*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*

*Osservatorio sulla normativa*

# (Sche)Dati. Il diritto alla protezione dei dati personali nella legislazione europea

di Chiara Spiniello *

## 1. *The Big Brother is watching you*

*The right to be alone*. Era il 1890 quando Samuel D. Warren e Louis D. Brandeis enunciavano – sulle pagine della *Harvard Law Review* – «il diritto ad essere lasciati da soli». In maniera del tutto dirompente rispetto alla tradizione costituzionale statunitense – che della libertà di stampa e di parola aveva fatto i capisaldi del suo Testo fondamentale[1] – si affermava,

* Dottoranda in Teoria dello stato e istituzioni politiche comparate presso la Sapienza Università di Roma. Contributo sottoposto a referaggio anonimo (*double blind peer review*).

[1] Sanciti dal primo emendamento del *Bill of Rights* (1789), il diritto alla libertà di stampa e il diritto alla libera manifestazione del pensiero sono così solennemente proclamati: «Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances». («Il Congresso non potrà porre in essere leggi per il riconoscimento uffi-

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



per la prima volta, l'idea secondo cui il diritto di informare e di essere informati trova (o meglio, deve trovare) una limitazione nella tutela della riservatezza personale.

Ma se durante il secolo d'oro della borghesia il diritto di conservare "una stanza tutta per sé" si sostanziava, grossomodo, nella protezione del domicilio e più in generale della proprietà privata, con l'evoluzione dei tempi gli ambiti della sfera personale potenzialmente fagocitabili si sono moltiplicati e si son fatti sempre più intimi.

Da allora, infatti, numerosissime sono state le innovazioni tecnologiche intervenute a modificare – talvolta fortificando, assai più spesso deteriorando – il rapporto tra libertà individuale e sviluppo tecnologico e nell'alveo del *right to privacy* hanno finito col rientrare tutta una serie di prerogative prima inimmaginabili. Il diritto alla protezione dei dati personali, tra queste.

Difatti, mentre nell'America ottocentesca la *défi* era rappresentata dai nuovi metodi della stampa e delle differenti metodologie del giornalismo[2], da inizio Novecento sono i sistemi di raccolta dei dati, prima, e l'avvento della digitalizzazione degli stessi[3], poi, a fare da antagonisti

ciale di una religione o per proibirne il libero culto, o per limitare la libertà di parola o di stampa o il diritto dei cittadini di riunirsi in forma pacifica e d'inoltrare petizioni al governo per la riparazione di ingiustizie»).

[2] La stampa *offset*, per un verso, e le dinamiche sempre più imprenditoriali a cui era legata la professione giornalistica, per altro.

[3] Il *Web 2.0*, i *Big data*, l'*Internet of Things (IoT)* sono soltanto alcune delle evoluzioni che hanno segnato, negli ultimi anni, il mondo della Rete.

alla tutela della libertà e della dignità umana e, dunque, altresì del libero sviluppo della personalità.

Lo sviluppo delle comunicazioni elettroniche, la diffusione di strumenti di divulgazione sempre più avanzati e connessi ad Internet, le accresciute capacità di conservazione e analisi dei dati hanno fatto sì che le preferenze, i gusti, le abitudini, le opinioni di ciascuno fossero alla portata di tutti. È divenuto facile, allora, arrivare a formulare, con vari gradi di specificità, la previsione di condotte e comportamenti degli utenti; è stato possibile, in questo modo, elaborare delle informazioni utilizzabili per le più disparate finalità, su di un terreno evanescente e difficilmente controllabile, com'è quello della Rete.

Se per un verso, quindi, le potenzialità delle nuove tecnologie si sono ingigantite a dismisura, per altro verso la consapevolezza dei fruitori s'è fatta più flebile: la comodità delle piattaforme informatiche, unita alla gratuità e alla semplicità d'impiego che le caratterizza, ha determinato un approccio e un ricorso alle stesse immediato a tal punto da essere superficiale. La resa senza condizioni con cui si è disposti a cedere il proprio patrimonio informativo devia, distorcendolo, il rapporto tra uomo e macchina.

Ecco perché, in una società che ci pone (perché ci vuole) costantemente sotto gli occhi di un *Big Brother*, la difesa dei dati personali diviene baluardo delle libertà fondamentali ed ecco perché il legislatore europeo – *in primis* – ha deciso di disciplinare la materia, tentando a più riprese di adeguarla all'evoluzione dei tempi. Dal momento che, come ricorda Stefano Rodotà (2005, 148) «la soluzione non può essere l'impedire che i dati circolino: io ho bisogno di appartenere al mondo d'oggi. Il punto è un altro. Riuscire a non perdere mai il controllo, a non aprire un baratro tra me e i dati che mi riguardano».

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



## 2. Origini e prime evoluzioni della legislazione europea in materia di protezione dei dati personali

### *2.1. Dalla Convenzione n. 108 del 1981…*

La nozione di *dato personale* fa parte del nucleo di istituti disciplinati dalla Convenzione di Strasburgo n. 108 del 28 gennaio 1981«sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale»[4]. Nel precisare, all'art. 2, che «dati a carattere personale significa ogni informazione concernente una persona fisica identificata o identificabile (persona interessata)», la Convenzione si prefigge lo scopo 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»[5].

[4] Prima di allora, la Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) – firmata a Roma il 4 novembre 1950 dai dieci Stati ai tempi parte del Consiglio d'Europa (Belgio, Danimarca, Francia, Irlanda, Italia, Lussemburgo, Norvegia, Paesi Bassi, Regno Unito, Svezia) – si era limitata a prevedere, all'art. 8, la necessità della tutela della riservatezza, sancendo il diritto al rispetto della vita privata e familiare. Nulla, invece, aveva detto circa l'esigenza di protezione dei dati personali, in linea con la concezione che si aveva della tecnologia: un mero strumento, un mezzo asservito a uno scopo, e non un fattore capace di influenzare le modalità di esercizio di un diritto o addirittura capace di elaborarne di nuovi. Si veda, a tal proposito, Pizzetti (2016, 57).

[5] In modo specifico, la Convenzione n. 108/1981 si incentra sulla tutela delle sole persone fisiche, con riguardo alle possibili violazioni dei diritti umani fondamentali tramite

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



La «registrazione di dati, l'applicazione ad essi di operazioni logiche e/o aritmetiche, loro modifica, cancellazione, estrazione o diffusione» – e, quindi, tutto ciò che rientra nella c.d. *elaborazione automatizzata*[6] – divengono oggetto, per la prima volta, di una disciplina che i Paesi contraenti sono chiamati ad attuare nell'ambito dei confini nazionali, rendendola operativa mediante una trasposizione nel loro diritto interno. E sono tenuti a farlo seguendo alcune fondamentali linee guida, derogabili solo per esigenze di ordine superioree a patto che le misure adottate in sostituzione siano «democratiche» e «necessarie»[7].

Innanzitutto, come recita l'art. 5, è indispensabile che i dati personali, per poter essere ritenuti di qualità adeguata, siano: a) ottenuti ed 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.

l'elaborazione automatizzata dei dati di carattere personale che le riguardano. Restano, di contro, al di fuori della copertura predisposta dalla disciplina convenzionale tanto le persone giuridiche, quanto i sistemi di elaborazione non automatizzati di dati, anche quando connessi con sistemi automatizzati.

[6] Definizione rinvenibile, anch'essa, all'art. 2.

[7] In particolare, la deroga può operare qualora risultino in pericolo beni quali: a) la protezione della sicurezza dello Stato, la sicurezza pubblica, gli interessi monetari dello Stato o la repressione dei reati; b) la protezione della persona interessata e dei diritti e delle libertà altrui.

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



Significativo è come tra i dati azionabili non vengano fatti rientrare – salvo l'intervento di una specifica autorizzazione – quelli c.d. *sensibili*, ossia l'insieme delle informazioni che caratterizzano un individuo e che sono in grado di rilevarne l'origine razziale, le opinioni politiche, le convinzioni religiose, lo stato di salute, l'orientamento sessuale e persino le condanne penali. Attenendo agli aspetti più intimi della persona umana, infatti, tali dati potrebbero essere fonte di discriminazione e, perciò, ostacolo al libero evolversi della personalità.

In secondo luogo, ai sensi dell'art. 7, gli Stati che hanno sottoscritto la Convenzione di Strasburgo debbono garantire adeguate misure di sicurezza nei casellari automatizzati contro la distruzione e la perdita accidentale o non autorizzata dei dati, ovvero contro gli accessi, la modifica e la diffusione non autorizzata; essi hanno l'obbligo, altresì, di assicurare agli interessati le dovute garanzie, sostanzialmente identificabili nel diritto alla conoscenza e alla gestione dei suoi dati e meglio specificate all'art. 8 dell'intesa[8].

Infine, relativamente al movimento oltrefrontiera dei dati, la Convenzione – a differenza della successiva Direttiva del 1995 di cui si dirà a seguire – prevede che i Paesi partecipanti non possano proibirne il trasferimento oltrefrontiera e tanto meno sottoporlo a particolari autorizza-

[8] Tra le garanzie che l'art. 8 riconosce alla persona interessata rientrano: essere informato dell'esistenza di un casellario automatizzato contenente dati a carattere personale nei suoi riguardi nonché i fini principali per cui sono conservati, ovvero l'identità e la residenza/sede amministrativa del responsabile del casellario; avere la possibilità di ottenere la rettifica o la cancellazione di tali dati se elaborati in violazione dei principi di cui agli articoli 5 e 6; avere la possibilità di esperire un ricorso qualora non venga dato tempestivo seguito ad una richiesta di prendere visione, rettificare o cancellare tali dati.

zioni. Fanno eccezione, in base a quanto statuito dal terzo comma dell'art. 12, quei casi in cui: a) la legislazione dello Stato trasferente prevede una regolamentazione specifica per alcune categorie di dati a carattere personale o in merito ai casellari automatizzati in cui essi sono custoditi, in ragione della natura di detti dati o casellari, a meno che la regolamentazione dell'altra Parte offra una protezione equivalente; b) il trasferimento sia effettuato verso il territorio di uno Stato non contraente per il tramite di un'altra Parte, al fine di evitare che simili trasferimenti si traducano in un aggiramento della legislazione della Parte dal cui territorio parte il flusso di dati o delle garanzie previste dalla Convenzione.

Capostipite dei testi in materia di protezione dei dati personali, la Convenzione di Strasburgo, nel ricollegare espressamente e solennemente la protezione dei dati personali alla tutela della riservatezza – e, nel farla rientrare, conseguentemente, nel novero dei diritti fondamentali – è stata la prima a farsi interprete dell'esigenza di arginare la dispersione delle informazioni personali, inevitabile conseguenza dell'incremento della circolazione di notizie virtuali e non.

### *2.2. …alla "Direttiva madre" n. 46 del 1995*

Ad ampliare contenuto e portata della Convenzione n. 108 del 1981, capovolgendone a tratti i contenuti, è stata la Direttiva europea 95/46/CE «relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati».

Approvata il 24 ottobre 1995 dal Parlamento e dal Consiglio, la Direttiva – pensata allo scopo di armonizzare le previsioni relative alla rimozione degli ostacoli alla circolazione dei dati personali, necessarie alla realiz-

zazione completa del mercato interno, con le opportune garanzie poste a salvaguardia dei diritti fondamentali della persona – ha stabilito principi e regole vincolanti relativamente al risultato da raggiungere, ma introiettabili dalla legislazione interna degli Stati membri nelle forme e con i mezzi favoriti, fatto salvo il rispetto del termine fissato dalla Stessa[9].

Sebbene le disposizioni di cui si fa portatrice non siano previste per i trattamenti di dati personali effettuati in ambiti di attività non inerenti al diritto comunitario – e, quindi, per quelli aventi a oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato e le attività dello Stato in materia di diritto penale – nonché a tutti iprocessi sviluppati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; essa, a differenza della precedente previsione normativa, risulta applicabile tanto ai dati trattati con mezzi automatici (come le banche dati informatiche) quanto a quelli contenuti o destinati a figurare in archivi non automatizzati (gli archivi tradizionali in formato cartaceo, ad esempio)[10].

Inoltre, la Direttiva del 1995 riprende e sviluppa la definizione di dato personale tracciata dalla Convenzione di Strasburgo, non limitandosi a definirlo come qualsiasi informazione che rimanda a una persona identificata o identificabile, ma specificando che si considera *identificabile* «la

[9] In particolare, come indicato nelle «Disposizioni Finali» (art. 32), «gli Stati membri mettono in vigore le disposizioni legislative, regolamentari ed amministrative necessarie per conformarsi alla presente direttiva al più tardi alla scadenza del terzo anno successivo alla sua adozione».

[10] L'art. 3, infatti, parla del «trattamento di dati personali interamente o parzialmente automatizzato nonché il trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi».

persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale» (art. 2).

A essere chiarificati sono, altresì, gli ambiti di azione ai quali possono essere sottoposti i dati di carattere personale, arrivando questi ad abbracciare operazioni tecnologiche più avanzate rispetto alla semplice raccolta e «schedatura dei dati» e divenendo, dunque, potenzialmente capaci di adattarsi a una futura evoluzione delle tecniche informatiche e delle comunicazioni[11].

Ciò detto, però e in modo del tutto innovativo, la Direttiva restringe a una serie di condizioni la possibilità di trattare i dati personali, prevedendo che ciò possa avvenire quando: sia fonte di un determinato obbligo (facente capo al responsabile del trattamento) avente origine contrattuale privata e quando risulti fondato direttamente in una disposizione di legge; oppure quando si riscontri la necessità di salvaguardare ulteriori beni «superiori», come l'interesse vitale della persona interessata, l'esecuzione di un interesse pubblico; o ancora, sia necessario al perseguimento di un interesse legittimo del responsabile del trattamento, a

[11] In specie, essi possono essere soggetti a «la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione», compiute con o senza l'ausilio di processi automatizzati (art. 2).

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 1, 2018
data di pubblicazione: 11 agosto 2018



condizione però che non prevalgano l'interesse, i diritti e le libertà fondamentali della persona interessata.

Ma l'aspetto davvero dirompente, che senza dubbio alcuno costituisce una delle principali novità in tema di diritto alla protezione dei dati personali, è contenuto nell'art. 7, lett. a).

Ivi, il legislatore europeo afferma che, affinché possa essere predisposto il trattamento dei dati personali, la persona interessata debba manifestare «il proprio consenso *in maniera inequivocabile*», laddove, per consenso si intende «qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento».

Identificandosi quale primo e fondamentale criterio di legittimità del trattamento, il consenso – che, *ça va sans dire*, deve essere libero (e quindi privo di coercizioni fisiche o morali), specifico (ossia rivolto verso quel determinato e individuato processo di trattamento dei propri dati personali), informato (nel senso che l'interessato deve essere consapevole dei fini e delle modalità di quel trattamento) – permette una tutela rafforzata nel caso dei dati c.d. *sensibili*[12]. Tuttavia, tali disposizioni – sia quella relativa all'utilizzo dei dati in generale sia quella specificatamente rivolta ai dati *sensibili* – trovano un temperamento nella previsione secondo cui il consenso non si reputa né presunto, né necessario quando il trattamento debba essere effettuato per motivi inerenti il pubblico inte-

[12] L'art. 8, come principio generale, afferma l'impossibilità di trattare quei dati personali capaci di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 1, 2018
data di pubblicazione: 11 agosto 2018



resse o nell'interesse legittimo del responsabile del trattamento o dei terzi che ricevono i dati[13].

Altra distinzione tra Direttiva e Convenzione si ritrova nella disciplina in tema di trasferimento di dati verso Paesi terzi prevista all'art. 25 della Direttiva 95/46. Rispetto allo speculare articolo della Convenzione, si attua un vero e proprio cambiamento di impostazione: se nella precedente normativa era imposto agli Stati il divieto di negare il trasferimento o condizionarlo a specifiche autorizzazioni, salvo determinate ipotesi, ora la Direttiva stabilisce che in linea di principio il trasferimento non può aver luogo a meno che il Paese terzo di cui trattasi garantisca un livello di protezione adeguato, il quale viene verificato dalla Commissione Ue su richiesta di uno Stato membro[14].

Infine, ulteriore innovazione apportata dalla nuova normativa comunitaria è l'istituzione delle «Autorità di Controllo» e del c.d. «Gruppo Articolo 29»: le prime hanno il compito di vigilare la corretta applicazione della Direttiva da parte degli Stati[15]; il secondo – conosciuto anche

[13] Anche se, nel caso di *dati sensibili*, la persona interessata – al fine di permettere il trattamento dei propri dati sensibili – deve prestare un consenso *esplicito*, non più solamente inequivocabile. Dunque, si configura la figura di un consenso *rafforzato*.

[14] Il criterio dell'adeguatezza è soggetto ad attenta verifica da parte della Commissione UE, che – seguendo la procedura di cui all'art. 31 comma 2 della Direttiva – constata se un Paese terzo abbia i requisiti di tutela adeguati secondo la sua legislazione nazionale o gli impegni internazionali presi o altrimenti avvia le negoziazioni per porre rimedio o pone in essere le misure necessarie a vietare il trasferimento.

[15] Si tratta di autorità pienamente indipendenti nell'esercizio delle funzioni loro attribuite, le quali si sostanziano in: a) poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo; b) poteri effettivi d'intervento, come quello di formulare pareri pri-

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



come *Working Party 29 - WP29*, è un organismo a carattere consultivo, tra le cui funzioni vi è, ad esempio, l'esame di ogni questione relativa l'applicazione delle norme nazionali di attuazione della Direttiva per contribuire alla loro applicazione omogenea[16].

Non si discosta di molto, invece, dalla Convenzione n. 108/1981 l'inquadramento dei principi in tema di qualità dei dati e del trattamento. Allo stesso modo, identiche paiono essere le misure di sicurezza, previste dall'art. 7 della precedente statuizione, che sanciscono l'obbligo da parte del responsabile di porre in essere tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità

ma dell'avvio di trattamenti, quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali; c) potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della direttiva ovvero di adire per dette violazioni le autorità giudiziarie. Inoltre, qualunque persona puòchiedere direttamente a un'autorità di controllo di verificare la liceità di un trattamento e quest'ultima la informa dell'avvenuta verifica e degli eventuali riscontri. In maniera ancora più innovativa viene previsto che le autorità di controllo collaborino tra loro nella misura necessaria allo svolgimento dei propri compiti, in particolare scambiandosi ogni informazione utile, al fine di rendere efficiente l'implementazione della disciplina e di diffondere il più possibile un'interpretazione di diritto conforme e comune su tutto il territorio.

[16] Composto da un rappresentante delle autorità di controllo di ciascuno Stato membro, da un rappresentante delle autorità per le istituzioni e gli organismi comunitari, nonché da un rappresentante della Commissione, il «Gruppo Articolo 29» si occupa, tra le altre cose, di formulare pareri sul livello di tutela nella Comunità e nei paesi terzi, a supporto del lavoro della Commissione e consigliare la Commissione in merito a ogni progetto di modifica della presente Direttiva ai fini della tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di dati personali.

per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati.

L'armonizzazione delle differenti discipline già vigenti negli Stati membri, per un verso; l'instradamento in senso uniforme delle previsioni che sarebbero conseguite alla sua applicazione nei Paesi manchevoli di una normativa in materia[17], per altro verso, sono gli obiettivi che muovono la Direttiva 95/46/CE, detta – non a caso – "Direttiva madre", in quanto primo atto normativo cruciale dell'Unione europea con oggetto il trattamento e la protezione dei dati personali.

### 3. La *costituzionalizzazione* del diritto alla protezione dei dati personali

Se è vero, come si è visto, che la Convenzione di Strasburgo, prima, e la "Direttiva madre", poi, hanno contribuito a dare risalto al tema del trattamento dei dati personali, la collocazione sistematica della tutela di questi nell'alveo dei diritti fondamentali della persona si deve alla «Car-

[17] Tra i Paesi allora sprovvisti di una normativa in materia vi era (anche) l'Italia, che si doterà – per la prima volta – di un Codice sulla protezione dei dati personali nel 1996, con la legge 31 dicembre 1996, n. 675, la quale era stata pensata altresì per ottemperare un altro impegno già assunto in sede europea, ossia l'accordo di Schengen del 1985 relativo alla creazione di uno spazio comune per la libera circolazione di persone e merci, mediante la progressiva soppressione delle frontiere. Per la creazione di questo, spazio comune, infatti, era necessaria la predisposizione di normative e strutture istituzionali relative alla protezione e al trattamento dei dati personali. Per un approfondimento sulla l. n. 675/1996 v. Acciai, Orlandi (2003)

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



ta dei diritti fondamentali dell'Unione europea», proclamata a Nizza – e per questo anche conosciuta come "Carta di Nizza" – nel dicembre del 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione.

Nel riconoscere l'autonomia del diritto alla protezione dei dati personali rispetto al diritto alla riservatezza, la Carta eleva il livello di protezione del diritto «all'autodeterminazione informativa», che anni prima il *Bundesverfassungsgericht* aveva riconosciuto come concretizzazione degli artt. 1 e 2 della Legge Fondamentale Tedesca, rispettivamente aventi ad oggetto la tutela della dignità umana e i diritti di libertà della persona[18].

Così, all'art. 8 del titolo secondo (dedicato ai diritti di libertà), può leggersi che «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano» e che «tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenere la rettifica». Inoltre, si specifica che «il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

Il diritto alla protezione dei dati personali, quello di lealtà e ancora l'altro che richiede finalità determinate del trattamento; il consenso della persona interessata; il diritto d'accesso ai propri dati; il diritto ad ottenerne la modifica; l'istituzione delle autorità garanti: vengono tutti ad

[18] Il riferimento è alla sentenza n. 209 del 15 dicembre 1983, in cui il Tribunale Costituzionale Federale tedesco sancisce il potere di ciascuno di decidere, in maniera autonoma e personale, circa la rivelazione e l'utilizzo dei propri dati personali, in quanto il libero sviluppo della personalità presuppone la protezione del singolo dalla memorizzazione, utilizzazione e trasferimento incontrollato di dati personali.

essere cristallizzati in una previsione di rango costituzionale, che – a partire dal fondamentale Trattato di Lisbona del 2007[19] – può vantare lo stesso valore giuridico dei Trattati istitutivi.

### 4. Ulteriori sviluppi: le Direttive n. 58 del 2002 e n. 24 del 2006

Succedono alla Direttiva 95/46/CE le Direttive n. 58 del 2002 e n. 24 del 2006, rispettivamente concernenti le telecomunicazioni elettroniche e le comunicazioni elettroniche accessibili al pubblico o di reti pubbliche.

Non sostitutive, ma puramente integrative, queste costituiscono un ampliamento e un rafforzamento del nucleo centrale della "Direttiva madre": un dilatamento perché si fanno portatrici di tutta una serie di norme in materia di telecomunicazioni e comunicazioni elettroniche non previste dalla Direttiva 95/46; un arricchimento in quanto inglobano nelle nuove discipline l'intero apparato di controllo e vigilanza della Direttiva del 1995.

Si inizia con l'analizzare la prima previsione.

Proteggere i dati personali – assicurandone allo stesso tempo la circolazione –con riguardo al trattamento di questi nel settore delle comunicazioni elettroniche, delle apparecchiature e dei servizi di comunicazione elettronici all'interno della Comunità, è la finalità principe che si prefigge l'intervento normativo del 2002.

[19] Firmato a Lisbona il 13 dicembre 2007, il Trattato di riforma per eccellenza ha apportato modifiche sostanziali alla struttura dell'Unione europea abolendo l'originaria suddivisione in tre pilastri e modificando i trattati istitutivi.

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



Ma non è il solo settore disciplinare a costituire elemento di novità, essendo cardine della Direttiva diverse disposizioni che concentrano l'attenzione direttamente sulla figura dell'utente, per la prima volta immerso e costretto a muoversi nello scenario dominato dall'Internet[20]. Espressioni fino ad allora sconosciute fanno la loro comparsa: *spy-ware*, *web bugs*, *cookies*, reti mobili digitali; sono tutti termini che iniziano ad arrivare alle orecchie dei più, la maggior parte dei quali è ignara del loro effettivo significato e delle conseguenze derivanti dalla loro implementazione.

Ecco allora che la Direttiva n. 58 del 2002 decide di disciplinare – e stabilisce di farlo, in particolare dall'art. 4 all'art. 15 – una serie di previsioni che consentano agli utenti di muoversi con maggiore agilità, e certamente sicurezza, nel poliedrico mondo della Rete.

Così, mentre l'art. 4 si occupa delle misure di sicurezza, prevedendo che il fornitore di un servizio di comunicazione elettronica accessibile al pubblico debba «prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della Rete»; l'art. 5 impone un obbligo di astensione che grava in capo agli Stati: l'autorità pubblica deve, infatti, astenersi dall'usufruire dei canali creati e creabili dalle comunicazioni elettroniche tramite la Rete Internet per esercitare un controllo di massa indiscriminato.

[20] Così recita il *considerando* n. 6 della Direttiva: «L'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata».

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



Ancora, gli artt. 6 e 7 predispongono la cancellazione e la *anonimizzazione* dei dati di traffico qualora gli stessi non siano più necessari ai fini della trasmissione delle comunicazioni, il primo; il diritto degli utenti a ricevere fatture dettagliate, il secondo. In aggiunta l'art. 9 – trattando un tema di importanza cruciale oggigiorno – stabilisce che i dati trasmettenti informazioni relative all'ubicazione della comunicazione, e dunque in grado di localizzare chi allo scambio di notizie dà vita, «siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto».

Infine, l'art. 15 – particolarmente significativo perché può considerarsi un «ponte» tra la vecchia disciplina e il nuovo contesto operativo delineato dalla Direttiva 2002/58 – sottolinea che gli Stati possono limitare i diritti e gli obblighi sanciti nella Direttiva solamente se tale restrizione costituisce «una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica», andando così a richiamare l'art. 13 della Direttiva 95/46.

Fondamentale è l'art. 15 altresì perché – ancora una volta riprendendo quanto era già stato statuito in precedenza – nel sottolineare l'importanza dell'informativa da rivolgere all'utente, impone agli Stati membri di assicurare che l'utilizzo delle reti di comunicazione elettronica, ai fini di archiviazione di informazioni o di accesso ad informazioni archiviate nell'apparecchio terminale dell'utente, possa essere eseguito legittimamente «unicamente a condizione che» il soggetto sia stato in-

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



formato in modo «chiaro e completo» sugli scopi del trattamento e che gli sia offerta la possibilità di rifiutare tale trattamento[21].

Ribadendo la centralità dell'utente e la necessità del suo consenso informato, quest'ultima disposizione si impone come perno della Direttiva 2002/58/CE, che – a buona ragione – è da considerarsi punto d'approdo dell'evoluzione degli strumenti di tutela predisposti dalla "Direttiva madre".

Non ha avuto, invece, la stessa fortuna il susseguente intervento normativo, la Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, relativa a «la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE». Nonostante fosse incentrata su una tematica fondamentale, quale quella della conservazione, memorizzazione e utilizzo del dato e – in particolare – sull'aspetto della «conservazione e del (relativo) uso per finalità di indagine, accertamento e perseguimento di reati gravi»[22], la-Direttiva c.d. "*Data Retention*"[23] è stata resa nulla da un intervento caducatorio della Corte di Giustizia dell'Unione europea.

[21] È fatto espresso divieto di procedere all'«ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'art. 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza».

[22] Tema divenuto assai pressante dopo gli attacchi terroristici di Londra del 2005.

[23] Detta altresì "Direttiva Frattini", per l'allora Vicepresidente e Commissario per la Giustizia e gli Affari Interni, Franco Frattini, che fortemente ne ha voluto l'emanazione.

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



A muovere il giudizio dei custodi della legge europei, nella celebre sentenza *Digital Rights Ireland*[24], è stata l'illegittimità della misura prevista all'art. 6 della Direttiva in esame. Ivi, infatti, è detto che «Gli Stati membri provvedono affinché le categorie di dati di cui all'art. 5[25] siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione».

Nel rilevare come le categorie di dati illustrate dal sopraccitato articolo, pur non attenendo direttamente al contenuto della conversazione, siano in grado di fornire informazioni importanti sulle comunicazioni, sui loro destinatari e sulla loro frequenza, la Corte ha sostenuto che l'accesso a tali dati da parte dell'autorità pubblica comporta in ogni caso una seria ingerenza nella vita privata dei cittadini, alimentando in loro l'idea di essere esposti a una *costante sorveglianza* in quanto la conservazione e il successivo utilizzo dei dati stessi avviene a insaputa dell'interessato[26].

Analizzando, poi, la previsione relativa ai termini di conservazione dei dati, i supremi giudici hanno individuato una violazione del «prin-

[24] La pronuncia origina da un rinvio pregiudiziale presentato sia dalla *High Court* irlandese che dalla *Verfassungsgerichtshof* austriaca in merito alla validità della Direttiva 2006/24/CE, con particolare riferimento ai diritti fondamentali del rispetto della vita privata e della protezione dei dati personali, sanciti entrambi dalla Carta dei diritti fondamentali dell'Unione europea.

[25] L'art. 5 contiene un lungo elenco di categorie di dati legati al settore delle comunicazioni elettroniche, qui si richiama integralmente il contenuto dell'art. 5 rubricato «Categorie di Dati da conservare».

[26] Sulla sentenza della Corte di Giustizia risulta particolarmente interessante l'intervento del Presidente del Garante per la protezione dei dati personali, Antonello Soro, visionabile in www.garanteprivacy.it.

cipio di stretta proporzionalità» e un contrasto con il diritto fondamentale alla protezione dei dati personali così come definito dalla normativa comune europea.

Cinque sono così divenuti i motivi con cui è stata motivata la bocciatura dalla Corte di Giustizia: 1) la previsione di termini indifferenziati e generalizzati all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza operare alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo della lotta ai reati gravi; 2) l'omissione di ogni criterio utile a definire quando i reati possano essere considerati sufficientemente gravi da giustificare una simile ingerenza; 3) l'omissione di ogni presupposto procedurale e sostanziale al quale subordinare l'accesso; 4) l'omissione di ogni criterio per differenziare la durata della conservazione dei dati, limitandosi solo a stabilire i termini minimi e massimi; 5) l'omissione di imporre che i dati acquisiti debbano essere conservati esclusivamente nel territorio dell'Unione.

La mancanza di specificazione e differenziazione normativa, da un lato, e – ancor più – la non proporzionalità tra limitazioni dei diritti fondamentali ed esigenze di pubblica sicurezza, dall'altro, sono le motivazioni che, in definitiva, hanno spinto la Corte di Giustizia dell'Unione europea a cassare la Direttiva 2006/24/CE, la quale pure – a suo modo – si era fatta portatrice di innovazioni significative, specialmente nel riguardo la conservazione dei dati di traffico delle comunicazioni elettroniche.

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*

*Osservatorio sulla normativa*

**5. L'approdo: il Regolamento UE 2016/679**

Entrato in vigore il 24 maggio 2016 e divenuto applicativo a partire dallo scorso 25 maggio[27], il nuovo Regolamento dell'Unione europea 2016/679 è stato pensato e introdotto– come recita il *considerando* n. 11 dello Stesso – per assicurare «il rafforzamento e la disciplina dettagliata dei diritti, degli interessi e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali».

L'esigenza di bilanciare i diritti della persona con gli straordinari interessi economici che derivano dall'impiego di sistemi elettronici, ha spinto il legislatore europeo a dotarsi di uno strumento giuridico immediatamente applicabile: non più, quindi, una Direttiva, col compito di armonizzare, mediante l'azione degli Stati membri, normative e culture giuridiche, a volte molto diverse tra loro; ma un Regolamento, obbligatorio in tutte le sue parti e direttamente applicabile nei Paesi dell'Unione.

Nel trarre spunto dai principi ispiratori contenuti nei Trattati istitutivi e da quelli appartenenti alle tradizioni comuni del costituzionalismo europeo, nonché nel riallacciarsi alle precedenti Direttive in materia, il Regolamento 2016/679 crea un ponte tra il passato, il presente e il futuro.

Così facendo esso non innova solamente la materia tramite l'introduzione di istituti completamente nuovi, facendosi interprete delle problematiche più pressanti della società digitale moderna, ma attua

[27] Un arco temporale che si spiega con la volontà di lasciareagli Stati Membri la possibilità di organizzare al meglio l'impianto normativo nazionale in modo tale da inserire efficacemente il Regolamento all'interno del proprio ordinamento.

un lavoro diconsolidamento di tutte quelle posizioni e determinazioni che negli anni hanno costituito il lavoro del «Gruppo art.29» e della giurisprudenza della Corte di Giustizia europea, e infine conferma, amplia e aggiorna l'insieme delle previsioni statuite dalla Direttiva del 1995.

Vista la vastità degli argomenti trattati dal Regolamento – e altresì la molteplicità delle innovazioni introdotte, tante e tutte significativamente interessanti – si è scelto, in questa sede, di procedere ad una rapida analisi delle modifiche relative a quei concetti e principi che paiono avere – a detta di chi scrive – un *quid pluris*[28], per poi soffermarsi in maniera più dettagliata sulla questione dei necessari standard di sicurezza.

Come non partire, allora,dalla stessa definizione di *dato personale*.

Se nella struttura la nozioneresta identica a quella prevista dalla «Direttiva madre», e dunque un dato di carattere personale consiste sempre in una qualsiasi informazione riguardante una persona fisica identificata o identificabile (il c.d. interessato); nella determinazione di quando una persona sia reputata *identificabile* si coglie indubbiamente un elemento di novità. Oltre alle tipologie classiche (il nome, il numero di identificazione e gli elementi caratteristici dell'identità fisica, fisiologica, psichica, economica, culturale e sociale), rientrano tra gli identificativi tutta una serie di caratteristiche personali strettamente collegate alle tecnologie sviluppatesi negli anni:i dati relativi all'ubicazione, identificativi generici online, elementi caratteristici dell'identità genetica di una persona. In questo modo, per la prima volta in assoluto, vengono introdotte catego-

[28] Per una trattazione organica e dettagliata dell'intera disciplina regolamentare si rimanda a Califano, Colapietro (2017)

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



rie di dati afferenti alla sfera biologica e genetica della persona[29], le quali – in determinati settori (ad esempio quello medico) e mediante l'utilizzo di determinate tecnologie (come quelle che permettono scanner biometrici facciali orilevazioni fotografiche particolarmente invadenti) – sono particolarmente suscettibili di violazioni in tema di privacy, di protezione dei dati personali e più in generale di libertà di autodeterminazione.

Altra importante definizione ad essereampliata è quella di *consenso dell'interessato*.

Col chiaro obiettivo di rendere il più puntuale possibile i requisiti del consenso, cosicché possa considerarsi validamente prestato, il legislatore del 2016 aggiunge la caratteristica della *non equivocabilità* a quella della libertà, della specificità e della consapevolezza che – nel loro insieme – devono contrassegnare l'espressione di volontà della persona interessata dal trattamento dei dati. In tal modo, si evita che il consenso possa essere interpretato come presunto: l'interessato manifesta il proprio assenso affinché i dati che lo riguardano siano oggetto di trattamento «mediante dichiarazione o azione positiva inequivocabile».

[29] Ossia, i *dati genetici* definiti come «i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione»; i *dati biometrici* descritti come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»;nonché infine i *dati relativi alla salute* considerati come quei «dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute».

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



Tra gli istituti più *rivoluzionari*, invece, rientrano: il diritto all'oblio e alla portabilità dei dati; la figura del *Data Protection Officer*, la privacy «by design» and «by default», la valutazione pre-impatto e la consultazione preventiva.

Il *diritto all'oblio* è senza dubbio una delle grandi innovazioni che il Regolamento UE 2016/679 codifica.

L'art. 17 prevede, infatti, che alla pretesa di cancellazione dei dati personali da parte del titolare degli stessi corrisponda un preciso obbligo, in capo al titolare del trattamento, di cancellazione senza ingiustificato ritardo, qualora ne sussistano i motivi.

Tuttavia, come si nota, pur avendolo inserito in un atto normativo vincolante, generale e direttamente applicabile (com'è, per l'appunto, il Regolamento), il legislatore europeo appiattisce il significato del diritto all'oblio sulla concezione di *erasure*, cioè di cancellazione del dato personale da parte del titolare del trattamento, con l'ulteriore conseguenza della cessazione del trattamento stesso.

Difatti, sono diverse le disposizioni in cui vengono trattati congiuntamente diritto alla cancellazione e diritto all'oblio. Si legga, ad esempio, il *considerando* n. 65, in cui è stabilito che all'interessato deve essere garantito «il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento».

La stessa previsione, inoltre, prosegue prevedendo dei limiti – poi ripresi all'art. 17 – al diritto dell'interessato, qualora si riscontri la necessi-

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 1, 2018
data di pubblicazione: 11 agosto 2018



tà della conservazione dei dati personali «per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di 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 riferimento al *diritto all'oblio* consente di citare quella che sarebbe divenuta una storica pronuncia della Corte di Giustizia europea: il giudizio espresso in occasione della causa C131/12 *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos, Mario Costeja González*[30].

Aggiungendo una sfumatura significativa al concetto di *diritto all'oblio* – inteso non tanto nel significato di diritto ad essere dimenticati, quanto di «diritto a non essere trovati facilmente» – la Corte ha voluto tutelare non la totale eliminazione del dato personale dal web, ma piuttosto un oscuramento, se non una vera rimozione, dei sistemi di *linkaggio* tra le operazioni del motore di ricerca e il dato così come conservato all'interno di archivi *on-line* di pagine *web*.

Di conseguenza, nella vicenda *Google Spain* il ricorrente – la cui richiesta era stata per l'appunto la rimozione dei suoi dati personali dal web – ha ottenuto soltanto la *deindicizzazione* degli stessi, ossia una dissociazione del proprio nome da un determinato risultato di ricerca, ren-

[30] Per un approfondimento sulle vicende che hanno portato all'emanazione della summenzionata sentenza si vedano le puntuali ricostruzione operate da Resta, Zeno-Zencovich (2015) e Pizzetti (2014).

dendo così impossibile per il motore di ricerca ricollegare le due informazioni nuovamente e unirle tramite *link*.

Così declinato il *diritto all'oblio* si traduce nella sottrazione al pubblico di una modalità di accesso semplificata e generalizzata ad informazioni sul proprio conto (D'Antonio 2016); una declinazione che pare essere stata ripresa dal Regolamento 2016/679.

Altra sentenza che merita di essere ricordata – e che ha ispirato il lavoro del legislatore europeo per quel che concerne la regolamentazione del trasferimento di dati personali verso Paesi terzi o Organizzazioni internazionali – è quella intervenuta a risoluzione del c.d. *caso Schrems*[31].

Adita dall'*High Court* irlandese, la Corte di Giustizia era stata chiamata a chiarire la possibilità per le autorità nazionali di controllo di discostarsi da una decisione di adeguatezza della Commissione, qualora successivamente all'adozione di essa si fosse palesata una sopravvenuta inadeguatezza del livello di protezione da parte di un Paese terzo.

In risposta, i giudici di Lussemburgo sostennero che le autorità garanti nazionali non possono disattendere, sospendere, vietare un trasferimento contrariamente a quanto stabilito da una decisone di adeguatezza della Commissione, per due ordini di motivi: a) il tenore letterale della direttiva 95/46 depone in tal senso quando afferma che «Gli Stati membri adottano le misure necessarie per conformarsi alla 155 Decisone della Commissione n. 520 del 26 luglio 2000» in base anche a quanto stabilito dall'art. 288 TFUE; b) il principio generale del primato del diritto comunitario su quello interno.

[31] Ha trattato in maniera approfondita la questione Zeno-Zencovich (2015).

Conseguentemente, la sola modalità operativa che si presenta ai Garanti nazionali è quella di proporre ricorso alle autorità giurisdizionali del proprio Stato membro di appartenenza ai fini di un successivo rinvio pregiudiziale di fronte alla Corte di Giustizia europea.

Specificato il principio regolatore, nell'entrare nel merito della questione, la Corte accertò l'inadeguatezza del sistema di tutela predisposto dal c.d. *Safe Harbor* – l'accordo concluso tra l'Unione europea e il *Department of Commerce* degli Stati Uniti a cui aveva dato esecuzione la decisione di adeguatezza della Commissione[32] – e di conseguenza invalidò quest'ultima, sottolineando altresì l'esigenza di limitare la discrezionalità della Commissione in merito alla valutazione dell'adeguatezza del sistema di protezione dei dati personali.

Una seconda significativa innovazione prevista dal Regolamento del 2016 è l'introiezione, nel catalogo dei diritti dell'interessato, del *diritto alla portabilità dei propri dati personali*, di cui all'art. 20.

Tale riconoscimento si configura come il diritto dell'interessato di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano, forniti a un titolare del trattamento; l'interessato ha inoltre diritto a trasmettere i dati che lo riguardano a un altro titolare del trattamento senza alcun impedimento da parte del titolare del trattamento cui li ha forniti qualora il trattamento si basi sul consenso o su un contratto e a patto che il trattamento sia effettuato con mezzi automatizzati.

[32] Si tratta della decisone della Commissione n. 520 del 26 luglio 2000.

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



Non più ostaggio dei fornitori di servizi on-line, coloro che vogliano cambiare fornitore si vedono così riconosciuta la possibilità di portare con sé la propria storia digitale e di usufruire di un servizio alternativo, riprendendo il rapporto laddove era stato interrotto.

Del tutto nuova è, ancora, la figura del *Data Protection Officer*, il DPO[33].

Già noto nel mondo anglosassone e in alcuni ordinamenti europei[34], quello del *Data Protection Officer* è una previsione estremamente garantista, posta a tutela degli interessi e diritti delle persone fisiche, la cui necessità di nomina (intesa come un vero obbligo gravante sul titolare del trattamento) è prevista in particolari settori, a carattere prevalentemente pubblicistico, o dove categorie di dati più o meno sensibili vengono trattati[35].

[33] Espressione tradotta in italiano come «Responsabile della protezione dei dati».

[34] In Germania, Austria e Repubblica Ceca esisteva già una figura similare, il *datenschutzbeauftragter*, introdotto con il *Bundesdatenschutzgesetz* del 2003 e con il quale il responsabile della protezione dei dati sembra presentare svariate analogie come: l'obbligo di nomina in base ad un numero minimo di dipendenti; la possibilità di avere accesso a tutte le informazioni relative ai trattamenti; il divieto di penalizzare per le funzioni esplicate in base al ruolo che riveste e l'approccio – derivante dal modello tedesco – di *corporate self-monitoring* dove sono le società che direttamente si fanno carico di un adeguamento e di uno scrupoloso controllo nella gestione dei dati personali (Sica, D'Antonio, Riccio 2016).

[35] Non solo, la nomina può essere necessaria anche qualora le attività del titolare trattino dati personali su larga scala, richiedendo altresì il monitoraggio costante e sistematico degli interessati; oppure, qualora sia previsto dal diritto dell'Unione o da una previsione normativa di uno Stato membro, nel caso in cui il titolare e il responsabile del trattamento volontariamente possono designare un responsabile della protezione dei dati personali.

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



In particolare, è previsto che il *Data Protection Officer* sia coinvolto tempestivamente e adeguatamente in tutte le questioni riguardante la protezione dei dati durante il trattamento e, al fine di garantirne l'autonomia e l'indipendenza, che sia sostenuto direttamente dal titolare e dal responsabile che hanno il compito di fornire le risorse necessarie al responsabile della protezione dati per assolvere i suoi compiti e mantenere la propria conoscenza specialistica.

Due ulteriori corollari del principio generale di trattamento dei dati personali in modo non rischioso sono rappresentati dalla *valutazione d'impatto* e dalla *consultazione preventiva*.

Ai sensi dell'art. 35 del Regolamento, il titolare è tenuto a effettuare una valutazione d'impatto, prima di procedere al trattamento, qualora una particolare tipologia digestazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto del fatto che all'interno del procedimento si prevedano l'uso di nuove tecnologie e considerati inoltre il contesto, la natura, l'oggetto e le finalità.

Alla disposizione subito successiva è previsto, invece, che ogniqualvolta la valutazione d'impatto riveli un reale rischio elevato, in assenza di misure adeguate ad attenuarne la pericolosità, il titolare prima di procedere al trattamento, debba consultare obbligatoriamente l'autorità di controllo. Quest'ultima, qualora il trattamento risulti illecito o carente sotto il profilo dell'adeguatezza per la prevenzione del rischio, ha l'onere di fornire un parere scritto entro otto settimane dalla richiesta di consultazione (prorogabile di ulteriori sei settimane, con il rispettivo obbligo di informativa nei confronti del titolare) con la facoltà di esercitare i poteri investigativi, correttivi, autorizzativi e consultivi previsti all'art. 58 del Regolamento.

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



Sempre in merito alla valutazione del rischio, acquistano rilevanza i concetti, pur'essi frutto della novella del 2016, di privacy *by design* and privacy *by default*[36].

Per *data protection by design and by default* si intendono dei modelli di progettazione prestabiliti secondo formule *standard*, e conformi ai criteri stabiliti dalla legge, ai quali ogni titolare deve adeguarsi affinché il trattamento possa ritenersi lecito.

In particolare, l'adozione della protezione *by design* fa sì che prima dell'elaborazione di un qualsiasi processo di trattamento dei dati, siano presi in considerazione già dal progetto i profili di riservatezza e di protezione dei dati personali degli interessati, permettendo così di elaborare la strategia organizzativa e tecnica migliore a seconda della tipologia del trattamento, senza dover aspettare il verificarsi di qualche "problema tecnico" perché possano configurarsi le misure di sicurezza pertinenti da applicare. Non a caso, la *protection by design* esplica la sua principale funzione nel momento preparatorio e progettuale delle attività di trattamento, dove le misure tecniche e organizzative sono preordinate dal titolare e successivamente vincolate in modo tale da rispettare efficacemente i principi attinenti alla protezione dei dati personali.

Diversamente la *protection by default*, opera in un momento successivo e riguarda nello specifico le modalità e le soluzione tecniche poste in essere dal titolare tramite impostazioni predefinite e corrispondenti ad aspetti

[36] Come sottolinea Franco Pizzetti (2016) «privacy» e «protezione dati» sono molto differenti non solo da un punto di vista terminologico, ma anche concettuale e storico. Non a caso il legislatore europeo, prima con la Direttiva 95/46, e ora con il Regolamento 2016/679, non usa mai il termine «privacy», bensì l'espressione *data protection*.

tanto quantitativi, quanto qualitativi, della raccolta, della durata della conservazione,delle finalità del trattamento e dell'accessibilità ai dati in modo tale che la configurazione predeterminata dei sistemi di sicurezza possa garantire che non si verifichino seri danni per le persone coinvolte.

Per quanto riguarda la protezione fin dalla progettazione si prevede che il titolare del trattamento sia al momento di determinare i mezzi che saranno utilizzati all'interno del procedimento, sia durante il trattamento, pone in essere tutte quelle misure tecniche e organizzative volte ad attuare in modo efficace i principi della protezione dei dati personali.

Al fine della determinazione di tali misure il titolare dovrà comunque valutare con attenzione tutto quell'insieme di variabili costituite dallo stato dell'arte delle tecnologie di volta in volta utilizzate, nonché dei costi di attuazione delle procedure.

Allo stesso modo andranno considerati la natura, l'ambito d'applicazione, il contesto, le finalità del trattamento e la probabilità insieme alla gravità dei rischi a cui sono sottoposti i diritti e le libertà delle persone. Il quadro che si delinea tuttavia non si presenta come delimitato da rigidi limiti d'applicazione invalicabili, poiché i principi della protezione fin dalla progettazione, come visto sono sottoposti a bilanciamenti e valutazioni in base a canoni di ragionevolezza e proporzionalità che richiamano delle modulazioni applicative variabili a seconda della rilevanza che assumono fattori come la natura, le finalità, il contesto del trattamento e i rischi che ne possono derivare.

Invece, per quanto riguarda la protezione per impostazione predefinita si prevede che il titolare ponga in essere le misure tecniche e organizzative adeguate affinché per impostazione predefinita siano trattati esclusivamente i dati necessari per ogni specifica, scongiurando il peri-

colo che i dati personali siano accessibili a un numero indefinito di individui, senza un intervento diretto della persona interessata.

### *5.1.* Focus*: gli* standard *di sicurezza*

Lungi dallo sminuire la portata rivoluzionaria delle innovazioni di cui si è detto finora, nell'analizzare le principali innovazioni introdotte dal Regolamento UE/2016/679, non si può far a meno di dedicare particolare attenzione all'ingente apparato di norme contemplanti le misure di sicurezza.

L'esigenza di vagliare con grande attenzione i rischi connessi alle attività di trattamento – così da garantire nella maniera più completa ed efficiente una protezione ai dati personali degli individui – ha fatto sì chenell'elaborare del Regolamento il legislatore europeo affrontasse con attenzione i temi delle misure di sicurezza da applicare. Parimenti, come si è visto[37], grande è stata l'attenzione prestata alla valutazione e alla gestione del rischio, cosicché si potesse apportare una tutela efficace preventivamente e non solo *a posteriori*.

L'art. 32, titolato *Sicurezza del trattamento*, aprendo la Sezione II del Capo IV (concernente la sicurezza dei dati), ribadisceil generale obbligo

[37] A supporto di una concezione di prevenzione del rischio e del danno per la tutela delle persone fisiche e dei dati che le riguardano, sono predisposti numerosi strumenti di cui i più innovativi all'interno del Capo IV sono senz'altro, oltre i vari regimi di comunicazione e notificazione in caso di avvenuta violazione dei dati personali, la valutazione d'impatto, la consultazione preventiva e l'elaborazione dei concetti di privacy *by design* e privacy *by default*.

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



in capo al titolare e al responsabile del trattamento di mettere «in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio»[38].

Riconducibili alla definizione di *data breach*[39]– riportata dal Regolamento 679/2016 all'art. 4– i rischi connessi alla mancata previsione di un opportuno sistema di misure di sicurezza, infatti,comportano unaviolazione che produce «accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»[40]. Di facile intuizio-

[38] In specie, i parametri variabili da sondare, prima di poter dare inizio al procedimento stesso, sono: a) lo stato dell'arte; b) i costi d'attuazione; c) la natura, l'oggetto, il contesto e la finalità del trattamento; e infine d) il rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

[39] Ai sensi del*considerando* n. 85 del Regolamento: «una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della *pseudonimizzazione*, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata».

[40] Nello specifico sono state individuate nove tecniche di attacco e/o modalità mediante le quali può verificarsi un incidente di sicurezza: 1) attacchi per mezzo di applicazioni on-line: si fa riferimento ad ogni incidente ad opera di un *malware*, cioè da un'applicazione o un software progettati ai fini di abuso, ad esempio per manomettere codici o meccanismi di autenticazione. Tali attacchi si registrano nei settori finanziari o dell'acquisto di beni di consumo, colpendo le informazioni rilasciate da utenti all'atto dell'accesso, della navigazione e dell'interazione all'interno delle pagine di offerta di beni e servizi; 2) intrusioni nei punti-vendita: la violazione avviene in relazione agli accessi non autorizzati a dati e informazioni rilasciati all'atto dei pagamenti elettronici, presso alberghi, ristoranti, negozi; 3) utilizzo abusivo di informazioni riservate: ogni violazione

ne, la portata estremamente dannosa che tali violazioni possono arrecare ai dati personali dei soggetti colpiti, può essere arginata da una serie di misure in grado di innalzare il livello di sicurezza. Tra queste, come cita l'articolo di cui sopra, si ricordano: la *pseudonimizzazione*[41] e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi

dei dati che riguarda flussi interni o riservati di informazioni trasmesse attraverso l'accesso a reti interne o aziendali (LAN); 4) errore: ogni tipo di azione non intenzionale che pone a repentaglio la sicurezza di un insieme di dati, ad eccezione dello smarrimento di dispositivi; 5) furto e perdita: ogni incidente avente ad oggetto beni tangibili che implichi la scomparsa di un insieme di informazioni ascrivibile a smarrimento o a condotte intenzionali; 6) *crimeware*: violazioni causate da un *malware* che non rientrano nelle classificazioni precedenti. Tali incidenti si registrano prevalentemente nel settore del consumo e sono motivate da interessi di carattere finanziario di gruppi criminali organizzati che operano a livello transnazionale; 7) *skimming*: fattispecie che comporta l'installazione fisica di apparecchi per la captazione fraudolenta di dati, idonei ad alterare il funzionamento di dispositivi di lettura di carte magnetiche o dispositivi di pagamento (ad es., prelievi di denaro presso gli sportelli bancari); 8) spionaggio informatico: atti di spionaggio svolti da enti paragovernativi o relativi ad attività di carattere industriale o manifatturiero; 9) interruzione del servizio: qualunque attacco che abbia ad oggetto la compromissione o la disponibilità assoluta, per un intervallo più o meno lungo, di una rete di comunicazione elettronica.

[41] Strumento più volte portato ad esempio dal legislatore europeo all'interno del Regolamento in varie disposizioni, la *pseudonomizzazione* appare una valida tecnica di sicurezza avente la capacità di non rendere più riconducibile un dato ad una determinata persona e consentirne di conseguenza un utilizzo che non violi la privacy del soggetto a cui i dati prima si riferivano. Cosa ben diversa dalla tecnica di *anonimizzazione* dei dati – in quanto il dato divenuto anonimo non è da considerare più un dato personale e, perciò, non soggetto alla disciplina del Regolamento – la *pseudoanonimizzazione* consente di trattare un dato in forma anonima, ma secondo modalità che, ove si renda necessario, rendono facile la identificazione della persona alla quale esso si riferisce.

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

L'art. 33 prevede, invece, che il titolare e il responsabile del trattamento, salvo che risulti improbabile che la violazione possa comportare un rischio per i diritti e le libertà delle persone fisiche, notifichi senza ingiustificato ritardo (quando possibile nel termine stringente di 72 ore dal momento in cui viene a conoscenza) l'avvenuta violazione, allegando in caso contrario successivamente i motivi del ritardo. Al fine di agevolare il controllo e la verifica dei requisiti in merito alla corretta adozione delle misure di sicurezza del trattamento la notifica deve essere corredata dai seguenti elementi essenziali: a) descrizione della natura della violazione nonché, ove possibile, delle categorie, del numero approssimativo di interessati in questione, delle categorie e del numero approssimativo di registrazioni dei dati personali; b) comunicazione del nome, dei dati di contatto del responsabile della protezione dei dati (DPO) o di altro punto di contatto presso cui ottenere più informazioni; c) descrizione delle probabili conseguenze che possono derivare dalla violazione dei dati personali; d) descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio o per attenuare i possibili effetti negativi della violazione dei dati personali.

In maniera speculare, all'art. 34, è previsto che, qualora la *data breach* sia suscettibile di comportare un «rischio elevato» per i diritti e le libertà delle persone, il titolare comunichi senza ingiustificato ritardo all'interessato, utilizzando un linguaggio semplice e chiaro (in piena ot-

temperanza al principio di trasparenza) i dettagli della violazione dei dati personali che lo riguardano, fornendo contemporaneamente le informazioni di cui all'art. 33, par. 3, lettere b), c) e d). In caso di inerzia del titolare nell'adempiere agli obblighi di comunicazione presso l'interessato, l'autorità di controllo può richiedere, dopo aver sondato la cogente probabilità che il rischio sia reale e si verifichi, che il titolare vi proceda.

Tuttavia, al fine di non aggravare in maniera eccessiva la posizione del titolare del trattamento, imponendo a quest'ultimo a forza adempimenti formali troppo rigidi e a volte non necessari, sono previsti al paragrafo 3 dei casi di esenzione dall'obbligo di comunicazione all'interessato. Di conseguenza il titolare potrà non inoltrare la comunicazione alla persona interessata se alternativamente dimostri che ha messo in atto tutte le misure tecniche di sicurezza adeguate e che tali misure fossero state applicate ai dati oggetto della violazione, di guisa da renderli incomprensibili a chi non avesse autorizzazione all'accesso; oppure se dimostri di aver adottato tali misure successivamente e aver così scongiurato il sopraggiungere del rischio elevato per i diritti e le libertà della persona; o infine quando la comunicazione richiederebbe sforzi sproporzionati, ma in tal caso sono previste forme equivalenti di informazione degli interessati come ad esempio una comunicazione pubblica.

Forte è il richiamo al principio di *accountability* in tutto il blocco normativo inerente alle misure di sicurezza e più in generale nella disciplina del trattamento.

In base a questo principio, infatti, il titolare è colui che si fa garante della correttezza, della liceità e della trasparenza delle varie fasi del trattamento dei dati, nonché dei vari principi inerenti alla qualità dei dati, le finalità e tutti gli altri aspetti correlati. Nell'ambito di una *data breach*, in-

fatti, il titolare – in ossequio al principio di responsabilizzazione –deve essere in grado di valutare autonomamente la portata di tale violazione e prontamente decidere di attuare quegli interventi settoriali tecnici e organizzativi di tipo riparatorio ed eventualmente attivare le procedure di carattere informativo. In base al medesimo principio, inoltre, incombe sul titolare l'onere di dimostrare, quando gli viene richiesto, la prova della conformità del suo operato alla *best practice* del settore e alle norme regolamentari, costituendo tale esito positivo una prova liberatoria della responsabilità in caso della verificazione dell'evento dannoso.

La previsione di specifici e rigorosi obblighi in capo ai soggetti che pongono in essere iltrattamento dei dati personali – e, in particolare, la prevenzione del danno e delle lesioni ai diritti fondamentali potenzialmente derivabili da una violazione delle misure di sicurezza o da un trattamento illegittimo –pare essere, congiuntamente alla specificazione puntuale dei principi regolanti la materia, il punto di forza di un Regolamento fortemente auspicato e altrettanto opportuno.

Per le dinamiche vorticose che la fanno da padrone in un mondo sempre più informatizzato (ed esponenzialmente meno informato), l'introduzione di una disciplina generale, mediante l'adozione di un atto vincolante e *self executing*, ha rappresentato la risposta più adeguata.

Ed è, infatti, proprio la veste giuridica con cui è stata avvolta la nuova disciplina a consentirle di raggiungere, ora più di prima, l'obiettivo sperato dell'omologazione ed eliminazione di tutte le discrepanze tra le differenti normative nazionali, predisponendo un sistema uniforme e coordinato sul territorio UE in materia di protezione dei dati personali.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 1, 2018
data di pubblicazione: 11 agosto 2018

Osservatorio sulla normativa

**6. «Liberi e connessi»: alcune considerazioni conclusive**

È l'età nuova del Web, della continua e massiccia produzione di informazioni virtuali, dell'intelligenza artificiale. È lo spazio dominato dalla diffusione capillare di tecnologie elettroniche, capaci di costruire e collegare gigantesche banche dati personali. È la società del controllo, della mercificazione del patrimonio individuale (e, in teoria, indisponibile) del singolo.

Dal villaggio feudale di March Bloch (1949) – in cui il *diritto alla riservatezza* era prerogativa dei soli monaci e banditi – all'attuale villaggio globale, che con le sue tentacolari reti ci imbriglia come pesci, il passo è breve.

Se, allora, il concetto di privacy nasce come un «no!» urlato nei confronti degli altri, affinché si tengano lontani dalla recinzione della «mia» terra, esso si evolve in una dimensione universale: non si tratta più della sola sfera privata del singolo, ma è l'intera rete di relazioni che ciascuno intrattiene con il mondo a necessitare strumenti di tutela adeguata.

La rivendicazione del *right to privacy* diviene, così, una richiesta volta ad ottenere «il diritto di mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata» (Rodotà 1995, 122). Insomma, «il diritto di scegliere liberamente il proprio modo di vivere» (Rigaux 1990, 167).

Scomposto oramai in due dimensioni, una fisica e una elettronica, il corpo umano si trova completamente in balia delle nuove frontiere della raccolta e del trattamento dei dati personali. Ma, se le violazioni della parte materiale – come sottolinea Stefano Rodotà – sono colte con immediatezza perché visibili, quelle relative al *corpo elettronico*, non vengo-

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 1, 2018
data di pubblicazione: 11 agosto 2018

Osservatorio sulla normativa

no percepite direttamente. Eppure, le conseguenze che ne derivano sono altrettanto (se non più) gravi: l'impropria circolazione delle informazioni sulla salute può provocare discriminazioni, stigmatizzazioni, isolamento. Significativo è l'esempio che «l'uomo dei diritti»[42] riporta: la donazione di un rene non pregiudica l'integrità fisica; la conoscenza dello stato di sieropositività di un individuo può danneggiarlo gravemente.

Non è un caso, quindi, se da anni si è deciso di accompagnare al tradizionale *habeas corpus* un nuovissimo *habeas data*:il «non metteremo mano su di te» – l'inviolabilità del corpo riconosciuto come valore fondamentale della democrazia, per la prima volta, dalla *Magna Charta* – è stato così esteso dalla dimensione fisica a quella elettronica.

La tutela della privacy – e, in particolare, la protezione dei dati personali – si configura, dunque, come elemento essenziale di una società che si fonda sul rispetto dell'eguaglianza (se non tutelato nella riservatezza delle informazioni l'individuo rischia di essere soggetto a discriminazioni per le sue opinioni, credenze religiose, condizioni di salute); della partecipazione (senza una protezione dei dati riguardanti i rapporti con le istituzioni e le formazioni sociali i cittadini rischiano di essere esclusi dai poteri democratici); della libertà (la mancata difesa del *corpo elettronico* compromette la libertà personale, alimentando la creazione di una società della sorveglianza); della dignità (in assenza di barriere che

[42] Ci si riferisce a Stefano Rodotà, così definito in onore al titolo di una delle sue opere più note, *Il diritto di avere diritti* (Rodotà 2012), che riprendeva – a sua volta – un passo della filosofa tedesca Hannah Arendt (1951): «Il diritto di avere diritto, o il diritto di ogni individuo ad appartenere all'umanità, dovrebbe essere garantito dall'umanità stessa».

arginino i controlli capillari e continui, l'individuo rischia di trovarsi nudo e debole di fronte ai poteri pubblici e privati).

*Il personale è politico*, è vero, ma fino ad un certo punto.

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*



**Bibliografia**

Acciai, R., Orlandi, S. (2003), *Le nuove norme in materia di privacy*, Santarcangelo di Romagna: Maggioli.

Bolognini, L., E. Pelino, C. Bistolfi (2016), *Il Regolamento privacy europeo, Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano: Giuffrè.

Bonfiglio, S., (2014), *Diritto alla privacy e lotta al terrorismo nello spazio pubblico europeo*, in *Democrazia e Sicurezza*, 3.

Bonini, M., (2016), *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *Rivista AIC.*, 3.

Brugiotti, E., (2013), *La privacy attraverso la "generazione dei diritti*, in *Dirittifondamentali.it*, 2.

Caggiano, G. (2014), *Attività di stabilimento e trattamento dei dati personali*, in Dir.inf., 4-5.

Caggiano, G., (2018), *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *Studi sull'integrazione europea*, 1.

Caldirola, D., (2006), *Il diritto alla riservatezza*, Padova: Cedam.

Califano, L., (2016), *Privacy; affermazione e pratica di un diritto fondamentale*, Napoli: Editoriale Scientifica.

Califano, L. (2014), *Trasparenza e privacy: la faticosa ricerca di un bilanciamento mobile*, in L. Califano, C. Colapietro (2014), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli: Editoriale scientifica.

Califano, L., C. Colapietro (cur.) (2017), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli: Editoriale Scientifica.

Ciampi, S., (2009), *Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea*, in F. Peroni, M. Gialuz (cur.), *Cooperazione informativa*, Trieste: EUT.

Commissione Europea, (2012), *Salvaguardare la privacy in un mondo interconnesso – Un quadro europeo della protezione dei dati per il XXI secolo*, COM (2012), 25 gennaio 2012.

D'Antonio, V. (2016), 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 (cur.), *La nuova disciplina europea della Privacy*, Milano-Padova: Wolters Kluwer – Cedam, Cap. X.

D'Orazio, R. (2016), *Protezione dati by default e by design*, in S. Sica, V. D'Antonio, G.M. Riccio (cur.), *La nuova disciplina europea della Privacy*, Milano-Padova: Wolters Kluwer – Cedam, Cap. V.

Finocchiaro, G. (2012), *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. Inf.*, 3.

Finocchiaro, G. (2014), *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. inf.*, 4-5.

Flor., R. (2009), *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* online durchsuchung, in *Riv. trim. dir. pen. econ.*, 3.

Mula, D. (2016), *Trasferimento verso paesi terzi*, in S. Sica, V. D'Antonio, G.M. Riccio (cur.), *La nuova disciplina europea della Privacy*, Milano-Padova: Wolters Kluwer – Cedam, Cap. XIV.

Pacileo, P., (2016), *Il diritto alla portabilità*, in S. Sica, V. D'Antonio, G.M. Riccio (cur.), *La nuova disciplina europea della Privacy*, Milano-Padova: Wolters Kluwer – Cedam, Cap. XI.

Pagallo, U. (2008), *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano: Giuffrè.

Pizzetti, F. (2013), *Il prisma del diritto all'oblio, in* Id., *Il caso del diritto all'oblio*, Torino: Giappichelli.

Pizzetti, F., (2014), *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni*, in *Federalismi.it*, 12.

Pizzetti, F., (2016), *Privacy e il Diritto Europeo alla Protezione dei Dati Personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, (vol. I de *I Diritti nella "rete" della Rete*), Torino: Giappichelli.

Resta, G., V. Zeno-Zenovich (2015), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma: RomaTrE-Press.

Rodotà, S., (1995), *Tecnologie e diritti*, Bologna: il Mulino.

Rodotà, S. (2005), *Intervista su privacy e libertà*, (a cura di P. Conti), Roma-Bari: Laterza.

Rodotà, S. (2012), *Il diritto di avere diritti*, Roma-Bari: Laterza.

Rossi Dal Pozzo, F., (2016), *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal Safe Harbor al Privacy Shield)*, in *Rivista di diritto internazionale*, 3.

Rubechi, M., (2016), *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *Federalismi.it*, 23.

Sica, S., V. D'Antonio, G.M. Riccio (cur.) (2016) (cur.), *La nuova disciplina europea della Privacy*, Milano-Padova: Wolters Kluwer – Cedam.

Soro, A. (2016), *Liberi e Connessi*, Torino: Codice Edizioni.

Tega, D. (2012), *I diritti in crisi. Tra Corti nazionali e Corte europea di Strasburgo*, Milano: Giuffrè.

Tiberi, G. (2011), *Protezione dei dati personali e sicurezza dopo il Trattato di Lisbona*, in G. Grasso, L. Picotti, R. Sicurella (cur.), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano: Giuffrè.

Tresca, M., (2016), *Sicurezza vs protezione dei dati: la CGUE cambia registro*, in Amministrazione In Cammino.

Warren, S.D., Brandeis, L.D., (1890), *The Right to Privacy*, in *Harvard Law Review*, Vol IV, Boston, n. 5.

Whitman, J. Q., (2004), *The Two Western Cultures of Privacy: Dignity versus Liberty*, in *The Yale Law Journal*, vol. 113.

Zeno-Zenovich, V., (2015), *Intorno alla decisione nel caso "Schrems": la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *Dir. inf.*, 4-5.

**Sitografia**

FRA (*European Union Agency for Fundamental Rights*) – CONSIGLIO D'EUROPA, (2014), *Manuale sul diritto europeo in materia di protezione dei dati*, www.fra-europa.eu, pdf.

Galgani, F., (2014), *La nascita del diritto alla privacy negli Stati Uniti e in Europa*, www.informatica-libera.net.

Guzzo, A., (2009), *Il concetto di Privacy Enhancing Technologies (PET)*, in *Sicurezza informatica e tutela della privacy*, www.diritto.it, 26 febbraio.

Lattanzi, R., (2014), *Diritto alla protezione dei dati di carattere personale: appunti di viaggio*, in AA.VV., *Diritto alla Privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, www.cde.unict.it/quadernieuropei/giuridiche/63_2014.pdf.

Remotti, R., (2002); *Il diritto alla privacy e ricerca scientifica, Qual è il bene giuridico tutelato*, da www.web.tiscalinet.it, par. 2.

Valensise, M., (2010), *The right to be let alone*, www.ilfoglio.it.

Varani, E., (2012), *Il "nuovo diritto" alla privacy. Dalla Carta di Nizza al "Codice in materia di protezione dei dati personali"*, www.filodiritto.com.

*Democrazia e Sicurezza – Democracy and Security Review*
*ISSN: 2239-804X*

*anno VIII, n. 1, 2018*
*data di pubblicazione: 11 agosto 2018*

*Osservatorio sulla normativa*

## Abstract

*Under (Data) Control. The Right to Protection of Personal Data in European Legislation*

From 25 May 2018 the Regulation (EU) n. 2016/679 of 27 April 2016 (General Data Protection Regulation - GDPR) is in force in all European Member States.

Reconstructing the right to the protection of personal data in the European normative framework, this paper analyses the regulatory interventions that followed the first Directive 81/108/CE. Especially, the focus is on the analysis of the new Regulation and on the necessary safety standards introduced for the processing of personal data.

Keywords: GDPR; European Legislation; Right to privacy; Personal Data Protection.