esistenziali per la violazione del diritto alla riservatezza, nel caso in cui i protagonisti di un servizio giornalistico, sebbene non citati espressamente, siano comunque di fatto riconoscibili.

In senso opposto si sono orientati i giudici di Strasburgo in una recentissima pronuncia (Affaire M.L. ET W.W. c. Allemagne) [248], nella quale hanno riconosciuto che gli archivi online di giornali e radio siano un bene da proteggere, in quanto garantiscono il diritto della collettività a ricevere notizie d'interesse generale che, non essendo attenuato dal passare del tempo, comporta la prevalenza del diritto a ricevere la diffusione d'informazioni su procedimenti penali, anche a distanza di anni, rispetto al diritto all'oblio.

E' ciò che ha stabilito la Corte europea dei diritti dell'uomo in una sua pronuncia, respingendo il ricorso di due cittadini tedeschi condannati all'ergastolo per omicidio e scarcerati con una misura di messa alla prova. A parere dei due ricorrenti il mancato accoglimento della loro richiesta di anonimizzazione di alcuni reportage che li riguardavano, avrebbe violato l'art. 8 CEDU, che assicura il rispetto della vita privata. Tesi respinta da Strasburgo che ha fatto pendere l'ago della bilancia a favore dell'art. 10 della Convenzione, privilegiando la libertà di espressione.

In quella pronuncia, in particolare, i giudici, pur avendo riconosciuto il diritto al rispetto della vita privata, che include anche quello di non essere ricordato per fatti del passato legati a condanne penali, hanno ritenuto prevalente il corrispondente diritto della

[245]Cass. Civ., Sez. III, sentenza del 9 luglio 2010, n. 16236, cit.
[246]Cass. Civ., Sez. III, sentenza del 9 luglio 2010, n. 16236, cit
[247]Cass. Civ., Sez. III, sentenza del 27 gennaio 2014, n.1608.
[248] Corte eur. dir. uomo, sentenza 28 giugno 2018, *Affaire M.L. ET W.W. c. Allemagne,* in.

collettività a ricevere informazioni sui procedimenti penali e sulla scarcerazione dei colpevoli, così come a poter svolgere ricerche su eventi del passato.

Non solo!

I giudici di Strasburgo, nell'intento di mettere in guardia dai rischi di un accertamento in sede giudiziaria delle richieste di rimozione presentate da individui a danno degli organi di stampa, che potrebbe spingere gli organi d'informazione ad omettere notizie d'interesse generale, ha definito alcuni parametri cui le autorità nazionali debbono attenersi per raggiungere un equo bilanciamento dei diritti in gioco.

Per i giudici europei, prima di tutto, è necessario verificare che la notizia contribuisca ad un dibattito d'interesse generale; di non secondaria importanza, risulterebbero gli altri parametri, quali la notorietà della persona, l'oggetto del reportage, il comportamento precedente della persona interessata, il contenuto, la forma e le ripercussioni della pubblicazione e, all'occorrenza, anche le modalità con le quali sono stati acquisiti eventuali documenti.

La Corte ha, infine, lanciato l'allarme sui rischi della libertà di stampa laddove si chieda, in una fase successiva rispetto alla pubblicazione, un accertamento sulla liceità della stessa pubblicazione. In questi casi, infatti, potrebbe accadere che gli editori arrivino a ritenere più conveniente non curare gli archivi: rischio assolutamente da evitare, anche attraverso il rafforzamento della libertà di stampa.

Il rapporto tra diritto alla riservatezza e diritto di cronaca non può che essere un rapporto dialettico che vedrà, come l'esperienza insegna, la prevalenza dell'uno o dell'altro diritto, in considerazione delle circostanze del caso concreto e che potrebbe anche non essere affrontato come contraddittorio, avendo la giurisprudenza tracciato una possibile terza via.

Infatti, relativamente alle 'notizie archiviate in Rete a fini di cronaca giornalistica', è riconosciuto al soggetto, cui le informazioni si riferiscono, il diritto di richiedere l'aggiornamento dei contenuti al fine di tutelare la propria reputazione. I giudici di legittimità, nel 2012[249], hanno affrontato la questione della raggiungibilità delle notizie archiviate nella edizione online dei giornali, a partire da una ricerca, sul motore, da parte dell'utente, evidenziando come tali ricerche permettano l'accesso a contenuti

[249]La questione è stata affrontata dalla Cass. Civ., Sez. III, sentenza del 5 aprile 2012, n. 5525.

decontestualizzati, che rischiano, a distanza di tempo, di ledere la reputazione del soggetto, nonostante si tratti di contenuti legittimamente archiviati a scopo giornalistico.
In casi del genere, quando la rimozione dei contenuti non sia possibile a fronte delle legittime finalità dell'archiviazione, i giudici di legittimità hanno stabilito che sia diritto dell'interessato richiedere che il contenuto archiviato venga aggiornato per tutelare la sua reputazione, altrimenti continuamente compromessa ed esposta ad una gogna mediatica *ad libitum,* sulla base di fatti verificatisi e conclusisi molti anni prima.
Soluzione, suggerita nel 2012, e quindi precedente alla Google Spain, con la quale la Suprema Corte ha tracciato una terza via circa le modalità con cui affrontare i casi aventi ad oggetto trattamento dati per finalità lecite, tuttavia incidente sul fattore reputazionale, e quindi sull'identità digitale, in un senso più ampio rispetto alla sola questione della privacy e della tutela dei dati personali.
La possibilità di richiedere l'aggiornamento di un contenuto, ove questo non possa essere rimosso, perché legittimamente tutelato dal diritto d'informazione, rappresenta senza dubbio, un punto d'incontro tra l'interesse legittimo del singolo alla tutela della propria reputazione, ove questa dipenda solo dalla permanenza o meno on-line della notizia, e l'interesse del pubblico ad acquisire informazioni, avendone libero accesso.
Ma la posizione assunta dalla giurisprudenza di legittimità nella pronuncia del 2012, ed ancor più in successive pronunce, risulta piuttosto scivolosa, fornendo un'interpretazione tanto inedita quanto pericolosa del diritto all'oblio. Stupisce che i giudici di legittimità non abbiano tenuto, in alcun modo, conto della giurisprudenza, se non italiana almeno europea, che mai in passato aveva chiesto la rimozione dei contenuti dell'archivio di un giornale, ben sapendo che ciò avrebbe indebolito fortemente la libertà di stampa, fulcro di una società democratica.
Nella pronuncia del 2016[250], la Corte ha stabilito che «un articolo di cronaca su un accoltellamento in un ristorante dovesse essere cancellato dall'archivio digitale perché, pur essendo corretto, raccontando verità e non travalicando i limiti di legge, aveva prodotto un danno ai ricorrenti, cioè i soggetti attivi della vicenda giudiziaria».
La Cassazione ha richiamato la celebre sentenza Google Spain, C-131/12, che per prima sancito l'esistenza di un diritto ad essere dimenticati, nonché le linee guida del W.P. 29, redatte nel 2014, successivamente alla famosa pronuncia europea.

[250] Cass. Civ., Sez. I, sentenza del 24 giugno 2016, n. 13161.

Ma gli indirizzi richiamati non sono stati affatto rispettati: la Corte di Giustizia dell'Unione Europea, in quell'occasione, aveva sancito il diritto alla de-indicizzazione dai motori di ricerca delle notizie riguardanti il ricorrente, se lesive della sua dignità, denigratorie, non più rilevanti per l'opinione pubblica, ma mai ha stabilito che tali informazioni possano essere rimosse dagli archivi dei giornali.

Il riferimento costante operato dalla giurisprudenza europea al diritto all'oblio è volto alla rimozione del collegamento alla notizia che compare nella lista dei risultati fornita dal motore di ricerca, mai alla recisione della notizia in sé.

Anche le linee guida del W.P. 29, nel paragrafo 18, confermano l'indirizzo appena esposto, giungendo ad affermare che la de-indicizzazione non si riferisca ai motori di ricerca di piccola portata, come quelli dei giornali on-line. Pertanto, per i siti di testate giornalistiche non vi sarebbe neppure l'obbligo di de-indicizzare la notizia dal motore di ricerca interno al sito, nonché, *a fortiori,* di rimuovere l'intero contenuto dell'articolo.

Con la pronuncia del 2016, i giudici di legittimità sono andati ben oltre il diritto del singolo alla de-indicizzazione dei risultati offerti da un motore di ricerca, determinando una palese distorsione di quanto sino a quel momento affermato rispetto al diritto all'oblio, stabilendo che buona parte dell'informazione giornalistica scivoli col tempo oltre i confini dell'essenzialità.

Ma al di là del bilanciamento tra interessi confliggenti, ciò che si contesta è il rimedio adottato dalla Corte, che lungi dal disporre la de-indicizzazione, ha previsto la definitiva rimozione dell'articolo: un rimedio sovradimensionato, che comporta una definitiva condanna a morte della memoria, determinando un insanabile *vulnus* nell'informazione.

La decisione domestica, nello stabilire la rimozione dei contenuti informativi allorquando la semplice de-indicizzazione non consenta una tutela completa dei diritti degli interessati all'oblio, stranisce maggiormente se confrontata con la giurisprudenza europea, che mai prima d'ora è giunta a tali aberranti approdi.

Nel caso Wegrzynowski and Smolczewski c. Polonia[251], nonostante i ricorrenti lamentassero che un articolo ritenuto lesivo della loro reputazione dall'autorità giudiziaria continuasse a permanere sul sito del giornale che lo aveva pubblicato, la Corte europea dei diritti dell'uomo ha ritenuto che il rimedio della completa rimozione di un articolo dall'archivio di un giornale on-line avrebbe rappresentato un rimedio sproporzionato.

[251] Corte europea dei diritti dell'uomo, 16 luglio 2013, application no. 33846/07.

La Corte di Strasburgo ha privilegiato altri strumenti di tutela meno invasivi della libertà di espressione, mediante l'inserimento di una nota o di un collegamento ipertestuale che rendano conto dell'intervenuta sentenza a favore dei ricorrenti, che aveva riconosciuto la violazione dei loro diritti. Lungi, pertanto, dall'avallare il rimedio della rimozione *tout court* dell'articolo, in quell'occasione la Corte ha privilegiato i rimedi della contestualizzazione e dell'aggiornamento della notizia qualificata obsoleta e lesiva.
A ben vedere la Corte di Cassazione, con la pronuncia del giugno 2016, si è palesemente discostata da questa linea, paventando conseguenze tanto preoccupanti quanto inaccettabili; ma si spera che si tratti, più che di un'affermazione di principio, di una scelta, frutto dell'approccio casistico adoperato dalla giurisprudenza di legittimità nelle decisioni, legato alle irripetibili peculiarità delle singole fattispecie e non costituisca, in alcun modo, l'abbrivio per l'affermazione di un nuovo diritto alla rimozione di un articolo dalla versione online di un giornale.

6) La ricerca di un giusto equilibrio tra tutela dei dati personali e libertà d'informazione estrinsecantesi nell'attività giornalistica

In considerazione del fatto che il diritto di cronaca, e più in generale l'esercizio dell'attività giornalistica, potrebbero entrare in collisione con il diritto alla protezione dei dati personali e con la sua costola, il diritto ad essere dimenticati, e considerata anche la natura e il rango costituzionale di entrambe le pretese, la soluzione del conflitto non può che trovare soluzione nel contemperamento e ponderazione delle due libertà[252].

[252]Principio enunciato per la prima volta da Cass. Civ., Sez. III, sentenza del 18 ottobre 1984, n. 5259, in *Foro it*. 1984, I, 2711 e successivamente ribadito da Cass. Civ., Sez. III, sentenza del 29 maggio 1996, n. 4993, in *Foro it*, 1996, I, 2368; Cass. Civ., Sez. III, sentenza del 7 febbraio 1996, n. 982, in *Foro it*, 1996, 12511 con nota di PALMIERI. In precedenza il rapporto tra il diritto di cronaca e la pretesa alla riservatezza non sempre era considerato un rapporto tra antagonisti. Al contrario, il diritto di cronaca era considerato come 'l'interlocutore naturale' di qualsiasi diritto della personalità in quanto, in considerazione della dimensione antropologica, cui è improntato il nostro ordinamento giuridico, tutti i diritti riconosciuti devono essere funzionali allo sviluppo della persona. In altri termini, poiché la scelta operata dal nostro costituente è stata quella di porre al centro del sistema giuridico la persona, nella sua dimensione individuale e sociale, la cosa comporta che tutti i diritti e le libertà riconosciuti dalla Carta costituzionale, o da qualsiasi altra disposizione di legge, avrebbero dovuto essere funzionalizzati al suo sviluppo, con l'ovvia conseguenza che tra quei diritti non avrebbe potuto esservi confliggenza, bensì integrazione, in quanto tutti convergenti verso la medesima finalità. Opinione tuttavia, che non sempre ha trovato riscontro nella realtà delle aule giudiziarie che, nella maggior parte dei casi, hanno visto trattare vicende nelle quali si sono evidenziati forti conflitti per la cui soluzione si è reso necessario il ricorso alla tecnica dell'equo bilanciamento.

In tutti i casi aventi ad oggetto lagnanze circa la violazione dell'una o dell'altra pretesa, i giudici di merito e di legittimità, secondo una giurisprudenza ormai consolidata, si sono orientati, ove rispettati i precetti del Codice deontologico, nel senso di ritenere 'prevalente' il diritto di cronaca rispetto al diritto all'oblio, che verrebbe ad essere compromesso dalla ripubblicazione dell'informazione, solo in presenza dei tre requisiti fondamentali: dell'utilità sociale della notizia (il c.d. interesse pubblico), della verità dei fatti divulgati e della forma civile dell'esposizione ispirata a serena obiettività, con esclusione di ogni intento denigratorio.

a) verità oggettiva della notizia pubblicata

Il requisito della verità, momento di mediazione tra '*ius narrandi'* e tutela della reputazione, richiede che l'oggetto dell'informazione diffusa corrisponda ad una verità oggettiva[253], frutto di un serio e diligente lavoro di ricerca dei fatti esposti, il cui obbligo grava su coloro che esercitano l'attività di cronaca, dal momento che la narrazione di fatti non veri verrebbe a ledere non solo l'interessato, ma la stessa collettività nelle sue aspettative ad una informazione corretta, finalizzata alla formazione di una retta opinione. Per verità deve intendersi la sostanziale corrispondenza tra i fatti come sono accaduti e il modo in cui gli stessi sono narrati, la qual cosa comporterà l'obbligo per il soggetto narrante di accertare l'attendibilità delle fonti e soprattutto il loro aggiornamento, qualora i fatti abbiano avuto ulteriori evoluzioni[254]. Per la verità, i giudici di legittimità, in alcune loro pronunce[255], hanno in qualche modo attenuato l'obbligo del controllo

[253]Così R. ZACCARIA – A. VELASTRO, *Diritto dell'informazione*, Padova, 2010, pag. 117. In questo senso l'art. 2 della legge professionale dei giornalisti (l. 69/1963) obbliga al rispetto della '*verità sostanziale dei fatti*'. L'ordinamento quindi, ha espressamente previsto per il giornalista l'obbligo di '*attenersi a una verità legata allo svolgimento degli accadimenti quotidiani*'. Avere una giustificazione, più o meno plausibile delle proprie credenze sui fatti, non sempre coincide con la loro verità. In altre parole '*la relatività della giustificazione non implica la relatività della verità", difatti 'giustificato non è sinonimo di vero*'.

[254]G. PUGLIESE, *Diritto di cronaca e libertà di pensiero*, in *Foro it*. 1958, I, pag. 186. Per salvaguardare l'attuale identità sociale di una persona, occorre garantire, oltre alla contestualizzazione, l'aggiornamento della notizia; aggiornamento e rettifica che devono sempre intervenire per i fatti sopravvenuti che definiscono meglio quelli passati e, quindi, la reale e attuale identità del soggetto. Le vicende personali infatti, fanno arte della vita dell'individuo che è in continua evoluzione per cui, l'informazione giornalistica può tradursi in una rappresentazione del soggetto parziale o distante dalla reale identità della persona, qualora si riferisca ad eventi ormai superati e non più significativi, per la reale valutazione di una persona nel presente. Rientra, tra l'altro, nella Carta dei doveri del Giornalista (*Documento CNOG-FNSI dell'8 luglio 1993*), «*l'obbligo per il giornalista dell'osservanza delle norme di legge, dettate a tutela della personalità altrui, il rispetto della verità sostanziale dei fatti, il dovere di rettifica di notizie che risultino inesatte nonché il dovere di porre riparo agli eventuali errori*».

[255]In questi termini si è espressa la Cass. SS.UU., 30 maggio 2001, n. 37140 (caso "Galero"), che ha ritenuto utile l'affrancamento del giornalista dall'osservanza dell'obbligo di controllo, nei casi in cui un'indagine

dell'attendibilità delle fonti da parte del giornalista, avendo riconosciuto come la rapidità con la quale il giornalista contemporaneo svolge il suo servizio informativo talvolta sia incompatibile con una precisa osservanza di quell'obbligo. I tempi e le modalità di apprendimento di alcune notizie, infatti, sono tali che un approfondito controllo comporterebbe l'impossibilità di pubblicarle tempestivamente, con innegabile pregiudizio dell'immagine e del credito della testata.

Il rispetto dell'obbligo della verità comporta, infine, l'assenza della cd 'verità alterata', ossia la presenza di allusioni, sottintesi, espressioni dubitative ad opera del giornalista che, al contrario, dovrà rappresentare la 'realtà oggettiva', che richiede che i fatti e le situazioni siano effettivamente accaduti, considerato che il suo ruolo è quello di mero mediatore tra il fatto e l'opinione pubblica e, quindi, di neutrale informatore.

b) continenza della notizia

La continenza richiede l'adeguatezza del linguaggio, con cui la notizia è riportata, alle esigenze richieste dalla cronaca. Il giornalista ha l'obbligo di adoperare termini 'proporzionati' alla gravità dell'accaduto ed il limite risulterà superato qualora, pur risultando il narrato vero, sia, tuttavia, impiegato un lessico improprio, che potrebbe trasformarsi in attacco personale al suo protagonista, qualora le espressioni dovessero risultare denigratorie e sovrabbondanti rispetto alle finalità della cronaca[256]. E' opinione,

---

rigorosa sul fondamento delle fonti, comporterebbe non solo un intralcio nell'informazione, ma inaridirebbe all'origine la vivacità e l'interesse della notizia, togliendo alla stessa il carattere dell'attualità che ne rappresenta la nota saliente. Ancora, Cass. Civ., Sez. I, sentenza 8 gennaio 2015, n. 13941 che ha di recente chiarito la differenza tra cronaca e storia: la prima presuppone l'immediatezza della notizia e la tempestività dell'informazione e, in presenza dell'interesse pubblico ad una notizia tempestiva, l'esigenza di velocità potrebbe comportare un qualche sacrificio dell'accuratezza della verifica sulla verità della notizia e sulla bontà della fonte dalla quale si è appresa. La storia, invece, ha ad oggetto fatti e comportamenti distanti nel tempo, sicché si giustifica meno il menzionato sacrificio dell'accuratezza della verifica.

[256]Trib. Milano, 1° ottobre 1999, in *Resp. Civ.*, 2000, 1448: dalla pronuncia emerge, tra l'altro, che la continenza consta di un 'aspetto formale', consistente nell'onere di presentazione misurata della notizia e di un 'aspetto sostanziale', che richiede la necessità di presentare e commentare la notizia in modo tale, da mettere a conoscenza il lettore dell'effettiva posizione dell'accusato. «*Il giornalista, nell'operazione di redazione dell'articolo giornalistico, deve scegliere le espressioni linguistiche idonee a comunicare la notizia. L'uso delle espressioni non è frutto di una scelta discrezionale, perché devono essere scartate tutte quelle che possono fornire una falsa rappresentazione del fatto accaduto nonché quelle e falsamente lesive della reputazione altrui. Le espressioni usate non devono essere oggettivamente denigratorie della sfera di tutela riconosciuta dall'Ordinamento giuridico; la propalazione è giustificata se mantenuta in termini strettamente necessari per esercitare il diritto, perché nessuno può erigersi a giudice dell'indegnità altrui*». Così anche per Cass. Pen., Sez. V, 19 aprile 2006 n. 19148. Requisito, quello della continenza, correlato alle modalità della comunicazione della notizia che comporta la necessità di riportare il fatto nei suoi elementi oggettivi, così come appresi dalla fonte. La comunicazione della notizia dev'essere priva di artifici, consistenti nell'uso di un linguaggio colorito e incauto, nell'adoperare termini tali da comunicare

tra l'altro abbastanza consolidata in dottrina,[257] che, qualora siano in discussione valori particolarmente importanti, quali la professionalità o l'etica di un giornalista, la valutazione della continenza venga a restringersi, per cui non dovrà essere superato il limite della stretta necessità delle espressioni che potrebbero rivelarsi offensive.

c) interesse pubblico alla conoscenza dei fatti

Il diritto alla protezione dei dati intanto retrocede rispetto al diritto di cronaca, in quanto vi sia l'interesse della collettività a che informazioni appartenenti alla sfera privata siano comunque diffuse e conosciute. Sarà dunque l'interesse pubblico (creazione giuridica oggetto di un lungo dibattito in dottrina e presso le Corti di merito e di legittimità) a paralizzare il diritto all'oblio.

Sebbene comunemente si affermi che l'utilità sociale consista "nell'esigenza di oggettive ragioni culturali, morali, ideali o politiche alla conoscenza dei fatti"[258], la locuzione non sempre ha presentato contorni ben definiti. Così nella riproduzione, a distanza di trent'anni, della pagina di un giornale recante un fatto di sangue al solo scopo di pubblicizzare un gioco a premi, i giudici di merito romani[259] non hanno giustamente ravvisato l'attualità di un interesse pubblico alla sua riproposizione, avendo al contrario, ritenuto la lesione della sfera privata dell'interessato, protagonista del fatto, dal momento

---

un messaggio sottinteso diverso, nell'accostare l'evento narrato ad altro evento, in modo da attribuire al soggetto un fatto diverso e ulteriore rispetto a quello originario. Tutto questo può, indubbiamente produrre un effetto lesivo, con la conseguenza che, qualora l'artificio adoperato dal giornalista condizioni la genuinità della notizia e quindi, «*ove si superi il limite della continenza, si realizzerebbe una lesione del bene tutelato*».

[257]A. SUTERA SARDO, *Dolo e diritto di critica*, in *Dir. pen. e processo*, 1999, n.998.

[258]Cass. Civ., Sez. I, sentenza del 22 giugno 1985, n. 3769, cit. La locuzione 'utilità sociale' pur nella sua varietà di significati, coincide con l'interesse della collettività alla conoscenza di determinati fatti di rilievo sociale. Per questo, a chi diffonde una notizia, viene imposto l'obbligo di verificare preliminarmente l'interesse che il pubblico possa avere per quei fatti. Interesse effettivo che non deve confondersi col 'desiderio di conoscenza', ossia con l'esigenza di soddisfare la propria curiosità. A conferma di ciò, i giudici di legittimità ritengono che: «le vicende private di persone impegnate nella vita politica o sociale, siano d'interesse pubblico quando, dalle stesse possano desumersi elementi di valutazione della personalità o della moralità di chi debba godere della fiducia dei cittadini. Non è, pertanto, la semplice curiosità del pubblico a giustificare la diffusione di notizie sulla vita privata altrui, perché è necessario che tali notizi rivestano un interesse oggettivo per la comunità» (Cass. Pen., Sez. V, sentenza del 9 ottobre 2007, n. 4267). In altre parole, il requisito dell'utilità sociale corrisponde alla necessità a che l'informazione sia innanzitutto uno strumento per permettere al fruitore di essa di rendersi conto dei fatti storici narrati, perché ne tragga una concreta possibilità di apprendimento e di miglioramento della comprensione della realtà contemporanea. In tal modo l'informazione avrà contribuito all'evoluzione della coscienza sociale degli individui.

[259]Trib. Roma, 15 maggio 1996, n. 2319, in *Foro it.* 1996. E' il provvedimento emesso per i caso del 'killer del Messaggero' nel quale i giudici romani hanno condannato la testata giornalistica per la ripubblicazione di un sua pagina per soli motivi di lucro, in assenza di qualsiasi utilità sociale per i fruitori, all'informazione.

che lo stesso aveva regolarmente scontato la pena e si era utilmente reinserito in società. I giudici hanno, pertanto, ritenuto che le informazioni sulla vita privata, capaci di ledere la reputazione, non debbano essere ripubblicate, a meno che la loro conoscenza non sia utile alla società[260].

In altri casi, invece, all'esito di un'operazione di ponderazione degli interessi in gioco, relativamente al fatto di cronaca che ha visto coinvolto il giocatore della Lazio, Luciano Re Cecconi, che avendo per scherzo simulato una rapina ad un gioielliere amico (poi processato e assolto per legittima difesa putativa), fu da questi ucciso, il diritto alla riproposizione dell'episodio è stato ritenuto prioritario, facendo recedere l'antagonista pretesa al silenzio. I giudici di legittimità, infatti, nel confermare la sentenza di secondo grado, nell'operazione di bilanciamento tra il diritto al silenzio ed il diritto di cronaca, estrinsecatosi in una ricostruzione romanzata dell'accaduto, da mandare in onda sulle reti RAI, hanno ritenuto la prevalenza del secondo, stante l'interesse della collettività alla conoscenza dell'accaduto, che ancora assolveva ad una funzione educativa e sociale[261].

Per i giudici di legittimità, pertanto, era necessario verificare 'l'utilità attuale' della notizia[262], e non quella relativa al passato, quando il fatto di cronaca è avvenuto ed è stato pubblicizzato.

---

[260]Cass. Civ., Sez. III, sentenza del 14 febbraio 1984, n. 1138; Corte d'Appello di Roma, 16 gennaio 1991, in *Foro it*. 1992, I, pag. 942 e 948. Su presupposto dell'utilità sociale pertanto, la pubblicazione d'informazioni intime o di contenuti sulla vita privata della persona, capaci di ledere la reputazione o la sfera personale, non può essere giustificata a meno che, ciò non sodisfi l'interesse della collettività alla migliore comprensione di sé medesima. Dottrina e giurisprudenza da tempo, pur ancorando l'utilità sociale della notizia, a presupposti oggettivi, diversi dalla mera curiosità del pubblico, ritengono tuttavia, direttamente correlata la notorietà dell'individuo a tale requisito, nel senso che più una persona è nota, maggiore sarà l'utilità sociale alla pubblicazione delle notizie che la riguardino.

[261]La Suprema Corte in questo caso ha ritenuto che i giudici di appello abbiano correttamente operato, alla stregua dei criteri validi pe tutta l'area dei diritti della personalità, il bilanciamento tra il diritto all'identità personale dei soggetti raffigurati nello sceneggiato e il diritto di cronaca (più esattamente il diritto di cronaca romanzata). Tale conclusione si è pestata a non poche critiche, tanto da aver portato all'interrogativo: '*Mala tempora currunt per i diritti della personalità?*' La sentenza si segnala altresì, all'attenzione dell'interprete soprattutto nella parte in cui si cimenta nell'ambizioso compito di dare un inquadramento sistematico al diritto dell'identità personale con il dichiarato intento di chiarirne '*la nozione, il fondamento giuridico, la scrittura, il contenuto, le forme e i limiti di tutela*'.

[262]L. CRIPPA, *Il diritto all'oblio: alla ricerca di un'autonoma definizione*, nota a ordinanza Trib. Roma, 27 novembre 1996 (caso Bozano), in *Giust. Civ*., 7, 1997, pag.1990. Nell'ordinanza, il giudice designato ha precisato che «*il sacrificio del diritto (...) dei ricorrenti non è ingiusto in quanto contenuto nei limiti della realizzazione dell'interesse sociale sotteso alla conoscenza del caso*». Seguendo, dunque, le indicazioni dell'organo giudicante tale diritto può essere sacrificato qualora la rinnovata diffusione di vicende note risponda ad un «interesse sociale alla conoscenza, quale conseguenza del diritto di cronaca e del più generale diritto alla ricostruzione storica di vicende rilevanti», dal momento che non può ignorarsi la sussistenza, nel nostro sistema giuridico, del principio costituzionale della libera manifestazione del pensiero e del diritto ad essere informati, quale sua esplicazione.

Sebbene rispetto al passato siano stati fatti passi avanti, quanto meno per aver piantato dei paletti, atti a perimetrare le modalità nelle quali debba estrinsecarsi il diritto di cronaca, in particolare, e di stampa ed espressione, in generale, siamo tuttavia ancora lontani dall'aver raggiunto una soluzione oggettiva in grado di appagare le pretese, tra loro conflittuali, delle varie parti in gioco.

Il mancato rispetto dei limiti alla 'libertà di cronaca', infatti, comporterà la richiesta, da parte dell'interessato, al motore di ricerca del taglio del link con i suoi dati o la cancellazione degli stessi o la loro anonimizzazione.

Sarà il motore di ricerca che, nel processare la richiesta, dovrà ponderare gli interessi in conflitto, considerando le inevitabili ripercussioni dell'esercizio del diritto alla cancellazione sul legittimo interesse degli utenti di Internet ad avere accesso alle informazioni e ricercare il giusto equilibrio tra tale interesse e i diritti fondamentali della persona. Non è dato non avere dubbi sull'effettiva idoneità di un soggetto privato, che segue logiche di mercato e che, pertanto, difetta dei necessari requisiti di neutralità e imparzialità, a svolgere il delicato compito di decidere in merito alle richieste di de-indicizzazione e/o cancellazione dei dati.

Potrebbe darsi, altresì, ed è ciò che si temeva all'indomani della *Google Spain*, che il motore di ricerca, in prima battuta arbitro unico della situazione, per l'enorme mole di richieste pervenute, e spinto dal timore di sanzioni pecuniarie pesanti, possa tagliare eccessivamente, accontentando i personalismi, nel qual caso i link o i dati scomparirebbero ingiustificatamente, non essendo più recuperabili dalla memoria collettiva.

In seguito alla pronuncia della Corte di Giustizia dell'Unione Europea, *Google Spain*, i motori di ricerca, Google in particolare, sono stati letteralmente inondati di richieste di de-indicizzazione: secondo il *Transparency Report*[263], periodicamente aggiornato da Google, dal maggio 2014 ad oggi, il motore di ricerca ha valutato le richieste di de-indicizzazione relative ad oltre due milioni di URL, accolte in circa il 44% dei casi, mentre circa mezzo milione di URL sono ancora sotto esame. Se a tutto questo si aggiunge che i motori di ricerca non hanno attivato commissioni di esperti per assolvere a questo lavoro titanico, oltre che estremamente dispendioso, affidando la soluzione, molto spesso ad algoritmi, è facile immaginare, ad oggi, la mole dei dati persi.

[263]Così in: *https://transparencyreport.google.com/eu-privacy/overview*.

Rispetto alle persone note, o che esercitano funzioni pubbliche, il giornalista dispone di più ampi margini di discrezionalità nella diffusione delle informazioni loro riguardanti, ove queste assumano rilievo in base al ruolo o al carattere pubblico dell'attività svolta[264], anche se la sfera privata delle persone note, o che esercitano funzioni pubbliche, dev'essere rispettata qualora le notizie o i dati non abbiano alcun rilievo sul ruolo ricoperto o sulla vita pubblica degli stessi. In questi casi, la pubblicazione è ammessa ma nell'ambito del perseguimento dell'essenzialità dell'informazione e nel rispetto della dignità della persona[265] e, come sostenuto, in più occasioni, dal Garante, nonostante margini più ampi per la diffusione di dati relativi allo stato di salute o alle abitudini sessuali possano essere previsti con riferimento a persone note, l'informazione potrà essere diffusa solo quando sia in grado di assumere rilievo sul loro ruolo o sulla loro vita pubblica e purché non vengano diffusi dettagli precisi[266].

Nello stesso senso il Consiglio d'Europa ha ricordato che i media devono evitare di diffondere informazioni sulla vita privata e familiare di politici e rappresentanti delle istituzioni, a meno che queste siano direttamente connesse alla condotta tenuta dal politico o dal rappresentante in questione[267].

---

[264]Garante per la protezione dei dati personali, Provvedimento del 15 luglio 2006, *Doc Web n. 1310796*, in *www.garanteprivacy.it*. In questo provvedimento il Garante ha vietato all'editore di un settimanale di diffondere ulteriormente dati personali di carattere sanitario riguardanti la principessa Diana Spencer, contenuti in un sevizio dedicato all'incidente mortale occorso a quest'ultima nel 1997. Il Garante ha rilevato che siffatta pubblicazione, oltre a caratterizzarsi nel suo insieme per un accanimento informativo rispetto ad un fatto ormai risalente nel tempo, non era giustificata sul piano dell'essenzialità dell'informazione e aveva concretizzato una manifesta lesione della dignità dell'interessata. Ha inoltre ricordato che le garanzie in materia operano anche a tutela di persone decedute.

[265]Articolo 10: Tutela della dignità delle persone malate

«*1. Il giornalista, nel far riferimento allo stato di salute di una determinata persona, identificata o identificabile, ne rispetta la dignità, il diritto alla riservatezza e al decoro personale, specie nei casi di malattie gravi o terminali, e si astiene dal pubblicare dati analitici di interesse strettamente clinico.*

2. La pubblicazione è ammessa nell'ambito del perseguimento dell'essenzialità dell'informazione e sempre nel rispetto della dignità della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica».

Articolo 11: Tutela della sfera sessuale della persona

«*1. Il giornalista si astiene dalla descrizione di abitudini sessuali riferite ad una determinata persona, identificata o identificabile.*

2. La pubblicazione è ammessa nell'ambito del perseguimento dell'essenzialità dell'informazione e nel rispetto della dignità della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica».

[266]Garante per la protezione dei dati personali, *Provvedimento del 6 maggio 2004*, *Doc. Web* n. *1007634*, in *www.garanteprivacy.it.*

[267]Newsletter Garante della privacy, 16 febbraio 2004, in *www.garanteprivacy.it*. Sono queste le indicazioni principali contenute nella Dichiarazione che il Comitato dei Ministri del Consiglio d'Europa ha approvato il 12 febbraio 2004 a Strasburgo. Nella Dichiarazione i Ministri ricordano che la libertà di espressione è un diritto fondamentale tutelato dall'art. 10 della Convenzione europea dei diritti dell'uomo, ma sottolineano anche che l'esercizio di tale diritto comporta doveri e responsabilità attinenti, in particolare al rispetto di

Il Garante della privacy, infine, ha sostenuto che, quando le notizie o le immagini relative a fatti privati di persone note siano raccolte in modo illegale o con artifici, è necessario che gli operatori del settore dell'informazione evitino che il legittimo esercizio del diritto di cronaca possa arrecare pregiudizio a persone che sono innanzitutto vittime di estorsioni[268].

Un peso notevole e garanzie particolari nell'operazione di bilanciamento sono riconosciuti alle persone, qualora oggetto di trattamento siano dati sensibili inerenti le stesse, che sarebbero suscettibili di essere utilizzati per fini discriminatori[269], per cui, nel riferire fatti di cronaca collegati alle abitudini o agli orientamenti sessuali di una persona, il giornalista è tenuto a tutelare l'interessato, non solo mediante l'omissione delle sue generalità, ma anche evitando di divulgare elementi che consentano una sua identificazione, anche solo nella ristretta cerchia di familiari e conoscenti.

Particolari garanzie di tutela sono state, infine, riconosciute ai minori, relativamente a fatti di cronaca che li hanno visti protagonisti. Recentemente i giornalisti italiani si sono dati uno specifico codice di autodisciplina a favore dei minori[270], alla stesura del quale ha

---

altri diritti fondamentali, come il diritto alla privacy, sancito dall'art. 8 della Convenzione. L'esigenza di bilanciare libertà di espressione e diritto al rispetto per la vita privata, entrambi principi fondamentali della Convenzione, impone di non rivelare particolari della vita privata delle figure pubbliche e dei loro familiari, a meno che tali informazioni siano direttamente pertinenti in quanto gettano luce sulle modalità con cui tali figure pubbliche svolgono le funzioni alle quali sono state chiamate. E' sempre necessario, ad ogni modo, evitare di causare un *vulnus* a soggetti terzi.

[268]Comunicato stampa del Garante della privacy, 7 dicembre 2006, in *www.garanteprivacy.it*. Nel provvedimento in esame il Garante ribadisce che occorre evitare che un'ingiustificata diffusione di dati comporti che, chi è già vittima di un reato di estorsione un'ulteriore e più grave violazione dei suoi diritti fondamentali.

[269]A questo proposito, si richiama l'art. 9 del Codice Deontologico che stabilisce che il giornalista, nell'esercitare il diritto-dovere di cronaca, è tenuto a rispettare il diritto della persona alla non discriminazione per razza, religione, opinioni politiche, sesso, condizioni personali, fisiche o mentali. Per le altre informazioni sensibili, invece, la segretezza non è strumento di per sé idoneo ad evitare le discriminazioni, poiché le manifestazioni di opinioni politiche e sindacali e gli atti di culto avvengono abitualmente in pubblico, ma il divieto di raccogliere questo tipo di dati è il presupposto per il libero esercizio di questi diritti fondamentali. Il divieto di operare schedature su tali attività risponde alla finalità di impedire discriminazioni tra i cittadini garantendo un «*uguale e libero esercizio di diritti costituzionalmente garantiti, come quelli di manifestazione del pensiero, di associazione e di riunione e di professare liberamente la propria fede religiosa. Più tutela alla privacy, in questi casi si deve parlare di difesa del principio di uguaglianza. Non è in questione la sfera privata, ma la posizione dell'individuo nell'organizzazione sociale, politica ed economica*». Così per S. RODOTÀ, *Tecnologie e diritti*, *Il Mulino*, 1995.

[270]T.U. dei Doveri del Giornalista, in vigore dal 1° marzo 2016, approvato dal Consiglio nazionale nella riunione del 27 gennaio 2016. Il T.U. è nato dall'esigenza di armonizzare i precedenti documenti deontologici al fine di consentire una maggiore chiarezza di interpretazione e facilitare l'applicazione di tutte le norme. Recepisce, infatti, i contenuti dei seguenti documenti: Carta dei doveri del giornalista, Carta dei doveri del giornalista degli Uffici stampa, Carta dei doveri dell'informazione economica, Carta di Firenze, Carta di Milano, Carta di Perugia, Carta di Roma, Carta di Treviso, Carta informazione e pubblicità, Carta informazione e sondaggi, Codice di deontologia relativo alle attività giornalistiche, Codice

collaborato il Garante e la cui osservanza è obbligatoria, tanto per i media tradizionali, che per il Web, che contiene un principio particolarmente impegnativo, quale 'il diritto all'anonimato' del minore, che prevale sempre sul diritto di cronaca. Il giornalista potrà rompere la regola dell'anonimato solo ove ritenga di agire nell'interesse del minore.

7) I criteri utili per un corretto bilanciamento tra diritto all'oblio e diritto di cronaca, espressi dai giudici di legittimità nell'Ordinanza 20 marzo 2018, n. 6919 e i dubbi manifestati, dalla III Sezione della Suprema Corte, nell'Ordinanza di rimessione alle Sezioni Unite del 5 novembre 2018, n. 28084

Con Ordinanza del 2018, la Suprema Corte[271] si è pronunciata su un caso sottopostole dal noto cantante italiano, Antonello Venditti, riguardante la nuova diffusione, a distanza di cinque anni dalla prima, di un servizio televisivo in cui veniva mostrata la reazione del cantautore che, raggiunto dalla troupe del programma RAI "La Vita in diretta", fuori da un ristorante, rifiutava in modo secco e perentorio di rilasciare un'intervista. Tale episodio veniva riproposto all'attenzione del pubblico dal medesimo programma, al solo fine di collocare l'autore all'interno di una classifica dei 'personaggi più antipatici e scorbutici del mondo dello spettacolo'.

L'episodio censurato dal cantante in sede giudiziaria si colloca all'interno del conflitto tra il diritto della persona ad 'essere dimenticata' e la libertà di comunicare, d'informare e di essere informati, nella sua declinazione di diritto di cronaca e di critica giornalistica, le quali, com'è noto, perché possano lecitamente esplicarsi, devono rispettare le tre condizioni della 'verità del fatto', della 'forma civile dell'esposizione' e della sussistenza di un pubblico interesse alla loro conoscenza.

Requisiti strettamente connessi e in composizione variabile a seconda che si eserciti un diritto di cronaca o un diritto di critica: nel primo caso sarà la 'verità dei fatti' ad assumere carattere determinante; nella critica, invece, i limiti scriminanti saranno rappresentati dalla rilevanza sociale dell'argomento trattato e dalle espressioni usate. Nel diritto di critica, infatti, l'opinione manifestata non la si può pretendere rigorosamente obiettiva ed asettica, come nella cronaca.

in materia di rappresentazione delle vicende giudiziarie nelle trasmissioni radiotelevisive, Decalogo del giornalismo sportivo.

[271] Cass. Civ., SEZ. I, sentenza del 20 marzo 2018, n. 6919.

In tale ottica, la critica, per non presentare profili d'illiceità, deve evitare di trascendere in attacchi e aggressioni personali, diretti a colpire sul piano morale la persona destinataria.

Rispetto alle tre condizioni come individuate, il diritto all'oblio chiesto dall'interessato incide, in particolare, sulla 'pertinenza': la riproposizione di una notizia, invero, non deve rispondere solo ad un'esigenza di pubblico interesse, ma ad una nuova o persistente attualità.

I giudici di legittimità hanno ritenuto che, affinché potesse valutarsi una compressione del diritto all'oblio in favore del diritto di cronaca, la diffusione della notizia o dell'immagine dovesse fondare le sue ragioni sulla necessità di garantire - anche a distanza di tempo - ragioni di giustizia, di polizia o di tutela dei diritti o delle libertà altrui.

Al contrario, il diritto all'informazione non avrebbe potuto mai prevalere se la diffusione della notizia avesse risposto solo ad un mero interesse commerciale o economico del soggetto che aveva deciso per la pubblicazione.

Dall'iter argomentativo seguito dalla Corte sembrano così emergere due aspetti: in primo luogo, è ribadito che sono solo le peculiarità del singolo caso e lo scopo informativo che si propone chi rivendica il diritto di diffondere una notizia a definire la sussistenza di un pubblico interesse alla sua divulgazione; in secondo luogo, è confermata una tendenza che vede, nella giurisprudenza civile, una maggiore attenzione a forme di tutela del diritto all'oblio, orientate a garantire effettività ai diritti di cronaca e di critica.

Nell'ordinanza in commento, la Corte di Cassazione ha escluso che nella fattispecie in esame potesse prevalere la libertà d'informazione rispetto all'oblio, poiché la riproposizione in televisione, a distanza di cinque anni, del rifiuto di rilasciare l'intervista, da parte del cantante, in alcun modo avrebbe potuto costituire un rilevante interesse per la collettività.

Nella fattispecie in esame erano assenti riferimenti ai 'fatti criminali connessi a interessi economici o politici preminenti' volti alla 'salvaguardia dell'ordine pubblico o della sicurezza delle persone', che avrebbero potuto fondare l'interesse pubblico a conoscerli, anche a distanza di tempo. L'episodio del diniego, seppur espresso in forma perentoria e poco cortese, di un'intervista da parte del cantante Venditti, personaggio seppur noto nel panorama radiotelevisivo italiano, comunque non investito di un ruolo primario nella vita

pubblica nazionale, riproposto in televisione a distanza di cinque anni, costituirebbe un fatto del tutto inidoneo ad aprire un dibattito di pubblico interesse e non risponderebbe, altresì, a ragioni di giustizia, sicurezza pubblica, interesse scientifico o didattico, che, sole, potrebbero giustificare una nuova diffusione della vicenda da parte di una trasmissione televisiva. Lungi dal soddisfare esigenze di pubblico interesse, secondo i giudici di legittimità, la reiterata messa in onda delle immagini televisive concernenti l'episodio in questione avrebbe perseguito, quale unico scopo, il soddisfacimento di un interesse esclusivamente divulgativo, per finalità commerciali e di audience del gestore televisivo.

Al fine di operare un corretto bilanciamento tra due diritti costituzionalmente rilevanti e dotati di eguale ed apprezzabile tenore applicativo, la Suprema Corte, nel riconoscere il soddisfacimento della pretesa di oblio vantata dal noto cantautore, ha, altresì, previsto un decalogo di specifici presupposti, desumibili dal reticolo di norme nazionali[272]ed europee[273], nonché dall'altrettanto nutrito panorama giurisprudenziale, in presenza dei quali il diritto fondamentale all'oblio potrebbe subire una compressione in forza dell'egualmente fondamentale diritto di cronaca. In particolare, la prevalenza del diritto di cronaca sarebbe riconosciuta in presenza: 1)del contributo arrecato dalla diffusione dell'immagine o della notizia ad un dibattito di interesse pubblico; 2)di un interesse effettivo ed attuale alla diffusione dell'immagine o della notizia per ragioni di giustizia, di polizia o di tutela dei diritti e delle libertà altrui, ovvero per scopi scientifici, didattici o culturali, da reputarsi mancante in caso di prevalenza di un interesse divulgativo o meramente economico o commerciale del soggetto che diffonde la notizia o l'immagine; 3)di un elevato grado di notorietà del soggetto rappresentato, per la peculiare posizione rivestita nella vita pubblica e nella vita economica e politica del Paese; 4)di corrette modalità impiegate per ottenere e divulgare l'informazione, affinché risulti corretta, diffusa con modalità non eccedenti lo scopo informativo, scevra da insinuazioni o considerazioni personali; 5)di una preventiva informazione circa la pubblicazione o trasmissione della notizia o dell'immagine a distanza di tempo, al fine di consentire all'interessato il diritto di replica prima della sua divulgazione al grande pubblico.

[272] Art. 2 Cost., art. 10 cc., art. 97 l. n. 633 del 1941.
[273] Artt. 8 e 10, comma 2, Carta dei diritti dell'Unione Europea e artt. 7 e 8 della Carta di Nizza.

Sicché, come chiarito nella pronuncia in esame, in assenza dei suindicati presupposti, la pubblicazione di un'informazione concernente una persona determinata, a distanza di tempo da fatti ed avvenimenti che la riguardano, non potrebbe che integrare una violazione del fondamentale diritto all'oblio.

Tuttavia, diritto all'oblio, diritto di cronaca e storia sono in perenne contrapposizione: il punto di equilibrio tra le opposte istanze è tutt'altro che stabile.

Proprio il decalogo di ipotesi, al ricorrere delle quali il diritto all'oblio sarebbe destinato a recedere in favore del diritto di cronaca, stilato dalla I Sezione della Corte di Cassazione, ha consentito di riaprire l'annosa e dibattuta questione, rimettendo definitivamente la decisione alle Sezioni Unite. La rimessione, operata dalla III Sezione con Ordinanza interlocutoria n. 28084 del 5 novembre 2018, trova ragione nella circostanza che, nell'indicare le cinque ipotesi al ricorrere delle quali il diritto fondamentale all'oblio può cedere il passo al diritto di cronaca, l'Ordinanza del marzo 2018 non abbia, tuttavia, precisato se detti presupposti siano richiesti in via concorrente o in via alternativa, nonostante la diversità di conseguenze che deriverebbero dall'adesione all'una o all'altra soluzione. Infatti, qualora si optasse per il cumulo, raramente il diritto all'oblio riuscirebbe a prevalere sul diritto di cronaca.

Il caso che ha originato la recentissima pronuncia del Supremo Consesso muove dall'istanza risarcitoria promossa da S. G., cittadino sardo, nei confronti del quotidiano Unione Sarda s.p.a. e della giornalista C.M.F, autrice di un articolo pubblicato su detto quotidiano il 19 aprile 2009, che rievocava una vicenda di cronaca nera di cui si era reso autore il ricorrente nel lontano 12 luglio 1982.

Il ricorrente lamentava la palese violazione del proprio diritto all'oblio, determinata dalla rievocazione, dopo un lunghissimo lasso di tempo dall'episodio, di fatti di cronaca nera che lo avevano visto protagonista, che avrebbe generato un profondo senso di angoscia e prostrazione, nonché un notevole danno per la sua immagine e per la sua reputazione, avendolo nuovamente ed ingiustificatamente esposto alla gogna mediatica, nonostante avesse espiato la sua condanna a dodici anni di reclusione e si fosse reinserito nel contesto sociale, anche attraverso lo svolgimento della sua apprezzata attività di artigiano.

I giudici di prime cure, in prima battuta, e la Corte territoriale di Cagliari, successivamente, hanno rigettato l'istanza, non ravvisando i presupposti per la concessione del diritto all'oblio vantato dal ricorrente e ritenendo preminente il diritto

all'informazione giornalistica, in ragione dell'esclusione di qualsiasi forma di ingerenza da parte dei poteri pubblici, attraverso controlli, diretti o indiretti, di meritevolezza, non solo preventivi ma anche successivi, in grado di incidere, limitandola, sulla libertà di comunicazione delle informazioni.

Il diniego dell'istanza di oblio era, altresì, giustificato, per i giudici di merito, dallo spirito della pubblicazione dell'articolo, coincidente con l'intento di offrire ai lettori, in una rubrica settimanale ben strutturata, spunti di riflessioni concernenti i temi della gelosia, della prostituzione, della depressione, dell'emarginazione, nonché dalla puntuale contestualizzazione operata nella rievocazione, che avrebbe escluso l'esistenza di qualsiasi intento lesivo alla base della volontà editoriale. Per di più, il giornalista avrebbe tracciato la figura dell'autore del delitto con una penna obiettiva, priva di accostamenti fuorvianti e con una corretta continenza espositiva, sicché si sarebbe dovuta escludere qualsiasi compressione del rispetto della libertà morale dell'individuo.

In ultima istanza è intervenuta, nel caso di specie, la III Sezione della Corte di Cassazione che, al fine di operare un corretto bilanciamento tra i confliggenti interessi in campo, nel richiamare i criteri indicati dall'Ordinanza del marzo 2018, si è interrogata sulla necessità che i presupposti debbano essere presenti in via concorrente, ovvero, come sembra maggiormente plausibile, in via alternativa, evitando così che il diritto all'oblio sia destinato a prevalere sul diritto di cronaca in ipotesi rare e del tutto eccezionali.

Proprio il forte impatto che il bilanciamento tra il diritto di cronaca ed il diritto all'oblio ha sul modo di intendere la democrazia nell'attuale società, tesa a salvaguardare il pluralismo informativo, pur non dismettendo la tutela della personalità del singolo nelle sue diverse espressioni, ha determinato la rimessione della delicata questione alle Sezioni Unite. Sembra ormai indifferibile, alla luce di questa istanza, l'individuazione di parametri di riferimento univoci, che consentano agli operatori del diritto di conoscere con certezza e preventivamente i presupposti in presenza dei quali possa trovare accoglimento l'istanza di un soggetto a che una notizia che lo riguardi, seppur legittimamente divulgata in passato, non resti indeterminatamente esposta alla possibilità di una nuova diffusione.

Appare evidente, dal quadro così delineato, come non sia possibile astrarre una regola che consenta di definire una volta per tutte, le situazioni in cui la libertà di manifestazione del pensiero o il diritto all'oblio siano destinati a prevalere. Tutti i diritti in gioco, infatti,

mostrano una struttura dinamica e flessibile, adattabile a realtà diverse e destinata a mutare a seconda delle variabili del caso concreto[274].

8) I poteri del Garante in materia di trattamento dati per finalità giornalistiche

Poiché è notoria la tensione, che talvolta sfocia in un vero e proprio conflitto, tra il diritto ad essere dimenticati, attraverso la cancellazione dei propri dati, e il diritto all'informazione della collettività, il Legislatore nazionale, a differenza della maggioranza dei Paesi europei che, nelle discipline nazionali di protezione dei dati personali, hanno omesso di prevedere poteri d'intervento dell'Autorità Garante in materia di libertà d'informazione, ha attribuito al Garante un ruolo forte su tale delicato versante. Un potere, il cui esercizio richiede equilibrio, senso della misura, adesione profonda allo spirito della Carta costituzionale e alle disposizioni europee e internazionali, senza tuttavia incorrere nel rischio di apparire censori.

Al Garante è consentito operare forme di controllo circa la liceità e la correttezza del trattamento dei dati effettuato dai giornalisti, sulla base di due particolari tipi di strumenti, quali la normativa sulla protezione dei dati, con i suoi principi generali e in particolare la regola che consente la pubblicazione delle informazioni che risultino 'essenziali' nell'ambito di 'fatti d'interesse pubblico', cui si aggiunge altro strumento più flessibile, rappresentato dal Codice deontologico, relativamente alle modalità di svolgimento dell'attività giornalistica che, in forza del principio di co-regolamentazione, ha consentito di applicare al giornalismo i principi generali di protezione dei dati, tenendo bene in conto, tuttavia, l'estrema varietà dei casi, la cui soluzione potrebbe richiedere l'esercizio della tecnica di bilanciamento tra i valori della persona e la libertà d'informazione.

I poteri attribuiti al Garante per le ipotesi di violazione delle disposizioni normative sono di diversa natura e di varia intensità: da quello di fornire ad una determinata persona informazioni che la riguardino (quali ad es. i dati che siano detenuti da un giornalista su

[274] Sul punto, Cass. Civ., Sez. III, Ordinanza di rimessione alle Sezioni Unite, 5 novembre 2018, n. 28084: «*Sembra al Collegio che, soltanto partendo dal caso concreto, sia possibile definire: quando possa effettivamente configurarsi un interesse pubblico alla conoscenza dei fatti (tali non essendo le insinuazioni di dubbi e le voci incontrollate); quando, nonostante il tempo trascorso dai fatti, detto interesse possa essere considerato attuale; in che termini, sulla sussistenza di detto interesse, possa incidere la gravità e la rilevanza penale del fatto, la completezza (o la incompletezza) della notizia del fatto, la finalità del trattamento del dato, (se, ad es., per fini di ricerca scientifica o storica, per fini statistici, per fini di informazione o per altri motivi, ad es. di marketing), la notorietà (o la mancanza di notorietà) della persona interessata, la chiarezza della forma espositiva utilizzata (anche evitando l'accorpamento e l'accostamento di notizie false a notizie vere)*».

una determinata persona o l'origine delle informazioni) a quello di disporre la rettifica di dati inesatti o incompleti, nonché a quello di riconoscere la prevalenza del diritto al silenzio della memoria rispetto a qualsivoglia forma di trattamento. Lo strumento più incisivo è sicuramente il blocco o il divieto di ulteriori diffusioni dei dati perché non essenziali rispetto all'interesse pubblico alla conoscenza o la cancellazione degli stessi perchè trattati in violazione di legge.

Il Garante, nel corso dell'ultimo decennio, ha usato i poteri più incisivi con estrema cautela, avendo preferito, nella maggior parte dei casi, su centinaia di reclami in materia giornalistica, la strada del dialogo e della fattiva collaborazione con le rappresentanze della categoria dei giornalisti, finalizzate alla sensibilizzazione di chi trasmette conoscenza e sapere in merito alla necessità di rispettare i diritti della persona, senza, tuttavia, dover rinunciare a 'fare informazione'.

CAPITOLO TERZO

I DIRITTI DIMENTICATI DAL LEGISLATORE EUROPEO: LA TUTELA DELLA MEMORIA STORICA E DEI TERZI INTERESSATI AL RICORDO.

SEZIONE I: La tutela della memoria storica collettiva a presidio dei diritti alla conoscenza e dell'infomazione.

1) L'esercizio del diritto all'oblio e il vulnus nella memoria collettiva

L'esercizio del diritto ad essere dimenticati, in tutto o in parte, è guardato con particolare attenzione, e talvolta con sfavore, allorché va ad impattarsi con il diritto alla storia e con quello alla memoria. Il taglio del link alla notizia o la cancellazione dei dati, ex art. 17 Regolamento europeo 2016/679, seppure contenuti nei limiti e nel rispetto delle disposizioni predisposte dal legislatore o suggerite dagli operatori giuridici, comunque creano lesioni, talvolta insanabili, nel ricordo e nella ricostruzione di fatti ed episodi di un passato più o meno remoto. Memoria e oblio, fattori entrambi di divisione, come di aggregazione, di emarginazione, come di adattamento (dimenticare per vivere ma anche ricordare per esistere), che non possiedono di per sé caratteristiche positive o negative in assoluto, ma sempre correlate all'uso che ne si vuol fare. Il linguista Harald Weinrich, in un suo recente studio[275], nell'affermare che ci sono casi in cui bisogna opporsi in maniera netta all'oblio, pur venendo a patti necessariamente con la memoria, ha suddiviso l'oblio in 'pubblico e privato' ed ha collegato l'oblio pubblico ai grandi eventi, ai cambiamenti storici, come la Rivoluzione francese, per cui esso diventa un dovere del cittadino, va oltre la *damnatio memoria*e (che colpiva singoli individui), ed impone ad un'intera nazione l'obbligo di dimenticare, di lasciare il posto ad una nuova memoria repubblicana. Nella stessa logica "l'oblivio sempiterna", che portò Cicerone, dopo l'assassinio di Cesare, a proporre una legge dedicata alla distruzione di ogni memoria della discordia, attraverso l'oblio eterno: in questo senso l'oblio diventa uno strumento di civiltà perché impone la dimenticanza di un passato scomodo, per far ripartire la vita in società.

Ma questa è un'accezione quasi romantica di oblio sociale, differente dall'oblio tecnico o informatico che comporta la cancellazione di dati o notizie dalla Rete, la quale si nutre delle informazioni e dell'incremento dei dati stessi, fondando il suo impero economico

[275] H. WEINRICH, *Oblio pubblico ed oblio privato*, Bologna, n. 4, 2000, 611-620.

sulla sorveglianza delle attività degli utenti e sulla costante rielaborazione delle informazioni che immagazzina. E' l'oblio privato quello che preoccupa e che vede contrapposti due grandi interessi: quello della Rete, che mira ad accumulare, manipolare e commercializzare i dati e che, in una società che ama i Big Data, ambisce ad un sempre maggior incremento delle informazioni al fine di profilare ciascun utente, commercializzare i risultati ottenuti e creare un patrimonio informativo; per altro verso, ed in senso contrario, vi è l'interesse, connesso ai diritti della personalità, proprio di chi si auspica e chiede la cancellazione di parte di quei dati per alleggerire il proprio passato e riprendere la sua vita in società, senza condizionamenti. E l'oblio privato risulta perfettamente in linea con la sua accezione primigenia, secondo cui l''oblivio' era effettivamente equiparato alle idee di 'amnistia' e 'grazia', ossia ad un'azione che segna una cesura per dimenticare il passato di una persona. Nel mezzo si pone il diritto fondamentale, tipico di una società democratica, a che la collettività sia informata e possa accedere con tempestività all'informazione, contando sulla sua completezza ed integrità. Ed oggi il solo modo più celere di fare informazione è il ricorso all'uso delle infrastrutture tecnologiche, quelle stesse aggredite da chi manifesta la pretesa contraria, ossia quella di cancellare quelle stesse notizie dalla Rete, per farsi dimenticare. All'interno di questa dialettica giuridica emerge anche l'interrogativo diretto a comprendere se sia giusto rimuovere da uno 'spazio pubblico', qual è la Rete, un'informazione veritiera e corretta che, quando è stata pubblicata, era di sicuro interesse di cronaca e pubblico. E tutto in nome dell'interesse del singolo, cui si viene a contrapporre un interesse maggiore, di carattere pubblicistico, visto che la storia ormai ci viene raccontata da Internet. Facendo passare, tra l'altro, il principio secondo cui ciascuno, in maniera incondizionata, possa riprendersi tutte le informazioni che lo riguardino, pubblicate dallo stesso autore o da terzi, ne deriverebbe la conseguenza che, fra qualche anno, chi volesse ripercorrere la storia degli anni Duemila, attraverso l'informazione online, probabilmente trarrebbe l'errata convinzione che sia stata un'età vissuta da gente per bene, dal momento che ciascuno, potendo, andrebbe a cancellare quello che non gradisse, fornendo di sé un'immagine sbiadita e falsata[276]. Il diritto all'oblio, nella sua accezione più evoluta e

[276] A questo proposito, interessante risulta la riflessione di S. RODOTÀ, I*l mondo nella rete. Quali diritti, quali vincoli*, Bari, 2014, 45, secondo cui: «può il diritto della persona di chiedere la cancellazione di alcuni dati trasformarsi in un diritto all'autorappresentazione, alla riscrittura stessa della storia, con l'eliminazione di tutto quel che contrasta con l'immagine che la persona vuole dare di sé? Così il diritto all'oblio può

dinamica, ha infatti ad oggetto l'esercizio della pretesa a riprendersi dei brandelli della propria storia, che l'individuo vorrebbe sottratti alla disponibilità dei cybernauti e che sono presenti in Rete. Oggi, pertanto, l'esercizio del diritto all'oblio è sempre meno diretto ad impedire la riproposizione di fatti già pubblicati in passato e sempre più volto ad ottenere l'eliminazione da Internet di dati e informazioni relative a ciascuno, sia pure pubblicate per la prima volta decenni addietro.

E' recente la pronuncia dell'autorità amministrativa[277] che ha negato l'oblio, riconoscendo valore storico alla vicenda di un professionista, oggi inserito nel mondo del lavoro, che aveva chiesto a Google la cancellazione dei link che, digitando il suo nome e cognome, rinviavano alla sua passata carriera di terrorista. Anche volgendo lo sguardo in Europa ci si rende conto che, nell'azionare il diritto all'oblio, si chiede sempre meno di vietare a qualcuno la riproposizione di storie passate, quanto, piuttosto, di deindicizzare dall'archivio storico di giornali o dagli stessi motori di ricerca contenuti che riguardino il passato di un singolo o dati allo stesso relativi. Non è più un problema di diritto all'oblio, inteso nella sua originaria accezione, ma di diritto ad essere dimenticati in tutto o in parte. Cosa assai grave per gli effetti devastanti che potrebbero riflettersi sulla memoria collettiva: nella specie, si sta parlando di rimuovere da uno spazio pubblico un'informazione reale, veritiera e corretta, che, quando è stata pubblicata, era di sicuro interesse collettivo e di cronaca.

E' doveroso prestare attenzione alla memoria storica, quale strumento di profilassi rispetto al pericolo di un ritorno ad errori ed orrori del passato. La storia va salvaguardata e, se passasse il principio che ciascuno possa riprendersi tutte le informazioni sul suo conto, si genererebbero informazioni parziali, lacunose e tendenziose, nella migliore delle ipotesi. Ecco perché è necessario trovare un punto di contemperamento tra il diritto del singolo ad essere dimenticato e quello della collettività, nella sua veste giuridica di diritto all'informazione o, meglio, diritto alla storia. E', altresì, un problema di educazione digitale: nessuno ha mai pensato di chiedere a qualcun altro di rimuovere dalla sua

---

pericolosamente inclinare verso la falsificazione della realtà e divenire lo strumento per limitare il diritto all'informazione, la libertà di ricerca storica, la necessità di trasparenza che deve accompagnare in primo luogo l'attività politica. Il diritto all'oblio contro verità e democrazia? O un inaccettabile tentativo di restaurare una privacy scomparsa come norma sociale, secondo l'interessata versione dei nuovi padroni del mondo che vogliono usare senza limiti i dati raccolti?

[277] Garante per la protezione dei dati personali, Provvedimento del 31 marzo 2016, n. 152, Doc. Web. n. 4988654.

memoria qualcosa che aveva sentito sul suo conto. L'esempio dell'ex terrorista è eclatante: esistono, infatti, decine di libri sugli anni di piombo, che contemplano, tra altri, anche il suo nome. Chiunque può leggerli ed a nessuno è mai venuto in mente di distruggerli in nome della tutela del singolo. Perché allora farlo se si passa ad una dimensione più ampia come Internet? Solo perché le notizie appaiono più vivide se lette nello specchio del monitor?

In nome dell'interesse collettivo alla conoscenza e all'informazione è giusto, altresì, abituarsi a convivere con il proprio passato, dando, tuttavia, il giusto valore a tutto ciò che la Rete ha conservato, collocando nello spazio e nel tempo le notizie immesse, contestualizzandole ed eventualmente collegandole con altre che siano in grado di fornire del protagonista un'immagine diversa e maggiormente edificante.

1.1) La memoria storica prevale sul diritto all'oblio di un ex terrorista

La storia personale di ciascuno, soprattutto di chi sia stato protagonista di una delle pagine più buie del passato, non può essere cancellata!

E' quanto deciso da Google, cui si era rivolto, in prima battuta, un ex terrorista, nel 2009, chiedendo la de-indicizzazione di dodici URL che rinviavano a fatti di cronaca in relazione ai quali l'interessato era stato condannato, nonché la cancellazione di alcuni riferimenti che associavano il proprio nominativo al termine 'terrorista'.

Google, rifiutatosi di procedere alla de-indicizzazione, ha sostenuto, a causa della gravità dei fatti contestati al ricorrente, l'inesistenza dei presupposti che avevano indotto i giudici europei, nella Google Spain, ad acconsentire al riconoscimento del diritto all'oblio.

Nella decisione il motore di ricerca ha, altresì, affermato, facendo riferimento alle Linee Guida, adottate il 26 novembre 2014 dal WP 29, che il diritto all'oblio non avrebbe potuto configurarsi rispetto ai 'reati più gravi', quali erano quelli di cui si era reso autore il ricorrente.

Decisione successivamente confermata dal Garante della privacy[278], cui l'ex terrorista si era rivolto, sostenendo la sussistenza dei presupposti per l'esercizio del diritto all'oblio in quanto, in virtù del lungo lasso di tempo trascorso dall'accadimento dei fatti e dell'impossibilità di qualificarlo come personaggio pubblico, sarebbe venuto meno

[278] Garante per la protezione dei dati personali, Provvedimento del 31 marzo 2016, n. 152, Doc. Web. n. 4988654.

l'interesse pubblico attuale alla conoscenza delle informazioni indicizzate, ritenute altamente pregiudizievoli e dannose per la propria sfera personale e professionale. Il Garante, dovendo intervenire in merito al difficile bilanciamento tra diritto alla riservatezza e oblio del singolo e l'opposto diritto di cronaca, nella sua veste di interesse o diritto della collettività alla conoscenza ed alla memoria storica, ha esplicitato gli stessi principi già affermati dal motore di ricerca, ritenendo prevalente il diritto di cronaca e dichiarando infondata la richiesta di de-indicizzazione formulata dall'ex terrorista. Il Garante ha fondato la sua decisione sulla circostanza che le informazioni riguardassero una delle pagine più buie della storia italiana, della quale il ricorrente non era stato un coprimario, ma il protagonista di spicco e che, avendo ormai assunto una valenza storica e segnato la memoria collettiva, nonostante il lungo lasso di tempo trascorso dagli eventi, l'attenzione del pubblico sulla questione era ancora molto alta. E' stata una decisione coraggiosa, quella del Garante, anche se occorre chiedersi quanti e quali elementi oggettivi possano far sì che un fatto sia considerato così storicamente rilevante da far prevalere l'interesse comune alla memoria storica sul diritto all'oblio del suo autore. Non sempre, infatti, sarà sufficiente il mero richiamo al punto 13 delle Linee Guida del 2014, secondo cui è necessario che le richieste di de-indicizzazione relative ad informazioni riferite a 'reati gravi' vengano valutate, sia pure nel rispetto di un'analisi fondata sulle singole esigenze, con minor favore da parte delle autorità di protezione dei dati. Decisione ancora più coraggiosa se si osserva il suo contrasto con una precedente pronuncia della Suprema Corte[279], nella quale gli Ermellini, al contrario, hanno riconosciuto il diritto all'oblio per un ex attivista ed estremista politico, statuendo il principio, secondo cui «il diritto all'oblio può cedere il passo al diritto di cronaca solo in quanto sussista un interesse effettivo e attuale alla diffusione della notizia; diversamente argomentando, altrimenti, si finirebbe col riconoscere una sorta di automatica permanenza dell'interesse alla divulgazione, anche in un contesto storico completamente mutato».

2) La Rete come bene pubblico

La Rete non è un mezzo, ma un luogo in cui oggi si forma l'opinione pubblica perché è lì che dimorano le informazioni e, più in generale, il sapere. E' un luogo veramente libero,

[279] Cass. Civ., Sez. I, sentenza del 9 maggio 2013, n.16111.

cui ogni giorno gli individui affidano tasselli della propria vita e dove non esiste alcuna regola, che non sia la regola di mercato, non esistono leggi e lo stesso mondo della cultura vira verso il libero mercato. E' un bene comune, per la prima volta non governato dall'alto, ma gestito dal basso, dagli utenti, in cui le scelte avvengono attraverso movimenti orizzontali, anziché verticali ed in cui qualsiasi meccanismo gerarchico salta al cospetto delle decisioni collettive[280]. In altri ambienti, in altri luoghi, il governo è nelle mani dei vertici: la cultura è nelle mani dei rettorati, sovrintendenti, dipartimenti universitari, case editrici, reti televisive; il Web, invece, è libero, da nessuna parte c'è lo Stato. Il Web seleziona partendo dal basso e, sottoposto alle leggi di mercato, opera secondo una logica che privilegia decisioni collettive. Sono, infatti, gli utenti a scegliere ogni giorno le aziende migliori e i siti più appetibili, contribuendo al fallimento di giganti (my space) e all'arricchimento di pochi eletti, massacrando esponenti politici o esaltando ideologie, che sempre più frequentemente ricorrono ai consensi che i cybernauti manifestano attraverso il Web. E' un bene comune privato che consente all'utente la promozione e la partecipazione ad un dibattito politico, l'esercizio in modo ampio della libertà di espressione, lo sviluppo di attività commerciali, nonché l'acquisizione e la diffusione di conoscenze. E' un bene che appartiene alla collettività e, pur non avendo uno *status*, né la titolarità di diritti e doveri, è la rete di telecomunicazioni più estesa al mondo, un insieme di infrastrutture, in grado di consentire il collegamento tra un numero indefinito di soggetti che si trovano nelle stesse condizioni.

Anche se da un punto di vista fisico si presenta come un insieme di beni materiali ed immateriali, non esiste uno solo di questi elementi che possa essere attribuito alla titolarità di Internet, essendo questa sfornita di personalità giuridica. Se da un punto di vista giuridico, quindi, si può affermare che Internet non esista, dal punto di vista fisico è la sola infrastruttura di comunicazione globale. L'uso di Internet ha profondamente trasformato il vivere quotidiano di ciascuno, la visione del mondo, il modo di fare politica e cultura, costituendo una vera e propria piattaforma pubblica, dove l'utente definisce la sua dimensione di cittadino. Internet ha, altresì, accentuato il progresso e l'innovazione, estendendosi alle cose ed ai luoghi concreti, con la visione dell'IOT, che connette gli oggetti di uso comune nel tentativo di semplificare la vita quotidiana. La Rete è un bene

[280] Interessanti, a tal proposito, le riflessioni di R. MARONE, *La rete: il bene comune privato*, in *Doppiozero*, 16 giugno 2011.

che appartiene alla collettività, creato e nutrito dagli utenti, accessibile a tutti, tanto da aver dato origine ad un nuovo diritto di rilevanza costituzionale, quale quello di accesso alla Rete, finalizzato al riconoscimento di tale possibilità a tutti gli individui. Se la Rete è valorizzata dagli apporti di ciascuno, è conseguenza logica e giuridica che quei contributi, una volta usciti dalla disponibilità dei titolari e fagocitati dall'infrastruttura telematica, diventino patrimonio comune.

E' però imprescindibile comprendere quale base giuridica possa giustificare il riconoscimento incondizionato a ciascuno di chiedere la cancellazione, dai canali del Web, di URL o di altre notizie o immagini postate. La fuoriuscita dal patrimonio individuale e la metabolizzazione nella Rete di una notizia comporta una trasformazione profonda della sua veste giuridica che, da una dimensione privata, muta in una pubblica, diventando patrimonio comune. Ma il patrimonio intanto è comune in quanto appartiene alla collettività, la qual cosa andrà a comportare una rigida perimetrazione dell'esercizio del diritto ad essere dimenticati, vietando la possibilità di ottenere in modo indiscriminato la cancellazione dei propri dati presenti sulle varie piattaforme, impoverendole, ammettendone al più l'operatività solo in presenza di condizioni assai più gravi, tutte predisposte al fine di evitare di esporre a gravi rischi la sfera individuale di ciascuno. Cancellare, essere dimenticati, quindi, non per costruire un alter ego edulcorato e con una reputazione digitale migliore, ma solo ed esclusivamente per evitare seri vulnera alla persona ed alla sua sfera privata. Allo stesso modo, il dato, presente sulla piattaforma telematica, sia pure riferito ad elementi strutturali dell'individuo, non può non essere considerato bene giuridico/economico.

3) Il dato: un bene giuridico/economico

I dati, che si tratti di informazioni accumulate durante le attività online della persona, di contenuti pubblicati in Rete, di opinioni manifestate all'interno di un forum, di notizie relative ad azioni e comportamenti della stessa, presentano una sicura valenza giuridica ed economica.

Da un punto di vista giuridico, il Codice Civile, nell'art. 810, definendo il bene giuridico come qualsiasi cosa che possa formare oggetto di diritto, gli assicura tutela, non tanto per le caratteristiche intrinseche dell'entità considerata, quanto per la possibile incidenza su di essa della qualificazione giuridica.

Dubbi circa la qualificazione dell'informazione quale 'bene giuridico' sono stati alimentati anche dall'assenza di omogeneità della normativa del settore e di una visione univoca del problema.

A giudizio di autorevole dottrina[281], il fondamento normativo del riconoscimento giuridico del bene-informazione andrebbe individuato nel rinvio ai principi dell'Ordinamento: il riconoscimento avverrebbe in via mediata, rifacendosi alle esigenze di conoscenza della collettività.

Altri, invece, in modo più formalista, ritengono che l'informazione sia un bene giuridico nei soli casi in cui il diritto positivo l'abbia riconosciuto come tale.

Nell'informazione convivono più anime: la titolarità di chi l'ha creata, la possibilità di essere messa in circolazione e il potere di disporne e di goderne in via esclusiva.

Analizzare se un'informazione sia configurabile come bene giuridico significa anche individuare il regime relativo alla sua tutela, alla sua disponibilità ed alla individuazione dei soggetti che sulla stessa possano vantare dei diritti.

L'informazione sicuramente appartiene, in via originaria, al suo creatore, a colui che le ha dato forma racchiudendola in qualsiasi supporto atto a realizzarne la comunicazione ad altri. Fino al momento in cui si realizza questa fase, l'informazione ancora non è stata creata: la semplice idea non esplicitata, ma insita solo nella mente del suo creatore, non costituisce informazione e, in quanto tale, non può ottenere alcun riconoscimento formale da parte dell'Ordinamento giuridico.

Potrà interessare il diritto, relativamente alle problematiche connesse alla sua tutela per presunte violazioni dei diritti della persona, nel momento in cui quell'informazione inizia a circolare.

Ma i dati immessi nella Rete, a differenza delle idee, che assumono la veste giuridica delle opere d'ingegno, o di altre notizie che circolano per volontà della legge (informazioni relative a persone o patrimoni che sono oggetto di pubblicazione per volontà del legislatore), sono perlopiù considerati 'dati liberi', 'res nullius', cadute in pubblico dominio, la cui circolazione è oggi per gran parte regolamentata, anche se non se ne potrà mai verificare la correttezza fino in fondo, perché i dati, una volta ingoiati dalla Rete, iniziano a vivere una nuova vita, autonoma rispetto alla volontà di chi li ha creati, anche in spregio delle previsioni legislative finalizzate a dar loro tutela.

---

[281] P. PERLINGIERI, *L'informazione come bene giuridico*, in *Rass. Dir. civ*.. 1987, 33.

L'informazione, quindi, è bene giuridico nel momento in cui, sia fuoriuscita dalla sfera personale del suo autore, ed entrata nella disponibilità delle infrastrutture telematiche, anche attraverso un atto di disposizione dell'autore stesso ed in adempimento alle esigenze di conoscenza della collettività, e richieda l'intervento del legislatore affinché sia regolamentata la sua circolazione, rielaborazione ed eventualmente anche la sua cancellazione o de-indicizzazione, verificatane l'obsolescenza.

Nel momento in cui l'informazione, infatti, abbia perso i caratteri della originalità e della novità, e la sua permanenza si riveli lesiva per la sfera privata dello stesso titolare, quest'ultimo potrà chiedere la sua cancellazione al motore di ricerca ed, eventualmente, in caso di esito negativo, alle Autorità amministrative o giudiziarie.

L'interesse del legislatore per la vita e la morte di flussi di dati personali che, fuoriusciti dalla dimensione privata, sono trasmigrati nella dimensione pubblica della Rete, è, altresì, dovuto al valore 'patrimoniale' del dato, sempre più suscettibile di sfruttamento economico, con o senza il consenso del titolare, che ha visto la nascita di un vero e proprio mercato parallelo.

Sempre più frequentemente l'utente cede volontariamente alcuni dati a lui relativi per usufruire gratuitamente di un servizio, quotidianamente semina tracce informatiche nel corso della navigazione in Rete, perdendo, altresì, sempre più il controllo di tutti i dati relativi alla sua persona immessi nei canali del Web da soggetti terzi, di cui spesso non ha neppure conoscenza[282]. Questo sterminato flusso di dati, che l'utente consapevolmente o inconsapevolmente dona alla Rete, ha contribuito nel tempo alla costruzione di un'identità digitale, parallela a quella reale. I dati circolanti on-line sono acquisiti dalle società commerciali ai fini di profilazione, volta alla definizione dei gusti e della propensione all'acquisto del consumatore. I grandi colossi dell'informazione, incrociando i dati in loro possesso, relativi a milioni di persone, sono in grado di ottenere profili molto precisi inerenti la personalità di ciascuno, sulla base dei quali realizzano degli archivi, che utilizzano per le finalità più svariate, non ultima quella di destinarli alla vendita. Gli individui sono sempre più visti come una massa indiscriminata di informazioni da raggruppare o dividere a seconda dell'uso commerciale che si intende farne: la

[282] Un aspetto di particolare rilievo, relativo al trattamento dei dati da parte di soggetti terzi, si pone in relazione alla morte del soggetto interessato. Sul punto si veda G. RESTA, *La morte digitale*, in *Dir. Inform.*, fasc. 6, 2014, 891 e ss.

commercializzazione digitale ha accelerato il processo di mercificazione degli individui.[283]

E' l'oro nero' dell'economia di Internet[284]!

Dati che il più delle volte è lo stesso titolare che cede, in cambio di servizi che solo apparentemente la Rete presenta come gratuiti e che, invece, hanno un prezzo, sia pure non immediatamente visibile, rappresentato dalla cessione di dati, di pezzi di privacy.

Il più delle volte gli utenti non si rendono conto di quanto paghino; i gestori, invece, sanno quanto ricevono!

I dati che ciascuno immette, infatti, sono infiniti, visto che nell'ultimo decennio si è passati dalla paura di lasciare le proprie tracce sul web (tipica della prima Rete), al presenzialismo massimo, che lascia tracce ovunque, mettendo in comune anche spazi fino a ieri estremamente privati[285].

Fenomeno che fa ritenere quanto mai indifferibile, da un lato la necessità di incrementare la consapevolezza negli utenti della Rete di valutare attentamente quanto si posti, che siano immagini, video, opinioni, perché tutto sarà utilizzato dalle aziende per ridefinire i confini della loro privacy, che, in forza dei loro stessi interessi economici, tenderanno ad annullare; dall'altro, l'intervento del legislatore, mirato all'ottenimento di una regolamentazione legislativa del dato digitale attenta a due sfaccettature del problema: il lato informatico, che comprende i nodi della sicurezza e delle modalità tecniche migliori per preservarlo alle generazioni future, visto che i dati potrebbero andare distrutti per l'obsolescenza degli stessi sistemi che ne consentono la vita e il lato giuridico, attento ai problemi economici connessi al valore patrimoniale dei beni.

Un simile insieme di dati è già stato definito dagli studiosi e nei progetti legislativi in corso, che si propongono di regolamentare il fenomeno, con l'espressione '*digital assest',* essendo in presenza di veri e propri beni, provvisti di un valore patrimoniale e che, pertanto, necessitano di una nuova e specifica regolamentazione, ben diversa da quella pensata per beni materiali.

---

[283] S. NIGER, *Sorveglianza e nuovi diritti di libertà*, in G. FINOCCHIARO (a cura di), *Diritto dell'anonimato. Anonimato, nome e identità personale*, in F. GALGANO (diretto da), *Trattato di diritto commerciale e di diritto pubblico dell'economia*, Vol. XLVIII, Padova, 2008.

[284] G. ARENA, *La tutela della riservatezza nella società dell'informazione*, in AA. VV., *Scritti in onore di P. Virga*, Milano, Vol. I, 1994, pag. 63; C. MANGANELLI, *Progresso tecnologico e protezione dei dati personali*, in G. SANTANIELLO (a cura di), *La protezione dei dati personali*, Padova, 2005, pag. 309.

[285] V.C. SAVIANO, *Facebook: spariti i gruppi pro e contro Tartaglia*, in *La Repubblica*, 15 dicembre 2009.

Negli USA almeno trenta Stati stanno adottando norme che mirano a risolvere i problemi connessi alla gestione di account, profili e dati. Anche in Europa, negli ultimi mesi, l'attenzione su questi temi è altissima!

Per dare un'idea degli interessi patrimoniali in gioco, cinque anni orsono, alcune analisi commissionate da aziende che operano nell'ambito della sicurezza informatica hanno stimato un patrimonio digitale, per un tipico utente on-line, che poteva agevolmente raggiungere la somma di trentacinquemila dollari pro capite.[286]

4) Opinioni discordi in merito all'immortalità o vita a tempo determinato del dato immesso in Rete

4.1) La difficoltosa tutela della memoria storica: la '*Digital Preservation*' e l'ambizioso progetto '*Internet Archive*'

La Rete, con le sue infinite sfaccettature, le centinaia di siti clone, o mirror, consente di far rivivere continuamente l'informazione, determinando l'impossibilità anche solo di pensare alla rimozione di un dato da un sistema, che sembra reagire ad un simile tentativo, moltiplicandolo, quasi come se i 'siti mirror' fossero anticorpi in grado di ribellarsi alla rimozione del sito principale.

Ma è realmente possibile che la Rete garantisca l'immortalità del dato digitale, preservando la memoria storica e restituendo l'incommensurabile patrimonio digitale a distanza di millenni?

Scritture antiche, affidate alla pietra o al papiro, seppure emaciate dal trascorrere del tempo, consentono, tuttavia, la trasposizione di un messaggio ancora fruibile. Probabilmente altrettanto non potrebbe dirsi per i miliardi di dati digitali che ogni giorno sono generati, nonostante la sconfinata capacità di archiviazione, oggi garantita dagli apparati tecnologici.

In una società digitale, priva di supporti cartacei - paperless society -, il dato digitalizzato sarà il solo a circolare, sicché la grande sfida della conservazione digitale sembra oggi indispensabile al fine di preservare la cultura, la conoscenza ed il patrimonio informativo della civiltà umana.

[286] G. ZICCARDI, *Il libro digitale dei morti: memoria, lutto, eternità e oblio nell'era dei social network,* Torino, 2017, 110.

La vita del dato digitale è in pericolo per l'obsolescenza di quella stessa tecnologia che lo ha reso 'dato', consentendogli di uscire dallo status di 'idea'.

La '*digital preservation*'[287] mira, appunto, ad individuare le strategie di conservazione di lungo periodo dei dati digitali. Si tratta di un insieme di buone prassi e scelte tecnologiche che permettono di evitare le insidie legate al deterioramento delle informazioni digitali e alla principale minaccia della conservazione nell'ambiente digitale: l'obsolescenza tecnologica.

I supporti di conservazione oggi in uso hanno una prospettiva di vita di gran lunga inferiore rispetto a quella di un papiro o di un libro stampato su carta e, per tale ragione, è necessario che i dati digitali conservati cambino supporto prima che diventino illeggibili a seguito del deterioramento dello stesso.

Un problema di non scarsa rilevanza è legato alla sostenibilità non solo dei dati, ma anche dei software che li gestiscono nel lungo periodo, per conferire loro immortalità, preservandone la vita eterna e la perpetuazione dei contenuti digitali.

L'obsolescenza dei supporti di memorizzazione, che subiscono un'evoluzione sempre più rapida e profonda, unitamente all'obsolescenza dei formati digitali, determinata dall'inesorabile successione di programmi software, espongono a serio pericolo la stessa accessibilità dei dati digitali.

Bisognerebbe generare software in grado di interpretare i dati del passato e produrre dati che possano essere compresi nel futuro, prevedendo, altresì, programmi che riescano a processarli al meglio e strumenti idonei per continuare ad utilizzarli al meglio, allo scopo di mantenere in vita l'unica via per la trasmissione della conoscenza.

Potrebbero essere d'aiuto le tecniche di virtualizzazione ed emulazione, che consentirebbero di mantenere i dati accessibili nel tempo, attraverso la creazione di ambienti all'interno dei sistemi che si stanno utilizzando, per consentire la riproduzione e l'utilizzazione di programmi ed ambienti obsoleti, come se fossero computer all'interno di altri computer o sistemi operativi all'interno di altri sistemi operativi.

Altra tecnica potrebbe essere la 'simulazione' che comporta la creazione di software, gli emulatori, in grado di emulare un computer, un ambiente: software in grado di superare le incompatibilità ed eseguire le applicazioni su programmi, su cui non sono supportate.

---

[287] Per un'introduzione al tema della digital preservation dei contenuti digitali, soprattutto delle news, si veda l'articolo di M. BROUSSARD, *The Irony of Writing Online About Digital Preservation*, in *The Atlantic*, 20 novembre 2015.

Al di là di queste tecniche, più o meno avanguardistiche, si è presa coscienza della difficoltà, spesso insormontabile, di preservare, nel lungo periodo, le informazioni a causa della fisiologica deperibilità di software e dati, pubblici o privati.

L'incessante e inarrestabile evoluzione tecnologica ha determinato uno smisurato aumento della capacità di memorizzazione delle informazioni, senza preoccuparsi della durata fisica dei sistemi di *storage*, ossia dei supporti che consentono la conservazione dei dati digitali.

E proprio al fine ultimo di mantenere inalterata la memoria del Web, negli anni Novanta del solo scorso, è partito il progetto 'Internet Archivie': Wayback Machine'[288] un gigantesco archivio di pagine web, mirante a recuperare informazioni da più siti web possibili e a custodire nel suo archivio anche le varie versioni di un medesimo sito, susseguitesi nel tempo.

E' così possibile che una pagina scoperta attraverso il motore di ricerca, che risulti scomparsa ad una normale 'chiamata' del programma di navigazione, sia raggiungibile in copia attraverso *webarchivie. Org.*: mediante il semplice inserimento dell'indirizzo, in caso di archiviazione della pagina, questa risulterà nuovamente accessibile.

Inserendo l'indirizzo, in realtà, sarebbe possibile ottenere qualcosa di ancora più ampio e significativo dell'accesso alla pagina Web cercata: ove questa avesse subito variazioni nel tempo, attraverso una tabella divisa per anni, sarebbe possibile accedere alle diverse versioni della pagina web.

Un poderoso progetto, sicuramente un'architettura della Rete, che permette, nel contempo, alla pari di una biblioteca virtuale, di tramandare il sapere alle future generazioni, consentendo loro di reperire la storia dal Web e che porta ad affermare che il problema oggi non sia solo 'dimenticare', ma anche e soprattutto ricordare per evitare di svuotare di contenuti la storia dell'era digitalizzata.

4.2) Morte dell'oblio o tutela solo provvisoria?

La pretesa di cancellare i dati, in questa corsa continua alla generazione di informazioni, richiama un po' la metafora del cucchiaino con cui si vorrebbe svuotare il mare. Il mondo del Web, con l'avvento di Internet, realtà talmente pervasiva da aver rivoluzionato le

[288] Le osservazioni di Rogers su archivi Internet e Wayback machines sono tratte da R. ROGERS, *Metodi digitali*, *Il Mulino*, Bologna 2016, 101 e 103.

relazioni tra gli esseri umani e soprattutto quelle dell'uomo con se stesso[289], ha determinato la completa immersione dell'uomo in un flusso continuo di informazioni, che si alimenta perennemente e non dà la possibilità di distinguere chi si adoperi per incrementarlo e chi, invece, si limiti ad usufruirne.

A differenza del passato, quando l'informazione era scelta da operatori qualificati del settore per essere sottoposta all'opinione pubblica, con Internet le notizie sono sempre in Rete, a disposizione degli utenti, con la conseguenza che ognuno, in qualsiasi momento, possa entrarne in contatto. Internet: un'immensa piattaforma, un'enorme banca di banche dati, continuamente arricchita da informazioni immesse da chiunque voglia farlo.

Una rete di reti. Caratterizzata da illimitatezza, in quanto i computer che possono prendervi parte sono potenzialmente infiniti, globalità, poiché chiunque, in grado di accedervi, può fruirne e diventare egli stesso creatore di contenuti, disorganizzazione, considerata la presenza di molteplici criteri di organizzazione creati dall'uomo per ordinare o dettati dalle stesse tecnologie che, tuttavia, sono applicati disordinatamente, densità, in quanto consente di concentrare un gran numero di informazioni in uno spazio fisico limitato, evanescenza, in quanto il dato digitale, rispetto a quello fisico è più propenso a rovinarsi e sparire, persistenza, quale rovescio della medaglia rispetto all'evanescenza, perché consente di recuperare informazioni intelligibili anche se sono state cancellate e anche a distanza di tempo.

In questo apparato sconfinato di informazioni, notizie, dati, immagini e video, riguardanti persone ben individuate, riprodotti e circolanti spesso nella loro totale inconsapevolezza, l'interrogativo è se sia ancora possibile parlare di oblio o se il suo esercizio, sia pure azionabile, rappresenti una magnanima illusione, destinata ad impattarsi quotidianamente con una realtà ben più audace di quanto sia immaginabile[290].

Un documento, o più in generale, un dato, una volta immesso in Internet e reso disponibile ai naviganti, esce immediatamente dalla sfera di disponibilità dell'autore o del sito sorgente, ove era primariamente apparso, essendo verosimilmente possibile che venga

---

[289] Così per F. DI CIOMMO, *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003; nonché Id, *Evoluzione tecnologica e categorie civilistiche*, in E. RUSSO (a cura di), *Interpretazione della legge civile e «ragione giuridica»*, Padova, 2003, 141; Id., *Internet e crisi del diritto privato: globalizzazione, dematerializzazione e anonimato virtuale*, in *Rivista critica di diritto privato*, 2003, 117.

[290] In proposito, si rinvia a F. DI CIOMMO, *Diritti della personalità tra media tradizionali e avvento di Internet*, in G. COMANDÉ (a cura di), *Persona e tutele giuridiche*, Torino, 2003, 3 e ss., nonché M. NISTICÒ-P. PASSAPAGLIA (a cura di), *Internet e costituzione*, Torino, 2014.

copiato e dunque memorizzato da altri siti e, quindi, raggiunto da qualsiasi altro utente abilitato. Una volta immessa l'informazione in quell'insieme articolato di connessioni che costituisce la Rete, non esiste tecnicamente la possibilità di rimuoverla da tutti i supporti che la contengono e di impedire che, a distanza di tempo, possa tornare in vita. Un qualsiasi contenuto, ingoiato dai canali del Web, entra nella libera disponibilità di qualunque utente, cui sarà consentita non solo la possibilità di fruirne, ma anche di copiarlo, condividerlo, trasporlo in pen-drive, in cloud, riversandolo negli anfratti della Rete, sicché esso risulterà presente in diversi siti e in diverse forme contestualmente.

E prevenire la copia delle informazioni è un compito improbo, se non impossibile. Nel mondo digitale, caratterizzato dallo sharing continuo di contenuti, non si tratta solo di impedire che permangano disponibili le informazioni personali di ciascuno, pubblicate dalla fonte originaria, quanto, piuttosto, di eliminare anche le successive ripubblicazioni delle stesse da parte di soggetti terzi. Pertanto, è l'architettura stessa dell'ambiente digitale, ed ancor più il panorama dei social network e dei motori di ricerca, che rende impossibile cancellare, ovvero distruggere per sempre quelle informazioni non più attuali, né di pubblico interesse, connesse al passato di ciascuno. La Rete ha diversi livelli e la parte visibile è quella indicizzata dai motori di ricerca; quella invisibile, invece, costituisce gran parte di Internet e comprende le reti private, siti cui per accedere sono necessari username e password. Uno spicchio di questo mondo sommerso è il Dark Web, fatto di reti in cui il traffico è crittografato e gli utenti sono anonimi: il diritto all'oblio dipende da quanto in profondità siano precipitate le informazioni immesse in Rete. Sono proprio i contenuti che raggiungono gli abissi, le profondità più recondite, precipitando nel Dark Web, quelli più difficilmente estirpabili. Si tratta dei contenuti più pruriginosi, scandalosi o estremi. Nel mondo digitale di Internet le informazioni possono essere memorizzate, duplicate, condivise con estrema facilità, con la conseguenza che tutte continuano a permanere, senza esigenza di selezione, in quanto le memorie al silicio sono pressoché illimitate e nel cloud non si ha contezza concreta di dove sia stata memorizzata e di chi vi abbia provveduto, duplicandola, indicizzandola e pubblicandola. La vastità di questa piattaforma digitalizzata, pertanto, non gioca certo a favore dell'oblio! Ed inventare una regolamentazione efficace è impresa davvero ardua: le dinamiche che si possono verificare on-line sono infinite ed imprevedibili. Per assurdo la scomparsa di alcuni articoli dai siti di quotidiani on-line, famosi in tutto il mondo, potrebbe determinare

l'effetto contrario, accendendo nuovamente il dibattito sulla sparizione ma anche sul contenuto improvvisamente scomparso da Google.

Viepiù, la Rete si presenta con diverse memorie virtuali: i motori di ricerca sono relativamente pericolosi perché possono essere controllati, ma anche perché si limitano a mostrare quello che trovano e, nel tempo, tendono a dimenticare, dismettendo i risultati più vecchi in favore dei nuovi. Tuttavia, attraverso la funzione c.d. "memoria cache", molti motori di ricerca operanti sul Web mettono a disposizione degli utenti una copia di dati testuali di ogni sito Internet archiviato, per quando la risorsa originale sarà irraggiungibile, finendo così per svolgere una vera e propria attività di memorizzazione di tutti i contenuti della Rete, affinché Internet non dimentichi nulla e nulla possa essere distrutto una volta caricato online[291]. Questo comporta l'impossibilità per gli utenti di lamentare la violazione del diritto all'oblio allorché la singola informazione indesiderata sia raggiunta mediante un semplice clic, finendo puntualmente per riemergere. E comunque, ove la lagnanza dovesse trovare accoglimento, il problema non sarebbe risolto perché il dato, sia pure eliminato da alcuni siti, continuerebbe a vivere in altri e numerosi, annullando gli sforzi di lunghi e dispendiosi processi, finalizzati all'ottenimento del diritto ad essere dimenticati. Si profila il paradosso, infatti, che il diritto all'oblio in Internet sia impossibile, una mera utopia, perché Internet non dimentica!

Ed è giusto che sia così: un archivio di qualità deve essere connotato da completezza, capacità di conservare a lungo le informazioni, consentendone, nel contempo, un accesso semplificato. Tutto quanto immesso in Internet diviene indelebile e resta memorizzato senza un termine di scadenza, sicché il diritto all'oblio probabilmente è morto o versa in condizioni di salute alquanto precarie[292]. Così, la conoscenza, la storia, il passato di ciascuno, albergano prepotentemente nella Rete, sfidando le leggi dello spazio e del tempo, impedendo il processo catartico del dimenticare e lasciando l'essere umano intrappolato nelle sue fragili e spesso disonorevoli radici, senza possibilità di alleggerirsi

---

[291] Cfr. V. M. SCHONBERGER, *Delete. Il diritto all'oblio nell'era digitale*, op. cit.; ID., *Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing*, in *KSG Working Paper*, Harvard, 2007, nel quale l'autore già proponeva, per ovviare alla impossibilità attuale di cancellare i contenuti di Internet, di utilizzare accorgimenti tecnologici che prevedano la distruzione degli algoritmi decorso un certo lasso di tempo dall'immissione del dato in Rete.

[292] Il 20 novembre 2012 la ENISA, European Network and Information Security Agency, ha pubblicato uno studio intitolato The right to be forgotten - between expectations and practice, nel quale si evidenza come sia tecnicamente pressoché impossibile, allo stato, ottenere con certezza la cancellazione definitiva di un qualsiasi contenuto pubblicato in Internet.

del passato e condannato all'ergastolo della sofferenza on-line. Senza dubbio, possono correre in soccorso delle operazioni, anche sofisticate, finalizzate a ridurre la visibilità di talune informazioni, che concedono però esclusivamente un oblio momentaneo in quanto il processo di digitalizzazione e la moltiplicazione dell'informazione nei più reconditi anfratti della Rete non abbatte completamente il rischio che quei contenuti tornino prepotentemente alla ribalta ed abbiano nuova vita online[293]. Tutte le operazioni miranti all'offuscamento ed alla riduzione di visibilità per talune informazioni possono garantire una soddisfazione relativa e solo momentanea per il soggetto che si senta leso, assicurando esclusivamente un oblio istantaneo, ma non a lungo termine[294].

5) Le ragioni socio-economiche che impedirebbero il decollo del diritto all'oblio

La pretesa ad essere dimenticati dalla Rete, a differenza di altri diritti, che pur attengono alla tutela della persona e della sua sfera intima, stenta a decollare, sia per ragioni politico-economiche, che per la sua confliggenza con ulteriori e non meno rilevanti diritti fondamentali, che trovano eguale fondamento giuridico nella Carta costituzionale. Come già visto in precedenza, i motori di ricerca più che cancellare, tendono a immagazzinare dati, a nutrirsi d'informazioni: il dato è la loro benzina, più ne ingabbiano, elaborano, commercializzano, più in maniera esponenziale si moltiplicano i loro introiti.

Così, la rimozione su larga scala di informazioni, su richiesta degli utenti, potrebbe creare buchi informazionali tali da rendere imprecisa o intralciare l'attività di profilazione, che è il punto di forza nel business di tutte le società.

Per Mark Zuckerberg "il diritto alla riservatezza è una vecchia regola che la gente ha ormai archiviato con i suoi comportamenti"[295]. Ed, infatti, i giovani, a parere del padre di

---

[293] Si è, altresì, rischiato un paradossale effetto boomerang, a danno di coloro che sono riusciti ad ottenere da Google l'agognata de-indicizzazione. A seguìto dell'epocale sentenza Google Spain, è nato in Rete un servizio, l'Hidden from Google, che prova appieno l'inefficacia dell'applicazione del presunto diritto all'oblio: attraverso un server, ubicato ovviamente fuori dall'Europa, sono stati catalogati tutti i risultati deindicizzati, aggiornando la lista man mano che Google accoglieva ed accoglie le istanze dei richiedenti oblio. Il progetto ha determinato un effetto boomerang: i cybernauti, che, svolgendo una comune ricerca tramite Google, si fossero imbattuti in una o più risposte prive di un effettivo collegamento al contenuto informatico, in quanto obliato, spinti dalla curiosità di conoscere il contenuto misterioso dell'informazione oscurata l'avrebbero rinvenuta utilizzando il servizio Hidden from Google.

[294] Come sostenuto da F. DI CIOMMO, *Internet e crisi del diritto privato: globalizzazione, dematerializzazione e anonimato virtuale*, in *Riv. crit. dir. priv.*, 2003, sarebbe opportuno cercare soluzioni metodologiche avanzate, maggiormente in linea con il diritto di Internet, nuove grandezze e dimensioni utili a superare le sfide del Terzo Millennio.

[295] Questo pensiero espresso da Mark Zuckerberg nel corso di un'intervista rilasciata al Corriere della Sera, in data 11 gennaio 2010. Il fondatore e CEO di Facebook dichiarava ancora: «Ormai gli utenti condividono

Facebook, sarebbero sempre meno preoccupati per la diffusione dei loro dati personali e la possibilità di renderli pubblici è la benzina che alimenta Google e le altre reti sociali.
Se la motivazione ufficiale fornita dal fondatore di Facebook è quella di ritenere il concetto di privacy stereotipato e superato, anche in forza dei comportamenti che assumono i giovani, alle spalle di una tale valutazione ufficiale si cela tutto il business economico che il giovane fondatore del social ha realizzato con la massiccia raccolta quotidiana d'informazioni, la cui manipolazione, rielaborazione e trasformazione in profilazioni, l'hanno portato ad essere uno degli uomini economicamente più influenti del pianeta.
La verità è, quindi, che nel terzo millennio la vera ricchezza è rappresentata dai dati: le compagnie che stanno vivendo la crescita maggiore nel settore delle nuove tecnologie sono quelle che hanno saputo instaurare una relazione precisa con i clienti, che oggi non sono più un semplice target di offerte promozionali indistinte, ma un vero e proprio partner con cui costruire un'offerta sartorializzata e accattivante[296].
La raccolta dei dati è diventata parte integrante, se non addirittura la più importante, di una qualsiasi strategia di marketing, in forza del meccanismo della profilazione che comporta un funzionamento ottimale di entrambi i lati della catena di commercio: da una parte il lato utente, perché si inviano suggerimenti pubblicitari più vicini ai reali interessi del potenziale consumatore; dall'altra parte il lato azienda, perché si consente ai giganti del Web di vendere pacchetti altamente caratterizzati, distinti per età, sesso, religione e molte altre variabili, che contribuiscono a rendere i prodotti più appetibili per le varie tipologie di utenti.

---

senza problemi le informazioni personali online. Le norme sociali cambiano nel tempo. E così è anche per la privacy. Quando ho iniziato a pensare a Facebook nella mia cameretta di Harvard, in tanti si chiedevano: 'Perché mai dovrei mettere informazioni online? Perché dovrei avere un sito personale?' Poi è iniziata l'esplosione dei blog e di tutti gli altri servizi che permettono di condividere informazioni online. Le abitudini sociali evolvono nel tempo».

[296] Ogni azione che si compie in un ambiente digitale interattivo viene tracciata, analizzata e conservata in un gigantesco database di profili utente, che cresce ogni giorno, costruendo un archivio globale fatto di comportamenti di acquisto, stili di vita, dati socio demografici. Se è pur vero che i dati di profilo utente sono resi anonimi, tradotti cioè in numeri identificativi di uno specifico insieme di attributi, i consumatori non sanno esattamente quali sono tutte le informazioni che i giganti del web raccolgono sui loro comportamenti, "schedandoli" ogni giorno mentre navigano all'interno di un social, fanno una ricerca on-line, utilizzano un servizio di e-mail. Il loro "file" cresce ogni giorno, con centinaia di dati che vengono pazientemente raccolti, classificati ed elaborati in modo da costruire profili appetibili per inserzionisti pubblicitari pronti ad acquistarli.

Nel nuovo capitalismo digitale, i dati non sono il petrolio che consente la produzione dell'energia che muove l'economia, ma diventano il nuovo fattore della produzione. Sono di proprietà degli utenti, che li cedono per l'utilizzo alle aziende, pur non ricevendo un compenso, nè partecipando al processo di distribuzione della ricchezza.

E' questo il motivo per il quale il motore di ricerca è sempre stato poco incline e disposto ad operare, più o meno chirurgicamente, sui dati, posto tra l'altro in una situazione di quasi monopolio per ciò che attiene alla valutazione dei link da rimuovere.

Considerato anche il rischio dell'assenza di oggettività, l'auspicio è sempre stato quello di fare in modo che le Autorità Garanti della Privacy, nei singoli Stati nazionali, assumessero un ruolo sempre più incisivo, operativo e formalizzato, per assicurare un corretto bilanciamento tra la tutela della riservatezza e l'interesse pubblico a conoscere le notizie da rimuovere dalla Rete, su istanza della parte interessata.

L'azione dei motori di ricerca, pur essendo in posizione di terzietà tra l'interessato alla cancellazione e il sito sorgente produttore dell'informazione, e in quanto tale interessato alla permanenza della stessa, è comunque unilaterale: i siti sorgente non possono obiettare in alcun modo e la discrezionalità di Google e dei suoi competitor, nel valutare la richiesta di cancellazione dei link, è totale.

Ove l'istanza di cancellazione dovesse essere respinta dal motore di ricerca, l'interessato avrebbe, comunque, la possibilità e la speranza di vedere accolte le sue ragioni da altri organi amministrativi o giudiziari; ma se il motore di ricerca, così come è successo nell'immediatezza della Google Spain, anche per timore di pesanti sanzioni, dovesse 'tagliare' in maniera coraggiosa, la memoria storica sarebbe gravemente vulnerata.

In aggiunta, l'Unione europea, in relazione al cd. 'diritto di notifica', che il motore di ricerca deve assecondare nei confronti dei siti sorgente per informarli delle richieste di de-indicizzazione, ha invitato Google ad una maggiore cautela nell'esplicazione dell'attività d'informazione delle avvenute rimozioni perché, in questo modo, venendo meno l'anonimato di chi ha chiesto di essere dimenticato dal Web, si andrebbe ulteriormente a violare la sua privacy, vanificando gli effetti dell'esercitato diritto all'oblio.

E', altresì, vero che i motori di ricerca sono stati sempre poco inclini a tagliare, consci che la possibilità riconosciuta agli utenti di cancellare i dati che li riguardano, rendendo

sempre provvisorio e revocabile il possesso degli stessi, avrebbe indebolito il loro valore, anche a fini economici.

Se fosse, infatti, riconosciuto, in maniera risolutiva, il diritto dell'utente alla cancellazione delle informazioni sulla sua persona, nessun fornitore di servizi in Rete saprebbe a priori per quanto tempo potrebbe trattarle e ciò conferirebbe un'elevata dose d'imponderabilità alla mole di traffico on-line e alla sua capacità di generare reddito[297].

D'altro canto, la motivazione economica a fondamento dell'avarizia nel praticare tagli chirurgici alle informazioni presenti in Rete costituisce un punto di forza per la tutela della memoria storica e collettiva.

Il nuovo petrolio però non è patrimonio di tutti ma una ricchezza che stanno accumulando pochi soggetti capaci di grandi investimenti in tecnologie e conoscenze, come Google e Facebook, per cui anche l'industria dei dati finirà per accrescere ulteriormente le disuguaglianze tra ricchi e poveri, tra i grandi colossi dell'informazione e le piccole imprese.

La stretta di mano sui dati farà la fortuna di Google e Facebook. L'entrata in vigore della GDPR, che tra gli obiettivi principali vede, oltre all'armonizzazione delle norme sulla Data Protection in Unione europea e dall'Unione europea verso il resto del mondo, soprattutto la regolarizzazione di attività di marketing e profilazione svolte dai grandi gruppi societari, potrebbe rivelarsi un vantaggio per i colossi del Web, come Google e Facebook, costituendo un ulteriore spinta ad un business già ultramiliardario e rischiando di penalizzare le piccole imprese, indebolendone la concorrenza. Ci sono più fronti su cui i big della tecnologia potranno vincere. La GDPR, infatti, ha posto una serie di obblighi a carico dei titolari/responsabili del trattamento, che si rivelano particolarmente dispendiosi dal punto di vista economico ed obbligano il motore di ricerca a porre in essere attività ulteriori, che richiedono la presenza di nuove figure professionali, oltre a grandi investimenti tecnologici.

A mero titolo esemplificativo vi è l'obbligo a carico di chi effettua il trattamento dati di operare la valutazione d'impatto prima di avviare il trattamento, che richiede l'uso di tecnologie particolarmente avanzate; la tenuta dei registri delle attività di trattamento, che comporta oltre alla necessaria presenza di particolari software, anche e soprattutto quella

[297] V. PORTALE- G. MIRAGLIOTTA, Osservatori Digital Innovation del Politecnico di Milano, *I tanti dubbi sul diritto all'oblio*, in *Agenda Digitale*, 7 novembre 2014.

di nuove figure professionali che debbano provvedervi; obbligo, quest'ultimo, previsto anche per le medie e piccole imprese, ad eccezione di quelle che trattino in maniera estemporanea informazioni specifiche per soddisfare le richieste della clientela, senza che tali informazioni siano concretamente utilizzabili per altri fini; la designazione del DPO: sebbene tale figura sia necessaria solo per ipotesi tassativamente previste, si sta facendo strada un'interpretazione in base alla quale sarebbe sempre conveniente individuare un responsabile indipendentemente dal coefficiente di pericolosità del trattamento e della relativa protezione; il rispetto di codici di condotta[298]. Le medie e piccole imprese dell'informazione on-line non sono in grado di sopportare i costi di adeguamento alla GDPR, non avendo gli introiti dei grandi colossi che, grazie agli investimenti operati nelle tecnologie più avenieristiche, aumentano sempre più il fatturato e i connessi guadagni.
Il gruppo Alphabet ha visto aumentare gli introiti pubblicitari, a scapito dei concorrenti, grazie al fatto che ha quasi interamente completato la raccolta del consenso degli utenti a ricevere ADS mirate. Merito ovviamente delle ingenti risorse di cui dispone il colosso di Mountain View per raccogliere in tempi rapidi il sì al trattamento dei dati, mentre i competitor procedono a ritmi più lenti. Lo strumento di Google DoubleClic Bid Manager [299](ODBM), usato dai buyer per acquistare pubblicità mirate on-line, sta indirizzando un numero crescente di risorse, stanziate dagli inserzionisti verso il mercato interno di Google a scapito di altri mercati di ADS digitali, dove Google dice di non riuscire a verificare che ogni individuo, cui vengono mostrate le pubblicità mirate, abbia dato il consenso. In questi casi, il colosso Google reindirizza gli investimenti verso il proprio

[298] La normativa in questione è entrata in vigore in un clima in cui serpeggiava il malumore, il senso di sfiducia e il timore per le nuove sanzioni (art. 83). In questo quadro, le imprese invocavano legittimamente flessibilità nei controlli e una più stretta collaborazione con il Garante della privacy.
Di conseguenza, sul modello del periodo di grazia già ottenuto in sede europea dalla Francia, si chiedeva la concessione di una fase transitoria di sei mesi nel corso della quale non avrebbero potuto essere irrogate sanzioni alle imprese che, a seguito di ispezioni, fossero rimaste indietro rispetto ai nuovi adempimenti. In altri termini, appariva opportuno concedere un lasso minimo di tempo per consentire ai soggetti interessati di completare i propri piani di adeguamento alla nuova normativa ed evitare quindi di incorrere in sanzioni considerevolmente onerose.
[299] Google renderà disponibili le inventory della tv tradizionale su DoubleClick Bid Manager negli Stati Uniti, fornendo agli inserzionisti anche metriche di analytics sull'impatto che la pubblicità sul grande schermo ha sulle attività search. Il che vuol dire che un brand che pianifica su Google potrà misurare l'aumento delle ricerche dei suoi prodotti su Google o YouTube dopo la messa in onda dello spot televisivo. Una novità con cui Google punta a "consentire ad aziende ed agenzie di gestire le loro campagne video su tv lineare e digitale in un modo più efficiente ed efficace", secondo quanto ha rivelato la stessa azienda. Attraverso DBM, infatti, i brand avranno una singola piattaforma per la gestione integrata delle campagne televisive e di digital video. In ultima istanza, la novità avvicinerà sempre più le modalità di acquisto dei due media, anche da un punto di vista delle misurazioni.

sito. Havas SA[300], uno dei maggiori buyer mondiali di ADS, ha detto di aver osservato un incremento a due cifre della spesa degli inserzionisti sul mercato di ADS di Google, tramite DBM, nel primo giorno di entrata in vigore della GDPR, lo scorso 25 maggio.
Luc Vignon, di Regie 366, che vende spazi pubblicitari per 12 gruppi editoriali francesi, ha avuto modo di affermare: «è presto per parlare di un trend consolidato, ma abbiamo visto un incremento nei volumi della piattaforma di Google ed un calo nelle altre»[301]. Inoltre Google ha intenzione di entrare presto in un sistema esterno, quello di IAB Europe[302], dove i siti Internet potranno trasmettere i moduli degli utenti online con il loro consenso, in conformità alla GDPR ed al tempo stesso stimola l'acquisto di ADS dal suo data base, dove è sicura che il consenso degli utenti alla pubblicità mirata sia stato fornito. Alphabet[303] ha, tuttavia, fatto sapere che sta usando soluzioni per evitare eccessivi squilibri, distribuendo ad esempio ADS non personalizzate sui siti di chi non ha un consenso esplicito degli utenti. Questa forte concentrazione economica nelle mani del motore di ricerca ha portato il Financial Times a scrivere che la GDPR avrebbe fatto un gran bene a Google e Facebook, perché alla base della regolazione europea c'è la convinzione che l'utente avrebbe letto per filo e per segno le policies sulla privacy, scegliendo di conseguenza come fare utilizzare i propri dati della piattaforma Web. Nei fatti le policies restano complesse, anche perché l'ecosistema di dati da cui Facebook e Google generano affari è estremamente sfaccettato e quasi sicuramente accadrà che l'utente darà rapidamente il consenso alla sua piattaforma preferita, pur di continuare ad

[300] Havas SA è un gruppo francese di consulenza nella comunicazione di impresa, principalmente mediante l'agenzia pubblicitaria Havas World Wide, e di acquisto di spazi pubblicitari, principalmente attraverso la succursale Havas Media. Due distinte imprese hanno portato il nome Havas: la prima, esistita dal 1835 al 1998, data della sua acquisizione da parte della Compagnie Generale des Eaux. La seconda è un'ex filiale della prima, chiamata Havas advertising, che è stata rivenduta ed ha ripreso il nome Havas nel 2002. Nel 2017 Havas, società quotata alla Borsa di Parigi è stata il primo gruppo pubblicitario in Francia ed il sesto a livello mondiale.
[301] Per un approfondimento dell'argomento in questione, si veda P. Licata, GDPR, è Google il vero vincitore delle regole europee. Boom di vendite di pubblicità digitali, in CorCom, 1° giugno 2018. A parere dell'autrice, la velocità di compliance dell'azienda rispetto alle piattaforme concorrenti la collocano in una posizione di forza maggiore. Per i rivali calo fino al 50% sul proprio inventario, mentre Google vende ADS mirate a prezzi quasi quattro o cinque volte superiori di quelle non personalizzate.
[302] IAB Europe è la federazione nata per promuovere e tutelare gli interessi dei player della comunicazione digitale interattiva in Europa, favorendo la cultura dell'advertising online attraverso la divulgazione di dati, regole e best practice.
[303] Alphabet Inc. è un'azienda statunitense, fondata nel 2015, a cui fanno capo Google Inc. ed altre società controllate. Ha sede in California e la sua fondazione ha risposto a due necessità: quella di rendere più trasparenti le attività inerenti a Google, il marchio più conosciuto in assoluto del gruppo e quella di concedere una maggiore autonomia alle società del gruppo che operano in settori diversi da quello dei servizi Internet.

usarla. Nonostante il Data Gate, i giganti dell'Hi-Tech continuano a godere di un potente asset: la fiducia dei loro utenti. Dopo il recente scandalo "Cambridge Analytica"[304], si pensava ad un passo indietro di Zuckergerg che, invece, ha avuto dalla sua l'onda lunga del pentimento mediatico che ha portato gli utenti del social ad un'invariata fede in Facebook o, addirittura, ad un boost di fiducia rispetto al passato.

Molti dei player minori potrebbero non avere lo stesso carisma di Google e Facebook nell'attrarre consensi all'uso dei dati. Facebook, infatti, ha affermato di non aspettarsi defezioni e Google ha addirittura ammesso che la GDPR potrebbe costituire un vantaggio indiretto per il business, indebolendo la concorrenza. Apple si muove in una posizione privilegiata, da un lato, e di svantaggio, dall'altro. Dovrà investire meno perché in sostanza la policy aziendale combacia con i punti cardine del nuovo Regolamento. La società non prevede per statuto la diffusione dei dati personali dei propri utenti. Le informazioni restano confinate sul singolo dispositivo e se, invece, vengono condivise nel cloud, sono crittografate e rese inaccessibili. Gli aggiustamenti compiuti in ottica GDPR, quindi, sono marginali: dalla possibilità di scaricare i propri dati, alla richiesta esplicita all'utente di consentire ad Apple, e non a soggetti terzi, di utilizzare e memorizzare dati personali in situazioni specifiche. Economicamente però l'accesso ad un minor numero di dati, rispetto a Google e Facebook, ha marginalizzato l'azienda nel mercato della compravendita on-line e l'ha lasciata indietro. La GDPR, in questo caso, potrebbe fungere

[304] Cambridge Analytica è stata fondata nel 2013 da Robert Mercer. Un miliardario imprenditore statunitense, con idee molto conservatrici. Specializzata nel raccogliere dai social network un enorme quantità di dati sui loro utenti: quanti "mi piace" mettono e su quali post, dove lasciano il maggior numero di commenti, il luogo da cui condividono i loro contenuti e così via. Queste informazioni sono poi elaborate da modelli ed algoritmi per creare profili di ogni singolo utente. Più "mi piace", commenti, tweet ed altri contenuti sono analizzati, più preciso è il profilo di ogni utente. La società è accusata di aver utilizzato illegalmente i dati di milioni di utenti di Facebook, al fine di arricchire il proprio database, parte dell'offerta che rivolge a partiti politici e grandi società con il fine di targhettizzare le campagne e migliorare i risultati di conversione. Ha contribuito alla vittoria di Donald Trump alle elezioni statunitensi del 2016 e quella del Sì all'uscita del Regno Unito dall'Unione europea in occasione del referendum Brexit. Quando la società cominciava a muovere i primi passi, la politica di Facebook era ancora molto permissiva e le App esterne potevano usare gli utenti per raccogliere le informazioni sui loro contatti, senza che la persona fosse avvertita, ma con una semplice specificazione delle varie condizioni che gli utenti spesso non leggono. Facebook, in seguito, decise di limitare queste intrusione, modificando i suoi sistemi e divenendo meno permissiva con i dati dei suoi utenti. Aleksandr Kogan, ricercatore presso l'Università di Cambridge e creatore dell'App "thisisyourdigitallife", utilizzava le tracce, lasciate dagli utenti su Facebook, per tracciare profili abbastanza accurati di ciascuno. Divenuta Facebook meno permissiva con i dati del suoi utenti, Kogan decise di violare i nuovi termini di utilizzo e vendette i dati che aveva raccolto a Cambridge Analytica. Vendita vietata da Facebook e sanzionata con sospensioni e cancellazione dell'account del colpevole. Da indiscrzioni, pare che la società di Zuckerberg, pur essendo al corrente di questo traffico di dati, non fece nulla. Che la società lo sapesse o meno, ciò che è certo è che fino al 16 marzo 2018, l'account di Cambridge Analytica era ancora attivo e libero di operare.

da livella e portare i big dell'informatica mondiale ad una quota via via paritaria, quantomeno in Europa. Un rafforzamento del dominio delle piattaforme dominanti: conseguenza ben lontana dalle intenzioni del Legislatore europeo.

Anche sul fronte delle sanzioni, l'entrata in vigore della nuova normativa europea potrebbe suonare come una possibile condanna a morte per le piccole e medie imprese. Un sondaggio effettuato da NetApp sul Regolamento[305] evidenzia come il 76% delle aziende statunitensi sia preoccupato per l'introduzione della GDPR (contro il 64% delle controparti europee). Negli USA, infatti, si teme un potenziamento del monopolio d*e facto* dei grandi competitor, dei soliti Google e Facebook in particolare, considerato che l'85% della pubblicità online appartiene a loro. Entrambi, infatti, sarebbero toccati marginalmente dalle sanzioni (multe equivalenti al 4% del fatturato aziendale, fino ad un massimo di 16 milioni di Euro), che, invece, potrebbero rivelarsi distruttive per le piccole realtà non adempienti agli obblighi regolamentari. I big sarebbero sì danneggiati, ma i piccoli competitor lo sarebbero maggiormente. A pochi mesi dall'entrata in vigore del Regolamento è apparso subito chiaro, da uno studio condotto sulle conseguenze dell'applicazione della GDPR relativamente ad imprese di un po' tutte le dimensioni, che le grandi aziende sono quelle abbastanza avanti nel percorso di adeguamento, in controtendenza rispetto a quanto ci si aspettava per via della maggiore complessità dell'organizzazione interna. Anche se da una parte è vero che le grandi aziende sono partite per tempo e con la giusta determinazione, iniziando a lavorare sulla GDPR ben più di un anno prima della sua entrata in vigore, non può non condividersi l'affermazione di chi ritiene che il Regolamento sia alla portata solo di una parte del mercato, quella maggiormente sensibile a regolamenti e normative, tecnologicamente più evoluta, mentre il resto stenta a reagire, anche imprenditorialmente, in modo adeguato. Il nodo realmente difficile da sciogliere è rappresentato dai costi degli investimenti necessari dal punto di vista tecnologico per l'adeguamento e ciò ha portato le aziende di piccole dimensioni ad essere suddivise in due categorie: quelle che, anche beneficiando di una dimensione più gestibile rispetto alle grandi aziende, hanno trovato i giusti tempi e modi per portarsi al corretto livello di compliance e quelle che sono ancora molto lontane dal raggiungimento del pieno rispetto di quanto richiesto dalla normativa europea. Posizione, quest'ultima,

[305] Riflessioni affrontate da G. SACCARDI, *A cinque settimane dall'entrata in vigore, il GDPR preoccupa le aziende*, in *Reportec,* 17 aprile 2018.

che non lascia eccessivi margini di tranquillità. Vi è, infine, da segnalare come le start up siano partite con il piede giusto, anche perché, rispetto ad organismi da tempo sul mercato, hanno la grande opportunità di regolarizzarsi sin dalla costituzione, sfuggendo, in tal modo, ai costi per i cambiamenti, cui sono, invece, sottoposte le imprese da tempo operanti nel mercato globale.

6) Le nuova Governance europea in materia di protezione dei dati personali: le ragioni politiche alla base del Regolamento europeo 2016/679

Nella società dell'informazione e dell'informatica, ove i dati degli utenti del Web sono raccolti massivamente, spesso senza che questi ne siano a conoscenza o, ancor più frequentemente, a seguito di un consenso quasi estorto perché espresso in modo disinformato[306], il diritto all'oblio appare l'unico strumento in grado di consentire ai titolari di riottenere un dominio, seppur solo precario e provvisorio, sui loro dati, limitando o parzialmente offuscando la loro libera circolazione nel Web.

Ma l'interesse dei cittadini a riappropriarsi del controllo delle informazioni che li riguardano si affianca ad altri interessi non meno rilevanti. Si pensi all'interesse della collettività ad informarsi ed essere informata, a ottenere risposte affidabili, nel senso di risposte che riflettano lo stato delle informazioni disponibili in Rete, che oggi si avvia a divenire il più efficiente e potente strumento di veicolazione del sapere e della conoscenza. Nonché l'interesse di editori o comuni utenti che pubblicano sul Web, desiderosi, forse anche per ragioni economiche, di diffondere il proprio pensiero e mantenerne la visibilità. E, senza ombra di dubbio, gli interessi prevalenti, che fanno da sfondo all'intervento a gamba tesa del Legislatore europeo con la nuova legge sulla protezione dei dati personali, sono quelli dei soggetti pubblici e privati a mantenere il controllo sui dati.

I dati, oro nero della Rete, oggi costituiscono uno strumento indispensabile per la profilazione degli individui, al fine di comprendere i loro gusti ed individuare le loro

[306] Tra queste tipologie di dati, rientrano i cookie, «*piccoli file di testo che i siti visitati dagli utenti inviano ai loro terminali, ove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla visita successiva». Si distinguono da questi i c.d. "cookie delle terze parti*», che «*vengono, invece, impostati da un sito web diverso da quello che l'utente sta visitando*». Ciò può avvenire in quanto «*su ogni sito possono essere presenti elementi (immagini, mappe, suoni, specifici link a pagine web di altri domini, etc.) che risiedono su server diversi da quello del sito visitato*». Cfr. Garante per la protezione dei dati personali, *Informativa e consenso all'uso dei cookie. Domande più frequenti*, disponibile al seguente link: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docwe b/3585077.

preferenze, ma sono altrettanto essenziali per le informazioni predittive di grande valore economico, sociale e politico, che da essi è possibile ricavare.

Si spiega, pertanto, facilmente la ragione per cui i colossi dell'informatica si affannino da decenni nella raccolta, condivisione ed elaborazione dei dati, il più delle volte in spregio ad ogni diritto alla privacy ed al corretto trattamento dei dati personali. In questa prospettiva, i dati non sono solo pregni di valore economico, ma costituiscono anche un incommensurabile strumento di potere[307]. E proprio in quanto espressione di supremazia e potere, la lotta per la regolamentazione di Internet e della privacy, nonché la rigida statuizione di regole per la sua applicazione territoriale, hanno animato il dibattito politico nel panorama internazionale, inasprendo i rapporti tra gli Stati.

Impossibile, pertanto, allontanare il sospetto che il nuovo Regolamento europeo per la protezione dei dati personali, identico nella sostanza alla normativa precedente, se non per l'aggiunta di talune regole più stringenti, altro non sia se non una reazione di carattere politico allo strapotere di Google e degli altri colossi americani dell'informatica. Gli Stati Uniti, patria delle maggiori aziende informatiche, nonché uno tra gli Stati più potenti al mondo, hanno negli anni accresciuto smisuratamente il loro potere: a loro le imprese europee si rivolgono per la fornitura di beni e servizi in ambito tecnologico, muovendo ingenti capitali oltreoceano e, cosa ancor più grave, fornendo una smisurata quantità di dati. I big dell'informatica americana, disonorando anche le più elementari forme di protezione di questo flusso transatlantico di dati, continuano ad accumularli, rielaborarli, trattarli indiscriminatamente, compiendo pratiche di profilazione massiva al dichiarato scopo di contribuire all'accrescimento di profitti e potere[308]. E', pertanto, ragionevole

---

[307]Per alcune riflessioni sull'argomento, si veda: A. MANTELERO*, The EU Proposal for a General Protection Regulation and the roots on the "right to be forgotten"*, in *Computer Law and Security Review*, 29, 2013, 229-335. Per la prima volta nella storia degli stati moderni, i principali detentori delle informazioni sui cittadini non sono più le autorità e gli organismi pubblici, ma le realtà private (le piattaforme software, i costruttori di device elettronici, i fornitori di servizi software su cloud, ecc.).
Dunque, se è vera l'equazione dati=potere, è vero anche che oggi stiamo assistendo ad una progressiva cattura del potere pubblico da parte di imprese guidate da un unico obiettivo, quello del profitto.

[308] Cfr. G. SARTOR- M. VIOLA DE AZEVEDO CUNHA *Il caso Google e i rapporti regolatori USA/EU, in Dir. Inform.,* 2010, 26, 645 – 671, secondo cui: «*Anche la libertà d'iniziativa economica viene spesso ad acquistare preminenza rispetto alla privacy nel contesto statunitense. Così la rilevazione e la cessione di profili di consumatori, la distribuzione di rapporti attinenti al credito, il riuso di dati personali per scopi diversi e ulteriori rispetto a quelli che ne hanno determinato la raccolta, sono ritenuti comportamenti leciti indipendentemente dal consenso dell'interessato. I vantaggi economici che queste pratiche possono comportare, facilitando gli scambi e la libertà d'iniziativa economica degli operatori, superano di regola, nella prospettiva statunitense, le esigenze di tutela della privacy, se non in ambiti nei quali i rischi siano particolarmente evidenti, come nel trattamento dei dati genetici*».

pensare che la 'privacy policy' dell'Unione europea rappresenti una reazione all'indiscriminato potere delle società americane, nell'ottica di promuovere le imprese europee, tutelare i propri cittadini e sviluppare un mercato unico digitale[309]. La sentenza Google Spain prima, ed il Regolamento europeo per la protezione dei dati personali poi, possono essere interpretati in forza del deliberato scopo di affermare la Governance europea dei dati, che non può non avere nella tutela dei dati il suo focus centrale. La deriva europeista, decisa all'affermazione della prospettiva europea, in aperto contrasto con quella statunitense, è stata alimentata anche dalle preoccupanti rivelazioni di Snowden e dai comportamenti fiscali, non propriamente leali, tenuti dai grandi operatori di Internet.

I grossi intermediari, infatti, hanno deciso di stabilire la propria sede europea a Dublino, in quanto, in forza degli accordi internazionali di quel Paese, è loro consentito ridurre in maniera significativa l'effettiva aliquota fiscale fino a valori minimi, inferiori al dieci per cento dei profitti. Come molte delle multinazionali, anche Google ha una capogruppo americana, la Google Inc., ed una capogruppo europea con sede in Irlanda, la Google Irland. La multinazionale, poi opera in Italia e negli altri Paesi dell'Unione, con proprie diramazioni, che però "prestano servizi" alle due società, Irland ed Inc. E dunque negli Stati europei dichiarano solo i redditi derivanti dai modesti compensi che ricevono dalle società superiori per i "servizi che prestano loro" e non quelli reali derivanti dalla vera attività. Questi, infatti, confluiscono tutti, utili compresi, nella capogruppo irlandese che paga le tasse in Irlanda, dove la fiscalità è ben più vantaggiosa.

Al fine di combattere l'elusione fiscale posta in essere dai giganti del Web nel vecchio Continente, la Commissione europea sta mettendo sul tavolo una serie di riforme che toccano nel vivo il business di quasi tutti i giganti del Tech: nel periodo immediatamente antecedente all'entrata in vigore del nuovo Regolamento, ha avanzato una proposta di riforma fiscale, la Web Tax europea,[310] che, come si poteva immaginare, ha scatenato una vera guerra commerciale tra Stati Uniti ed Unione europea.

---

[309] Cfr. G. SARTOR - M. VIOLA DE AZEVEDO CUNHA, op. cit., secondo cui: «*Il legislatore europeo invece, benché oggetto esso stesso di forti pressioni lobbystiche, sente l'esigenza di contribuire a limitare lo strapotere delle imprese statunitensi della new economy, a tutela dei consumatori, ma anche delle imprese europee, cosicché la restrizione delle pratiche commerciali che incidono sulla privacy può assumere connotazioni protezionistiche*».

[310] Una tassa del 3% sui ricavi che i colossi del web pubblicità online, attività social e vendita di dati. Poi, se gli Stati europei raggiungeranno un accordo, si passerà a un sistema fiscale per tassare gli utili là dove vengono generati: questa la proposta che la Commissione europea ha presentato lo scorso 21 marzo al fine

Il piano europeo intende tassare le aziende americane dei media digitali in base al Paese in cui generano il fatturato e non in base al luogo in cui sono state situate le loro sedi regionali, al fine di impedire che, con sedi strategicamente posizionate, in Irlanda e Lussemburgo, i colossi Hi-Tech godano di regimi fiscali più favorevoli e facciano concorrenza sleale alle altre aziende.

Nonostante la proposta europea sia stata letta dagli Stati Uniti come un tentativo di colpire direttamente i colossi della Silicon Valley, in realtà gli sforzi in materia fiscale sono nati a causa della preoccupazione condivisa tra i governi globali che le grandi multinazionali non paghino la giusta quota di tasse nei Paesi in cui realmente operano.

In assenza di un accordo globale su come rimediare a questa forma di elusione fiscale e nell'intento di arginare lo strapotere economico detenuto dai colossi del Web, il Legislatore europeo, nel suo intervento ultimo in materia di protezione dei dati personali, ha previsto regole particolarmente stringenti nella raccolta, manipolazione, rielaborazione e circolazione dei dati, affinché sia operato un trattamento trasparente, adeguato e consapevole, fondato su un consenso realmente informato prestato dall'interessato.

Condizioni vincolanti, imposte ai colossi americani, in forza del loro stabilimento europeo. In particolare, per rendere più difficili i guadagni sulla pubblicità, l'Unione europea ha pensato, in considerazione dei grossi introiti scaturenti dai banner profilati, quelli cioè creati in base ai clic dell'utente, e nella certezza di ridimensionare fortemente il fenomeno della profilazione massiva, di rendere obbligatorio il consenso preventivo dell'utente alla profilazione dei propri dati. D'ora in poi, sempre in ottica di adeguamento alla GDPR, gli utilizzatori europei dovranno decidere se concedere o meno il placet per la personalizzazione degli annunci pubblicitari. Non basterà più l'assenso passivo previsto dalle vecchie informative sui cookie: si dovrà, invece, visionare un apposito modulo che prevede il consenso attivo in una direzione o nell'altra. Consenso, che difficilmente sarà prestato dall'interessato, consapevole che, diversamente, verrà seguito da un algoritmo anonimo in tutte le sue manifestazione sul Web.

Come prima reazione alle pericolose ed antieconomiche strettoie imposte dal Legislatore europeo, come riferito dall'agenzia britannica Reuters, Zuckerberg era determinato a portare tutti gli utenti extraeuropei sotto la legislazione della California, sottraendoli alla

---

di creare un'imposta europea sul fatturato dei giganti del Web tra cui Google, Amazon, Facebook, Apple ecc.

legge irlandese e quindi ai paletti in arrivo con il Regolamento europeo in materia di protezione dei dati personali[311]. Una mossa che avrebbe comportato lo spostamento di un miliardo e mezzo di utenti nella più morbida e flessibile giurisdizione americana, da sempre paladina della libera ed indiscriminata manifestazione del pensiero e disattenta alle seppur minime forme di protezione dei dati[312], e limitato l'applicazione del Regolamento a meno dei quattrocento milioni di utenti europei, sui più di due miliardi di profili presenti nei server dell'azienda.

La scelta di dirottare gli utenti extraeuropei sotto la legislazione americana non è isolata: in vista del Regolamento europeo molte delle aziende con doppia sede avevano avviato una revisione delle proprie policies anche in considerazione dei rischi di elevatissime sanzioni che avrebbero corso. Pertanto, solo i cittadini residenti nell'Unione europea ed in Svizzera saranno sottoposti alle leggi irlandesi e quindi al Regolamento europeo 2016/679. Tutti gli altri, inclusi coloro che vivono fuori degli Stati Uniti, saranno sottoposti alle norme previste dallo Stato della California. E' indubbio che proprio quelle strettoie imposte dal nuovo Regolamento europeo in materia di protezione dei dati

---

311 Sull'argomento, si veda l'interessante articolo di A. MAGNANI, *Tasse in Irlanda, dati negli Usa: Facebook «sposta» 1,5 miliardi di utenti,* in *Il Sole 24 ore*, 20 aprile 2018, secondo cui: «*Michael Veale, l'esperto di privacy contattato anche dalla Reuters, spiega al Sole 24 Ore che il salto dalla giurisdizione europea a quella americana permetterà di «trasportare dati» in un contesto più morbido dal punto di vista legislativo. La Gdpr avrebbe ristretto il campo di azione di Facebook sotto al suo perimetro, obbigandolo - ad esempio - a informative chiare sull'uso delle informazioni o alla notifica di qualsiasi violazione entro 72 ore. Con il passaggio delle responsabilità negli Stati Uniti, gli utenti extra-europei finiranno così per «perdere i diritti», indebendolendosi in caso di contenzioso con il colosso social di Zuckerberg. Ad esempio la legge americana non considera «sensibili» una serie di dati che potrebbero risultare tali ai sensi della Gdpr, moltiplicando il margine di azione di Facebook oltre ai confini previsti finora*».

312 Così anche per G. SARTOR - M. VIOLA DE AZEVEDO CUNHA, op. ult. cit., «*mentre negli ordinamenti europei il diritto all'oblio rispetto a informazioni pregiudizievoli per l'interessato e non più attuali è variamente riconosciuto, negli Stati Uniti non c'è praticamente alcun limite alla pubblicazione di informazioni vere su eventi passati. È vero che alcuni precedenti e testi legislativi sembrano attribuire un diritto all'oblio su alcuni fatti del passato (per esempio reati giovanili), ma essi sono stati superati dalla costante giurisprudenza della Corte Suprema che ha affermato il primato della libertà di espressione. Ad esempio, nel caso Cox v. Cohn (429 US 469, 493-496 [1975]), concernente la pubblicazione del nome della vittima di uno stupro, la Corte Suprema affermava che, in generale, nessuna responsabilità poteva discendere dalla divulgazione di informazioni contenute in documenti pubblici. Il fatto che notizie vere siano pregiudizievoli alla reputazione dell'interessato non esclude la liceità della loro pubblicazione. Per i giudici statunitensi la pubblicazione della fedina penale di una persona è garantita dal Primo Emendamento. Secondo il diritto statunitense Wikipedia può legittimamente respingere la richiesta, presentata da due cittadini tedeschi, condannati per aver ucciso un attore famoso, che i loro nomi fossero rimossi dalla pagina su questo attore. La preminenza attribuita alla libertà di espressione ha inoltre condotto i giudici statunitensi, nella loro interpretazione della sezione 230 del Communication Decency Act, a riconoscere la più ampia tutela al provider che ospiti informazioni accessibili al pubblico, anche quando la distribuzione di tali informazioni un comportamento illecito da parte di chi le carica in rete. Ogni limitazione dell'immunità del provider comporterebbe infatti il rischio di una «censura collaterale» limitatrice della libertà di espressione, poiché il timore di incorrere in sanzioni indurrebbe il provider a rimuovere anche informazioni lecite, nel timore che possano esporlo a responsabilità*».

personali e, più in generale, la nuova Governance europea intrapresa a partire dalla Google Spain, costituiscano un'europea affermazione di sovranità digitale e di supremazia sulle entità economiche[313] che, seppur utilizzando Internet[314], operano nel territorio comunitario, celata dietro il pregevole intento di tutelare i dati personali, come parte essenziale dei diritti e delle libertà fondamentali.

[313] Sulle influenze politiche che hanno dato origine alla pronuncia della Corte di Giustizia dell'Unione europea, nel caso Google/Spain, si veda ancora G. SARTOR- M. VIOLA DE AZEVEDO CUNHA, op. cit: «*È impossibile specificare con precisione il ruolo che i sentimenti appena descritti possono aver giocato nella decisione della Corte. Certamente essi non sono direttamente rilevanti per la giustificazione giuridica di tale decisione, restando estranei alle sue motivazioni giuridiche. Tuttavia, quei sentimenti possono aver contribuito a determinarla, dandole legittimità 'politica' quale scelta a favore dei valori e dei cittadini europei contro il superpotere economico degli operatori statunitensi di Internet e il superpotere politico del loro governo*».

[314] Cfr. V. ZENO- ZENCVICH, *Intorno alla decisione nel caso Scherms: la sovranità digitale ed il governo internazionale delle reti di telecomunicazione*, in G. RESTA, V. ZENO- ZENCOVICH, *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shild"*, in *Roma Tre-Press*, Roma, 2016, il quale evidenzia, in particolare, che la sentenza Scherms porta ad abbandonare completamente l'idea della a-territorialità connessa ad Internet, riaffermando anche in tale ambito il concetto di sovranità, sebbene in questo caso l'espressione dei poteri sovrani sia assunta direttamente dalle Corti e tradotta nel «*termine elegante e tecnico di giurisdizione*».

SEZIONE II: **'Terzi interessati al diritto alla memoria' dimenticati dal Legislatore europeo: diritti e tutele.**
La de-indicizzazione dei dati e le possibili soluzioni alternative.

Premessa

La legislazione europea e quella nazionale sono state attente nel delineare le responsabilità e le tutele spettanti ai molteplici protagonisti coinvolti nel diritto a dimenticare, producendo una normativa via via più vigile e rigorosa a carico dei soggetti attivi della manipolazione delle informazioni e più pregna di tutele a favore dei destinatari della gogna mediatica.

Nelle numerosissime leggi nazionali ed europee, che negli anni si sono avvicendate, non risultano disposizioni dirette a tutelare la figura e le ragioni dei controinteressati al diritto alla memoria, ossia di coloro che dalla reiterazione e/o riproposizione della notizia, o anche solo dalla permanenza in Rete dei dati e delle informazioni, potrebbero trarre vantaggio, perché quei dati, quelle 'informazioni naviganti', e come tali facilmente accessibili, li hanno visti positivamente protagonisti.

In casi simili, il taglio dei link, come deciso dalla Corte europea, o il diritto alla cancellazione (diritto all'oblio), come riconosciuto dal legislatore europeo nell'attuale Regolamento 2016/679, potrebbero arrecare danni al diritto alla memoria, al diritto a che quelle informazioni non siano ingoiate dalla Rete o, quantomeno, non ne sia reso più difficile l'accesso.

L'esercizio del diritto all'oblio, infatti, non può essere un mero colpo di spugna per cancellare vicende gravi del passato, bonificando l'identità che la persona presenta nella Rete, in quanto, quelle stesse notizie, quelle medesime informazioni, potrebbero contestualmente essere utili, giovando, oltre che alla comunità ai fini della conoscenza, anche ad altri individui, coinvolti nella medesima vicenda, ma con connotazioni e profili positivi, a causa delle azioni poste in essere, che, quindi, aspirerebbero alla permanenza dell'informazione nei canali della Rete.

E' decisamente evidente come il riconoscimento legislativo del diritto alla cancellazione/diritto all'oblio, abbia comportato l'emersione di due interessi contrapposti: al diritto alla rimozione dei dati 'scomodi' dalla Rete, si oppone

l'antagonista diritto al mantenimento di quelle stesse informazioni in quanto utili all'identità digitale di altri soggetti.

Il taglio del link alla notizia, come stabilito dalla CGUE nel 2014 e confermato dal legislatore comunitario nel suo ultimo lavoro, sebbene nei limiti e nel rispetto delle perimetrazioni stabilite dai giudici europei in prima battuta e dall'art. 17 del Regolamento 2016/679, e nonostante la permanenza della notizia sul sito-fonte, sicuramente non gioverebbe ai controinteressati al diritto alla memoria dal momento che, rendendo particolarmente complicato e più difficoltoso l'accesso all'informazione, di fatto farebbe cadere nell'oblio comportamenti ed azioni invece meritevoli di memoria.

E' pur vero che non è stato riconosciuto un diritto assoluto alla cancellazione di notizie scomode, un lasciapassare dei 'colpi di spugna', che realmente potrebbe determinare falle nella ricostruzione storica, dal momento che le informazioni comunque continueranno a vivere nei siti-sorgente in cui sono archiviate e, all'occorrenza e con altre chiavi di accesso, potranno essere rispolverate.

Il danno potrebbe evidenziarsi nei casi in cui la consultazione fosse diventata più complessa rispetto a quella azionabile in un motore di ricerca attraverso la mera digitazione del nome e cognome dell'individuo ed un semplice clic, che avrebbero determinato la comparsa di una serie di link, dai più recenti a quelli più desueti, relativi al fatto storico inerente al protagonista.

Per la verità, posizioni assai estreme in dottrina, in riferimento al diritto alla de-indicizzazione, come sancita dalla sentenza 131/2014 CGUE, hanno accusato di "falsa tutela", perché la regola operativa avrebbe dovuto essere quella esattamente contraria, nel senso che l'interessato, e solo lui, avrebbe dovuto decidere quali link, su digitazione del suo nome, sarebbero dovuti comparire sul motore di ricerca, trattandosi pur sempre di informazioni personali riportate, senza filtro e senza regole, su una piattaforma accessibile a tutti. Al di là di queste posizioni-limite, tendenzialmente paladine della garanzia di impunità e scappatoia per la ricostruzione di un'identità in Rete, non è remoto il rischio che il solo taglio del link alla notizia, su digitazione del nome e cognome dell'interessato, possa rivelarsi dannoso per l'immagine e l'identità digitale dei controinteressati alla memoria, la cui posizione, considerata l'assenza di un qualsivoglia riferimento normativo, non ha destato l'interesse di alcuno: né degli operatori tecnici, che non si sono prodigati nel cercare soluzioni informatiche volte a salvaguardare il loro

diritto a non essere dimenticati, né tantomeno degli operatori giuridici, che non hanno previsto alcuna forma di tutela, neanche risarcitoria, lasciando gli interessati alla memoria in balia dell'unica soluzione possibile, consistente nel ricorso alle Autorità amministrative e/o giurisdizionali, ove il conflitto dovesse emergere. Autorità che non potranno che utilizzare, per dare soluzione al caso concreto, la solita operazione di bilanciamento, all'esito della quale l'interesse, tra i due in concorso, ritenuto meritevole di tutela, verrebbe a far recedere il concorrente, con la conseguenza che, ove il diritto al taglio del link dovesse risultare prevalente, i controinteressati alla memoria, *ob torto collo*, si vedrebbero privati del giovamento del ricordo del loro passato.

1) Nozione di terzo-destinatario e destinatario-terzo

Il Regolamento, come del resto la precedente normativa europea e nazionale di protezione dei dati personali, riconosce, quale soggetto passivo, che, subendo un trattamento illecito dei propri dati, ha facoltà di agire, in via amministrativa ed eventualmente giudiziaria, per il ripristino delle condizioni di liceità, la figura dell'interessato, ossia di quella persona, fisica o giuridica, cui i dati personali, oggetto di manipolazione, si riferiscono. Figura che non ha mai posto particolari problemi di esegesi e che rappresenta il cuore del sistema di protezione dei dati personali.

Merita rilievo, a tale proposito, l'assenza nella Convenzione 10, nella Direttiva 95/46, e nel Regolamento 2016/679, di un'espressa definizione di "persona interessata", dal momento che i riferimenti normativi indicati definiscono in prima battuta il concetto di dato personale e, solo successivamente ed attraverso questo, individuano quello di persona interessata, ossia "il soggetto cui i dati trattati si riferiscono". Allo stesso modo il Codice italiano per la protezione dei dati personali, all'art. 4 comma 1, lett. i)[315],

[315]La lettera i) comma 1 dell'art. 4 del Codice, originariamente aveva un diverso tenore. Suonava così: «*interessato, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali*». Era cioè una formula che estendeva alle persone giuridiche e alle associazioni la protezione dei dati, così come la Direttiva 95/46 consente, rimettendo agli Stati ogni decisione su questo punto. Il legislatore italiano aveva inizialmente fatto la scelta più ampia, estendendo la protezione dei dati anche a quelli delle persone giuridiche e associazioni. Successivamente il D.L. 6 dicembre 2011, n. 201, convertito con modificazioni dalla Legge 22 dicembre 2011, n. 214, ha previsto la soppressione di questa norma e la sua sostituzione con quella oggi in vigore. Si è trattato di una scelta del Governo dell'epoca, che ha in tal modo corrisposto a una pressione da molti anni proveniente soprattutto dal mondo delle imprese, le quali pensavano così di sgravarsi da pesanti attività burocratiche. In realtà la modifica non ha affatto esonerato le imprese dagli oneri di protezione dei dati personali e di liceità del loro trattamento rispetto alle persone fisiche. Per contro, la modifica normativa ha fatto venire meno ogni tutela sui dati, di quelle giuridiche, e quindi, in linea generale, anche delle imprese.

definisce l'interessato come "la persona fisica cui si riferiscono i dati personali", definizione coerente con quella della Direttiva 95/46, ma che, al contrario di quella, ha il pregio di isolare e qualificare la persona interessata o l'interessato come una figura specifica.

Il Gruppo Art. 29[316] ha anche affrontato la problematica scaturente dall'eventuale morte dell'interessato per giungere alla conclusione che, sebbene la qualità di interessato cessi con la morte, ossia con il venir meno della persona fisica, il suo decesso non fa, tuttavia, venir meno il legittimo interesse di altri, ad esempio degli eredi, di avere accesso ad informazioni del deceduto e dunque a far valere disposizioni regolamentari relative a dati allo stesso riferibili[317]. Nella citata opinione i Garanti Europei hanno opportunamente precisato la possibilità che "un Legislatore nazionale decida di estendere le disposizioni delle leggi nazionali sulla protezione dei dati ad alcuni aspetti riguardanti il trattamento dei dati dei defunti, qualora un interesse legittimo lo giustifichi"[318]. Del resto, il Codice nazionale Privacy aveva opportunamente previsto che "i diritti dell'interessato riferiti ai fatti personali concernenti persone decedute, avrebbero potuto essere esercitati dal soggetto portatore di un interesse proprio o agente a tutela dell'interessato o per ragioni familiari meritevoli di protezione"[319]. La norma, che sicuramente sopravviverà all'entrata in vigore del Regolamento 2016/679, stante il disposto dell'art. 4.1, la precisazione del Considerando 27[320] e la non incompatibilità con altre disposizioni regolamentari, è finalizzata non tanto a ritenere perdurante la qualità di interessato anche dopo la morte, quanto, piuttosto, ad apprestare tutela a soggetti viventi, portatori di interessi meritevoli rispetto ai dati del defunto.

---

[316]Gruppo Art. 29 - *Parere 4/2007* sul concetto di dati personali*, Doc. Web 20 giugno 2007*, n. 1607426, 22.

[317]Si pensi, ad esempio, alle informazioni detenute da Istituto di Credito, relative ad operazioni bancarie o alla consistenza di fondi del deceduto, che resterebbero chiuse entro una sfera di opacità, ad esclusivo beneficio dell'Istituto medesimo, ove non fosse possibile esercitare il diritto di accesso da parte di chi vi abbia interesse.

[318]Gruppo Art. 29 - *Parere 4/2007* sul concetto di dati personali, *Doc. Web 20 giugno 2007*, n. 1607426, 21.

[319]D.lgs. 30 giugno 2003, n. 196, *Codice della privacy,* art. 9, comma 3: «*I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione*».

[320]Regolamento 2016/679, Considerando 27: «*il presente Regolamento non si applica ai dati personali delle personale decedute. Gli Stati Membri posso prevedere norme riguardanti il trattamento dei dati personali delle persone decedute*».

Il Regolamento, all'art. 4.10, definisce altresì la figura del "terzo", dandone una caratterizzazione in negativo, quale "persona fisica o giuridica, Autorità pubblica, servizio o altro Organismo, che non sia l'interessato, il titolare, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali, sotto l'autorità diretta del titolare o del responsabile".

Definizione che richiama integralmente la nozione di terzo di cui alla Direttiva madre[321], dalla quale emerge che: "è terzo la persona che non ha alcun rapporto con nessuno dei soggetti che, a vario titolo, sono coinvolti nel trattamento dei dati".

In una nozione di terzo priva di specifici contenuti e come tale aperta ad accogliere soggetti portatori di svariati interessi personali, differenti dai soggetti attivi del trattamento e dall'interessato allo stesso, ben potrebbe essere accolta e fatta rientrare la figura di colui che, in una vicenda passata, in qualche modo vi rientri anche solo per aver compiuto azioni degne e meritevoli di essere ricordate e che, per questo stesso motivo, in qualità di interessato alla memoria, potrebbe essere danneggiato, nel diritto al ricordo, da eventuali tagli di link.

Nel leading case del processo Caruso[322], terza interessata alla memoria è sicuramente Maria Ricottini che, avendo avuto un figlio ucciso alle ardeatine, si è resa parte attiva nel processo contro il questore di Roma, Pietro Caruso, in qualità di testimone d'accusa, nel tentativo di linciaggio contro Leonardo Caretta, ex Direttore di Regina Coeli. In quell'occasione, in verità, il diritto all'oblio, vantato dalla vedova Caruso, non è stato riconosciuto agli interessati dai Giudici di legittimità, i quali, pur avendo positivamente valutato il diritto al 'segreto del disonore', lo hanno ritenuto recessivo rispetto all'utilità sociale alla conoscenza dei fatti, decidendo per il permanere della notizia e per la sua riproposizione, ai fini della conoscenza storica, sotto forma di documentario. Ove, al contrario, avessero ritenuto prevalente il primo, autorizzando il taglio del link alla notizia, oltre a ledere il diritto alla memoria storica della comunità, i Giudici di legittimità si sarebbero resi autori di un vero e proprio vulnus nei confronti di quei soggetti interessati alla permanenza dell'informazione che li ha visti in qualche modo protagonisti in

[321]Direttiva 95/46 CE del Parlamento europeo e del Consiglio, 24 ottobre 1995: *Terzi*: «*la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia la persona interessata, il responsabile del trattamento, l'incaricato del trattamento e le persone autorizzate all'elaborazione dei dati sotto la loro autorità diretta*».

[322]Cass. Civ., Sez. I, sentenza del 13 maggio 1958, n. 1563, in *Foro it*., *Repertorio 1943-1945*, voce Fascismo, 84-86.

positivo: nel caso specifico della Sig.ra Ricottini, in proprio, nella qualità di madre di un giovane ragazzo ingiustamente fucilato nell'eccidio delle fosse ardeatine, e nella qualità di esponente e parte attiva del comitato costituitosi per richiedere la condanna di individui protagonisti di periodi bui della storia.

E' bene precisare, tra l'atro, che un po' tutti gli accadimenti e le vicende, per come si enucleano nel tempo, accanto agli attori protagonisti, che sicuramente occupano la scena e le cui posizioni sono oggetto di vaglio da parte delle Autorità amministrativa e giudiziaria e di previsioni normative puntuali, presentano figure di comprimari, erroneamente ritenute sbiadite, di cui il Legislatore, europeo e nazionale, non si è occupato, non avendo loro espressamente riconosciuto alcuna forma di tutela inibitoria e men che meno risarcitoria. Sarebbe pertanto utile individuare, anche se, in verità, la casistica giurisprudenziale di merito e di legittimità e le pronunce amministrative del Garante per la Protezione dei dati personali sembrano non essere mai state investite di una tale problematica, eventuali forme di tutela e/o soluzioni tecniche da adottarsi laddove il diritto all'oblio sia ritenuto preminente, rispetto a quello all'informazione, volte a tutelare anche la posizione di quei soggetti che, in quanto titolari di azioni meritorie, aspirerebbero al ricordo, senza correre il rischio di essere sepolti dalla polvere del tempo su decisione dei titolari dei motori di ricerca e/o di pronunce amministrative e giudiziarie.

2) Titolare del sito sorgente: "terzo" interessato alla permanenza della notizia in Rete?

L'interrogativo sul quale sarebbe opportuno orientare taluni sforzi di speculazione giuridica è relativo alla possibilità di capire se nella nozione di terzo interessato alla permanenza in Rete dell'informazione possa rientrarvi anche il titolare del sito sorgente, fornitore del contenuto che si vorrebbe obliare. Mentre con riguardo alla tradizionale cancellazione dei dati, solo due soggetti risultano tipicamente coinvolti, in qualità di titolare del trattamento e di persona interessata, nella de-indicizzazione, i protagonisti invece sarebbero tre: la persona interessata, il "titolare del trattamento-motore di ricerca" ed il "titolare del trattamento- autore del sito d'origine".

La problematica che potrebbe delinearsi da una tale premessa è legata alla possibilità che, a seguito di una richiesta di de-indicizzazione rivolta dalla persona interessata al motore di ricerca, quest'ultimo si trovi a decidere autonomamente, in assenza di alcuna possibilità

di difesa dell'autore del contenuto. Infatti, se la de-indicizzazione è comunque idonea ad incidere sulla diffusione di un'informazione o sul suo oblio, riducendo ampiamente l'accessibilità per gli utenti a quel contenuto, allora sarebbe opportuno il coinvolgimento, ai fini della decisione su di essa, di tutti e tre i soggetti interessati (webmaster o autore del contenuto, motore di ricerca e persona interessata), sia in prima istanza, dinanzi al motore di ricerca stesso, sia nelle eventuali fasi successive, dinanzi all'autorità amministrativa o giudiziaria.

Il verità, l'obbligo di notifica è stato previsto dal Legislatore europeo, nel paragrafo 2 dell'art 17 GDPR e nel Considerando 66 (al fine di rafforzare la tutela della persona cui i dati si riferiscono), allorché ha posto in capo al titolare del trattamento dei dati personali di cui si chiede la cancellazione, l'obbligo aggiuntivo di informare gli altri titolari del trattamento dei medesimi dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione degli stessi, adottando misure ragionevoli che tengano conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento[323]. In base a tali previsioni, se una richiesta di de-indicizzazione dei link è inoltrata ad un motore di ricerca, quest'ultimo dovrà avere cura di informare anche i siti sorgente, relativamente al fatto che i link contestati non verranno più indicizzati e riceveranno una minore visibilità, senza, tuttavia, che questi ultimi siano giuridicamente obbligati a procedere alla cancellazione dei dati dalle informazioni in loro possesso, a meno che l'interessato non rivolga direttamente ad essi tale richiesta.

Sebbene la presenza di una tale previsione normativa abbia garantito una seppur minima tutela degli interessi del titolare del sito sorgente, limitandosi a prevedere un semplice obbligo di notifica, fine a se stesso e tra l'altro privo di sanzione laddove inadempiuto, di fatto si svuota di contenuto nel momento in cui non include il diritto di partecipazione e

[323] Ciò al fine di consentire la cancellazione dei dati nei trattamenti concatenati: nel momento in cui una persona esprime il consenso al trattamento dei propri dati nei confronti di uno specifico titolare potrebbe, infatti, non essere del tutto consapevole che, in realtà, è assai probabile che quegli stessi dati verranno trattati anche da altri titolari nei confronti dei quali il consenso non è stato espresso direttamente. I motori di ricerca, attraverso la loro attività di aggregatori di informazioni, svolgono trattamenti di dati secondari e correlati a quelli effettuati dai gestori dei siti Internet che hanno ricevuto direttamente il consenso dell'interessato; attraverso l'utilizzo dei cookies, cui spesso gli utenti di Internet acconsentono senza avere piena consapevolezza delle relative implicazioni, i dati forniti a un sito Internet vengono trasmessi a terze parti e trattati da questi ultimi per le proprie finalità; i dati condivisi da una persona con i propri contatti selezionati all'interno di un social network possono essere trasmessi da questi ultimi ad altre persone, senza che l'interessato ne sia al corrente. In tutti questi casi, e in molti altre situazioni analoghe, non si verifica un singolo trattamento di dati personali, ma una serie di trattamenti concatenati fra loro effettuati da diversi titolari.

difesa del titolare del sito sorgente o dell'autore della pubblicazione alla decisione in merito alla de-indicizzazione della notizia che il motore di ricerca andrà ad assumere[324].
E' evidente che il motore di ricerca non possa essere anche portatore degli interessi, propri dell'autore della pubblicazione o del webmaster del sito d'origine, alla conservazione ed alla indicizzazione del contenuto, pur condividendone le finalità per ragioni strettamente economiche.
Stranamente il motore di ricerca, che è direttamente coinvolto nell'istanza di de-indicizzazione, nella fattispecie in esame si presenta come un soggetto in cui si annidano più anime: lo stesso, infatti, rivestirebbe il ruolo di terzo nella decisione di de-indicizzazione, stretto tra la pretesa dell'interessato all'oblio e quella del fornitore del contenuto della notizia alla conservazione dello stesso, senza, tuttavia, essere dotato dei requisiti di oggettiva indipendenza ed imparzialità. Se da un lato, spinto dal timore di incorrere in possibili ed esose richieste risarcitorie, conseguenti al mancato riconoscimento del diritto all'oblio, sarebbe ben disposto all'accoglimento dell'istanza di de-indicizzazione, sull'altro versante sarebbe poco incline al riconoscimento dell'oblio, onde evitare il depauperamento del patrimonio di dati sul quale fonda il suo potere economico. In quest'ultima accezione, l'interesse al mantenimento in vita dell'informazione viene a coincidere con quello del titolare del sito sorgente e dell'autore della pubblicazione, interessati alla conservazione, nella sua integrità, del patrimonio informativo divulgato. Sicché l'opportunità di coinvolgere il titolare del sito sorgente, nonché l'autore della pubblicazione, nella dialettica giuridica che condurrà alla decisione finale, si trasforma in necessità, al fine di operare un equo contemperamento delle posizioni confliggenti.
Tale necessità risulta ancora più evidente laddove si proceda alla de-indicizzazione per nominativo, relativa alle sole ricerche effettuate a partire dal nominativo dell'interessato, sopprimendo, dall'elenco dei risultati, i link verso pagine web pubblicate da terzi e contenenti informazioni relative a tali persone. Infatti, pur potendo l'interessato alternativamente o cumulativamente rivolgersi al motore di ricerca o al webmaster, tuttavia, attualmente, non è tecnicamente possibile per il webmaster effettuare la de-

[324] Anche le Guidelines prodotte nel 2014 dall'Article 29 Working Party per la corretta esecuzione della sentenza Google Spain, al punto n. 23, ammettevano la legittimità di contatti fra il motore di ricerca ed i siti-sorgente «*prior to any decision about a de-listing request, in particularly difficult cases, when it is necessary to get a fuller understanding about the circumstances of the case*».

indicizzazione soltanto per nominativo, alla quale è legittimato il solo motore di ricerca. Pertanto, ciò renderebbe necessario fornirsi di procedure che consentano comunque di chiamare in causa tutti i soggetti coinvolti, in primis l'autore del contenuto che si vorrebbe obliare, al fine di poter vagliare tutte le diverse possibilità ed evitare che la soluzione finale dipenda dalla scelte spesso non completamente consapevoli, del ricorrente o mosse da interessi strettamente economici, del motore di ricerca.

La de-indicizzazione per nominativo, come prevista dalla Corte di Giustizia dell'Unione europea nella Google Spain, comporta la permanenza in Rete dell'informazione, consentendo all'utente di raggiungere la pagina sorgente, nella quale è comunque contenuta, attraverso forme d'interrogazione del provider maggiormente articolate e circostanziate.

Allorché, viceversa, si vada oltre il rapporto di diretta associazione nome/pagina sorgente, ed il collegamento sia meramente indiretto, comparendo la pagina sorgente tra i risultati, soltanto a fronte di ricerche particolarmente articolate, ove il nome dell'interessato rappresenti magari soltanto uno degli elementi della *query,* allora deve ritenersi non possa più trovare applicazione il principio enunciato dalla Corte di Giustizia[325].

Questo perché la sentenza non è volta a favorire forme di censura della Rete.

Pertanto non pare possibile ipotizzare istanze di rimozione di risultati di ricerca che vadano oltre la dissociazione di quella data pagina sorgente da quel determinato nome, sino a coprire magari tutte le possibilità di accesso alla pagina stessa, attraverso differenti modalità di interrogazione del motore di ricerca.

Anche la modulistica predisposta da Google sembra non concedere al richiedente l'oblio la possibilità di indicare le sequenze di parole che, se associate al proprio nome, conducano ai risultati da rimuovere, fornendogli esclusivamente la possibilità di indicare 'il nome che, quando utilizzato come chiave di ricerca, produce una lista di risultati da cui richiede che uno o più risultati siano rimossi[326]'.

Sebbene tecnicamente non sia agevole per tutti i motori di ricerca effettuare la distinzione tra ricerca per nominativo e ricerca mediante altra parola chiave che rimandi al medesimo contenuto, si tratta comunque di soluzioni suscettibili di incidere in modo notevolmente diverso sul diritto alla libertà di espressione e il diritto ad informarsi e ad essere informati.

---

[325] Per un approfondimento sull'argomento della de-indicizzazione per nominativo, si veda: S. SICA- V. D'ANTONIO, *La procedura di de-indicizzazione*, op. cit., 703 e ss.

[326] Indicazioni tratte dal modulo on-line predisposto da Google alla data 30 settembre 2014.

Effettuando la de-indicizzazione dei soli link direttamente collegati al nominativo dell'interessato, infatti, si interviene eliminando esclusivamente la possibilità di rinvenire il contenuto attraverso una ricerca effettuata con riferimento alla specifica persona in merito alla quale si richiedono informazioni, senza tuttavia incidere sulla possibilità di rinvenire il medesimo contenuto, attraverso ricerche effettuate mediante altre parole - chiave correlate a un fatto o a un evento. Grazie a tale distinzione è possibile ristabilire un equilibrio tra il diritto ad informarsi e ad essere informati e il diritto alla tutela della riservatezza e dell'identità personale.

Pertanto, se l'unica forma di de-indicizzazione possibile, in quanto paladina del diritto alla conoscenza, risulta essere quella effettuata "per nominativo" e se l'unico soggetto titotato a porla in essere è il motore di ricerca, si ritiene quanto mai indispensabile che il produttore dell'informazione ed titolare del sito sorgente / webmaster, siano coinvolti dal motore di ricerca nella decisione, consentendo loro il legittimo esercizio del diritto di difesa.

Si tratta di problemi aperti, ai quali non è stata data sufficiente attenzione e che, invece, richiedono la definizione di criteri e procedure comuni negli Stati membri, idonei a tutelare tutti i soggetti coinvolti.

3) Possibili soluzioni utili a tutelare indirettamente il diritto alla memoria dei terzi

L'istituto dell'oblio informatico, sancito dalla sentenza 131/2014 CGUE e successivamente confermato dal Legislatore comunitario, avendo stabilito che chiunque possa chiedere la rimozione di uno o più link verso informazioni che lo riguardino, allorquando "inaccurate, inadeguate, irrilevanti o eccessive" secondo una valutazione ad opera dell'azienda che di fatto dovrebbe procedere all'oscuramento sulla base di criteri e parametri normativi e giurisprudenziali, ha indotto Google, il principale motore di ricerca, all'indomani della pronuncia, a predisporre un modulo di richiesta di de-indicizzazione degli abbinamenti o disallineamenti, indirizzata ai providers, onde evitare di incorrere in processi lunghi ed dispendiosi o in sanzioni pecuniarie. Il motore di ricerca si è trovato ad operare, barcamenandosi in uno scenario giuridico nel quale, se avesse cancellato un po' troppo avrebbe creato un serio vulnus alla memoria collettiva, nel diritto all'informazione costituzionalmente protetto, ed alla memoria dei controinteressati, dando del mondo un'immagine falsata; se, al contrario, avesse generosamente respinto le

richieste di tagli di link, avrebbe corso il rischio (visto che la parola d'ordine era "cancellare!") di incorrere in processi lunghi e dispendiosi che, ove l'avessero visto soccombente, avrebbero imposto il pagamento di cospicue somme di danaro.

In effetti a dicembre 2015, a circa un anno e mezzo dalla pronuncia della CGUE, le richieste pervenute al motore di ricerca sono state 333.450, tutte aventi ad oggetto tematiche molto delicate e sensibili, che hanno imposto al motore di ricerca l'adempimento di un lavoro titanico. Dei link indicati, tuttavia, ne è stata accettata la rimozione solo del 41,9%, meno della metà.

Secondo un'indagine successiva, relativa al periodo 2014-2017, le richieste di cancellazione delle informazioni sono state circa due milioni e mezzo, delle quali il 57% non avrebbe trovato accoglimento[327]. La percentuale delle richieste respinte negli anni è rimasta più o meno la stessa. Ciò che realmente fa riflettere e discutere è che i link tagliati nei primi sei mesi successivi alla Google Spain, nella misura del 41%, e i ricorsi complessivamente accolti negli anni 2014-2017, nella misura del 57%, non sono pervenuti all'esito di una valutazione in cui le diverse parti in causa hanno avuto modo di far valere le loro ragioni, bensì in forza di una valutazione individuale, ad opera di un soggetto privo dei requisiti di terzietà, in quanto parte in causa e soprattutto inizialmente intimorito dalle eventuali sanzioni pecuniarie nelle quali sarebbe potuto incorrere. Valutazione, tra l'altro, affidata ad algoritmi piuttosto che a comitati di esperti in grado di dare un'esatta e giusta collocazione a tutti gli interessi in gioco.

Gli esiti delle domande di de-indicizzazione, sia di quelle accettate che delle altrettante respinte, hanno portato gli operatori giuridici a ritenere che il taglio dei link non fosse la soluzione al problema: le richieste andate a buon fine avrebbero danneggiato la memoria collettiva, avrebbero spento informazioni relative ad azioni e comportamenti di terzi meritevoli di essere ricordati. D'altra parte, le pronunce che avessero privilegiato quella

---

[327] A. BARCHIESI, *La tentazione dell'oblio. Vuoi subire o costruire la tua identità digitale?*, Milano, 2016, 64. «*Circa un terzo delle richieste ha riguardato individui che chiedevano la rimozione di riferimenti ed informazioni personali contenuti nel social media, mentre un alto 20% chiedeva la cancellazione di accadimenti di natura legale, come le menzioni in rapporti sul crimine. Anche se la grande maggioranza delle richieste ricevute da Google è pervenuta da soggetti privati, l'88% delle richieste totali, altre sono pervenute da studi legali o da servizi di consulenza reputazionale. Negli ultimi due anni, in particolare, personaggi pubblici non governativi, come le celebrità, hanno chiesto la rimozione di 41.213 links, mentre politici e funzionari governativi, di altri 33.937. Dai dati emerge una tendenza crescente per star e personaggi pubblici a ricorrere all'oblio informatico, come soluzione estrema per curare la propria immagine*».

causa, respingendo le richiese di de-indicizzazione, sarebbero potute risultare lesive della sfera privata dei soggetti cui le informazioni si riferivano.

Lo studio dei dati personali, peraltro, potrebbe essere particolarmente utile per l'interesse pubblico, ad esempio per l'anamnesi di determinate patologie e la scoperta di nuove cure, per cui, anche per questo, è necessario operare un bilanciamento tra interesse pubblico e privato, intervenendo sul dato in modo da introdurre un quadro più flessibile di tutele che, pur nel rispetto della sfera privata di ciascuno, non sacrifichi il valore di interesse collettivo del dato, altrimenti difficilmente estraibile in un quadro di tutele rigido come quello cui siamo stati abituati in passato, senza, tuttavia, aprire la strada ad una generalizzata conoscibilità delle manifestazioni di ciascuno. Un equilibrio estremamente delicato da raggiungere, eppure più che mai necessario, anche in considerazione del fatto che l'attivazione del diritto all'oblio non rappresenta la soluzione allorquando il motore di ricerca, pur ottemperando alla rimozione dei link, di fatto conservi in eterno quelle stesse informazioni in archivi interni, comunque accessibili con chiavi di ricerca più complesse. Si è tentato, pertanto, di percorrere altre vie, sia tecniche che giuridiche, che potessero offrire soluzioni idonee, atte a tutelare gli interessi di tutte le parti in conflitto, anche facendo ricorso a quella stessa fonte che ha generato il mostro, ossia all'informatica, e lasciando così il taglio dei link come *extrema ratio*.

3.1) La possibilità di disporre di 15 millimetri di buona memoria

L'itinerario tra le possibili soluzioni atte a tutelare i vari e contrapposti interessi, dell'interessato ad essere dimenticato dalla Rete, della collettività all'informazione e dei terzi controinteressati alla conservazione della memoria, non può non tener conto di due differenti situazioni, entrambe meritevoli di tutela: la prima è data da tutte quelle informazioni, relative ad un individuo che, in quanto presenti in Rete, prive di aggiornamento circa le successive evoluzioni positive rispetto alla notizia originaria, sarebbero, in quanto tali, lesive della sfera privata del soggetto interessato (si pensi ai provvedimenti disciplinari o sanzionatori relativi ad un determinato soggetto, divulgati in Rete, poi caducati ma che tuttavia continuano a permanere nella loro dimensione originaria nei canali del Web); la seconda situazione è rappresentata dalla richiesta dell'interessato di rimozione da quei canali, attraverso il taglio del link, di qualsiasi informazione che lo riguardi, a prescindere dal suo aggiornamento.

Premessa indispensabile ed utile ad entrambe le situazioni è che la "posizione" che ogni link, relativo ad una persona individuata, ha nel motore di ricerca non è determinata da una scelta del motore stesso, ma dalla cosiddetta "*wisdom of the crowd*", dal momento che il motore colloca le pagine web disponibili sulla Rete in modo automatico e, nelle posizioni più alte del *rank*, quelle maggiormente citate. La qualcosa rende difficile chiedere che Google garantisca un'adeguata *search neutrality*, assicurando che per ogni notizia siano conoscibili, con analoga facilità, anche le informazioni connesse a quella indicizzata ma di contenuto diverso, assicurando in tal modo un'oggettiva neutralità della ricerca. Come sottolineato infatti da FTC *(Federal Trade Commission*) USA[328], Google persegue unicamente un interesse economico e commerciale che lo spinge ad utilizzare ai fini dell'accessibilità dei link soltanto la Wisdom of the crowd, non altri criteri. D'altra parte, il motore di ricerca non è un editor, né un produttore di informazioni e notizie, per cui non gli si può chiedere di provvedere a collocare in Rete e rendere accessibile, con più efficacia di quella linkabile, una notizia che ne rettifichi il contenuto, applicando in modo pedissequo alla Rete ed ai motori di ricerca la normativa sulla stampa, che prevede, appunto, l'obbligo di pubblicare quanto richiesto dall'interessato a titolo di rettifica. Proprio in relazione alla indispensabile esattezza dei dati circolanti in Rete, una via esplorata da Bianchi e D'Acquisto ha portato alla formulazione della proposta "15 millimetri di buona memoria"[329], ossia all'ipotizzabilità di uno spazio necessario che, accanto al link che rinvia alla notizia ritenuta lesiva della propria reputazione, con la stessa efficacia di ranking, indichi un URL nel quale sia reperibile anche un'altra notizia che, concernendo gli stessi fatti di quella che si vuole rettificare, contenga gli elementi a questo scopo necessari o, comunque, faccia conoscere anche un'altra versione dei fatti, giudicata dall'interessato più conforme a quella che lui ritenga vera o che voglia rendere nota. La proposta presentata dagli Autori suggerisce che il motore di ricerca possa essere obbligato a garantire "15 millimetri di buona memoria", consentendo all'interessato di chiedere ed ottenere, a sua disposizione, uno spazio minimo, che possa ospitare, accanto al link che rinvia alla notizia lesiva della propria reputazione, versioni differenti e più corrette dei fatti. Un'idea sicuramente interessante che, muovendo dalla logica della Rete

[328]Cfr. FTC, *State of Federal Trade Commission Regarding Google's Search Practices in the Matter of Google Inc.*, *FTC File number 111- 0163* Jannuary 3, 2013.
[329]Cfr. L. BIANCHI– G. D'ACQUISTO, *Il trattamento di dati personali effettuato dai motori di ricerca e il diritto di rettifica dopo la sentenza della Corte di Giustizia*, in *I quaderni di Astrid*, 2015, Vol. 225.

e da quella del motore di ricerca, sia idonea a tutelare più efficacemente l'identità digitale e l'immagine dell'interessato cui la notizia si riferisca, gli utenti per l'accesso a informazioni più complete, anche in relazione ai diversi punti di vista con cui si può guardare ad un medesimo fatto, e la posizione dei terzi interessati alla memoria che, in tal modo, non vedrebbero affatto lesa la loro prospettiva. La proposta verrebbe, altresì, a favorire una migliore *search neutrality,* tanto agli utenti che agli interessati, altrimenti difficile da raggiungere attraverso il motore di ricerca, assicurando indirettamente una modalità di diritto di rettifica compatibile con la Rete.

Il limite della via percorsa dagli Autori è che la richiesta di poter collegare ad un link '15 millimetri di buona memoria', sia necessariamente limitata all'uso del nome e del cognome dell'interessato, perimetrando in tal modo il diritto dello stesso alle sole notizie efficacemente individuabili con i suoi dati anagrafici, escludendo la possibilità di rettifica di tutte quelle contenute in altri siti accessibili con i dati di altri individui ma comunque includenti la sua persona.

Altra problematica sorta, che potrebbe generare esternalità negative per l'interessato, sta nel fatto che il collegamento assicurato dal link postato sui 15 millimetri di buona memoria potrebbe essere facilmente frustrato dalla possibilità di accedere alla medesima notizia, alla quale si vuole replicare, anche senza utilizzare i dati dell'interessato, attraverso altri elementi della query o interrogando altri motori di ricerca.

In questo caso l'informazione che si vuole rettificare sarebbe accessibile senza che la medesima accessibilità fosse garantita alla replica; la soluzione, di per sé non risolutiva del problema, potrebbe diventarlo attraverso la sua interazione con altre proposte di seguito individuate.

3.2) L'opportunità, per il motore di ricerca, di garantire una *search neutrality*

Se è vero che il motore di ricerca, nel campo dell'informazione, abbatte i tempi di accesso alle informazioni, non è men vero che la 'questione cognitiva' che verrebbe a configurarsi ogniqualvolta in cui il motore rinvii a notizie e a dati non corretti, o anche solo vetusti, potrebbe trasformarlo in uno strumento di disinformazione on-line. Onde evitare il rischio, secondo il parere di alcuni studiosi del problema[330], è interesse dello stesso

[330] B. SAETTA, *Google e la neutralità dei motori di ricerca tra USA ed Europa*, in *Internet e Diritto*, 23 novembre 2014.

motore di ricerca associare alla sua attività algoritmica e meccanica un servizio di commento attraverso social network, allo stesso modo di quanto già avviene nel rapporto tra il motore di ricerca Google e Google+. Una sorta di connessione, quindi, tra un motore di ricerca e un social che offra un servizio specifico, riservato agli iscritti e finalizzato a consentire agli utenti del social la possibilità di commentare il contenuto del link che rinvia alla notizia. Un modo alternativo per assicurare una forma di replica o rettifica al contenuto della notizia, senza incorrere nella de-indicizzazione e comunque lasciandola quale *extrema ratio.* Ipotesi che, a parere dei suoi propugnatori, potrebbe avere maggiore spessore se il social associato al motore fosse offerto a tutti gli utenti alle stesse condizioni d'uso del motore di ricerca e potesse essere costruito in modo da riservare uno spazio dedicato alle rettifiche ed alle repliche; uno spazio separato, per evitare di confondere quella che si configura come una rettifica o una replica da parte dell'interessato con ogni altro tipo di commento che un qualsiasi utente volesse postare sul social. Uno spazio per assicurare all'interessato, quindi, un diritto di rettifica sartorializzato alle sue esigenze. Con le stesse modalità, inoltre, si verrebbe ad assicurare un più ampio diritto di replica, necessario nei casi in cui la rettifica non si manifestasse sufficiente a ristabilire la verità, quantomeno quella dell'interessato.

Una soluzione che va a mediare, bypassando la de-indicizzazione, il rapporto tra l'interessato ed il motore di ricerca, fornendo una risposta adeguata ai casi in cui l'interessato consideri la notizia, oggetto di indicizzazione, non solo a contenuto diffamatorio, sotto il profilo penalistico, ma anche solo unicamente lesiva delle norme civilistiche poste a tutela dell'immagine. Il diritto alla de-indicizzazione riconosciuto nella *Google Spain* non sarebbe utile, né sufficiente ad assicurare la tutela delle posizioni dell'interessato, men che meno dei terzi controinteressati alla memoria e della collettività, al mantenimento delle informazioni.

Sempre in ambito italiano si segnala la proposta di gestione reputazionale ed integrata segnalata da A. BARCHIESI, *La tentazione dell'oblio. Vuoi subire o costruire la tua identità digitale?*, op. cit., in cui l'autore propone di riconsiderare il processo attuale, a suo dire, caratterizzato da un flusso unico e da unico interlocutore. Il Barchiesi sottolinea come sarebbe molto più efficiente disporre di un unico registro delle segnalazioni e non di registri diversi e distribuiti sotto il controllo di un'istituzione o quantomeno sotto la sua supervisione. Ciò consentirebbe, oltre alla stardandizzazione dei dati acquisiti, l'eliminazione della ridondanza delle richieste ed una possibile maggiore celerità del processo. Possibilità che si tradurrebbe concretamente nella presenza dello stesso form standard all'interno di più motori di ricerca, nonché eventualmente nelle pagine web dei vari Garanti europei. La creazione di un archivio centrale unico, contenente tutti i documenti relativi al processo, consentirebbe maggiori facilità di gestione e maggiore trasparenza.

Attraverso la proposta di uno spazio riservato sul motore di ricerca, molto simile e vicina ai "15 millimetri di buona memoria", formulata da Bianchi- D'Acquisto, si andrebbe ad assicurare all'interessato non il mero diritto di rettifica nella prospettiva della protezione dei dati, ma, in una visione più ampia, il diritto di replica ed integrazione che, non comportando solo la correzione dei dati consentirebbe di offrire, delle informazioni, una lettura ed un'interpretazione diverse e più vicine alla verità.

3.3) La possibilità di disporre di uno spazio reputazionale

La proposta avanzata da Durst – Morley - Fletcher, frutto di una visione preoccupata dei rischi che si corrono in Rete, segue le orme di quanto sostenuto da Urlich Beck[331], secondo cui "la nostra è, e sempre sarà, l'era del *global digital freedom risk*", rischio di perdita del controllo sulle informazioni, sia da parte dello Stato, che degli individui-interessati. A parere dei due Autori, nei canali della Rete, non sarebbe sufficiente la massimizzazione del diritto alla privacy, ma occorrerebbe una protezione dei dati scambiati, che richiede un'attenzione molto più ampia e diffusa, più di quanto oggi avvenga da parte di tutti gli operatori economici, sociali, politici e culturali, dal momento che la Rete presenta caratteristiche e criticità tali da rendere estremamente difficile, non solo la protezione dei dati personali, ma anche il controllo delle informazioni che riguardano ciascuno di noi. A tal scopo, non sarebbero sufficienti le sole regole giuridiche dirette al rispetto del diritto alla protezione dei dati, ma necessiterebbero soluzioni incentrate su un uso più intelligente ed appropriato del Web. Per il raggiungimento di tale obiettivo, e partendo dai limiti insiti nella Google Spain, gli Autori sono approdati all'idea di uno "spazio reputazionale", un meccanismo in grado di assicurare al soggetto interessato che, ogni qual volta in Rete si svolga una ricerca a partire dai suoi dati anagrafici, un link rinvii in modo automatico, tramite un segno grafico differenziato, in uno spazio riservato, analogo a quello degli adversiting pubblicitari, ad una pagina strutturata secondo alcune caratteristiche standard, resa disponibile dallo stesso motore di ricerca e compilata dal soggetto interessato, nella quale quest'ultimo possa inserire anche altri link a informazioni corrette che lo riguardino e/o fornire una sintesi della propria verità e della propria identità. Una prospettiva interessante[332] perché consente di garantire

[331]Crf. U. BACK, *The digital Freedom risk: too fragile an acknowledgment*, 30 august 2013.

[332]G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, op. cit., 601. Secondo L'autore l'integrità della proiezione sociale della personalità dell'individuo può essere lesa anche tramite

all'utente l'accesso ad informazioni più complete, favorendo nel contempo una migliore *search neutrality* da parte del motore di ricerca, altrimenti difficilmente raggiungibile.

In sostanza la proposta consiste nel prevedere una sorta di spazio reputazionale utilizzando il quale ognuno può definire la propria identità digitale ed esporre le proprie verità. Uno "spazio" che verrebbe segnalato automaticamente a chiunque faccia una ricerca, tramite il motore, utilizzando come chiave i dati anagrafici della persona e che non sarebbe la reazione ad un link che rende accessibile la notizia, che non si vorrebbe accessibile, ma la creazione sul Web di una nuova notizia che ne costituisca rettifica o replica, alla quale rinviare grazie ad un URL connesso con il link già contenuto nel motore. Al contrario, nella visione di Durst e Morley- Fletcher, lo spazio reputazionale sarebbe uno spazio facoltativo di memoria in Rete, contenente ciò che ciascuno voglia dire di sé e della sua verità, una sorta di autobiografia, il cui contenuto, nei limiti del formato standard a disposizione, esprima ciò che ciascuno vuole che gli altri conoscano di sé, consentendo in tal modo la tutela e la salvaguardia della reputazione on-line. Gli stessi Autori hanno, altresì, precisato che lo spazio reputazionale ipotizzato non verrebbe a costituire un'integrazione del diritto alla replica, ma sarebbe una risposta alla diversa logica di tutela dei diritti, la cui fruizione potrebbe anche prevedere forme di pagamento, validando per un verso il business del motore e offrendo nel contempo ad ognuno la concreta possibilità di autodefinirsi, a protezione della propria identità digitale.

Ciò anche in considerazione del fatto che non sia nuova la possibilità che il mondo di Internet possa diffondere informazioni non aggiornate, o anche solo decontestualizzate, che richiedono interventi correttivi, nel rispetto dell'identità dell'interessato e della finalità della diffusione di informazioni, che non può non essere diretta a garantire che le informazioni siano corrette e quindi prive di esternalità negative derivanti dalla permanenza in Rete di notizie non vere.

La predisposizione regolamentata di un simile "spazio reputazionale" a pagamento potrebbe anche agire come deterrente rispetto al rischio di possibili richieste di rettifica

---

l'attribuzione di opinioni e idee che non sono in sé offensive o illecite ma semplicemente diverse da quelle realmente professate dall'interessato. La tutela dell'identità personale non coincide quindi con quella dell'onore e della reputazione che presuppone invece l'attribuzione al diffamato di fatti offensivi. Così anche G. PINO, *Il diritto all'identità personale ieri e oggi. Informazione, mercato dei dati personali,* in R. PANETTA (a cura di) *libera circolazione e protezione dei dati personali*, Milano, 2006, Tomo 1, 260.

gratuite e pretestuose, vere e proprie autorappresentazioni dell'interessato e dell'immagine che lo stesso ha di sé[333].

Per altri versi il ricorso a tale meccanismo consentirebbe di manifestare chiaramente agli utenti la posizione dell'interessato qualora decidesse di ricorrere ad un servizio teso a fornire un profilo reputazionale corretto, attraverso la precisazione o argomentazione di una notizia esatta.

La proposta dello spazio reputazionale appare, tuttavia, agli stessi Autori, non facilmente praticabile in concreto, laddove non si abbia certezza che l'algoritmo che regola il motore di ricerca potrebbe, contestualmente all'indicizzazione di una notizia, rinviare anche allo spazio reputazionale della persona, i cui dati personali siano utilizzati per fini di ricerca. Una via, quindi, assai difficile da praticare proprio a causa della tecnologia, almeno fino a che, a parere degli Autori, il Web semantico non diventi realtà.

Anche se la limitata durata dell'esperimento, a causa del recente avvio, non consente di manifestare giudizi di qualsiasi tipo sulla proposta in esame, altri meccanismi che possano fungere da deterrente, diretti a far sì che le informazioni circolanti sul Web siano perfettamente rispondenti al vero, sono stati generati; tra questi le attività dei motori di ricerca che potenzino l'impiego di algoritmi in grado di determinare uno story ranking, ossia che siano capaci di risalire alla fonte dell'informazione, soprattutto se di tipo mediatico, per gli opportuni aggiornamenti.

Tentativi in tal senso, attraverso brevi unità semantiche, definite "meme" ed utilizzate come genetic signatures di una notizia, a prescindere dal suo specifico contesto, sono stati condotti in una sperimentazione volta ad indagare il cd. "*news cicle*" da Jure Leskovec della Stanford University[334].

[333]Sulle tentazioni pirandelliane e il diritto all'identità personale, vedi G. FINOCCHIARO, *La memoria della Rete ed il diritto all'oblio*, op. cit., 398-399. Uno spazio simile, per certi versi, è già predisposto da Google tramite il link *https://support.google.com/acconts/answer/1228138?=it, "gestione della tua reputazione on-line*".

[334]*Meme- tracking and the Dynamics of the News Cicle International Conference on Knowledge Discovery and Data Meaning*, 2009, Paper reperibile sul sito *www.memetraker.org*.

3.4) Le tecniche di anonimato e la pseudonimizzazione dei dati

Le soluzioni esaminate rivelano tutta la loro utilità nel caso in cui la finalità dell'interessato, cui il trattamento dati si riferisca, sia quella di rettificare o aggiornare gli stessi, senza nulla togliere alla permanenza in Rete delle informazioni. La finalità è, infatti, quella di fornire esattezza alle notizie circolanti nel Web, a tutela del diritto ad 'un'esatta conoscenza' da parte della comunità, in uno con la necessità di fornire un'identità digitale dell'interessato il più possibile vicina a quella reale.

Soluzioni che a poco servono se la persona sia interessata alla cancellazione del link all'informazione che la riguardi, piuttosto che alla rettifica, di modo che la notizia non sia più reperibile, o quantomeno risulti difficilmente raggiungibile in Rete.

Il perseguimento di una tale finalità, se si vuole escludere il ricorso a interventi chirurgici, quali il taglio del link alla notizia o la sua cancellazione, richiede l'applicazione di tecniche differenti che, nel salvaguardare la presenza in Rete della notizia, ne modifichino le sue connotazioni, eliminando quei dati che permettano di risalire all'identità della persona.

Rendere la notizia anonima.

Consentire la conoscenza del fatto e non dei soggetti protagonisti del fatto, quantomeno di coloro che, dalla conoscenza dell'accadimento, riceverebbero discredito sociale.

Le tecniche cui frequentemente si fa ricorso sono quelle della pseudonimizzazione e anonimizzazione dei dati.

Pseudonimizzazione e anonimizzazione sono due facce della stessa medaglia, entrambe dirette ad oscurare i dati; tuttavia, mentre la pseudonimizzazione permette d'identificare in un secondo momento i dati, anche in maniera indiretta o da remoto, i dati resi anonimi, invece, non consentono la successiva reidentificazione dell'individuo cui gli stessi si riferiscono.

Entrambe le tecniche sono efficaci per ridurre al minimo i rischi conseguenti all'aggregazione e circolazione delle informazioni personali.

La facilità con cui è possibile generare e acquisire informazioni sugli individui, infatti, ha messo a dura prova le capacità di regolamentazione della protezione dei dati personali, la cui manipolazione, a causa del progresso tecnologico, che ha consentito al titolare del trattamento di acquisire e aggregare informazioni senza che l'interessato sia consapevole

di poter essere identificato o di rendersi identificabile, comporta minacce sempre più gravi alla privacy.

Anche per queste ragioni, ivi comprese le preoccupazioni derivanti da fenomeni, quali le analisi, spesso predittive, dei comportamenti on-line degli utenti, a partire dai Big Data, si è giunti a parlare, in modo sempre più frequente di 'anonimato' o di 'tecniche di anonimizzazione' dei dati, volte a rendere l'interessato non più identificato o identificabile, oscurandone l'identità contenuta in una serie di informazioni, attraverso la sostituzione e/o modifica della variabile identificativa contenuta in un insieme di dati.

La 'pseudonimizzazione è emersa anche dal dibattito che ha preceduto l'entrata in vigore della GDPR, che per questo nella lettura finale del testo l'ha compresa, essendone stata riconosciuta tutta l'utilità, in particolar modo dalla delegazione tedesca che, nell'ottica della conservazione dei dati pseudonimizzati, nell'ottobre del 2014, nella Comunicazione al *Working Party on Information Exchange and Data Protection*[335], ebbe a precisare che una tale tecnica "potrebbe non rimpiazzare altre misure protettive, ma rinforzarle", laddove non "preveda la cancellazione di alcun codice d'identificazione senza la possibilità di reidentificare il titolare dei dati, facilitandone la manipolazione e facendo correre bassi rischi al soggetto cui i dati si riferiscono".

Sebbene la tecnica di pseudonimizzazione dei dati non sia stata espressamente menzionata nella Convenzione 108, nella Direttiva 95/46 CE e nelle legislazioni nazionali, non si può non riconoscere come costituisca uno degli strumenti più importanti, volto a garantire la protezione dei dati su larga scala. A questo proposito, giova precisare che, laddove l'art. 42 del Rapporto esplicativo alla Convenzione 108[336] stabilisce che "l'obbligo relativo ai termini per la conservazione dei dati in forma nominativa non va inteso nel senso che i dati, dopo qualche tempo, debbano irrevocabilmente essere separati dal nome della persona cui si riferiscano, ma soltanto che non debba essere più possibile

[335]Council of UE, *Comunicazione Working Party on Information Exchange and Data Protection (DAPIX),* 21 novembre 2017, in *www.consilium.europa.eu*.

[336]Alla Convenzione 108/1981 è seguito un *Protocollo addizionale*, relativo alla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri, entrato in vigore il 1° luglio 2004. Il testo è teso a migliorare la protezione dei dati a carattere personale e della vita privata, apportando modifiche alla Convenzione originale del 1981, in due settori. In primo luogo, prevede l'istituzione di autorità nazionali di controllo, responsabili di garantire il rispetto delle leggi o delle norme adottate conformemente alla Convenzione in materia di protezione dei dati a carattere personale e del flusso dei dati oltre le frontiere. La seconda modifica riguarda i flussi transfrontalieri di dati verso paesi terzi. I dati possono essere trasferiti unicamente lo stato o l'organizzazione internazionale che li ricevono sono in grado di garantire un adeguato livello di protezione.

collegare facilmente i dati e gli elementi identificativi, effetto che potrebbe essere ottenuto mascherando le informazioni mediante uno pseudonimo», esso contenga un richiamo indiretto ma esplicito alla tecnica della pseudonimizzazione . Sicché, per chiunque non fosse in possesso della chiave di decifratura, i dati pseudonimizzati sarebbero identificabili con difficoltà; per contro, solo chi avesse accesso alla chiave di decifratura serebbe in grado di risalire all'identità.

Il Gruppo Art. 29 ha messo a punto un pregevole documento[337] nel quale sono illustrate le tecniche che possono essere attivate per rendere un dato personale, un'informazione, non riconducibili ad uno specifico interessato e dal quale risulta che tra gli elementi che consentono d'identificare una persona vi è una notevole variabilità: un cognome molto comune potrebbe non bastare per risalire all'identità di un soggetto ma potrebbe essere sufficiente in un altro scenario in cui quel cognome è più frequente.

Sovente l'identificazione indiretta avviene quando è possibile aggregare un certo numero di dati personali, ognuno dei quali, di per sé, non permetterebbe d'identificare la persona ma, unito agli altri, ne consentirebbe l'identificazione con ragionevole certezza.

Ecco perché è opportuno che il criterio applicabile all'insieme dei mezzi che possono essere ragionevolmente utilizzati, dal responsabile del trattamento o da altri, per abbinare un dato personale ad un interessato, non possa non tener conto di tutti i fattori in gioco. Se in un articolo di giornale, infatti, si fa riferimento ad un evento delittuoso verificatosi venti o trenta anni prima, pur senza dare alcun nome dei soggetti coinvolti, ma fornendo alcune indicazioni sul periodo e sulla località in cui l'evento delittuoso si è svolto, accedendo all'archivio dei quotidiani del periodo, è possibile trovare, senza troppe difficoltà, quei dati che in prima battuta non erano stati forniti.

Il medesimo rischio è stato paventato dai ricercatori tedeschi e denunciato al Gruppo dei Garanti europei nella relazione del 2014, nella quale hanno sottolineato la possibilità che attraverso il confronto delle variabili, utilizzate in sede di pseudonimizzazione con una serie di dati esterni alle stesse, si possa facilmente risalire alle variabili rese anonime, senza considerare il costo del tempo impiegato per realizzare le misure e bilanciarle con le probabilità di identificazione e con il tipo di informazioni a rischio. La ricerca ha, tra l'altro, mostrato la scarsa sicurezza del metodo, laddove consenta il recupero dei dati

[337] Gruppo art. 29, *Parere 5/2014* sulle tecniche di anonimizzazione, adottato il 10 aprile 2014, n. 0829/14/IT, WP 216.

attraverso sofisticate tecnologie: è possibile, ad esempio, identificare individui che usano *twitter* attraverso calcoli algoritmici, nonostante il dato sia stato anonimizzato dai codici di identificazione. La sicurezza di un processo di questo tipo, pertanto, sarà fortemente dipendente dalla natura della tecnologia utilizzata per l'oscuramento e, nell'ultimo decennio in particolare, la tecnologia si è evoluta a tal punto da rendere praticabili processi di calcolo fino a qualche anno prima impensabili e a costi via via più contenuti, attraverso la progettazione di nuove tecniche per l'anonimizzazione dei dati, molto più difficilmente vulnerabili rispetto ai meri codici d'identificazione sostitutivi.

In accordo con la visione della delegazione tedesca, l'art. 4.5 GDPR[338] ha espressamente previsto, quale soluzione alla tutela dei dati personali e dell'identità della persona, la tecnica della pseudonimizzazione, una modalità di trattamento dei dati che consente che gli stessi non siano più attribuibili ad un interessato specifico, senza l'ausilio di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche ed organizzative, tese a garantire che tali dati non siano attribuiti a una persona fisica identificata o identificabile.

Un processo finalizzato a mascherare l'identità dell'interessato, riconoscibile solo attraverso informazioni aggiuntive o con l'impiego di chiavi criptografiche, frequentemente utilizzato nel contesto della ricerca scientifica e della statistica, il cui obiettivo è quello di raccogliere dati afferenti persone, senza doverne necessariamente conoscere l'identità: con la pseudonimizzazione, infatti, gli elementi identificativi sono sostituiti da uno pseudonimo che si potrebbe ottenere criptografando quegli stessi elementi identificativi contenuti nei dati personali.

L'adozione dello pseudonimo, se non si usano liste di corrispondenza tra identità e pseudonimi, ma si fa ricorso ad un algoritmo utilizzato per la criptografia di tipo unidirezionale o irreversibile, in nessun caso consente la risalita dal dato criptografato a quello originario, per cui il ricorso, da parte del motore di ricerca, ad una soluzione di questo tipo consentirebbe la tutela contestuale dell'interessato qualora, ricorrendo i presupposti di cui all'art. 17 GDPR, i dati identificativi della sua identità non siano più

[338]Regolamento europeo 2016/679, art. 4, comma 5: Pseudonimizzazione:
«*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*».

liberamente accessibili e dei terzi che, nell'ambito delle stesse informazioni, siano interessati alla memoria, i cui dati identificativi, non venendo pseudonimizzati, rimarrebbero nella loro integrità originaria.

La tecnica della pseudonimizzazione implica e richiede, tuttavia, la presenza di una serie di condizioni, tra le quali l'assenza d'identificabilità diretta dell'interessato (i dati personali non potranno essere più attribuiti ad un interessato specifico), l'adozione di misure di sicurezza ulteriori da aggiungere alla pseudonimizzazione (le informazioni aggiuntive dovranno essere conservate separatamente) e l'incorporazione della pseudonimizzazione nella *privacy by design* (le informazioni aggiuntive dovranno essere soggette a misure tecniche e organizzative tese a garantire che i dati personali non siano attribuibili ad una persona fisica identificata o identificabile).

Il Considerando 28 GDPR, nell'avallare l'utilità della tecnica ai fini della protezione delle in formazioni personali, sottolinea che: "l'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati". L'utilità è altresì, confermata dall'art. 32 GDPR, relativo alla 'Sicurezza del trattamento', il quale inserisce tra le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio', proprio la pseudonimizzazione, il cui plusvalore sta nel non essere solo una tecnica da combinarsi con ulteriori misure di sicurezza, ma nell'avere un'efficacia che consente di considerarla già di per sé una misura adottata a tutela dei dati personali dei soggetti interessati, atta a ridurre i rischi d'identificazione diretta, rendendo il trattamento aderente ai principi di proporzionalità, necessità e garanzia di bassa invasività.

E' evidente che la sicurezza del procedimento e le relative difficoltà di identificazione dipendano da una pluralità di fattori, tra i quali lo stadio in cui il procedimento viene applicato, la dimensione della popolazione in cui è mascherata la persona, la necessità che lo pseudonimo venga generato casualmente, in modo che non sia possibile tracciare una qualsiasi corrispondenza tra lo stesso e il soggetto coinvolto, per cui l'interessato potrà, al più, essere identificabile solo indirettamente e qualora si venga in possesso della lista di corrispondenza.

3.4.1) Le tecniche di pseudonimizzazione e le possibili criticità

La tecnica della pseudonimizzazione, descritta nel testo della GDPR come quel trattamento dei dati personali eseguito in modo tale che le informazioni non possano più essere attribuite ad un interessato specifico, senza, tuttavia, eliminare tutti gli elementi identificativi della stessa, ma semplicemente riducendo il collegamento di un set di dati con l'identificazione dell'individuo, viene spesso affiancata alle nozioni di privacy by design e privacy by default, ossia al fatto che il sistema stesso, sin dalla nascita o con istruzioni ad hoc, si presta ad essere configurato come un ambiente rispettoso della privacy degli utenti.

Non è un caso che pseudonimizzazione e cifratura siano previste, come prime due tecniche, nell'art. 32 GDPR laddove sono suggerite alcune misure di sicurezza, adeguate alla società dell'informazione, volte a garantire una reale protezione delle informazioni.

Adempimenti, con la cifratura, che comportano una serie di passaggi obbligati. Il primo adempimento consiste nel verificare se i dati della realtà presa in considerazione (es. il data base di un'assicurazione, l'archivio di un ospedale, i dati di una banca), siano cifrati o meno e con quali tecniche. In questo caso il titolare dovrà necessariamente confrontarsi con il reparto IT per cercare delucidazioni circa la presenza o meno della crittografia. In caso di risposta negativa sarà obbligatorio, soprattutto nel caso di trattamento di dati particolarmente delicati, migrare nel sistema cifrato, anche se questo è comunque consigliabile per qualsiasi tipo di dato. In secondo luogo la pseudonimizzazione, come anche la crittografia, richiede il rispetto di un minimo di regole (policy) per una corretta gestione del sistema. Si pensi, ad es. all'indicazione chiara di chi detenga le chiavi di cifratura oppure all'obbligatorietà, per tutti i dipendenti, di ricevere smartphone, chiavetta USB e portatili già cifrati.

Esistono numerose varianti che consentono di porre in essere questa tecnica; la scelta di quella più opportuna dipenderà dall'effetto che s'intende ottenere sulla struttura del dato. Quella più frequente, cui si ricorre, è l'uso di chiavi di accesso e funzioni di *hash:* ove si tratti di dati importanti e non s'intenda, in alcun modo, alterare la struttura del set di dati, è possibile selezionare le informazioni identificabili e usare la crittografia mediante l'impiego di una chiave di accesso forte o una funzione di *hash* che consente di mantenere il file integro, senza incidere più di tanto sul contenuto effettivo dello stesso. In questo modo le informazioni contenute in quel file saranno mascherate e rese illeggibili; solo le

persone che avranno a disposizione la chiave di accesso (comunemente chiamata chiave di decrittografia) o la *password* potranno leggere il contenuto del file.
Altra tecnica è quella che impiega il *token,* che si usa solitamente per criptare i dati finanziari e si basa sull'impiego di un meccanismo di crittografia univoca e sull'assegnazione, tramite una funzione indicizzata, di un numero sequenziale o di un numero generato casualmente, che non deriva esattamente dai dati originari. Entrambi i sistemi si prestano ad essere inseriti nel processo e nel software stesso di trattamento dei dati, di modo che non siano sollevate complicazioni inutili, nell'utilizzo, all'utente comune. Molti software, infatti, consentono di svolgere tali operazioni in maniera automatizzata, riducendo notevolmente i costi di adeguamento alla GDPR.
La scelta tra le due tecniche è rimessa ai titolari/responsabili del trattamento che potrebbero optare per l'una o per l'altra, a seconda del contesto in cui dovranno essere applicate, in ragione della tipologia dei dati trattati e dei rischi connessi al trattamento stesso.
Ovviamente, come anche la crittografia, rappresenta uno strumento estremamente sicuro, soprattutto in caso di *data breach*, a condizione, tuttavia, che anche i comportamenti degli utenti siano corretti; in caso contrario, anche il migliore strumento di sicurezza esistente rischia di crollare inesorabilmente.
La tecnica della pseudonimizzazione, valutata positivamente e ritenuta utile e sicura nel rendere più difficoltosa l'identificabilità della persona, ha, tuttavia, manifestato delle criticità relativamente al diritto vantato dalla collettività a conoscere e ad essere informata. Per questa causa, infatti, se risulta meno invasiva rispetto all'alternativo taglio del link, presenta tuttavia il vulnus di un'informazione che, se priva delle sue connotazioni identificative, è pur sempre un'informazione monca.

3.5) Il ruolo della crittografia nella Cyber Security

Crittografia e pseudonimizzazione dei dati personali rispondono in modo pressoché esaustivo alle sfide dell'era digitale, limitando i rischi di violazioni degli stessi da parte degli utenti, avallate in tale loro intento dalla stessa GDPR che spinge le organizzazioni a pseudonimizzare e/o crittografare i dati in loro possesso, in vari e distinti punti.
L'uso dello strumento della crittografia è sempre più stato al centro del dibattito giuridico, la cui discussione, perloppiù incentrata su interessi di rilevanza nazionale e

sovranazionale, pur potendo apparire lontana dalle istanze dei comuni cittadini, ha certamente contribuito ad alzare la sensibilità verso un tema che prima era noto solo agli addetti ai lavori, se è vero che, nel post elezioni in USA, la vittoria di Trump ha fatto registrare un incremento della domanda di servizi di comunicazioni crittografate.

La tecnica della crittografia, procedura trasparente per l'utente, ma che protegge l'informazione con modalità, nella maggior parte dei casi, insuperabili, si basa, su di un algoritmo e su di una *passphrase* (una password ma più lunga e complessa) che 'apre' e 'chiude' i dati, di solito al momento dell'autenticazione.

Si è molto parlato di crittografia nel corso del 2016 in particolare in relazione alla possibilità riconosciuta ai governi di forzare le comunicazioni e acquisirne il contenuto, per ragioni di sicurezza, per fronteggiare il terrorismo o prevenire la consumazione di altri crimini assai gravi. Si è discusso della possibilità d'introdurre o creare delle *backdoor* negli *smartphone* dei cittadini, dei *pass partout* virtuali in grado di consentire alle forze dell'ordine o ai servizi segreti di 'aprire' le comunicazioni e l'agenda personale nonché le rubriche dei contatti.

Lo scontro più famoso è certamente quello che ha opposto l'Apple all'FBI, nel corso del quale a lungo si è discusso dei rischi connessi all'indebolimento della crittografia e dei costi (in termini non solo economici, ma anche di sicurezza) dell'operazione, che apparivano, nel lungo termine, ben maggiori dei benefici[339].

[339]Il conflitto tra il sistema di sicurezza USA e il colosso dell'informazione ha avuto origine da una richiesta di aiuto, avanzata nel 2016 dall'FBI, per 'entrare' nella lista dei contatti contenuta nell'iPhone di Syed Rizwan Farooh, uno degli attentatori della strage di San Bernardino, California, che nel dicembre 2015 uccise ben quattordici persone. Entrambi gli attentatori morirono nello scontro a fuoco con la polizia. L'iPhone, con sistema operativo iOS9, dato all'attentatore dal suo stesso datore di lavoro, finì in mano all'FBI che avrebbe voluto accedere ai suoi contenuti tutti cifrati. Avendo il colosso Apple negato una tale possibilità, i magistrati federali aditi dal sistema di sicurezza, valutate positivamente le ragioni, nell'intento di aiutare l'FBI, con ordinanza imposero l'acceso ai contenuti telefonici. Il giudice Shery Pym impose quindi alla Apple di fornire al sistema di sicurezza un software in grado di disattivare o scartare i meccanismi di protezione e sicurezza dell'iPhone, in particolare di aggirare il meccanismo automatico di distruzione di dati del telefonino che si attivava automaticamente dopo dieci tentativi falliti nell'inserimento del codice di acceso. Poiché né FBI né Apple erano a conoscenza del codice usato da Farook, l'idea è stata quella di provare ad entrare nel telefonino tentando molte password diverse ma, ovviamente, il limite dei dieci tentativi costituiva un problema.
Inoltre, per il giudice, la 'ragionevole assistenza tecnica' da parte di Apple avrebbe dovuto anche consentire all'FBI di inerire i codici sull'iPhone in questione, attraverso la 'porta' fisica dell'apparecchio, via blootooth o via WI-FI, cioè attraverso un software, per evitare l'inserimento manuale di quelli che sarebbero stati innumerevoli e di fatto impraticabili tentativi di accesso. Nella sua risposta ufficiale, sotto forma di lettera aperta ai propri clienti, la multinazionale dell'informazione, nel manifestare il suo disappunto, ebbe a precisare che quella del giudice Pym era una «*decisione senza precedenti, una grave minaccia per i suoi clienti*».

Anche nel Regno Unito, durante la procedura di approvazione dell' IPBILL si è assistito ad un dibattito particolarmente acceso tra i portatori dei vari interessi in gioco: le innumerevoli osservazioni alla bozza, avanzate non solo dai giganti della *Silicon Valley*, ma anche dagli attivisti e dalle associazioni di difesa dei diritti umani, non si sono limitate a porre sul piatto della bilancia privacy e sicurezza (anch'essa paradossalmente minata da proposte che ne sbandieravano la tutela), ma estendevano la loro attenzione alla libertà di espressione e alla tutela dei diritti inviolabili dell'uomo[340].

All'obiezione dell'FBI che tale strumento sarebbe stato usato solo per l'iPhone in questione e che sarebbe stato in grado di sbloccare solo quel telefonino, la Apple ebbe modo di replicare che una volta creata, la tecnica avrebbe potuto essere usata molte altre volte e su qualsiasi numero e tipo di apparecchio. Nel mondo fisico sarebbe stata l'equivalente di una chiave maestra, master key, capace di aprire centinaia di miliardi di lucchetti.
Per l'FBI, la Apple avrebbe dovuto solo creare una versione aggiornata del suo software che avrebbe dovuto funzionare unicamente sul telefonino di Farook, identificato da un unico numero seriale, facendo dell'azienda l'unica compagnia al mondo in grado di formare crittograficamente questo software che non avrebbe potuto essere usato dai servizi di sicurezza USA, nonostante l'appoggio del presidente Trump, per entrare in altri iPhone e con l'ulteriore garanzia che il software in questione sarebbe restato sempre all'interno della sede dell'Apple, nella quale sarebbe stato portato il dispositivo.
Per l'azienda dell'informazione invece, la richiesta avrebbe costituito un pericoloso precedente legale che avrebbe potuto essere replicato dallo stesso governo USA o da altri governi, a partire dalla Cina.
Dello stesso avviso il fronte degli attivisti digitali e la maggioranza dei crittografi ed esperti di sicurezza informatica, per una volta schierati compatti con Apple, secondo i quali «*se si può ordinare questo alla Apple, potenzialmente qualsiasi venditore di software potrebbe essere forzato ad aggiornare qualsiasi apparecchio con del malware, del software malevolo", come sostenuto nella battaglia condotta dall' avvocato Kevin Bankstar. In tal senso anche il fondatore di WhatsApp, Jan Koum che, nell'appoggiare Kevin Bankstar, ha sostenuto che "la nostra libertà è in gioco*».
L'ordinanza giudiziale ha tuttavia, visto prevalere le finalità di sicurezza e prevenzione del terrorismo.
[340]Il Regno Unito nel 2016 ha legalizzato una delle leggi più estreme nella storia della democrazia occidentale, che ha ampliato le possibilità di sorveglianza di massa, ad opera delle agenzie d'intelligence o, per dirla come le stesse agenzie preferivano, sulla raccolta di dati di massa. Tutte le pratiche di raccolta di informazioni su privati seguite a GCHQ, Mi5 e Mi6, che qualche tempo prima erano state dichiarate illegale da un Tribunale speciale, sono state legalizzate. Si è legalizzato lo hacking da parte delle agenzie di sicurezza in computer e telefoni cellulari, permettendo l'accesso a masse di dati personali memorizzati, anche se la persona in esame non era sospettata di illecito alcuno.
Tra le varie possibilità, era altresì previsto che i provider di internet e della telefonia fossero tenuti a registrare e memorizzare per un anno l'attività mobile e web dei loro clienti e le agenzie fossero in grado di accedere ai metadati, ossia al 'chi, cosa, dove e quando' delle comunicazioni, ma non al loro contenuto in assenza di un mandato.
«*Si va oltre molte autocrazie*» ha scritto su Twitter Edward Snowden a proposito dell'approvazione della legge, avvenuta peraltro, senza troppo rumore e tra la docilità delle opposizioni parlamentari. Google, Apple, Twitter, tra gli altri, si sono opposti al disegno legislativo che «*avrebbe potuto avere implicazioni per i nostri clienti, per i cittadini e per il futuro del settore tecnologico a livello mondiale*».
Anche Joseph Cannataci, responsabile ONU delle questioni relative alla privacy, durante una Keynate Speach in Brasile per *L'Internet Governance Forum*, ha attaccato il progetto inglese, definendolo «*spaventoso*».
Unico aspetto positivo, individuato dal *Guardian*, era che «*la normativa definisce chiaramente, per la prima volta, i poteri di sorveglianza a disposizione dei servizi segreti e della polizia*».
Il Regno Unito ha ora una legge di sorveglianza che è più adatta ad una dittatura, che ad una democrazia. «*Lo Stato ha poteri senza precedenti per monitorare e analizzare le comunicazioni dei cittadino, indipendentemente dal fatto che siano sospettati di qualche attività criminosa*» ha commentato Jim Killoch, direttore esecutivo dell'*Open Rights Group*.

Il problema è capire se davvero possa configurarsi una contrapposizione tra sicurezza e privacy.

Se guardiamo alla normativa italiana sembra vero il contrario: alla crittografia si ricorre per proteggere alcune particolari categorie di dati che, per la loro importanza e per i rischi connessi alla loro perdita o sottrazione, richiedono maggiori cautele.

Alla crittografia o cifratura fa cenno il Codice della Privacy, all'art. 22[341], in ordine al trattamento dei dati sensibili o giudiziari, all'art. 34, relativamente al trattamento dei dati

---

Per la premier Theresa May invece, la normativa rappresentava «*una mera necessità per far fronte all'aumento delle minacce emergenti rappresentate dal procedere della tecnologia*».

La nuova normativa potrebbe anche comportare un conflitto giuridico e politico tra il Regno Unito e l'Unione europea in materia di privacy, qualora le Autorità di Bruxelles non dovessero ritenere adeguato il rispetto del livello di privacy dei cittadini europei in base al diritto del Regno Unito, nonostante la Brexit.

«*Questo non sembra semplice*», scrive il sito Politico, «*se non si riuscirà a raggiungere un Accordo che consenta il trasferimento dei dati tra i due blocchi, sarà molto più difficile per le aziende britanniche vendere agli europei e viceversa. Gli scambi commerciali tra Londra e l'Europa infatti, sono legati molto ai servizi, come quello interbancario, in cui vengono messi in campo dati sensibili. L'Europa a questo punto ha buon diritto a pretendere tutte le tutele necessarie a che essi non finiscano indiscriminatamente nelle mai del Governo inglese*».

[341]D.lgs 196/2003, *Codice della Privacy*, art. 22:

«1. *I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.*

2. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.

5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

idonei a rivelare lo stato di salute o la vita sessuale, effettuato da organismi sanitari e, ancora, nell'All. B al Codice Civile in cui, al punto 22, sotto la rubrica 'Ulteriori misure di trattamento di dati sensibili o giudiziari', si dispone che il trasferimento dei dati genetici in formato elettronico debba essere cifrato.

E' anche vero che, se da un lato le misure minime, imposte direttamente dal legislatore, sono obbligatorie, dall'altro quelle idonee ed opportune dipendono dalla sensibilità del titolare e dalla sua determinazione a sfuggire alle responsabilità civili derivanti da patologie del trattamento.

La crittografia appare, altresì, in numerosi provvedimenti del Garante[342], nelle Linee Guida sul Dossier sanitario elettronico[343], così come l'Autorità amministrativa ne ha consigliato l'uso nel *cloud computing* accennando, seppure in modo informale, all*'Internet of Things.*

Il ricorso a tecniche di cifratura, infine, compare in molti provvedimenti tarati su casi concreti portati all'attenzione delle Autorità, aspetto che farebbe della crittografia una misura di sicurezza decisamente nota ai titolari italiani. La grande diffusione, nell'ultimo decennio, del '*ransomware'* avrebbe dovuto incoraggiare il ricorso a misure di protezione idonee: non si può, infatti, sapere se pagando i 'riscatti' per rendere nuovamente accessibili i dati, questi tornino ad essere nella esclusiva sfera di controllo del titolare o se sia invece possibile che gli stessi siano sottratti o duplicati, diffusi o venduti. Qualora, infatti, venissero criptati dati già crittografati, resterebbe l'inconveniente di doverli

10. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.

11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dai di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.

12. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale».

[342]Garante per la protezione dei dati personali, *Doc. Web 17 gennaio 2008*, n. 1482111 in materia di sicurezza del traffico elettronico e telematico; *Doc. Web 4 aprile 2013*, n. 2388260, in materia di attuazione della disciplina sulla comunicazione delle violazioni dei dati personali, i cd. 'data breach'; *Doc. Web 18 luglio 2013*, n. 2551507 in materia di misure di sicurezza nell'attività d'intercettazione delle Procure della Repubblica; *Doc. Web 2 luglio 2015*, n. 4129029, in ordine alle misure di sic e modalità di scambio dei dati personali tra amministrazioni.

[343]Garante per la protezione dei dati personali, *Doc. Web 4 giugno 2015*, n.4084632, in *www.garanteprivacy.it.*

ripristinare ma, se i dati venissero sottratti, potrebbero restare efficacemente intellegibili per i malintenzionati, riducendo il rischio di violazioni.

La Direttiva 95/46 CE per contro, non faceva direttamente riferimento a tecniche di cifratura, se non nell'art. 17, rubricato 'Sicurezza dei trattamenti', che imponeva al titolare 'l'adozione di misure tecniche ed organizzative appropriate, al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati…'. Tali misure avrebbero dovuto 'garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere'.

La protezione dei dati e la sicurezza informatica non risultavano essere campi perfettamente coincidenti: la sicurezza dei dati personali veniva tratteggiata in maniera assai generica, considerando nel bilanciamento da operare anche i costi materiali da sostenere.

Una novità importante nel riavvicinamento tra protezione dei dati personali e *cybersecurity* si ha con l'entrata in vigore della GDPR, nella quale la crittografia risulta essere menzionata in più punti e considerata strumento di cui titolare e/o responsabile possono avvalersi per annullare, o quantomeno mitigare, i rischi connessi ai trattamenti.

Si fa, tra gli altri, riferimento a quella tecnica nel Considerando 83, nel quale il Legislatore europeo ha disposto che: "Per mantenere la sicurezza e prevenire trattamenti in violazione al presente Regolamento, il titolare o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la 'cifratura'.

Il Considerando è stato poi tradotto nell'art. 32 che, collocato nella sezione riferita alla sicurezza dei dati personali, e rubricato 'Sicurezza del trattamento', dispone che "tenendo conto dello stato dell'arte, dei costi di attuazione, della natura dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità o gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile mettono in atto misure tecniche e organizzative adeguate, per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, la pseudonimizzazone e la cifratura dei dati personali.'

Pseudonimizzazione e cifratura, pertanto, sono riconosciute come misure di sicurezza che il titolare deve tenere in considerazione nel valutare i rischi che corre la sicurezza e ai

quali sono concretamente esposti i dati, operando per predisporre un livello di sicurezza adeguato al rischio.

La crittografia è, altresì, menzionata nell'art. 34 GDPR che, nel disciplinare la 'comunicazione di una violazione dei dati personali all'interessato, esonera dalla comunicazione del data breach, la cifratura. Dal comma 3 lettera a) dell'art. 34 GDPR emerge, infatti, l'esclusione della comunicazione all'interessato, qualora il titolare del trattamento abbia messo in atto le misure tecniche ed organizzative adeguate di protezione e tali misure siano state effettivamente applicate ai dati personali oggetto della violazione, in particolare 'quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura'.

Ulteriore riferimento alla cifratura è altresì contenuto nell'art. 6 GDPR in merito alla liceità del trattamento laddove prevede, nel caso in cui il titolare raccolga dei dati personali ma intenda poi trattarli per una finalità diversa da quella per la quale siano stati originariamente raccolti e non abbia il consenso dell'interessato o non possa fondare il trattamento su una norma di legge, l'obbligo di valutare che questa seconda finalità sia compatibile con la prima e, nel compiere queste valutazioni, lo stesso dovrà tener conto, tra l'altro, a norma del comma 4 lett. e), 'dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Va, altresì, precisato che il Legislatore europeo, nella redazione del testo della GDPR ha avuto in mente in particolare la cifratura dei grandi server, dei sistemi che gestiscono credenziali, di quelli che trattano dati sensibili (si pensi al settore sanitario), di quei computer che processano una grande mole d'informazioni per profilare i consumatori e, in generale, di tutti quegli archivi che contengono dati personali. L'idea del Legislatore europeo è stata quella di far sì che ben presto, nella società dell'informazione, tutti i dati, da in 'chiaro' diventassero 'offuscati', con un innalzamento del livello di sicurezza non solo dei sistemi ma anche degli utenti comuni.

Il ricorso alla cifratura, che pertanto è venuto ad assumere grande rilievo, per alcuni aspetti è lasciato all'iniziativa dei titolari, in un'operazione di bilanciamento, a presidio della sicurezza informatica, che andrà valutata sulla scorta del 'principio di responsabilizzazione', che impone un approccio organizzativo e strategico da inquadrare in apposite linee di bilancio nella doppia eventualità che si cerchino soluzioni esterne o interne all'ente titolare.

E’ appena il caso di ricordare le criticità che tale pratica reca in sé in ordine alle esigenze di riservatezza, ai rischi connessi al danneggiamento, al riparto delle responsabilità, alle implicazioni rispetto alla generale disciplina dei dati personali. Implicazioni che in caso di esternalizzazione si aggiungono all’obbligo di selezionare un idoneo contraente, in conformità a quanto disposto dal Considerando 81, secondo il quale “il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenze specialistiche, affidabilità e risorse, per mettere in atto misure tecniche ed organizzative che soddisfino i requisiti del presente Regolamento, anche per la sicurezza del trattamento”.

3.5.1) Vantaggi e criticità dei sistemi crittografici

La scienza della crittografia, con la messa a punto di dispositivi di sicurezza o algoritmi che vanno ben oltre un semplice codice di cifratura per proteggere i propri dati, mantenendo segrete tutte quelle informazioni che non si vogliono divulgare pubblicamente, in maniera tale che la possibilità di accedervi sia data solamente ad uno o a un ristretto numero di persone autorizzate, che ‘sappiano come farlo’, è in prima linea sul fronte della sfida alla protezione e difesa dei dati personali e delle comunicazioni di massa, messi a dura prova dalla veloce evoluzione tecnologica.

E’ una scienza che, nell’individuare dispositivi di sicurezza o algoritmi diretti a proteggere i dati personali ‘che navigano in Rete’, va ben oltre l’individuazione di un semplice codice di cifratura. Grazie alla potenza dei computer, infatti, oggi si è in grado di utilizzare la crittografia a livelli che non erano immaginabili poche decine di anni fa, con una diffusione su larga scala del fenomeno. A partire dalle organizzazioni politiche e militari, passando per le imprese per arrivare al mondo consumer, è diventata popolare al punto che oggi chiunque potrebbe utilizzare file criptati, algoritmi e matematica avanzata nell’intento di salvaguardare la circolazioni di dati e l’informazione che non s’intende rendere pubblica.

E’ un sistema che, tramite l’utilizzo di un algoritmo matematico agisce su una sequenza di caratteri, trasformandoli. Tale trasformazione si basa sul valore di una chiave segreta, ovvero il parametro dell’algoritmo di cifratura/decifratura. Proprio la segretezza della chiave rappresenta il sigillo di sicurezza del sistema.

In base al genere di chiave utilizzata, è possibile suddividere in due tipologie il sistema di decifratura informatica: se è presente una chiave singola si parla di crittografia a chiave simmetrica o a chiave segreta (la chiave del mittente e quella del destinatario sono la stessa); quando, invece, vi sono due chiavi di cifratura distinte, si parla di crittografia a chiave asimmetrica o a chiave pubblica: la chiave di cifratura è pubblica, mentre quella di decifratura è privata.

La chiave simmetrica, quindi, prevede l'uso di un'unica chiave, sia per nascondere il messaggio che per sbloccarlo, risultando relativamente veloce e semplice da implementare rispetto ad altri tipi di cifratura. L'ulteriore svantaggio della crittografia a chiave simmetrica è che, poiché prevede l'utilizzo di una chiave comune, e quindi l'unicità dell'algoritmo sia per la codifica che per la decodifica, necessita che tutte le parti coinvolte debbano scambiarsi la chiave utilizzata per crittografare i dati, prima di poterli decifrare. L'esigenza di distribuire e gestire un elevato numero di chiavi in modo sicuro per la maggior parte dei servizi crittografici, implica la necessità di fare uso di altri tipi di algoritmi di cifratura, oltre alla quella di cambiare frequentemente la chiave segreta, che dovrà essere distribuita ad ogni utente che intende comunicare e che a sua volta, dovrà mantenere segreta. Lo stesso onere di segretezza che incombe sul mittente.

L'algoritmo oggi più diffuso, usato in crittografia a chiave simmetrica è l'AES *(Advanced Enscryption Standard*), sviluppato a fine anni '90 da Joan Daemen e Vincent Rijmen, due crittografi belgi, su richiesta del *National Institute of Standard and Technology*, divenendo uno standard pubblico alla fine del 2001.

L'AES si basa su diverse operazioni eseguite su blocchi di dati e nel 2003 la National Security Agency statunitense ha approvato l'utilizzo del sistema per proteggere tutte quelle informazioni governative classificate come *secret.*

La vera novità del secolo scorso è stata l'invenzione di una tecnica criptografica che utilizza chiavi diverse per cifrare e decifrare un messaggio, facilitando il compito di distribuzione delle chiavi.

Infatti, in questo caso non è necessario nascondere le chiavi o le password; c'è una chiave per crittografare che è pubblica perché chiunque può vedere e che, pertanto, è condivisa da tutti i corrispondenti ed un'altra per decodificare, privata, conosciuta solo dal destinatario, che va tenuta segreta e non dev'essere condivisa con nessun altro.

Il fatto di essere a conoscenza della chiave pubblica non permette di risalire in alcun modo alla chiave privata. Uno degli algoritmi più utilizzati è il River Shamir Adleman (RSA), creato nel 1977 da tre ricercatori del MIT di cui porta il nome. Spesso usato nei 'protocolli del commercio elettronico', come SSL, l'RSA è ritenuto sicuro per via delle chiavi sufficientemente lunghe e dell'uso d'implementazioni aggiornate. Poiché l'RSA presenta la criticità di un'eccessiva lentezza rispetto alla criptografia simmetrica, si ricorre alla prassi di cifrare i dati con un algoritmo simmetrico e poi la chiave simmetrica, relativamente breve, è criptografata mediante RSA, potendo, in tal modo, inviare, in modo sicuro, ad altre parti la chiave necessaria per decodificare i dati, insieme ai dati simmetrici come crittografati.

Tradizionalmente, per crittografare si è fatto ricorso a due sistemi: alfabetico e a codice.

Il primo è fondato sul metodo della 'sostituzione' che comporta, appunto, la sostituzione, a ciascuna lettera del testo, di altra lettera, cifra o segno convenzionale che le corrisponde regolarmente o sul metodo della 'trasposizione', che consiste nel cambiare di posto ciascuna lettera del testo, secondo un ordine convenzionale, ottenuto per mezzo di una parola chiave.

I sistemi a codice, invece, particolarmente usati nelle operazioni militari, consistono nello stabilire per ciascuno dei corrispondenti un codice o dizionario in cui ogni parola o espressione porta a fianco un numero (codice cifrante) e un codice in cui sono riportati in ordine di successione i numeri (contenuti nel codice cifrante), al lato dei quali è riportata la parola corrispondente (codice decifrante). Per renderli più sicuri, i testi cifrati sono sottoposti a sovracifratura, cioè ogni numero ricavato dal codice (in genere di 4 o 5 cifre) è alterato secondo un sistema convenzionale definito da uno o più gruppi di cifre (chiave), posti in posizione convenuta.

Oggi s'impiegano frequentemente, macchine cifranti, in grado di fornire rapidamente l'esatto testo cifrato secondo una chiave inserita convenzionalmente, a sua volta collegata direttamente ai mezzi di trasmissione o incorporata in essi.

I sistemi più moderni, invece, si basano sulle 'funzioni pseudounidirezionali', funzioni facilmente computabili, la cui inversa non può essere computata a meno che non si posseggano certe informazioni particolari utilizzate nella loro costruzione e che fungono da parola d'ordine.

3.5.2) La "codifica con una chiave" relativamente al trattamento dei dati sensibili

La tecnica della decodificazione con chiave simmetrica è la soluzione, riportata nella direttiva 2001/20 CE del 4 aprile 2011, relativamente alle 'buone pratiche', nell'esecuzione della sperimentazione clinica.

Il ricercatore che effettua i test dei medicinali raccoglie dati sui risultati clinici presentati da ogni paziente, ognuno dei quali è contrassegnato da un codice. Il ricercatore comunica le informazioni alla società farmaceutica o a terzi interessati, solo nella forma codificata, perché a questi soggetti operanti come '*data controller'*, interessano solo le informazioni biostatistiche.

Il ricercatore, pertanto, terrà separata la chiave che associa il codice delle informazioni, che permette d'identificare i pazienti: chiave che dovrebbe conservare per poter successivamente risalire agli stessi, ove la sperimentazione clinica avesse messo in evidenza rischi, per poter somministrare terapie appropriate al fine di proteggere la loro salute.

Questa soluzione, che si è rivelata molto utile nel trattamento dei dati sensibili, consente l'identificazione delle persone fisiche coinvolte, solamente a chi possiede la tabella di corrispondenza, mentre alle aziende farmaceutiche, che analizzano la ricerca, non è dato alcuno strumento per collegare i dati con i pazienti.

Responsabile del trattamento, che dovrà garantire un'adeguata protezione dei dati, pertanto, sarà il ricercatore, mentre le industrie farmaceutiche non saranno soggette a vincoli stringenti di legge, applicabili al trattamento dei dati personali.

Sistema che, tra l'altro, permetterebbe di tutelare gli interessi di eventuali terzi interessati al permanere dell'integrità dell'informazione e alla sua circolazione, sebbene depurata dei soli elementi identificativi, la cui posizione non sarebbe in alcun modo danneggiata.

3.6) La tecnica di anonimizzazione dei dati

A differenza della già esaminata pseudonimizzazione e della minimizzazione dei dati, quest'ultima consistente nella raccolta dei soli dati pertinenti e limitata allo stretto necessario rispetto alle finalità per le quali i dati raccolti siano trattati, l'anonimizzazione è una 'tecnica sottrattiva' in quanto, se portata alle sue estreme conseguenze, si configura come un trattamento quasi chirurgico, nel quale è impedita l'identificazione dell'interessato.

L'espressione riportata nella Direttiva 2001/20 CE prende in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati per classificare le informazioni relative ad un interessato, che non potrà e non dovrà essere identificato né dal titolare o responsabile del trattamento, né da altri. Così l'inserimento del singolo individuo nell'ambito di un *cluster* anonimizzato verrebbe ad impedire la sua identificazione, permettendo comunque le operazioni di profilazione e di individuazione di gruppi/target estesi. In tal modo, mediante l'utilizzo dell'aggregazione non si avrebbe più un impatto concentrato sul singolo componente del cluster poiché l'obiettivo amplia la sua portata, estendendosi all'intero gruppo.

Da un punto di vista pratico, questo risultato può essere ottenuto attraverso l'applicazione di diverse tecniche, sostanzialmente raggruppabili in due famiglie: la 'randomizzazione', che modifica il grado di verità del dato al fine di eliminare la correlazione che esiste tra lo stesso e la persona e la 'generalizzazione', consistente nella diluizione degli attributi della persona interessata, attraverso la modifica della scala o ordine di grandezza: si pensi, ad esempio, all'indicazione di una fascia d'età anziché all'età precisa del soggetto o ancora della Regione piuttosto che della città di residenza.

Appartiene anche a questa famiglia la promettente tecnica di k-anonimato, con le sue varianti, per le quali molte metodologie sono già disponibili e applicabili[344].

Grazie allo sviluppo di queste tecniche, che hanno significativamente ridotto i rischi per la privacy degli interessati, si è assistito negli ultimi anni al moltiplicarsi di servizi che impiegano i dati per fini di utilità sociale. Ad esempio, nel settore medico, si parla di '*digital health'* per riferirsi a quelle tecnologie che si propongono di contribuire al miglioramento della salute delle persone, grazie all'uso di dati resi anonimi[345].

Un esempio concreto di questa opportunità viene dalla Francia: l'art. 143 della Legge 41 del 2016, sulla modernizzazione del sistema sanitario, ha esteso e regolamentato l'utilizzo

[344]Questo sistema, che si differenzia dalla pseudonimizzazione per il fatto che non sostituisce il dato con altri criptati ma, il più delle volte, lo cancella, è piuttosto frequente allorché si riportino provvedimenti giudiziari nei quali le informazioni relative a persone, luoghi e tempi sono cancellate, così come, nell'operazione di mascheramento dei volti, in immagini riprese da impianti di videosorveglianza che vengono successivamente trasmesse, via televisione o via Internet, per le quali, nonostante tutto, bisogna essere molto attenti e puntuali, dal momento che un familiare potrebbe riconoscere il soggetto coinvolto anche se il volto è oscurato, facendo riferimento ad altri elementi per lui significativi, come l'altezza, il portamento, l'andatura, piuttosto che l'abbigliamento.

[345]In un Paese come gli Stati Uniti, alcune ricerche hanno evidenziato come per quattro tipologie di patologie: diabete – asma – riabilitazione cardiaca e riabilitazione polmonare, si potrebbero, in molti casi, prevenire crisi acute, evitando il ricorso a cure di emergenza ed offrendo cure più efficaci a costi minori a carico della sanità pubblica.

di tutte le banche dati pubbliche per progetti di ricerca volti al perseguimento di un pubblico interesse.

Per garantire la privacy degli interessati, su poco meno di settanta milioni di cittadini sono state utilizzate diverse tecniche di anonimizzazione: alcuni dati identificativi, come nomi, cognomi e indirizzo, sono stati cancellati e in aggiunta sono state applicate tecniche di k-anonimato, raggruppando i dati sulle età degli interessati in mesi o anni e creando raggruppamenti ampi per i dati inerenti i codici postali.

Dall'approvazione di questa legge molti sono stati i progetti di ricerca proposti in quello Stato e, in alcuni casi, già portati a termine. Alcuni hanno riguardato l'efficacia e il confronto fra differenti medicinali e la correlazione tra patologie e l'uso di farmaci o vaccini.

Un progetto particolarmente interessante ha previsto l'utilizzo di dati sanitari per studiare l'efficacia di farmaci somministrati ai pazienti ricoverati d'urgenza per problemi cardiaci. Attraverso uno studio accurato, condotto sulle caratteristiche dei pazienti, sulle loro patologie e sulla risposta ai farmaci, è stato possibile constatare quale sia stato il farmaco più efficace per determinate patologie. E' stato, altresì, valutato che tale studio potrebbe permettere di salvare mediamente circa settanta vite umane ed evitare 228 complicanze ogni 9000 pazienti, garantendo ad ognuno la cura più efficace[346].

Un'iniziativa analoga è stata intrapresa dalla *European Medicines Agency*, che ha istituito uno Board multidisciplinare, composto da medici, tecnologi, filosofi ed esperti di bioetica per pervenire ad una *policy* di anonimizzazione dei dati sanitari, capace di configurare le tutele per la persona interessata e per gli interessi pubblici[347].

Questi benefici sociali non sono prerogativa del solo campo medico. Vi sono molti altri esempi di impieghi di dati anonimizzati come nel caso della promozione, ad esempio, delle politiche di efficienza energetica[348], dell'imparzialità dei test di ammissione

[346]Per approfondire altri progetti medici e ricerche basate sull'uso di dati raccolti nella banca-dati SIIRAM: *http://www. rennes-donnes-sante-2017.cfr*.

[347]Così in *http://www.emer.europa.eu/em/index.JSP?curl=pages/regulation/general-content-bd880.* L'intento del Board multidisciplinare è stato quello di trovare u bilanciamento tra interesse pubblico e privato, intervenendo sul dato, in modo da introdurre un quadro più flessibile di tutele, che non sacrifichi il valore di interesse collettivo del dato in un quadro di tutele rigido come quello attuale. Un equilibrio estremamente delicato da raggiungere, eppure oggi più che mai necessario

[348]Così in *http://www.gov.wales/statistics-and-research/general.poverty-data-linking-project/?lang-eu*.

all'istruzione superiore[349], nonché della verifica circa l'efficacia delle politiche governative in tema di mercato del lavoro[350].

Si tratta di molti e significativi esempi di come l'applicazione della privacy by design ai trattamenti possa garantire il raggiungimento di risultati importanti per la ricerca e per lo sviluppo di molte tecnologie in grado di migliorare la vita delle persone[351].

Rimangono aperti alcuni quesiti, il primo dei quali è relativo alla possibilità che ad anonimizzare debba essere solo lo Stato ovvero anche un privato, così come sarà necessario stabilire precisi criteri per valutare in quali casi l'anonimizzazione riesca realmente nel suo obiettivo di tenere indenni le persone, valorizzandone soltanto i dati.

Bisogna, altresì, precisare che anche quando i dati vengano anonimizzati per un interesse pubblico, che prescinda da quello del titolare degli stessi, non va omessa l'opportunità dell'informazione degli interessati, sulle finalità che s'intendono perseguire, offrendo loro la possibilità di esercitare il proprio diritto a sottrarsi a quella tecnica.

Come nel caso dell'uso dello pseudonimo, la tecnica dell'anonimizzazione dei dati ben si presta a tutelare le ragioni dell'oblio dell'interessato, i cui soli dati saranno resi anonimi, lasciando sopravvivere, per consegnarle all'eternità, notizie e informazioni relative a terzi interessati al ricordo, che desiderano che le stesse siano rese visibili nel tempo.

Danneggiato potenzialmente sarebbe il diritto ad un'informazione completa, caratterizzata da notizie integre, spettante alla collettività che, con l'applicazione della tecnica di anonimizzazione verrebbe a trovarsi di fronte ad informazioni che, in quanto prive di dati identificativi, sarebbero parziali e monche, incidendo e creando comunque un vulnus nell'esercizio del diritto ad informare e ad essere in formatiti.

---

[349]*Evaluating the fairness of admissionins decision making in UK higher education*, in *https://adrn.ac.UK/research-impact/research/prpoject.107*.

[350]Così in *https://adrn.ac.uk/provider-data/casa-studiues/benefits*.

[351]Il rischio dell'anonimizzazione, finalizzata all'aggregazione dei dati di un cluster è quello di non poter più ricostruire i processi che hanno condotto all'individuazione del 'target' e quindi, di non poter risalire a colui che detiene le responsabilità rispetto al trattamento dei dati personali, a differenza della pseudonimizzazione in cui quel rischio è scongiurato dal fatto che uno o più soggetti assumono la funzione di custodi dei dati e che, garantendo la ricostruibilità dei processi di mascheramento dell'identità, e permettendo quindi la reidentificazione, assicura l'accountability, ossia la responsabilizzazione, ex art. 5.2 GDPR, del titolare del trattamento. Questa riflessione rende chiari ed apprezzabili i motivi per cui la pseudonimizzazione ha assunto enorme rilevanza all'interno del GDPR: «*L'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per l'interessato e aiutare i titolari del trattamento e i responsabili a rispettare i loro obblighi di protezione dei dati» ricorda il Considerando 28 del GDPR*».

3.6.1) Ulteriori utilità e criticità della tecnica dell'anonimizzazione

Il ricorso all'uso di tecnologie informatiche che, pur lasciando integra la notizia nella sua dimensione originaria, la priva dei dati e dei riferimenti soggettivi, impedendo all'utilizzatore di risalire ai suoi protagonisti, se da un lato preserva il diritto all'informazione, anche se reso molto più difficoltoso, dall'altro fornirebbe un'informazione comunque monca e sicuramente parziale. Verrebbe ad essere favorito, invero, il solo interesse del titolare dei dati che, a quell'informazione presente nei canali del Web, non vedrà più associato il suo nome alla notizia, la quale, pertanto, continuerà a navigare in maniera anonima, con l'aggiunta che chiunque fosse interessato alla sua conoscenza non avrebbe più le chiavi di riferibilità alla stessa, dovendone utilizzare altre, non facilmente individuabili e accessibili, subendo oneri non solo economici, ma anche temporali.

Operazioni di questo genere, utili e regolarmente operanti nei trattamenti dei dati sensibili e ancor più in quelli aventi finalità scientifiche e statistiche, avrebbero una qualche valenza, con il limite, tuttavia, che quella stessa tecnica, applicata in un ambito che prescinda dalle suddette finalità e persegua lo scopo esclusivo d'informare e di far conoscere le azioni, ma anche gli individui che a tali azioni sono legati nel bene e nel male, manifesta tutte le sue criticità allorché ci si imbatte nella difficoltà, meglio impossibilità, a raggiungere l'informazione, in quanto priva dei suoi riferimenti soggettivi. Un'impresa titanica!

Partendo dal presupposto che il diritto all'informazione, nelle sue molteplici accezioni, è il diritto fondamentale di una società democratica, faro di uno stato di diritto, eventuali bavagli dovranno e potranno essere consentiti in via di mera eccezione e solo e nei casi in cui la circolazione di quell'informazione, in quanto obsoleta e svuotata di qualsiasi interesse pubblico alla conoscenza, potrebbe rivelarsi gravemente dannosa per alcuni, quanto inutile alla conoscenza di altri perchè priva di elementi di arricchimento culturale. In attesa che quelle tecnologie che hanno generato il problema trovino al loro interno gli anticorpi in grado di dare soluzioni adeguate al contemperamento e alla tutela di tutti gli interessi in gioco, ivi compreso quello dei terzi controinteressati alla permanenza della memoria, la via da percorrere non è solo quella individuata dai giudici europei del taglio dei link alla notizia, cui ha dato fondamento normativo il Legislatore europeo nel suo ultimo lavoro, ma, perché il diritto all'informazione non sia ridotto ad una mera

declamazione, potrebbe essere utile alla causa percorrere anche altre vie, tra le quali, appunto, la pseudonimizzazione dei dati che si vuole oscurare e, in via subordinata, la loro anonimizzazione.

4) La de-indicizzazione all'esito di un'operazione di ponderazione e bilanciamento dei differenti interessi in gioco, nell'ottica della tutela dei terzi interessati alla memoria e del diritto alla conoscenza

Il diritto alla de-indicizzazione può essere definito come il diritto dell'interessato di rivolgersi immediatamente al motore di ricerca per ottenere la rimozione dei link risultanti a seguito di una ricerca effettuata a partire dal suo nominativo, ove non vi siano altri interessi prevalenti, che legittimino la permanenza del risultato della ricerca. In particolare, sia la Corte di Giustizia che l'Article 29 Working Party sottolineano che la persona interessata potrebbe trovarsi eccessivamente esposta nei confronti di chiunque avesse accesso ad Internet, per effettuare ricerche ed indagini, in modo celere ed economico, mediante ricerche per nominativo, che consentono il reperimento del contenuto anche a quegli utenti che probabilmente non avrebbero altrimenti mai trovato la pagina Web ricercata. Mediante la ricerca per nominativo, infatti, è possibile, per coloro che la effettuano, ottenere, attraverso l'elenco dei risultati, una visione complessiva e strutturata delle informazioni relative alla persona, reperibili su Internet, che consente loro di attribuirle un profilo più o meno dettagliato, incidendo in modo significativo sui diritti fondamentali alla vita privata ed alla protezione dei dati personali.

Sebbene già prima della pronuncia della Corte di Giustizia fosse stato possibile rivolgersi al gestore del sito sul quale le informazioni erano state originariamente pubblicate per l'esercizio del diritto alla cancellazione, con la sua pronuncia del 2014, C-131/2012, la Corte ha affermato il diritto per i consociati di richiedere la de-indicizzazione, rivolgendosi direttamente al motore di ricerca, cui ha riconosciuto lo status giudico di titolare del trattamento[352], in considerazione del fatto che: «tenuto conto della facilità con

[352] E' soprattutto l'autorità garante per la protezione dei dati personali a essersi fatta carico di bilanciare le opposte pretese alla rimozione e alla pubblicità delle informazioni, riscontrando, seppur su base casistica, le istanze degli interessati secondo un approccio tendenzialmente uniforme a seconda che le notizie indicizzate dai motori di ricerca presentassero un persistente interesse pubblico, il Garante ne ordinava o meno la rimozione. Tale risultato, sotto un profilo tecnico, veniva ottenuto mediante il collocamento delle notizie in una sezione del sito Internet non soggetta a indicizzazione. Per tale via, la notizia continuava a essere disponibile e consultabile tramite l'apposito motore di ricerca interno al sito sorgente della testata giornalistica, senza che venisse infirmata la sua idoneità a soddisfare la finalità

cui informazioni pubblicate su un sito Web possono essere riprodotte su altri siti, nonché del fatto che i responsabili della loro pubblicazione non sempre sono assoggettati alla normativa dell'Unione, non sarebbe possibile realizzare una tutela efficace e completa delle persone interessate nel caso in cui queste dovessero preventivamente o in parallelo ottenere dagli editori di siti Web la cancellazione delle informazioni che le riguardino[353]».
Il trattamento effettuato dal motore di ricerca risulta essere peculiare e diverso dal trattamento della medesima informazione effettuato dal sito Web d'origine, sia per le differenti finalità che per le modalità adottate. Ciò ha determinato, come affermato dalla Corte di Giustizia[354] ed in alcune pronunce del Garante per la protezione dei dati personali[355], una diversa valutazione degli interessi coinvolti, che avrebbe potuto condurre anche a decisioni nelle quali fosse negata la cancellazione dei dati dal sito Web d'origine e concessa la de-indicizzazione dal motore di ricerca in ragione del maggior pregiudizio che la indicizzazione comporta.
Peraltro, la sola forma di de-indicizzazione consentita, in quanto riconosciuta dai giudici europei, è quella per nominativo, che consente il raggiungimento della pagina sorgente, ove permarrebbe l'informazione, utilizzando, quale forma di interrogazione, il nome e cognome della persona "ricercata". L'utilità ed il vantaggio che tale soluzione verrebbe ad apportare al diritto all'informazione e conoscenza della collettività, a seguito della permanenza in Rete della notizia, comunque reperibile sul sito sorgente o accessibile interrogando il motore di ricerca attraverso elementi della query differenti dai dati del richiedente l'oblio, sono indubbi. Ancor più, tale soluzione consentirebbe di

storica= archivistica. Non veniva però coinvolta la figura del gestore del motore di ricerca, che di fatto era esclusa dal circuito della decisione, che si estrinsecava generalmente in un ordine rivolto a una testata giornalistica (nonostante alcune decisioni relative alla posizione del motore di ricerca non siano mancate) affinché impedisse la sua indicizzazione. Diversi sono stati anche i procedimenti archiviati nei quali il ricorrente aveva trovato soddisfazione alla propria pretesa alla cancellazione ben prima che l'autorità potesse pronunciarsi con un ordine, a significare la tendenziale riluttanza al contenzioso da parte degli stessi operatori dell'informazione e la scarsa percezione di un effettivo pregiudizio per le ragioni della libertà di espressione come conseguenza della rimozione dagli indici dei motori di ricerca.

[353] Corte di Giustizia dell'Unione europea, Grande Sezione, sentenza C-131/2012, 13 maggio 2014, punto 84.

[354] La quale sottolinea che «*da un lato, i legittimi interessi che giustificano questi trattamenti possono essere differenti e, dall'altro, le conseguenze che tali trattamenti hanno per la persona interessata, e segnatamente per la sua vita privata, non sono necessariamente le stesse*», Corte di Giustizia dell'Unione europea, Grande Sezione, C-131/12, 13 maggio 2014, punto 86.

[355] Cfr. Garante per la protezione dei dati personali, Provvedimento 27 novembre 2014, n. 548, Doc. Web n. 3710907; Provvedimento 21 maggio 2015, n. 310, Doc. Web n. 4205825; Provvedimento 14 gennaio 2016, n. 8, Doc. Web n. 4714994.

salvaguardare le pretese dei terzi controinteressati alla memoria che, in quanto soggetti positivamente coinvolti nella notizia che si vorrebbe obliare, vantano l'interesse contrario al ricordo, al fine di evitare che la loro posizione venga irrimediabilmente offuscata. Questi ultimi, infatti, non sarebbero danneggiati dalla de-indicizzazione per nominativo, dal momento che la notizia continuerebbe comunque a permanere nei canali del Web e sarebbe pur sempre raggiungibile su digitazione dei loro dati personali o di altri elementi ad essa connessi. Al più potrebbe risultare maggiormente difficoltoso l'accesso all'informazione, poiché, come spesso accade, avendo le vittime meno visibilità dei carnefici, i loro dati potrebbero non essere noti a tutti.

Peraltro, è opportuno precisare che le richieste di rimozione pervenute a Google sino a dicembre 2015, ad un anno e mezzo dalla sentenza Google Spain, da parte di interessati italiani, sono state 333.450 e, avendo ognuna di queste tre pagine in media da valutare, il motore di ricerca, almeno inizialmente, è stato chiamato a svolgere un lavoro titanico di valutazione di tematiche delicate e sensibili assai difficile da gestire. Dei link segnalati, solo per il 41,9% è stata accettata la rimozione, consentita nonostante la mancata trasparenza dei criteri applicati, stante anche l'assenza di norme o criteri oggettivi sulla base di quali valutare la singola richiesta.

La percentuale dei contenuti non rimossi, rispetto alla media europea, è stata molto alta, quasi venti punti percentuali e questo non solo perché Google ha dato prova di essere un attento paladino del diritto di cronaca, valutando attentamente caso per caso, contenuto per contenuto, ma anche perché la semplicità e la facilità di accesso al modello che il motore di ricerca aveva messo in Rete a disposizione degli interessati, avevano creato una falsa aspettativa di facilità dell'operazione e certezza del risultato: le richieste, infatti, molto spesso, sono risultate poco accurate e del tutto improprie. Molti dei casi sottoposti non erano nemmeno pertinenti all'oblio perché a confine con forme di diffamazione o violazione della privacy.

Delle richieste di rimozione respinte da Google, circa 25.000, solo 50 sono approdate innanzi al Garante nazionale della privacy, pari allo 0,2%: un numero estremamente esiguo, un vero e proprio corto circuito che, da una parte, lascia perplessi e, dall'altra, è chiaro indice di richieste che, probabilmente, già a priori non avevano senso, anche se v'è da escludere che talvolta gli interessati possano essere stati condizionati negativamente dai costi di accesso e dalle difficoltà della procedura.

Dalle modalità di esercizio del diritto all'oblio, immediatamente successive alla Google Spain, si è altresì osservato come il Garante sia stato poco percepito come figura idonea a fornire tutela ai dati personali dell'uomo comune; è stato avvertito come uno strumento di difesa più per addetti ai lavori. Il 30% dei ricorsi presentati al Garante hanno avuto un esito positivo: in un caso su tre l'organo amministrativo ha ritenuto che Google avesse torto, esito a cui è giunto non solo per il particolare garantismo che ha inteso assicurare alla sfera privata delle persone, ma anche per la supponenza e, non raramente, superficialità con cui titolare e responsabile del trattamento avevano valutato in prima istanza le richieste.

Ad ogni modo, pur essendo la de-indicizzazione una misura meno drastica della cancellazione, comunque solleva l'esigenza di un bilanciamento con il diritto alla libertà di espressione e quello all'informazione. Ed è qui che si evidenziano talune criticità, che meritano il giusto rilievo. L'aspetto che desta maggiori perplessità, all'occhio critico della dottrina, è legato all'affidamento, dell'operazione di bilanciamento tra le opposte posizioni in conflitto, in prima battuta, alle cure del motore di ricerca, soggetto mosso da logiche di mercato, quindi carente della terzietà necessaria affinché sia operata un'equa ponderazione degli interessi in gioco e al quale non si può ragionevolmente chiedere di mutare il proprio *status* a fronte delle istanze degli utenti.

Nel compito affidato dalla Corte di Giustizia al gestore del motore di ricerca, questi dovrebbe ergersi a sorta di "paladino" della libertà di accesso all'informazione in Rete, rigettando l'istanza dell'interessato nell'ottica della tutela dell'interesse collettivo alla conoscenza ed anche contro il proprio interesse d'impresa.

Ma un'aspettativa di questo tipo è mera utopia: non si può pretendere, infatti, da un operatore di mercato privato di anteporre al proprio interesse d'impresa, quello della collettività alla conoscenza, soprattutto allorquando ciò possa comportare esternalità negative non preventivabili o difficilmente sostenibili[356].

[356] In riferimento all'assenza di terzietà nell'operazione di bilanciamento compiuta da Google, si veda, *ex multis*, S. SICA- V. D'ANTONIO, *Il diritto all'oblio su internet dopo la sentenza Google Spain,* op. cit.: «*Chiaramente, la linea di demarcazione rispetto agli interlocutori istituzionali cui l'interessato può rivolgere la propria istanza in seconda battuta è segnata anche e soprattutto dalla natura privatistica che caratterizza il gestore del motore di ricerca, che non può essere confuso con una sorte di paladino del diritto alla conoscenza nel Web. Questi, infatti, nella identificazione del point of balance tra il diritto alla riservatezza e quello alla conoscenza di una data informazione presente in Rete non sarà animato dalla prospettiva del migliore equilibrio tra posizioni individuali in un dato contesto sociale, secondo una sorta di rimozione logica (para)pubblicistica e con surrettizio riconoscimento allo stesso di funzioni quasi costituzionali*».

Il motore di ricerca, infatti, è stretto tra due opposti interessi: da una parte, è motivato a respingere le istanze di de-indicizzazione, al fine di evitare il depauperamento del patrimonio digitale, che comporterebbe un indebolimento del gigante dell'informazione sul mercato, a causa della perdita di appeal, ed in questo il suo interesse al mantenimento della notizia coincide perfettamente con quello della collettività e dei terzi controinteressati al ricordo; dall'altra, il timore di incorrere in pesanti e massicce richieste risarcitorie, conseguenti al mancato riconoscimento dell'oblio, lo indurrebbe ad operare tagli indiscriminati, mosso dalla logica di minimizzazione del rischio, che è alla base delle strategie imprenditoriali[357]. Nell'uno o nell'altro caso, ciò che emerge è l'assenza, nel motore di ricerca, delle qualità di oggettività, terzietà, imparzialità ed indipendenza, che notoriamente appartengono agli organismi giurisdizionali. Proprio al fine di evitare distorsioni di questo calibro, anche in coerenza con i principi espressi dalla Corte di Giustizia, sarebbe stato auspicabile affidare il vaglio delle istanze di de-indicizzazione direttamente ai garanti nazionali o prevederne l'interpello necessario da parte dei motori di ricerca: ciò avrebbe consentito un'indubbia garanzia di obiettività di giudizio ed un effettivo contemperamento degli interessi coinvolti. L'incauto affidamento al motore di ricerca dell'operazione di bilanciamento costituisce uno dei punti critici del diritto all'oblio, quale diritto alla de-indicizzazione[358]. L'affidamento a soggetti privati della regolazione di interessi rilevanti, scaturente dalla necessità di ponderare il diritto alla libertà di informazione ed i diritti della personalità, con il compito di istituire procedure ed operare valutazioni sostituendosi, almeno in prima istanza, al ruolo tradizionalmente rivestito dalla giurisdizione, in un settore nel quale vi è una forte posizione dominante, pone serie perplessità.

A parte la necessità, per garantire l'equo contemperamento degli interessi, di consentire il diritto di difesa a tutti i soggetti coinvolti nella decisione, appare comunque un paradosso che a garantire l'equità e la correttezza del procedimento siano soggetti privati

[357] Così per S. SICA- V. D'ANTONIO, op. ult. cit., 184: «*Sebbene la decisione della Corte di Giustizia taccia completamente sul punto, sarebbe ingenuo,* rectius *illogico, attendersi che il gestore del motore di ricerca sia mosso, nel vagliare le istanze proposte dai consociati, da una finalità diversa da quella d'impresa: siffatta prospettiva, che non può non animare qualsivoglia operatore di mercato, nella maggior parte dei contesti economici, indica come obiettivo primario, innanzitutto la minimizzazione del rischio*».

[358] Così per O. POLLICINO, *Google rischia di "vestire" un ruolo para-costituzionale*, in *Il Sole 24 Ore*, 15 maggio 2014.

che, nonostante mossi da logiche di mercato, diventino «arbitri della fruibilità dell'informazione online[359]».

Tale aspetto risulta tanto più rischioso a causa dell'assenza, tanto nella sentenza Costeja quanto nei lavori legislativi, di criteri uniformi in forza dei quali operare il bilanciamento tra i confliggenti interessi in gioco.

Nell'intento di sopperire a questa lacuna giudiziaria e legislativa, il Gruppo di lavoro dei Garanti europei ha previsto una serie di criteri utili alla causa[360], tra i quali un peso particolare è da attribuire all'eventuale ruolo nella vita pubblica rivestito dal richiedente, che può aumentare in modo significativo l'interesse pubblico al mantenimento della indicizzazione. Il documento affronta anche la non semplice definizione di cosa debba intendersi per 'public figure', in particolare per personaggio pubblico legittimamente soggetto a potenziali compromissioni del proprio diritto alla riservatezza. Il documento si premura di precisare che, anche in riferimento ai personaggi pubblici, alcune informazioni, come ad esempio quelle attinenti alla loro salute o relative ai membri della loro famiglia, possono presentare carattere decisamente privato, tanto da implicare una legittima lesione della loro sfera di riservatezza, in caso si divulgazione. Tra gli altri elementi da tenere in considerazione, nel deliberare sull'accoglibilità o meno di una richiesta di de-indicizzazione, oltre alla minore età dell'interessato, all'eventuale pertinenza dell'informazione a profili sensibili, all'aggiornamento del dato, al tempo trascorso dalla sua iniziale pubblicazione, il W.P. 29 richiama esplicitamente anche il riferimento del dato a fatti di natura penale: in questo caso le autorità nazionali dovranno propendere per la de-indicizzazione nel caso di reati minori, rispetto ai quali sia trascorso un lungo lasso di tempo, mentre un approccio più cauto è raccomandato per i reati più gravi commessi in epoche più recenti.

---

[359] A. MANTELERO, *Il futuro Regolamento EU sui dati personali e la valenza politica del caso Google: ricordare e dimenticare nella Digital economy,* in *il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di G. RESTA, Z. ZENCOVICH, Roma, 2015, 267.

[360] Guidelines on the Implementation of the Court of Justice on the European Union Judgement on "Google Spain And Inc V. Agencia Espanola de Proteccion de Datos (AEDP) and Mario Costeja Gonzalez" C-131/12, Parere del Gruppo europeo dei Garanti (Article 29 Working Party), pubblicato il 26 novembre 2014, finalizzato a fornire un'interpretazione univoca della Google Spain ed i criteri di applicazione comune di tutte le Authorities europee. La Corte di Giustizia, nella sentenza C-131/2012, ha sollevato notevoli problemi interpretativi: l'alto Collegio ha previsto infatti che il NO INDEX potesse essere reclamato direttamente nei confronti del motore di ricerca. La politica giudiziaria celata dietro la sentenza Costeja si offre ai nostri occhi grazie alla lettura delle linee guida forgiate dai Garanti europei, dirette a risolvere problemi interpretativi ed applicativi della famosa pronuncia.

Pronunce successive, anche provenienti da organi di giurisdizione interna, avallano questa impostazione. E' stato, infatti, negato il diritto all'oblio rispetto a fatti collegati ad episodi di terrorismo risalenti al 1975[361] e riconducibili a soggetti che nell'attualità, lungi dall'adottare un profilo di riservatezza, hanno scelto di svolgere attività pubblica[362]in ambito politico e sociale o in relazione a vicende che, pur risalenti al 1997, riguardino la commissione di reati gravi e rispondano all'esigenza di descrivere in modo analitico le origini del fenomeno mafioso[363]. Coerente, in tal senso, è la sentenza della Corte europea dei diritti dell'uomo, relativa al caso Fuschsmann c. Germania[364], che conferma, con il mantenimento nel tempo o la riproposizione di una notizia che associ un soggetto ad un contesto criminale, nei limiti del rispetto di alcuni criteri, precisamente individuati[365], un legittimo esercizio della libertà di espressione. Le linee Guida dei Garanti UE, fortemente garantiste, rifuggono dalla logica delle soluzioni precostituite in protocolli statici e focalizzano, quale principio fondamentale, la disamina caso per caso sulla scorta del bilanciamento comparativo degli interessi in gioco, tutto ciò secondo due criteri fondamentali: quello della potenziale gravità dell'impatto privacy negativo ed il criterio della proporzionalità, pertinenza e non eccedenza.

Successivamente e per reazione alle precisazioni operate dai Garanti europei in calce alla sentenza Costeja, anche Google, tramite il suo 'Advisory Council on the Right to be Forgotten[366]', ha previsto alcuni parametri e regole di condotta per affrontare l'emergenza dell'assenza di criteri oggettivi in base ai quali operare il bilanciamento.

---

[361] Trib. Milano, sentenza del 19 agosto 2014, n. 10258. Si veda in ultimo anche Cass. Civ., Sez. I, sentenza del 3 agosto 2017, n. 38747.

[362] Trib. Milano, sentenza 18 giugno 2015, n. 7610.

[363] Trib. Torino, sentenza 14 luglio 2015, n. 4977.

[364] Corte europea dei diritti dell'uomo, Fuschsmann v. Germania, ric. 71233/2013, (2017). La vicenda trae origine dal caso di un uomo d'affari ucraino, Boris Fuschsmann, residente in Germania, amministratore di una società televisiva, si cui il New York Times nel 2001, aveva pubblicato un articolo riguardante il suo coinvolgimento in attività di corruzione, finalizzate ad ottenere licenze televisive in Ucraina. Con sentenza emessa nell'ottobre 2017, la terza sezione della CEDU, ha rigettato il ricorso del cittadino tedesco proposto sulla base dell'art. 8 Cedu. L'uomo sosteneva che il rifiuto di oscurare un articolo on-line, lesivo della sua reputazione, violasse il suo diritto al rispetto per la vita privata.

[365] La Corte richiama espressamente i criteri sanciti in recenti decisioni: CEDU, Conderc e altri v. Francia, ric 404572007 (2015); CEDU, Axel Springer A.G. c. Germani, ric. 39954/2008 (2012): Von Hannover c. Germani, ric 40660/2008 (2012).

[366] Dopo la sentenza Google Spain il motore di ricerca ha predisposto un modello online per inoltrare la richiesta di de-indicizzazione, costituendo un Consiglio di esperti per redigere le Linee Guida interne della Compagnia, *Linee guida di Google*, su indicazione dell'"*Advisory Council to Google on the Right To Be Forgotten*" del 6 febbraio 2015, nelle quali si esplicitano i criteri in base ai quali Google opererà il bilanciamento di interessi.

Nel Report sono *in primis* evidenziati quattro criteri (nessuno dei quali di per sé determinante o predominante), in base ai quali la società ritiene corretta una valutazione in merito alla possibilità di de-indicizzare alcuni dati. Il primo criterio è rappresentato dal ruolo svolto dall'interessato nella vita pubblica, per il quale è prevista, nel documento, una sorta di gerarchia in forza della quale, maggiore è la rilevanza pubblica, minore sarà la possibilità che una richiesta di de-indicizzazione sia accolta dal motore di ricerca, alla luce del predominante interesse pubblico alla ricerca di informazioni. Un ruolo importante, tanto da assurgere a secondo criterio in forza del quale operare il bilanciamento, è rivestito dalla tipologia di informazione oggetto della richiesta, per cui ove l'informazione dovesse concernere aspetti privati della vita della persona sarà più facilmente obliabile che non se dovesse riferirsi a temi di attenzione collettiva, storica e di rilievo scientifico, per i quali l'interesse pubblico alla conoscenza si presume prevalente rispetto al diritto all'oblio.

Quanto alla fonte dell'informazione, quale terzo criterio indicato dal motore di ricerca, Google privilegia il diritto all'informazione rispetto all'oblio qualora le notizie siano diffuse nell'esercizio dell'attività giornalistica o, comunque, dell'attività propria di siti di informazione di conclamata autorevolezza.

Relativamente al fattore temporale, infine, quale ultimo criterio, per il motore di ricerca il tempo riveste particolare importanza nei casi in cui il ruolo dell'interessato, nella sua dimensione pubblica, sia effettivamente mutato e non desti più pubblico interesse.

L'accostamento tra i due documenti è improprio e le differenze sono di tutta evidenza laddove il documento del WP 29, essendo di natura istituzionale è da ritenersi un riferimento sia per il contenzioso amministrativo che per quello giudiziario e, non ultimo, anche per tutti i cittadini e le altre Istituzioni; mentre il Report di Google è a tutti gli effetti una procedura aziendale implementata da una multinazionale leader nel settore, che prevede una serie di disposizioni in materia di Data Protection più blande da sovrapporre alla disciplina europea.

Due ordinamenti che si scontrano: la visione americana più aperta verso la libertà di pubblico accesso alle informazioni e verso la libertà di impresa, che vede la prevalenza del diritto all'autodeterminazione informativa, piuttosto che dell'interesse pubblico; la visione europea più garantista per i diritti della persona, che sancisce la prevalenza della Data Protection con l'unica eccezione dell'interessato-persona pubblica.

D'altro canto, obbligare Google al rispetto del diritto all'oblio, significherebbe riappropriarsi della sovranità perduta sui cittadini europei, della Governance europea sulla protezione dei dati personali, evitando che un privato, appartenente ad una disciplina sulla Data Protection piuttosto morbida, possa imporla in sostituzione della disciplina europea.

Per parte europea, invece, i metodi dell'azienda non devono essere quelli della Giustizia: una policy sulla questione interna del sistema oblio non può assurgere a paradigma applicativo per le Authorities e per le Corti.

E' vero il contrario!

Sono le Linee Guida dei Garanti UE la disciplina che l'azienda deve osservare.

Google, invece, riluttante a sottoporsi alla disciplina europea ha costruito una policy che riafferma la propria sovranità digitale sui propri sudditi elettronici europei, venendo ad ergere una vera e propria muraglia tra Internet USA ed Internet UE.

Il rapporto Google, infine, esclude a priori la concezione del nuovo diritto all'oblio come elaborato dalla CGUE Costeja: il 'nuovo diritto all'oblio' non è il diritto all'oblio, ma quello all'autodeterminazione informativa online, di cui il diritto all'oblio originario è solo una piccola parte. Si tratta della Data Protection applicata alla Rete, che richiede ai titolari del trattamento l'adozione di tutte le misure di sicurezza minime idonee ad evitare la asimmetria decisionale tra interessato e titolare del trattamento, prodotta dalla prevaricazione del più forte che, ormai, privo del consenso iniziale, continua nella raccolta di dati, in modo sproporzionato ed arbitrario. Il nuovo diritto all'oblio, quale esercizio del potere di controllo sul proprio patrimonio informativo, in quest'ottica, serve a riequilibrare la sbilanciata situazione.

Anche il Legislatore europeo ha mancato di indicare criteri oggettivi in forza dei quali i titolari del trattamento *in primis*, nonché le Autorità amministrative o giudiziarie, avrebbero dovuto operare il bilanciamento, perdendo in tal modo una grande opportunità. Stante la diretta applicabilità, senza oneri di recepimento, del Regolamento negli Stati membri dell'Unione, se il Legislatore europeo avesse opportunamente predisposto i necessari criteri oggettivi, avrebbe dettato un *modus operandi* comune, sollevando in

parte le Autorità dell'Eurozona dalle problematiche che l'operazione di bilanciamento pone in relazione ai singoli casi concreti[367].

In assenza di opportuni interventi legislativi, attesi e non manifestatisi, ancora una volta la giurisprudenza si è accollata l'onere di colmare le lacune, individuando, nell'Ordinanza del marzo 2018[368], un decalogo di presupposti, in presenza dei quali il diritto all'oblio risulterebbe recessivo rispetto al diritto di cronaca, pur non chiarendo se tali criteri debbano essere presenti in via cumulativa o alternativa. Al fine di sciogliere i nodi tutt'ora presenti è stata investita della questione la Suprema Corte, nel suo più autorevole Consesso[369], nell'intento di consegnare agli operatori del diritto un quadro sistematico ed oggettivo di criteri operativi, sottraendoli al gioco delle geometrie variabili.

5) Forme di tutele possibili per i terzi controinteressati al ricordo

Le molteplici soluzioni prospettate dal Legislatore europeo o le innovative tecniche proposte dagli operatori del sistema, sebbene utili alla causa, presentano delle asperità, anche a causa di un'evoluzione tecnologica non completamente perfezionatasi, che ancor oggi le rende vulnerabili ed inidonee alla soluzione del problema.

---

[367] In verità, un unico riferimento all'operazione di bilanciamento è possibile rinvenirlo nel Considerando 47, laddove ha stabilito che l´interesse legittimo del titolare o del terzo debba prevalere sui diritti e le libertà fondamentali dell´interessato per costituire un valido fondamento di liceità.
Il regolamento chiarisce espressamente che l´interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti: «*I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali. Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Costituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto*».

[368] Cass. Civ., Sez. I, Ordinanza 20 marzo 2018, n. 6919, cit. Il tema, qui solo richiamato, è trattato più diffusamente nel capitolo secondo, sezione seconda, paragrafo 7), di questa tesi.

[369] Cass. Civ., Sez. III, Ordinanza di rimessione alle Sezioni Unite, 5 novembre 2018, n. 28084, cit.

La tecnica sottrattiva dell'anonimizzazione, comportando l'oscuramento dei dati, se da un lato impedisce l'identificazione dell'interessato, riducendo i rischi per la privacy, dall'altro, cancellandoli definitivamente ed impedendo per sempre l'identificazione dei titolari degli stessi, crea un vero e proprio *vulnus* nell'informazione, determinando l'esistenza di una notizia che, sebbene integra, è tuttavia slegata dai suoi protagonisti. Un *vulnus* irrecuperabile dal momento che l'identità persa non sarà più possibile recuperarla. La pseudonimizzazione, invece, risulta più utile alla causa, dal momento che i dati non sono definitivamente cancellati ma semplicemente sostituiti con lettere o cifre. A differenza della prima non determina un processo irreversibile dal momento che, attraverso l'utilizzo di informazioni aggiuntive, conservate separatamente e soggette a misure tecniche ed organizzative, tese a garantire l'anonimato, è possibile risalire all'identità della persona, reidentificandola. Anche questa tecnica, tuttavia, non è esente da criticità, in quanto agli occhi della collettività l'informazione circolante in Rete è comunque priva degli elementi identificativi, che restano nella disponibilità di pochi, ossia solo di coloro che sono in possesso delle liste di corrispondenza.

Allo stato dell'arte, la tecnica chirurgica meno invasiva risulta probabilmente il taglio del link alla notizia, che salvaguarderebbe le pretese di tutte le parti interessate, in attesa di soluzioni di ingegneria informatica che appianino le criticità delle soluzioni precedentemente analizzate, a seguito di un equo contemperamento dei contrapposti interessi.

La tecnica proposta dalla Google/Spain, mediante il taglio dei soli link alla notizia strettamente connessi al nominativo dell'interessato è sottoposta ad una regolamentazione stringente, quanto ai limiti entro i quali può essere operata, evitando rimozioni o cancellazioni indiscriminate quanto dannose, rese su mera richiesta di chi intenda semplicemente edulcorare la propria identità digitale e sartorializzare le informazioni circolanti in Rete.

L'uso delle tecniche di anonimizzazione, pseudinimizzazione e de-indicizzazione, comportando la permanenza della notizia in Rete, anche se talvolta monca di riferimenti soggettivi, fanno salve le ragioni della collettività e dei terzi interessati alla memoria. Quanto alla tutela dell'interesse della collettività alla conservazione della memoria storica, oggi contenuta e divulgata in massima parte attraverso i canali del Web, la tecnica della de-indicizzazione per nominativo, realizzabile dai soli motori di ricerca, si presenta

sicuramente come un'operazione chirurgica meno invasiva in quanto, tagliando i soli link che compaiono su digitazione del nominativo della persona interessata, consente la permanenza della notizia, nella sua integrità, nelle pagine Web dei siti sorgente. Le alternative tecniche di anonimizzazione e pseudonimizzazione, adoperate dai soli siti sorgente, pur privando la notizia delle sue connotazioni soggettive, utili all'identificazione del protagonista, la lasciano comunque vivere in Rete per cui, la stessa sarà vera ed integra nei suoi contenuti ad eccezione dei riferimenti soggettivi relativi al protagonista della vicenda. Nel primo caso, l'informazione continuerebbe a vivere in Rete, subendo una riduzione di visibilità agli occhi dei fruitori, che ne vedrebbero reso più difficile l'accesso, dovendo utilizzare altre chiavi che non siano i dati personali del protagonista. Nella seconda ipotesi, invece, l'informazione sarà violata nelle sue connotazioni soggettive, a causa dell'oscuramento dei dati del protagonista, offrendo una conoscenza solo parziale della notizia, motivo di un probabile vulnus al cuore dell'informazione, che se pur integra nei suoi contenuti, mancherà di qualche riferimento soggettivo. Tale osservazione trova riscontro nell'attività di analisi delle pronunce giudiziarie, nelle quali i nomi dei protagonisti sono oscurati: la lettura e la comprensione del testo risultano talvolta meno agevoli proprio a seguito dell'assenza dei riferimenti soggettivi. Un sacrificio sopportabile in nome della tutela di diritti fondamentali della persona!

L'uso in combinato disposto della tecnica di de-indicizzazione da un lato, e anonimizzazione o pseudonimizzazione dall'altro, scaturente da richieste avanzate rispettivamente al motore di ricerca ed al sito sorgente, probabilmente potrebbe arrecare qualche danno in più all'integrità del ricordo. Precisazione valida ma non assoluta, perché quella stessa informazione vulnerata dalle recisioni operate dal motore di ricerca o dal sito sorgente continuerà in ogni caso ad essere presente negli anfratti della Rete, a seguito delle infinite memorizzazioni, copie e condivisioni che porteranno il dato a sopravvivere nella sua integrità originaria. Gli interessi della collettività, ad ogni modo, sarebbero fatti salvi. La Rete, per sua stessa natura, non dimentica!

Altrettanto può dirsi per il terzo controinteressato alla permanenza del ricordo. Lo stesso non sarebbe danneggiato in alcun modo dalle tecniche di anonimizzazione e pseudonimizzazione, in quanto ad essere oscurati sarebbero esclusivamente i dati dell'interessato all'oblio e non quelli relativi ad altri soggetti coinvolti nella vicenda.

Quanto, invece, all'adozione della tecnica di de-indicizzazione per nominativo, anche in questo caso, essendo recisi esclusivamente i link collegati al nome del richiedente l'oblio, la posizione del terzo interessato al ricordo non verrebbe lesa, data la possibilità di raggiungere la notizia, interrogando il motore di ricerca attraverso altre credenziali, ivi compresi i loro dati anagrafici. Probabilmente, in questo caso si registrerebbe una maggiore difficoltà di accesso all'informazione perché le vittime sono, quasi sempre, meno esposte nei ricordi della pubblica opinione, per cui i loro dati potrebbero non essere in possesso del patrimonio di conoscenze dei fruitori della Rete.

Dall'esame di entrambe le posizioni giuridiche considerate emerge che il taglio del link, come previsto dalla CGUE nel 2014, si presenti come la risposta all'istanza di oblio meno invasiva, tanto più in quanto dovrà essere concessa entro i parametri stringenti stabiliti dalla giurisprudenza europea e nazionale prima e dal Legislatore UE successivamente, sempre all'esito di un'operazione di bilanciamento degli interessi confliggenti vantati dai diversi protagonisti della vicenda oggetto di oblio. Sarebbe, altresì, opportuno che il bilanciamento non fosse operato acriticamente, attraverso algoritmi, ma fosse frutto di un'attenta valutazione operata da una Commissione di esperti istituita presso ogni motore di ricerca, ovvero affidata ai Garanti nazionali o ad organismi giurisdizionali. Verrebbe, in tal modo, ad essere ridimensionato il rischio di un private enforcement del motore di ricerca, sia per i margini di discrezionalità, piuttosto ristretti, consentiti nell'adozione della decisione circa l'operatività o meno del taglio del link alla notizia, che per la maggiore garanzia di terzietà propria dell'autorità amministrativa/giurisdizionale. Il bilanciamento, secondo le descritte modalità, avrebbe il pregio di essere operato da soggetti esperti e sulla base di valutazioni razionali, ponderate e giuridicamente fondate, rispetto a quelle generate da automatismi tecnico-matematici, scaturenti da algoritmi.

A conforto ulteriore delle ragioni dei terzi interessati alla permanenza della notizia in Rete nella sua integrità, potrebbe ipotizzarsi una soluzione che preveda, attraverso l'integrazione del contraddittorio, la loro partecipazione all'attività di ponderazione, congiuntamente agli altri soggetti, pur interessati alla conservazione dell'informazione, quali il titolare del sito sorgente e l'autore della pubblicazione[370]. In particolare, sin dalla fase di richiesta di rimozione dei link alla notizia, avanzata dall'interessato al motore di

[370] In merito al necessario coinvolgimento del titolare del sito sorgente e del fornitore del contenuto, si veda: S. MARTINELLI, *Diritto all'oblio e motori di ricerca. Memoria e privacy nell'era digitale*, Milano, 2017, 184.

ricerca, quest'ultimo, valutata la presenza di eventuali soggetti terzi non dovrà pronunciarsi senza essersi preliminarmente assicurato dell'avvenuta notifica nei loro confronti dell'istanza di oblio, onde consentire di controdedurre alle pretese del ricorrente, sollecitando le proprie. Il processo di ponderazione, in questo modo, verrebbe a considerare in un'ottica più ampia e completa, il fondamento giuridico e razionale delle pretese avanzate dai controinteressati.

Al fine di riequilibrare i poteri riconosciuti alle parti dovrà essere consentita, anche ai terzi controinteressati la possibilità di adire l'Autorità amministrativa e/o giudiziaria al fine di ottenere una nuova e più opportuna valutazione delle loro posizioni ed un bilanciamento più oculato degli interessi in gioco. Ove, all'esito del giudizio di ponderazione, fosse riconosciuta la prevalenza del diritto all'oblio, potrebbe prospettarsi la possibilità di prevedere il riconoscimento di un indennizzo da attività, sia pur lecita, tuttavia dannosa per le ragioni dei terzi controinteressati, a condizione che di tale pregiudizio ne siano fornite le prove, rivenienti da una perdita di visibilità per il webmaster, da un affievolimento della circolazione della notizia per l'autore della pubblicazione, e, non ultimo, dalle accresciute difficoltà di accesso all'informazione per il terzo controinteressato al ricordo.

La previsione di una qualche forma indennitaria a carico di colui che aziona il diritto all'oblio potrebbe altresì costituire un valido deterrente per le richieste indiscriminate di de-indicizzazione, obbligando l'interessato ad una preliminare e più attenta ed oculata valutazione della sua pretesa.

Nulla quaestio al diritto al riconoscimento del risarcimento del danno per il caso in cui fosse operata una rimozione in violazione dei limiti imposti dal Legislatore.

6) Sommersi e salvati nel mare del Web: uno scenario ancora tutto da definire

E' indiscutibile che le forme di tutela apprestate alle violazioni dei diritti della personalità, in generale, e ai diritti all'identità digitale ed all'oblio, in particolare, abbiano percorso, negli ultimi sessant'anni, un cammino tortuoso, sicuramente in salita, teso alla protezione della sfera più intima e privata dell'individuo, anche in forza della dimensione antropologica cui è informato il nostro sistema giuridico.

Nell'era digitale, se da un lato il problema del diritto all'oblio si pone con rinnovata urgenza poiché le informazioni su di una persona sono suscettibili di una conservazione

e stratificazione potenzialmente infinite, la sua tutela, d'altra parte, non si pone più come un'alternativa stringente tra cancellazione e non cancellazione dei dati: non si tratta di cancellare un contenuto oppure renderlo conoscibile a tutti, perché la soluzione migliore non può non consistere nella modulazione della facilità con cui il contenuto dell'informazione può essere reperito in Rete.

E' un diritto che si colloca esattamente sul crinale tra libertà e controllo, tra indipendenza ed omologazione, tra dignità umana e mercificazione.

E se il diritto fosse azionato e contenuto nei limiti e nelle strettoie imposte dagli operatori giuridici, non risulterebbe solo utile alla causa del singolo, ma rappresenterebbe la punta di diamante nel panorama dei diritti inviolabili della persona, costituendo il fondamento giuridico della dignità ed identità personale.

Il diritto all'oblio è invocato dal singolo per proteggere il proprio presente e il proprio futuro dal proprio passato, senza la pretesa di modificare la sua stessa natura, che potrebbe condurre ad una vita anonima, spersonalizzante, immersa nella quotidianità anestetizzante di un eterno presente. Un diritto che fa da bussola etica tra due antipodi: la memoria, museo chimerico dei rimorsi e messaggera dell'antichità, ed il privilegio della libertà, l'abbandono di un passato ingombrante.

È chiamato a sostegno dell'interessato per tutelare la sua identità personale attuale e futura da trascorsi spiacevoli, per difendersi da indebite intrusioni nella propria sfera privata, per mantenere un controllo sui dati e sulle informazioni un tempo immesse in Rete, in ossequio ai principi cardine di scelta e controllo.

Lungi dal determinare un'eugenetica privata ed arbitraria di quanto la collettività debba ricordare, l'oblio rappresenta l'unico antidoto in grado di sconfiggere l'ergastolo della memoria eterna. L'universo sterminato della Rete e la *net economy* impongono un ripensamento del ruolo degli attori ed un perfezionamento delle forme di tutela, volte a contemperare tutti i valori in campo, che trascendono gli interessi del singolo, comunque sempre orientate alla salvaguardia della memoria collettiva e della coscienza civile. Lungi dalla velleità di perseguire il principio dell'oscuramento selettivo di brandelli di storia, il silenzio del memoria rappresenta l'unico strumento oggi in grado di proteggere i singoli dagli abusi di una Rete che non è in grado di non ricordare. In gioco c'è la libertà del più potente mercato delle idee finora inventato dall'uomo, Internet, e la ricerca di una

dimensione nella quale sia possibile sospendere il fardello di esperienze dolorose che hanno segnato il passato.

Si insegue, infatti, una memoria forsennata sempre più bulimicamente memorizzante, che rende sempre più difficile cancellare da archivi mostruosamente onnipresenti ciò che magari imbarazza o offende. Potrebbe essere l'alba di una società trasparente.

Ma dimenticare l'oblio potrebbe costituire un prezzo troppo alto da pagare per realizzare l'intelligenza collettiva!

Siamo abituati a vivere in un contesto di democrazia e tolleranza ma la sicurezza del futuro si radica nelle garanzie del presente.

La Rete ha determinato una strabiliante dilatazione delle facoltà di relazione e di comunicazione delle informazioni, ma la sfida deve essere raccolta, senza rinunciare ai diritti di fronte al progresso tecnologico, elaborando soluzioni bilanciate e rispettose delle conquiste di civiltà già raggiunte e consolidate.

Probabilmente le soluzioni informatiche atte a soddisfare la pretesa al silenzio della memoria sono ancora perfettibili: ulteriori tecniche di ingegneria informatica potranno prender corpo dalla stessa tecnologia che ha generato il problema. Tuttavia, senza dubbio, all'oblio non si può più rinunciare. E, per vero, «non esiste né cultura, né godimento estetico, né possibilità di essere generosi o compassionevoli o coraggiosi senza una qualche veniale forma di oblio; e non c'è neppure amore - che prima di tutto consiste nel dimenticarsi di sé per vivere nell'altro - né, più ancora, esiste la capacità di vivere una vita piena, dato che l'oblio è un antidoto infallibile contro la fossilizzazione della persona: abbiamo bisogno di dimenticare parzialmente per smettere di essere noi stessi, per essere un'altra volta o essere altri, per emanciparci dalla schiavitù dell'Io e conquistare la felicità di essere un altro senza smettere di essere noi stessi, che è, poi, l'unica forma concepibile e sensata di felicità»[371].

[371] R. MORENO PIQUÉ, *La farmacia del olvido*. *(Un ensayo filosófico)*, RBA Libros, S.A., Barcelona 2007, 323.

BIBLIOGRAFIA

AID M., *The Secret Sentry; the untold History of National Security Agency*, in *Bloomsbury Press*, 2010

ARENA G., *La tutela della riservatezza nella società dell'informazione*, in AA. VV., *Scritti in onore di P. Virga*, Milano, Vol. I, 1994

ASHTON K., *That 'Internet of Things'*, in *RFID Journal*, 22 luglio 2009

AULETTA T., *Diritto alla riservatezza e "droit a l'oublì",* in ALPA-BESSONE-BONESCHI -CAREZZA, *L'informazione e i diritti della persona*, Napoli, 1983

BACK U., *The digital Freedom risk: too fragile an acknowledgment*, 30 august 2013

BACONE F., *Religious meditations of heresias*, Londra, XVI Sec

BARCHIESI A., CEO di Reputation Manager, Intervista alla *Repubblica*, 14 febbraio 2016

BARCHIESI A., *La tentazione dell'oblio. Vuoi subire o costruire la tua identità digitale?*, Milano, 2016

BARILE P., *Libertà di manifestazione del pensiero*, in *Enciclopedia del diritto*, XXIV, Milano, 1974

BELLEZZA M., *L'oblio è legge in Russia*, in *Medialaw*, 16 novembre 2016

BEVERE A. – ZENO-ZENCOVICH V., *La rete e il diritto sanzionatorio. Una visione d'insieme*, in *Dir. inform.*, 3, 2011

BIANCHI L. –D'ACQUISTO G., *Il trattamento di dati personali effettuato dai motori di ricerca e il diritto di rettifica dopo la sentenza della Corte di Giustizia*, in *I quaderni di Astrid*, 2015

BIASOTTI A., *Il nuovo regolamento europeo sulla protezione dei dati. Guida pratica alla nuova privacy e ai principali adempimenti del Regolamento UE 2016/679*, EPC, Roma, 2017

BINNEY B., *Welcome to Utah, the NSA desert home for eavesdropping on America*, in *The Guardian*, 14 giugno 2013

BLACK E., *L'IBM e l'olocausto*, trad. it. a cura di R. Zuppet e S. Mancini, Milano, 2001

BONGIOVANNI S. - MOTTINO C., *Il vademecum sul Regolamento europeo 2016/679*, Frosinone, 2017

BROUSSARD M., *The Irony of Writing Online About Digital Preservation*, in *The Atlantic*, 20 novembre 2015

BURTON C. - DE VOEL L. - KUNER C. - PATERAKI A., *The Proposed EU Data Protection Regulation Three Years Laters: The Council Position*, in *BNA Privacy e Security Law Report*, 29 giugno 2015, in *Internet*, https://www.wsgr.com/eudataregulation/pdf/BNA-0615.pdf

BUSIA G., *Una vera rivoluzione copernicana*, in *Il Sole 24 Ore*, 10 maggio 2014

CAMERA G. - POLLICNO O., *La legge è uguale anche sul web*, Milano, 2010

CAPUTO L., *Il diritto all'oblio, Dylan Dog e il desiderio di dimenticare,* in *www.iurisprudentia.it*

CASSANO G. - SORIANO A., *I diritti della personalità dall'actio iniuriarum alle banche dati,* in *Vita not.*, 1998

CASSANO G., *Diritto dell'internet: il sistema della tutela delle persone*, Milano, 2005

CASTELLANETA M., *Così l'oblio mette a rischio la libertà di espressione*, in *Guida dir.,* 7 giugno 2014

CRIPPA L., *Il diritto all'oblio: alla ricerca di un'autonoma definizione*, in *Giust. Civ*., 1997

CROLLA S., *Dal Safe Harbour al Ue-Us Privacy Shield*, in *Formiche*, marzo 2016

D'ACQUISTO G., *Diritto all'oblio tra tecnologia e diritto*, *in* PIZZETTI F. (a cura di), *Il caso del diritto all'oblio*, Torino, 2013

D'ANTONIO V., *Il diritto all'oblio on line come diritto alla de-indicizzazione del dato. Oblio e cancellazione dei dati nel diritto europeo*, in SICA S., D'ANTONIO V., RICCIO G.M., (a cura di), *La Nuova Disciplina Europea della Privacy*, Padova, 2016

D'ANTONIO V., *Oltre la cancellazione dei dati personali: l'originaria concezione del diritto all'oblio offline, Oblio e cancellazione dei dati nel diritto europeo*, in SICA S., D'ANTONIO V., RICCIO G.M., (a cura di), *La nuova disciplina europea della Privacy*, Padova, 2016

V. D'ANTONIO - S. VIGLIAR, *Studi di diritto della comunicazione*. *Persone, società e tecnologie dell'informazione*, Padova, 2009

DE BIASE L., *Patto sui dati, successo europeo e della privacy*, in *Il Sole 24 ore*, 3 febbraio 2016

DE CUPIS A., *Condizioni morali e tutela dell'onore*, in *Foro Pad*., 1960, I

DETERMAN L., *Social media Privacy*: *a dozen myths and fact*, in *Stanford Technology Law Review*, 2012

DI CIOMMO F.- PARDOLESI R., *Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. E' la rete, bellezza!*, in *Danno e resp*., 2012, fasc. 7

DI CIOMMO F., *Diritti della personalità tra media tradizionali e avvento di Internet*, in COMANDÉ G. (a cura di), *Persona e tutele giuridiche*, Torino, 2003

DI CIOMMO F., *Evoluzione tecnologica e categorie civilistiche*, in RUSSO E. (a cura di), *Interpretazione della legge civile e «ragione giuridica»*, Padova, 2003

DI CIOMMO F., *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003

DI CIOMMO F., *Internet e crisi del diritto privato: globalizzazione, dematerializzazione e anonimato virtuale*, in *Riv. crit. dir. priv.*, 2003

DI COCCO C. - SARTOR G., *Temi di diritto dell'informatica*, Torino, 2017

DRUSHEL P. - BACKES M. - TIRTEA R., *Impossible, the right to be forgotten between expectations and practice: report by Eupean Network and Security Agency*, in *Internet* http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten

FEROLA L., *Dal diritto all'oblio al diritto alla memoria sul web. L'esperienza applicativa italiana*, in *Dir. Inform.*, 6, 2012

FERRARA M. –SANTAMARIA E., *Il Diritto all'illesa intimità privata*, in *Riv. Dir. Priv.*, 1937, I

FERRI G. B., *Diritto all'Informazione e diritto all'oblio*, in *Riv. Dir. Civ.,* 1990, I

FINOCCHIARO G., *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir.Inform.*, fasc. 4 – 5 2014

FINOCCHIARO G., *La memoria della Rete ed il diritto all'oblio*, *in Dir. Inform.,,* fasc. 3, 2010

FLOR R., *Tutela penale ed autotutela tecnologica dei diritti d'autore nell'epoca di Internet*, Padova, 2010

FRANCESCHINELLI V., *La tutela della privacy informatica*, Milano, 1998

FROSINI T. E., *Il diritto all'oblio e la libertà informatica*, in *Dir. Inform.*, fasc. 4 – 5, 2012

GARDINI G., *Le regole dell'informazione. L'era della postverità*, Torino, 2017

GIACOBBE G., in A.A.V.V. *Il diritto all'oblio – atti del Convegno di Studi del 17 maggio 1997,* a cura di GABRIELLI E., Napoli, 1999

GIANNOTTI F., *Ricerche sulla tradizione manoscritta delle sentenze di Publilio Siro*, Firenze, 1963

GRAZIADEI M., *Diritto Soggettivo, Potere, Interesse*, in *La parte generale del diritto civile. 2. Il diritto soggettivo*, in SACCO R. (diretto da), *Trattato di Diritto Civile*, Torino, 2001

GREENWALD G. - MAC ASKILL E. - POITRAS L., *Edward Snowden: the whistleblower behind the Nsa Surveillance revelations*, in *The Guardian*, 10 giugno 2013

GREENWALD G., *No place to hide, Edward Snowden e la sorveglianza di massa*, Milano, 2014

HORNUNG G., *Eine Datenschutz-Grundverordnung fur Europa, in Licht und Schatten im kommissionsentwurf vom*, ZD, 2012, vol. XXV

IASELLI M., *Video offensivo on-line: nessuna responsabilità per l'Internet provider*, in *www.altalex.com*, 26 marzo 2014

KELLER D., *The final draft of europe's right to be forgotten law*, in *Internet, all'indirizzo* http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europe's-right-be-forgotten-law

LA TORRE A., in A.A.V.V., *Il diritto all'oblio – atti del Convegno di Studi del 17 maggio 1997,* a cura di GABRIELLI E., Napoli, 1999

LADOR J. - LEDERER, *Capitalismo mondiale e cartelli tedeschi tra le due guerre*, Torino, 1959

LEVINSON C., *Vodka-Cola,* Firenze, 1978

LICATA P., *Privacy Shields*, *Vera Jourovà: La Commissione al lavoro sulle criticità*, in *www.corrierecomunicazioni.it*., 13 aprile 2016

LIPARI N., *Libertà di informazione o diritto ad essere informati*, in *Dir. Radiodiff*, 1978

LOIODICE A., *Le radici nella Costituzione*, in JACOBELLI J. (a cura di), *Verso il diritto all'informazione*, Bari, 1991

MAGGIO E., *Sentenza Google – Vividown, Non esiste la sconfinata prateria di Interne dove tutto è permesso e niente può essere vietato*, in *www.dmt.it*

MAGNANI A., *Tasse in Irlanda, dati negli Usa: Facebook «sposta» 1,5 miliardi di utenti,* in *Il Sole 24 ore*, 20 aprile 2018

MAGRO M.B., *Internet e riservatezza: profili di tutela penale dell'utente telematico*, in *www.dirittoegiustizia.it,* 30 luglio 2005

MANGANELLI C., *Progresso tecnologico e protezione dei dati personali*, in SANTANIELLO G. *(a cura di)*, *Trattato di diritto amministrativo, Vol. XXXVI, La protezione dei dati personali*, Padova, 2005

MANTELERO A., *Il futuro Regolamento EU sui dati personali e la valenza politica del caso Google: ricordare e dimenticare nella Digital economy,* in RESTA G., Z. ZENCOVICH V. (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015

MANTELERO A., *Right to be forgotten ed archivi storici dei giornali*, in *Nuova giur. civ. comm.,* 10, 2012

MANTELERO A., *The EU Proposal for a General Protection Regulation and the roots on the "right to be forgotten"*, in *Computer Law and Security Review*, 29, 2013

MANTELERO A*., U.S. Concern about the Eupean Right to Be Forgotten and Free Speech*, in *Contemporary Private Law/Sylvia Kirkegaard International Association of it lawyers*, 88

MANTELERO A., *Us concern about the european right to be forgotten and free speech: much ado about nothing?*, in *Contr. impr*., III, 2012

MARCHETTI G., *Diritto di cronaca online diritto all'oblio*, in AA.VV., *Da internet ai social network*, Rimini, 2013

MARINI P., *Web and Tech Privacy,* 5 maggio 2016

MARONE R., *La rete: il bene comune privato*, in *Doppiozero*, 16 giugno 2011

MARTINELLI S., *Diritto all'oblio e motori di ricerca. Memoria e privacy nell'era digitale*, Milano, 2017

MAYER D. V. -SCHONBERGER, *Delete – Il diritto all'oblio nell'era digitale,* Milano, 2013

MEGALE M., *ICT e diritto nella società dell'informazione*, Torino, 2017

MERCANTALLI R., *Gartner Trends 2017: un'analisi di dettaglio su IA, Things e App Intelligenti*, in *http://www.zerounoweb.it*, 18 aprile 2017

MEZZANOTTE M., *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009

MORENO PIQUÉ R., *La farmacia del olvido. (Un ensayo filosófico)*, RBA Libros, S.A., Barcellona, 2007

NIGER S., *Sorveglianza e nuovi diritti di libertà*, in FINOCCHIARO G. (a cura di), *Diritto dell'anonimato. Anonimato, nome e identità personale*, in GALGANO F. (diretto da), *Trattato di diritto commerciale e di diritto pubblico dell'economia*, Vol. XLVIII, Padova, 2008

NISTICÒ M. - PASSAPAGLIA P. (a cura di), *Internet e costituzione*, Torino, 2014

NOZICH R., *Philosophical explanation*, in *Harvard University Press*, 1981, 584

PACE A., *Replica (XXVIII Congresso nazionale di studio dell'UGC)*, I, Roma, 9-11 dicembre 1977

PAPA A., *Espressione e diffusione del pensiero in internet. Tutela dei diritti e progresso tecnologico*, Torino, 2009

PERLINGIERI P., *L'informazione come bene giuridico*, in *Rass. Dir. civ.*. 1987

PINO G., *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali,* in PANETTA R. (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006

PIZZETTI F., *Dalla Direttiva 95/46 al Nuovo Regolamento Europeo*, Torino, 2016

PIZZETTI F., *Il prisma del diritto all'oblio,* in ID., *Il caso del diritto all'oblio*, Torino, 2013

PIZZETTI F., *La decisione della Corte di Giustizia sul caso Google Spain: più problemi che soluzioni*, Roma, 2014

POLITI F., *Diritto pubblico*, Torino, 2017

POLLICINO O. - BASSINI M., *Il diritto all'oblio*, in http://www.academia.edu/33139336/Il_diritto_alloblio

POLLICINO O., *Google rischia di "vestire" un ruolo para-costituzionale*, in *Il Sole 24 Ore*, 15 maggio 2014

PORTALE V. - MIRAGLIOTTA G., *Osservatori Digital Innovation del Politecnico di Milano*, *I tanti dubbi sul diritto all'oblio*, in *Agenda Digitale*, 7 novembre 2014

PUGLIESE G., *Diritto di cronaca e libertà di pensiero*, in *Foro it*. 1958, I

RATTIN L., *Il diritto all'oblio*, in *Arch. Civ*, 2000

RAVÀ A., *Istituzioni di Diritto Privato*, Padova, 1938

RESTA G. - ZENO-ZENCOVICH V. (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015

RESTA G., *La morte digitale*, in *Dir. Inform.*, 6, 2014

RODOTÀ S., *Dai ricordi ai dati: l'oblio è un diritto?*, in *La Repubblica*, 20 gennaio 2012

RODOTÀ S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Bari, 2014

RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995

RODOTÀ S., *Tecnopolitica: la democrazia e le nuove tecnologie delle comunicazioni*, Bari, 2004

RODOTÀ' S., *Il diritto di avere diritti*, Bari, 2012

ROGERS R., *Metodi digitali*, Bologna 2016

SACCARDI G., *A cinque settimane dall'entrata in vigore, il GDPR preoccupa le aziende*, in *Reportec*, 17 aprile 2018

SAETTA B., *Google e la neutralità dei motori di ricerca tra USA ed Europa*, in *Internet e Diritto*, 23 novembre 2014

SARTOR G. - VIOLA DE AZEVEDO CUNHA M., *Il caso Google e i rapporti regolatori USA/EU, in Dir. Inform.,* 2010, 26

SAVIANO V.C., *Facebook: spariti i gruppi pro e contro Tartaglia*, in *La Repubblica*, 15 dicembre 2009

SCHONBERGER V. M., *Delete. Il diritto all'oblio nell'era digitale*, Milano, 2010

SCHONBERGER V. M., *Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing*, in *KSG Working Paper*, Harvard, 2007

SCIULLI G., *Il diritto all'oblio e l'identità digitale*, *Narcissus*, Milano 2014

SENG D., *The state of Discordant Union: An Empirical Analysis of DMCA Take down Notices*, in *Virginia Journal of Law and Techonology*, 2014, vol. 18

SEVERINO E., *Democrazia, tecnica e capitalismo*, Brescia, 2009

SHARON G., *Total recall: storing every life memory in a surrogate brain*, in *Computer world*, aprile, II, 2008

SICA S. - D'ANTONIO V., *La procedura di de-indicizzazione*, in *Dir. Inform.*, 2014, fasc. 4-5

SICA S. - D'ANTONIO V., *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015

SNOWDEN E., *Sfido il Grande Fratello*, in *L'Espresso*, 4 giugno 2014

SORO A., *Tentazioni totalitarie dei Governi che in risposta agli attentati terroristici tornano ad ipotizzare strumenti di controllo di massa sulle comunicazioni*, intervista rilasciata al quotidiano *La Repubblica*, 28 giugno 2016

STRADELLA E., *Cancellazione e oblio*: *come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche*

nella Rete, quali anticorpi si possono sviluppare, e, infine, cui prodest?, in AIC, n. 4, 12 dicembre 2016

SUTERA SARDO A., *Dolo e diritto di critica*, in *Dir. pen. processo*, 1999

TOMANELLI A., *Internet e diritto all'oblio: quando la memoria cade in prescrizione*, Bologna, 2009

UBALDI A., *Diffusione e diritto di cronaca: più spazio alla libertà di stampa, a patto che le dichiarazioni siano d'interesse pubblico*, in *Dir. Giustizia*, 2003

VITALI S., *Il potere degli archivi. Usi del passato e difesa dei diritti nella società contemporanea*, in GIUVA L. – VITALI S. – ZANNI ROSSIELLO I. (a cura di), Milano, 2007

WEINRICH H., *Oblio pubblico ed oblio privato*, Bologna, n. 4, 2000

ZACCARIA R. –VELASTRO A., *Diritto dell'informazione*, Padova, 2010

ZACCARIA R., *Diritto dell'informazione e della comunicazione*, Padova, 2013

ZACCONE E., *Social Media e permanenza dei contenuti*, Palermo, 2015

ZANINI S., *Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?*, in *www.federalismi.it: Rivista di diritto pubblico italiano, comparato, europeo*, 18 luglio 2018

ZARZACA P., *Vividown, La fine della caccia alle streghe*, in *www.leggioggi.it,*11 febbraio 2014

ZENO-ZENCOVICH V., *Intorno alla decisione nel caso Scherms: la sovranità digitale ed il governo internazionale delle reti di telecomunicazione*, in *Dir. Inform., Anno XXX,* 4-5, 2015

ZICCARDI G., *Il libro digitale dei morti: memoria, lutto, eternità e oblio nell'era dei social network,* Torino, 2017

ZWENNE G. J., *Nog veel onzekerheden over het recht om te worden vergeten, in Tijdschrift voor Internetrecht*, 2012, vol. 9