rivista techne
FORUM
e-government nel nord-est

le regole sono cambiate
privacy ue 679/16

a cura di Glauco Riem

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
FormAzione TERZIARIO
Unione Industriali Pordenone Sezione Terziario Avanzato
Comune di Pordenone
Camera di Commercio Pordenone - Udine
Unione Territoriale Intercomunale del Noncello

ASSOCIAZIONE CULTURALE
PER LO STUDIO DEL DIRITTO

techne

n. 23/2018

Direttore responsabile
Glauco Riem

Via Tessitura, 23 - 33170 Pordenone
tel. 0434 522866
associazione@e-curia.it
www.rivistatechne.it

Realizzazione editoriale
Forum Editrice Universitaria Udinese
FARE srl con unico socio
Società soggetta a direzione e coordinamento
dell'Università degli Studi di Udine
Via Palladio, 8 - 33100 Udine
www.forumeditrice.it

Stampa
Press Up srl, Ladispoli (RM)

Reg. Trib. di Pordenone n. 514 del 27.07.2004

SOMMARIO

EDITORIALE

Glauco Riem*

La rivista *Techne* dedica questo numero alla pubblicazione degli atti e della nutrita serie di materiali (slide, video, fotografie) che sono stati 'prodotti' nel corso del convegno dedicato al Regolamento Privacy UE 679/2016 tenutosi a Pordenone il 23 febbraio 2018.
Il convegno, il cui slogan annunciava *Le regole sono cambiate*, è stato organizzato dall'Associazione Culturale per lo Studio del Diritto e dell'Informatica per Unindustria e il Terziario Avanzato di Pordenone.
L'iniziativa si è sviluppata su un articolato programma che qui di seguito riportiamo e che ha visto la partecipazione di quasi cinquecento addetti provenienti dal Triveneto e anche da molte altre regioni italiane. L'iniziativa è stata patrocinata dalla Regione Friuli Venezia Giulia, dal Comune e dalla Camera di Commercio di Pordenone, dall'Ordine degli Avvocati e dall'Ordine dei Dottori Commercialisti e degli Esperti contabili e dal Consiglio Notarile di Pordenone e inoltre da Unindustria Servizi e Formazione Treviso e Pordenone.
Hanno sponsorizzato l'iniziativa Ars Distribuzione, Real Comm, Nordpas, Cosmos, Onsolution, CentroFriuli e AdasPn, a cui va un sentito ringraziamento da parte dell'associazione e di tutti gli enti che hanno contribuito e patrocinato l'iniziativa.
Nel formato elettronico la rivista reca i link ai materiali video, alle slide e alle fotografie pubblicati su youtube e presenti sul sito di Unindustria Pordenone: http://bit.ly/galleria-convegno-privacy-unindustria-PN.
Il formato cartaceo della rivista riporta i QR Code. Ulteriori informazioni su di essi sono facilmente reperibili online.
Di seguito si riportano la premessa, il programma, i temi e i relatori intervenuti al convegno.

Il Regolamento Privacy UE 679/2016 (*General Data Protection Regulation* - GDPR) e la Circolare AgID n. 2/2017, del 18 aprile 2017 costituiscono, per diverso aspetto, gli strumenti per la tutela della riservatezza più avanzati e credibili nel trattamento dei dati personali.
Il Regolamento è entrato in vigore nel maggio 2016 ed è direttamente applicabile, anche nella sua parte sanzionatoria (artt. 83 e 84), dal 25 maggio 2018. La Circolare AgID sulle Misure minime di sicurezza ICT riprende le *best practices* sulla sicurezza logica nel trattamento dei dati dettati dal SANS 20 v. 6.0/2015 e ciò con l'indicare finalmente, in modo semplice e chiaro, quelle procedure che sono oggi ritenute necessarie per assicurare quelle ulteriori tutele nel trattamento che avviene attraverso l'uso di strumenti info-telematici. Ciò sicuramente a confortare ulteriormente gli adempimenti previsti dal citato Regolamento (art. 32, C83).
Imprese, pubbliche amministrazioni, associazioni di categoria, professionisti e, riteniamo, anche i singoli cittadini sono chiamati a dare spessore e risalto ad un comportamento sociale civilmente rispettoso dei dati e delle informazioni personali dei singoli individui che sempre più sembra essere messo a rischio dall'uso delle tecnologie info-telematiche e dei social media.
Il convegno ha l'obiettivo di chiarire da un punto di vista giuridico-dottrinale, ma soprattutto da un punto di vista pratico e operativo, gli adempimenti previsti dalla citata normativa valida in tutto il territorio dell'Unione Europea.

Il sito dell'Associazione Culturale per lo Studio del Diritto è reperibile all'indirizzo http://www.e-curia.it; il link alle attività di maggior rilievo da essa svolte dal 1991 ad oggi è http://ge.tt/8AKovzo2 (scaricabili in formato pdf).

* Glauco Riem: presidente dell'Associazione Culturale per lo Studio del Diritto di Pordenone.

Programma

Conduce
Avv. Glauco Riem
Docente di Diritto delle nuove tecnologie
Introduzione e presentazione dei relatori

Dott. Pasquale Costanzo
Referente Servizi Compliance UNIS&F
L'Osservatorio di Unindustria Pordenone e Treviso sui temi Privacy, anche alla luce del GDPR

Prof. Giovanni Buttarelli
Garante europeo per la protezione dei dati personali
La legge delega sul coordinamento tra il Codice Privacy e il Regolamento UE 679/2016

Prof. Avv. Gianluigi Ciacci
Docente di Informatica giuridica, Università LUISS 'Guido Carli' in Roma
La protezione dei dati personali: dal D.Lgs. 196/2003 al Regolamento UE 679/2016

On. Giovanna Bianchi Clerici
Garante per la protezione dei dati personali
Il ruolo del Garante e del nuovo Comitato europeo della protezione dei dati personali

Dott. Floretta Rolleri
Consulente informatico della Corte Costituzionale

Dott. Daniela Intravaia
Direttore Coordinamento attività internazionali AgID
La circolare AgID 2/2017 sulle misure minime di sicurezza ICT ed impact assessment *(DIPIA)*

Prof. Avv. Andrea Sirotti Gaudenzi
Il nuovo 'diritto all'oblio': tra tutela dell'identità personale ed esigenze di riservatezza

Avv. Andrea Lisi
Il trattamento di categorie particolari di dati personali

Dott. Filippo Trifiletti
Direttore generale di Accredia
Il valore dell'accreditamento per le certificazioni previste dal Regolamento 679/2016

Ing. Alessandro Da Re
Risk management: cinque brevi note per accelerare il processo di conformità al GDPR

Domande, conclusioni

Patrocinio

Sponsor

La pubblicazione della rivista *Techne* che raccoglie gli Atti del convegno sulla privacy *Le regole sono cambiate* chiude una prima e importante iniziativa di analisi e commento del Regolamento Privacy UE 679/2016. Altre seguiranno.
Unindustria Pordenone, il Terziario Avanzato e UNIS&F, congiuntamente all'Associazione Culturale per lo Studio del Diritto, vista l'importanza, l'attualità e la complessità della materia e il necessario coordinamento alle regole europee della normativa italiana recata dal D.Lgs. 101/2018, hanno fermamente voluto detta iniziativa.
La partecipazione di oltre cinquecento fra imprenditori, professionisti, dirigenti di pubbliche amministrazioni, convenuti nelle due sale del Teatro Don Bosco a Pordenone, ne attesta il successo.
Importanti chiarimenti sulla materia sono infatti venuti direttamente da coloro che, a diverso titolo, hanno anche contribuito a redigerla, come ad esempio il Garante Privacy europeo, professor Giovanni Buttarelli, e il componente dell'Autorità garante italiana, onorevole Giovanna Bianchi Clerici.
Molti poi sono stati i chiarimenti sul Regolamento delineati dagli altri importanti relatori intervenuti, tra i quali Floretta Rolleri, consulente informatico della Corte Costituzionale, la dottoressa Daniela Intravaia, direttore del Coordinamento attività internazionale dell'AgID, il dottor Filippo Trifiletti, direttore generale di Accredia, l'ente italiano di accreditamento, e il professor Gianluigi Ciacci dell'Università LUISS che, con la collaborazione del dottor Baldo Meo, capo ufficio stampa del Garante, hanno anche significativamente contribuito alla riuscita del convegno.

Gli argomenti proposti e trattati costituiscono, per esaustività, una visione della materia a tutto tondo sicuramente utilissima a fugare molti degli interrogativi posti dal Regolamento e a chiarire, a titolo quasi di *interpretazione autentica*, le molte domande dell'uditorio.
La rivista *Techne* che state consultando, così come curata dall'avvocato Glauco Riem, è poi un innovativo esempio di editoria 'ibrida' dove al supporto cartaceo si aggiungono moltissimi ulteriori contenuti *documentali*, reperibili mediante smartphone, che legge i QR Code inseriti nel testo e permette di effettuare il download degli ulteriori approfondimenti.
Ugualmente è possibile fare, nel formato elettronico della rivista, cliccando su semplici link. Si tratta di un nuovo modo di pubblicare e di fare editoria ibrida che integra contenuti nei diversi e possibili formati rendendo la materia trattata maggiormente intellegibile al lettore. Detta modalità è già stata definita come Editoria 4.0.
Tali strumenti ampliano e aggiungono importanti e corposi materiali di approfondimento e di riflessione per il lettore, che difficilmente potrebbero trovare spazio in una rivista tradizionale.

Michelangelo Agrusti
Presidente di Unindustria Pordenone

Paolo Candotti
Direttore generale di Unindustria Pordenone

Raul Pietrini e Fabio La Malfa
Presidente e vicepresidente del Terziario Avanzato di Pordenone

le regole sono cambiate
privacy ue 679/16

a cura di Glauco Riem

PRIVACY E IMPRESE: ONERE E OPPORTUNITÀ

Pasquale Costanzo*

Unindustria Servizi e Formazione Treviso e Pordenone (UNIS&F) è la società di formazione e servizi di Unindustria Treviso e Unindustria Pordenone, associazioni territoriali di Confindustria che assieme rappresentano 3.097 aziende associate ed occupano circa 126.000 dipendenti. Il nostro osservatorio è in grado di fotografare, da un'angolazione sicuramente privilegiata, le dinamiche legislative, come ad esempio quella della normativa in materia di protezione dei dati personali, verificandone l'impatto sui processi decisionali ed operativi aziendali e di monitorare il trend di ottemperanza e di relativa *compliance*, oltre ad essere il luogo di condivisione e di promozione delle *best practices*[1]. Tutto ciò ci consente di suggerire alle nostre aziende associate delle soluzioni di *compliance* che siano proporzionali rispetto all'impresa destinataria del nostro intervento e di formulare proposte, attraverso i gruppi di lavoro interni a Confindustria nazionale[2], in grado, il più delle volte, di orientare le scelte normative e applicative, nella logica di favorire e bilanciare l'ottemperanza alla norma con l'esigenza dell'impresa di non subire delle rigidità che potrebbero a loro volta compromettere il business aziendale.
Il tema della protezione dei dati personali e della sua regolamentazione è sempre stato visto dal mondo industriale del nostro territorio (e non solo) come un insieme di adempimenti e regole di natura burocratica, ritenute poco utili e spesso incomprensibili. Sul punto, si pensi a quanti (inutili) fax e raccomandate sono state inviate prima delle semplificazioni intervenute nel 2011 con l'obiettivo di regolamentare il trattamento dei dati personali nell'ambito delle finalità meramente amministrative e/o di fatturazione tra clienti e fornitori che nella maggior parte dei casi erano persone giuridiche; oppure a

quanti consensi al trattamento sono stati chiesti, anche quando gli stessi non erano assolutamente necessari, ma sollecitati per la semplice paura di non rischiare di incorrere in sanzioni amministrative particolarmente onerose. Sicuramente ad alimentare la disaffezione del mondo imprenditoriale nei confronti di tale materia hanno contribuito la complessità e la difficoltà di decifrazione della norma stessa, atteso che, ancora oggi, le 'regole' previste dal Codice della Privacy (D.Lgs. 196/2003) vanno lette unitamente alle indicazioni contenute nei Provvedimenti del Garante per la protezione dei dati personali, le quali in alcuni casi, pochi per fortuna, rappresentano una deroga allo stesso Codice: ci si riferisce alla nomina obbligatoria a responsabile del trattamento a favore degli agenti prevista dal Provvedimento del Garante Privacy[3] in materia di titolari del trattamento che si avvalgono di soggetti esterni per le proprie attività di marketing e promozionali.
La fase acuta di tale insofferenza è stata raggiunta con il provvedimento generale sulla figura dell'amministratore di sistema del 27 novembre 2008, la cui norma, nonostante la proroga di un anno, generò fin dall'inizio una serie di criticità attuative sul piano pratico per le imprese, le quali a loro volta furono oggetto di complicate implementazioni sul piano tecnico e, quindi, eccessivamente gravose in termini di costi di adeguamento. Proprio su quest'ultimo punto, anche per effetto di una spinta commerciale da parte delle software houses, furono diverse le aziende che investirono migliaia di euro nell'acquisto di soluzioni informatiche in grado di tracciare i log di accesso degli amministratori di sistema, prescrizione richiesta dal provvedimento in oggetto. Anche il tardivo intervento chiarificatore dell'Autorità garante[4] non aiutò a calmierare tale disagio, nonostante la stessa nota dell'Autorità suggeriva soluzioni informatiche a basso costo e soprattutto gratuite (open source) quali valide alternative a prodotti più strutturati. Tali disagi provenienti dal mondo industriale trovarono una risposta, anche se parziale, da parte del legislatore nazionale il quale, anche su spinta del sistema confindustriale, intervenne con tre provvedimenti di legge a distanza di poco più di un paio di anni: 1) Decreto Sviluppo-bis[5]; 2) Decreto Salva Italia[6]; 3) Decreto Semplifica Italia[7].
Il primo intervento da una parte definì i trattamenti effettuati per finalità amministrativo-contabili, individuando i casi di esclusione dall'ambito di applicazione del Codice della Privacy, dall'altra sostituì l'obbligo di redazione

e aggiornamento del Documento Programmatico sulla Sicurezza (DPS), con una semplice autocertificazione.
Il secondo intervento, agendo sulla definizione di dato personale e di interessato, escluse dall'ambito di protezione del Codice della Privacy il riferimento alle persone giuridiche, enti e associazioni, riducendo in questo modo gli oneri derivanti dal trattamento dei dati nei rapporti tra le persone giuridiche, quali ad esempio gli obblighi di informativa e consenso.
Con il terzo intervento, invece, il legislatore eliminò l'obbligo di predisposizione e aggiornamento periodico (entro il 31 marzo di ogni anno) del DPS, adempimento superfluo non previsto dalla normativa europea sulla privacy, e della relativa annotazione nella relazione accompagnatoria al bilancio.
Tuttavia tali interventi del legislatore, effettuati in maniera disorganica, con una tecnica normativa alquanto discutibile e dettati più dalla fretta che dalla logica, generarono tutta una serie di dubbi interpretativi[8] tali da vanificare gli effetti semplificatori che il legislatore intendeva raggiungere. A complicare tale quadro di incertezza contribuì anche l'Autorità garante che, al susseguirsi dei tentativi di semplificazione normativa, rispose con una proliferazione di provvedimenti generali in vari settori, dalla cui lettura emersero prescrizioni ed adempimenti addirittura ulteriori rispetto agli stessi vincoli contenuti nelle norme[9].
Se è vero che nelle realtà aziendali, in particolare per le PMI, è consuetudine vedere il complesso delle norme in materia di protezione dei dati personali come un mero adempimento burocratico al quale i titolari di impresa e/o i loro delegati pensano solo nel momento in cui è necessario intervenire per evitare sanzioni o rispondere a reclami, è altrettanto vero che tra gli stessi titolari vi è maggiore consapevolezza che tale sistema di norme non solo può impattare in modo significativo sui processi aziendali, in alcuni casi migliorandoli anche in maniera sostanziale, ma che può anche generare benefici nella relazione duratura con il cliente finale e/o con i vari *stakeholders*. Basta pensare a tutte le aziende che operano nell'ambito del marketing e che privilegiano con i loro clienti un approccio basato sulla relazione (*relationship marketing*), attraverso la quale vengono trattate tutta una serie di informazioni di natura personale. Nella quasi generalità dei casi tali informazioni vengono poi codificate all'interno di 'contenitori' informatici denominati CRM[10], sistemi in grado di raccoglierle, organizzarle ed elaborarle per un utilizzo sia interno

che esterno. È evidente che in questo caso l'adozione di comportamenti etici è in grado di differenziare le aziende che agiscono senza il rispetto della normativa sulla privacy da quelle che invece la rispettano.
Unindustria Treviso già nel 2008 si fece promotrice di un'iniziativa a favore delle proprie aziende associate e più in generale verso quelle seguite dal servizio di *compliance* erogato dalla sua società di servizi (oggi UNIS&F, prima Iniziative Unindustria), mettendo a disposizione un logo, registrato in CCIAA, dal nome: «Il rispetto della privacy, nostro valore aziendale». Tale iniziativa riscosse un discreto successo, tanto che furono diverse le aziende che inserirono il logo all'interno del proprio sito web, nella sezione dedicata alla presentazione dell'azienda, ed in alcuni casi direttamente nella propria carta intestata. L'eccezionalità e l'importanza dell'iniziativa, ottenne il riconoscimento dell'Autorità garante, e l'ex segretario generale, oggi Garante europeo, dottor Giovanni Buttarelli rilasciò una dichiarazione a mezzo stampa con la quale riconobbe a Unindustria Treviso «l'impegno nella promozione di una cultura aziendale in tema di privacy» e nei confronti dell'azienda beneficiaria di «creare valore aziendale e di evidenziare all'esterno la propria attenzione non solo alla norma, ma anche al cliente».
L'attenzione al tema della protezione dei dati personali vuol dire anche aumento della sensibilità sulla protezione del *know-how* aziendale. Oggi nelle relazioni quotidiane con le aziende associate, molti interlocutori ci chiedono se, alla luce delle prossime novità normative (GDPR), le attuali misure (minime) previste dal Codice della Privacy - Disciplinare tecnico (allegato B) – quali ad esempio l'utilizzo della password per l'accesso al sistema informatico oppure il salvataggio settimanale dei dati – siano ancora misure necessarie o di fatto ritenute ridondanti. Tale atteggiamento conferma come sia fondamentale che in azienda venga diffusa una cultura proattiva al corretto trattamento del dato e al rispetto di determinate misure di sicurezza, al fine di assicurare una protezione a trecentosessanta gradi. La lista dei clienti (persone fisiche) ha una doppia rilevanza sia sotto il profilo della privacy, quando si chiede l'autorizzazione al trattamento e quando vengono trattati i dati, sia sotto il profilo di segreto commerciale dell'azienda. Una delle misure che la privacy impone è la segregazione degli accessi, vale a dire che non tutti i dipendenti dell'azienda possono accedere ai database aziendali e ai dati per-

sonali. I sistemi informatici aziendali sono settati sulla base di diritti riservati ai singoli utenti secondo una logica di competenza, per cui soltanto gli addetti e i dipendenti che svolgono un certo tipo di mansioni possono avere accesso a determinati database. Questa misura di sicurezza, richiesta dalla normativa privacy e prevista a tutela dei dati, può avere ricadute positive nella difesa dell'azienda dai dipendenti che vogliono trafugare segreti aziendali.
Dell'esigenza di favorire un nuovo approccio ne è consapevole anche Confindustria, la quale, seppur in ritardo nel rispetto delle specifiche esigenze di semplificazione delle micro, piccole e medie imprese nell'applicazione delle nuove regole, sta contribuendo all'azione di sensibilizzazione in favore delle aziende associate promuovendo un nuovo approccio, non solo per quanto concerne i nuovi adempimenti (Registro dei trattamenti, nomina del responsabile della protezione, ecc.) ma soprattutto sul piano operativo, generando un vero e proprio cambio culturale. A testimonianza di ciò sono diverse le iniziative formative promosse e/o patrocinate dalle varie articolazioni territoriali, il cui obiettivo non è solo quello di definire il perimetro degli adempimenti, ma diffondere, appunto, un nuovo messaggio – in linea con il principio di *accountability* che impone di dimostrare la conformità GDPR – di trasformare la *compliance* in materia di protezione di dati personali da adempimento normativo a un vero e proprio sistema di gestione.
Segnali incoraggianti in tale direzione stanno venendo dalle aziende[11] del territorio, caratterizzate da un discreto dimensionamento, le quali hanno colto le opportunità che offre la nuova normativa, strutturando il proprio modello organizzativo privacy come leva di miglioramento/ottimizzazione dei propri processi organizzativi, agendo sulla responsabilizzazione delle figure aziendali coinvolte a vario titolo nelle operazioni di trattamento di dati personali e più in generale nei dati aziendali considerati rilevanti e da proteggere.

Intervento al convegno
L'Osservatorio di Unindustria Pordenone e Treviso sui temi Privacy, anche alla luce del GDPR
https://www.youtube.com/watch?v=99HP1_UDIC8&feature=youtu.be

NOTE

[1] UNIS&F, in collaborazione con i colleghi delle rispettive associazioni, ha promosso diverse iniziative seminariali e convegnistiche, coinvolgendo diversi attori appartenenti alle varie categorie.

[2] Confindustria ha creato un gruppo di lavoro 'Privacy e Legalità', il cui obiettivo è quello di elaborare osservazioni e propose su progetti di atti normativi destinati ad incidere sull'attività d'impresa.

[3] Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali, 15 giugno 2011.

[4] Amministratori di sistema: precisazioni del Garante 10 dicembre 2009.

[5] Decreto legge 70/2011 (c.d. Decreto Sviluppo), convertito nella legge 12 luglio 2011, n. 106.

[6] Decreto legge 06 dicembre 2011, n. 201, così come convertito con modificazioni dalla legge 22 dicembre 2011, n. 214, denominato *Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici*.

[7] Decreto legge 09 febbraio 2012, n. 5, così come convertito con modificazioni dalla legge 4 aprile 2012, n. 35, denominato *Disposizioni urgenti in materia di semplificazioni e di sviluppo*.

[8] Il dato personale relativo alle ditte individuali resta o meno nell'ambito di protezione del Codice della Privacy?

[9] Ad esempio, il provvedimento 'Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro' del 4 ottobre 2011.

[10] *Customer Relation Management* (CRM).

[11] Esempi di aziende che hanno avviato processi di adeguamento privacy in un'ottica migliorativa: Permasteelisa Group Spa, Silca Spa, Mcz Group, ecc.

* Pasquale Costanzo: è responsabile dei Servizi alle imprese - area legale/societaria di Unindustria Servizi e Formazione Treviso e Pordenone (UNIS&F). È referente anche operativo del servizio *Risk management* di Unindustria Treviso; tale attività consiste nell'analisi delle coperture assicurative delle aziende a cui viene erogato il servizio (*risk insurance*) e della mappatura e trattamento dei rischi industriali (*risk analysis/risk management*). Si occupa del coordinamento delle attività di *compliance* in materia di privacy e D.Lgs. 231/2001 e del coordinamento delle attività di supporto alle imprese per le tematiche relative all'utilizzo della piattaforma di acquisto Mercato Elettronico della Pubblica Amministrazione (MEPA).

LA LEGGE DELEGA SUL COORDINAMENTO TRA IL CODICE PRIVACY E IL REGOLAMENTO UE 679/2016

Giovanni Buttarelli*

Riportiamo qui di seguito le considerazioni svolte da Giovanni Buttarelli, Garante Privacy europeo nell'audizione avanti alla Commissione del Senato della Repubblica Italiana - Commissione speciale sugli atti urgenti del Governo, nell'ambito dell'esame dell'atto del Governo n. 22 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, 7 giugno 2018. Il documento rappresenta, per le considerazioni svolte, una importante chiave di lettura dei temi legati al coordinamento fra il Codice della Privacy, così come poi novellato dal decreto legislativo n. 101, del 10 agosto 2018, pubblicato nella Gazzetta Ufficiale Serie Generale n. 205, del 4 settembre 2018 (http://www.gazzettaufficiale.it/eli/gu/2018/09/04/205/sg/pdf) e il Regolamento Privacy UE 679/2016, del quale ha trattato anche in occasione dell'intervento al convegno al cui video si rimanda.

Osservazioni generali e introduttive

È con piacere che accetto questo invito come Autorità europea e anche per il ruolo 'terzo' che vorrei svolgere in relazione al dibattito che si è istaurato sulla qualità dello schema di decreto legislativo. Terrò, come d'obbligo, un approccio istituzionale, ma chiedo la vostra autorizzazione a utilizzare il linguaggio della sincerità, per un contributo cooperativo e disinteressato, volto a consentire al nostro Paese di mantenere il ruolo guida che in questa materia ha da molti anni. Nutro rispetto per il lavoro svolto a vari livelli, *in primis* dalla commissione scientifica istituita presso il Ministero della Giustizia, dal Ministero stesso e dalle altre istituzioni e autorità che hanno già formulato il proprio punto di

vista. Si è trattato di un lavoro obiettivamente difficile da esaurire, in termini qualitativamente alti, nei circa sessanta giorni di funzionamento della commissione. A questo si aggiunga che, come noto, la delega è stata approvata assai tardivamente rispetto al maggio del 2016.
Tutto ciò premesso, nonostante i miglioramenti intervenuti, la tecnica legislativa utilizzata è risultata, e appare ancora, piuttosto discutibile e controversa. Se da un lato si deve esprimere apprezzamento per la profonda rivisitazione avvenuta prima e dopo la presentazione del primo elaborato, è ancora elevato il numero delle disposizioni tecnicamente imperfette o immature per un'immediata adozione nella loro attuale formulazione.
La mia autorità ha contribuito ai lavori della commissione scientifica, ma i nostri suggerimenti, prima e dopo la conclusione dei lavori stessi, sono stati solo parzialmente tenuti presente; comunque l'odierno testo è molto diverso da quello rispetto al quale abbiamo avuto la possibilità di dare il nostro contributo iniziale.
Mi soffermerò sui punti più direttamente rilevanti per il rapporto Italia-Europa, tralasciando in linea di principio quelli di più rilevanza 'domestica', sui quali resto comunque a disposizione per ogni utile suggerimento, ad esempio quelli riguardanti la *vexata quaestio* del trattamento economico del personale del Garante.
Per iniziare, non è condivisibile il preambolo della relazione illustrativa nella parte in cui si afferma che:

- il Codice ha perso la sua centralità, e che
- la massima parte delle sue disposizioni è da abrogare espressamente in quanto incompatibili con il Regolamento europeo (abrogazione che peraltro lo schema di decreto legislativo non opera, perché molte disposizioni vengono novellate, sia pure in chiave cosmetica).

Nel principale parere che l'Autorità europea che presiedo ha reso sul Regolamento europeo, abbiamo individuato cinque categorie di norme nazionali che continuano ad avere 'cittadinanza', nonostante l'ulteriore passo in avanti effettuato in chiave di armonizzazione[1]:

1. La prima categoria riguarda le norme che servono a dare piena funzionalità al Regolamento. Si pensi all'applicazione di sanzioni amministrative e a quelle riguardanti la costituzione di poteri dell'Autorità garante.

Vi sono, poi, altre categorie di norme che non rinvengo nello schema di decreto legislativo e che avrebbero dovuto invece rappresentare un'occasio-

ne per un 'tagliando' alla nostra disciplina, la quale, nel 2003, ha già beneficiato di una prima rivisitazione, ma che, sedici anni dopo, avrebbe richiesto una modifica anche alla luce dell'evoluzione tecnologica.

2. La seconda categoria riguarda le disposizioni che permettono di precisare o chiarire alcuni aspetti operativi del Regolamento, nei limiti consentiti da quest'ultimo. Lo stesso è avvenuto nel 1996 quando si è parlato, ad esempio, di consenso non ambiguo, categoria che il nostro ordinamento ha trovato di difficile collocazione, portando a preferire, sia nel 1996 che nel 2003, che si parlasse di consenso 'espresso'. A questo proposito, sebbene questa seconda categoria richieda più ampie riflessioni, oggi noi procediamo ad abolire alcune definizioni, ma potremmo trovare utile, per evitare 'incidenti' di questo tipo, lasciare il riferimento ad una delle categorie del consenso, appunto quello espresso.
3. La terza categoria include norme con le quali si possono introdurre obblighi di trattamento dei dati personali in deroga al principio del consenso, sempre nei limiti del Regolamento e con una particolare cautela qualora si deroghi all'esercizio dei diritti dell'interessato.
4. Vi sono poi norme, in particolari settori, rispetto alle quali l'Europa prende atto che sussiste meno armonizzazione e lascia quindi più spazio ai Paesi membri, poiché in ragione della diversità degli approcci culturali l'armonizzazione è meno intensa: rapporto di lavoro, giornalismo, dati sulla salute, ricerca scientifica, archivi storici e statistica.
5. Infine, vi è un'ultima categoria di norme, quelle non direttamente classificabili come di protezione dei dati personali, ma che, sebbene non coinvolte dal Regolamento stesso, richiedono un'attenzione da parte del legislatore in termini di raccordo normativo, ad esempio: e-government, banche dati regionali, proprietà intellettuale, e tutela del diritto d'autore.

Analisi dello schema di decreto legislativo

Parte I del Codice

L'articolo 1 dell'attuale Codice, giustamente, ed anticipando la *Carta dei diritti fondamentali* come annessa al Trattato di Lisbona, stabilisce che chiunque ha diritto alla protezione dei dati personali. Non si comprende perché questo riferimento debba essere oggi eliminato. Soprattutto, non si comprende per-

ché l'ulteriore norma del Codice (articolo 2), che cerca di individuare l'obiettivo di queste norme, vale a dire assicurare che il trattamento si svolga nel rispetto di tutti i diritti e di tutte le libertà fondamentali, ivi compreso quello della dignità umana, ponendo così un canone operativo ed interpretativo per il legislatore, per il Garante, per l'autorità giudiziaria e per i titolari del trattamento, debba essere sostituito con una norma priva di concreto senso giuridico, la quale si limiterebbe ad affermare che il trattamento dei dati personali deve avvenire nel rispetto dei diritti e delle libertà fondamentali. Di questo tipo di norma, al contrario di quella riscritta, non ve ne è reale necessità.
L'articolo 2 è di pari imprecisione, prescrivendo che il Codice contiene disposizioni di adeguamento al Regolamento. In realtà, vi sarebbero molteplici disposizioni che non sarebbero affatto collegate al Regolamento. Quindi, questa interpolazione avrebbe senso solo in riferimento alle disposizioni connesse con il Regolamento stesso.
Il Codice poi, benché novellato, continua a dare una centralità ai diritti dell'interessato per precisa scelta del legislatore delegante e delegato del 2001. Per tale ragione, la norma che individua nel Garante l'autorità di controllo (articolo 2-*bis*) dovrebbe posta in altra parte del testo.
L'articolo 2-*ter*, ed anche i successivi, contengono riferimenti a norme di carattere regolamentare, peraltro già presenti nel Codice. Ci si riferisce, cioè, alla possibilità che un regolamento, benché fonte secondaria, possa individuare un interesse pubblico rilevante oppure introdurre un obbligo normativo di trattare i dati.
Secondo costante giurisprudenza della Corte di giustizia, ogniqualvolta si fa riferimento ad una fonte secondaria, come un regolamento governativo o ministeriale, occorre (specie dopo il trattato di Lisbona e la Carta) una linea di maggiore cautela che porti, quantomeno nei casi di restrizioni all'esercizio dei diritti, a prevedere che la legge individui essa stessa i caratteri essenziali dell'eccezione o delle limitazioni introdotte dal regolamento. C'è, altrimenti, il rischio che, quantomeno per i trattamenti in ambito pubblico, sia l'amministrazione stessa che tratta i dati a prendere decisioni sullo spazio riservato agli interessati per l'esercizio dei loro diritti e che, attraverso il regolamento, l'amministrazione fissi essa stessa le regole del gioco, che dovrebbero essere invece determinate in chiave di terzietà.

L'articolo 2-*quater* contiene, a mio avviso, erronee modifiche nell'attuazione dell'articolo 12 del Codice. I codici di condotta non devono essere approvati da un'autorità. Questa, dovrebbe piuttosto verificarne la conformità al diritto vigente e promuoverli all'interno delle categorie interessate, non in chiave 'orizzontale' come lo schema prevede.
L'articolo 2-*quinquies* contiene, al comma 1, in materia di consenso dei minori, una duplicazione dell'articolo 8, paragrafo 1, del Regolamento, inutile e soprattutto non consentita dal Regolamento stesso.
Non si comprende poi il senso del comma 2, il riferimento alla chiarezza dell'informativa, anche perché tale informativa verrebbe diretta, in ragione del comma 1, a chi esercita la potestà genitoriale e quindi rispetto a questa varrebbero le norme generali per gli adulti. Il comma 2 dovrebbe, semmai, piuttosto riferirsi ai minori tra i 16 e i 18 anni. Inoltre, il riferimento al linguaggio dell'informatica andrebbe rapportato alle nuove tecnologie.
Gli articoli 2-*sexies* e 2-*septies* sollevano le medesime considerazioni, a proposito dell'espressione «nei casi previsti dalla legge», svolte in merito alle maggiori cautele che occorrono in riferimento alle fonti secondarie. Trattandosi qui di dati sensibili, le considerazioni stesse valgono in modo più incisivo.
Disposizioni come quelle dell'articolo 2-*septies*, che, richiamando il Regolamento europeo di per sé immediatamente operativo, sembrano attribuire al legislatore italiano la scelta di confermare quanto dice il Regolamento, fanno irritare l'Europa.
Rispetto alle misure di garanzia stabilite, o disposte dal Garante ai sensi dell'articolo 2-*septies*, si sottolinea l'opportunità di evidenziare meglio la loro complementarietà in relazione a quanto previsto dal Regolamento europeo, e con riferimento più specifico a particolari settori, non potendo essere le misure eccessivamente 'orizzontali'.
Si segnala il singolare riferimento ai contrassegni sui veicoli per persone portatrici di handicap, parzialmente inutile, considerando che il modello di contrassegno è stabilito a livello europeo.
L'articolo 2-*undecies*, sugli organi giudiziari, contiene sgrammaticature nel comma 2 per quanto riguarda «l'indipendenza dei procedimenti giudiziari». Inoltre, è stata eliminata impropriamente la necessità che, si possano ritenere effettuati per ragioni di giustizia i soli trattamenti di dati personali «*diretta-*

mente correlati alla trattazione giudiziaria di affari o di controversie, o che in materia di trattamento giuridico ed economico del personale di magistratura, hanno una *diretta* incidenza sulla funzione giurisdizionale».
In termini più generali, soprattutto a seguito dell'art. 16 del TFUE, la magistratura non è, in questi temi, una zona franca, anche in materia penale.
C'è, quindi, un problema di necessaria individuazione di un meccanismo indipendente di supervisione. Il D.Lgs. 51/2018, di attuazione della direttiva 680/2016, ha escluso che il Garante sia l'organo di supervisione per le autorità giudiziarie preposte a funzioni di prevenzione, accertamento e repressione dei reati. La scelta può essere legittima, ma in tal caso resta individuare chi svolga tale funzione indipendente. La mancanza di un organo di supervisione indipendente in questa materia, si tratti di quella penale come previsto in attuazione della predetta direttiva oppure delle ragioni di giustizia previste dall'articolo 2-*undieces*, rappresenta una violazione dell'articolo 8 della *Carta dei diritti fondamentali* e dell'articolo 16 TFUE. L'articolo, poi, contiene una specificazione rispetto all'attività del pubblico ministero, la quale è curiosa se si considera che il Regolamento si riferisce soltanto alle corti e non anche agli uffici della magistratura inquirente.
L'articolo 2-*duodecies*, relativo alle persone decedute, presenta una formulazione fragorosamente umoristica, non degna di essere inserita in un decreto legislativo quantomeno nella sua attuale stesura. Mi riferisco con sarcasmo al riferimento alla possibilità di modificare la volontà delle persone decedute, o a quella di esercitarne i diritti.
L'articolo 2-*terdecies* in materia di incaricati del trattamento contiene al comma 1 una specificazione che quasi intenerisce. Il titolare del trattamento è infatti l'organizzazione nel suo complesso, anziché una persona fisica, ed è quindi normale che esistano, in un'organizzazione pubblica o privata, diversi incaricati del trattamento.
Ci si chiede, poi, quale sia il senso (rispetto al Regolamento europeo che investe sull'*accountability*) del riferimento alle modalità più opportune per autorizzare gli incaricati del trattamento, di cui al comma 2.
Nell'articolo 2-*quinquiesdecies*, relativo ad accreditamento e certificazione, non è dato capire cosa possa accadere nel caso in cui il Garante decida di svolgere una funzione di accreditamento. Non si comprende in particolare se

in tal caso l'organismo nazionale, pur incaricato all'inizio, possa continuare a svolgere tali funzioni in parallelo al Garante stesso.
Nell'articolo *2-sexiesdecies* sui dati relativi a minori, si segnala che l'aggiunta della norma riferita alla sanzione penale deve essere piuttosto collocata nel capo riguardante le sanzioni.
Gravemente erronea in relazione all'articolo 52 dell'attuale Codice, in materia di pubblicazione dei dati identificativi riportati su sentenze giudiziarie, la soppressione delle parole «per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica».
La norma riguarda infatti la possibilità che sentenze, acquisibili in base ai codici di rito, civile e penale, una volta pubblicate online, su cd-rom o supporto cartaceo, al momento della pubblicazione non riportino le generalità e altri dati identificativi dell'interessato. Le sentenze devono tuttavia essere complete dei dati necessari. Non si può, attraverso questa modifica, gettare nel panico gli uffici giudiziari e far loro pensare che debbano oscurare i nomi dalle sentenze o che i giudici debbano cambiare modalità di scrittura dei provvedimenti.

Parte II del Codice
A partire dall'articolo 60 in poi delle norme novellate, occorre fare distinguere le proposte di modifica chirurgica di alcuni articoli del Codice rispetto a casi in cui interi articoli vengono riscritti senza sostanziali novità. Quest'ultima circostanza si verifica ad esempio per l'articolo 96 in materia di trattamento di dati personali relativi a studenti. Quest'approccio dà l'impressione che queste disposizioni conservino ancora una loro attualità, il che è controverso considerato il tempo trascorso, circa vent'anni dalla loro iniziale introduzione in Italia.
L'occasione del Regolamento europeo avrebbe dovuto stimolare invece una rivisitazione più sostanziale della disciplina, all'altezza dei tempi. Ciò, ad esempio, sarebbe auspicabile nel settore della scuola, della sanità e della ricerca scientifica (artt. 106, 110 e 110*bis*).
Un diverso approccio potrebbe portare oggi a un dimagrimento del decreto legislativo, posponendo a un momento successivo e più meditato l'intervento sulle disposizioni della parte II del Codice. Per le disposizioni della medesima parte II che fanno attualmente riferimento ad articoli che verrebbero abrogati o modificati si potrebbe inserire una tabella di corrispondenza.

Controllo a distanza dei lavoratori
L'articolo 9 dell'odierno schema di decreto legislativo, in riferimento all'articolo 114 del Codice, avrebbe richiesto un sostanziale intervento correttivo dell'articolo 4 della legge n. 300 del 1970, in riferimento al pasticcio normativo emerso con il Jobs Act.

Comunicazioni elettroniche
È particolarmente controversa, a parte la conservazione delle rilevanti definizioni, la disciplina proposta nell'articolo 11 dello schema di decreto legislativo contenente modifica della parte II titolo X del Codice. L'intero titolo sarà infatti oggetto a breve termine di una integrale rivisitazione per effetto del Regolamento e-Privacy.
Consolidati principi giurisprudenziali europei prescrivono che, quando una norma europea è in dirittura d'arrivo, gli Stati membri debbano astenersi dall'intervenire oppure legiferare nel senso prefigurato dal legislatore europeo. Il trilogo europeo, tuttavia, non si è ancora completato. La novellazione di queste norme comporterebbe anche la loro ri-notifica, per confermare all'Europa che esse costituiscono attuazione della direttiva e-Privacy, modificata nel 2009. Confuso sarebbe inoltre il messaggio che verrebbe dato ai titolari del trattamento.
Era invece, e rimane urgente, la necessità che il nostro Paese metta mano all'attuale inosservanza delle regole europee concernenti le comunicazioni commerciali indesiderate, l'uso indebito dei dati degli elenchi telefonici per finalità di comunicazione commerciale, l'uso non corretto del database unico degli operatori economici e infine, il manifesto, reiterato e pacifico malfunzionamento del registro delle opposizioni disciplinato nell'articolo 130 del Codice.

Segnalazioni dei cittadini al Garante
Possibili novità sembrano emergere nel rapporto tra cittadini e Garante, per effetto della modifica proposta all'articolo 144 del Codice in relazione alle segnalazioni. L'aggiunta dell''anche' potrebbe far pensare che non via sia obbligo di trattarle. La modifica deve essere oggetto quindi di una riflessione stilistica. Un ripensamento in proposito deve essere riflesso anche nell'elencazione dei compiti del Garante di cui all'articolo 154.

Requisiti per i componenti del Garante
L'articolo 153 del Codice viene legittimamente modificato proponendo che i componenti del Collegio assicurino «comprovata esperienza» invece che la «riconosciuta competenza» della formulazione dell'attuale Codice. Qualora si proceda in tal senso, non si comprende però perché i requisiti di nomina siano più «severi» per il segretario generale, cui si richiederebbe «elevata e comprovata qualificazione professionale» nell'articolo 156.
In secondo luogo, il nuovo articolo 153 richiederebbe il possesso di esperienze più specifiche nel settore della protezione dei dati personali: anche in questo caso, il riferimento all'informatica andrebbe invece correlato formalmente alle nuove tecnologie.
La durata settennale del mandato dei componenti del Garante è conforme al Regolamento, ma potrebbe essere oggetto di una riflessione alla luce dell'esperienza degli ultimi vent'anni in Europa e in Italia.
Parimenti, potrebbe essere meglio affinata la disciplina dell'imparzialità richiesta dopo la cessazione del mandato presso il Garante dall'articolo 153 comma 8, che potrebbe risultare debole in rapporto a quanto previsto dall'articolo 54, lett. f), del Regolamento europeo. La scelta di lasciare alla stessa Autorità, come è stato nel caso di quella che presiedo, il compito di individuare in dettaglio alcuni obblighi deontologici, potrebbe essere di ausilio.

Potere di agire in giudizio del Garante
La previsione per il Garante di agire in giudizio nei confronti di un titolare o del responsabile del trattamento (articolo 154-*ter*) è il risultato di un 'copia e incolla' del Regolamento, non accompagnato da una piena riflessione sulla sua applicazione concreta. La funzione connaturata al Garante non è quella di citare in giudizio i titolari del trattamento, ma, *in primis* di intervenire per esercitare i suoi poteri, difendersi se i suoi provvedimenti sono impugnati, se vi sono azioni legali di cittadini o di titolari del trattamento che non si sono rivolti al Garante, il quale, in caso di interesse pubblico, il Garante si potrebbe costituire *ad adiuvandum*. La possibilità che il Garante trascini soggetti in tribunale, pur se prevista dal Regolamento, va plasmata in modo da renderla consona al nostro ordinamento. Il sistema inserito nel Regolamento proviene dall'ordinamento irlandese, dove fino ad ora l'Autorità, avendo le armi spun-

tate, si è vista costretta a citare in corte i soggetti interessati per far dichiarare l'inosservanza di una disposizione. I poteri del Garante saranno tuttavia più forti, quindi una formulazione diversa può esser fatta.

Sanzioni amministrative
L'articolo 166, comma 5, non è perfettamente formulato in relazione all'eventualità che la sanzione amministrativa sia contestata da parte di organi preposti a controlli di vario tipo, ad esempio come previsti cui all'articolo 17 della legge 24 novembre 1981, n. 689.

Sanzioni penali
Trattamento illecito di dati personali
Il delitto previsto e punito dall'articolo 167 del Codice Privacy non presenta profili di incompatibilità con il Regolamento generale. All'opposto, esso ha presentato e presenta uno scopo generale preventivo rivelatosi molto utile nella prassi.
Nello schema di decreto, la nuova formulazione coprirebbe i trattamenti dei dati personali effettuati in violazione dei seguenti articoli:
- dati relativi al traffico (art. 123 Codice Privacy novellato);
- dati relativi all'ubicazione (art. 126 Codice Privacy novellato);
- comunicazioni indesiderate (art. 130 Codice Privacy novellato).

Restano profili di criticità dell'intervento, se si considera che l'intervento determina un'abrogazione parziale sotto un duplice aspetto:
1. abrogazione parziale della norma, nella parte relativa alle condotte di trattamento poste in essere senza il consenso (art. 23);
2. abrogazione parziale della norma in tutti i casi nei quali vi è la coscienza e volontà di trattare dati personali al fine di danneggiare terzi soggetti. Difatti, la previsione del dolo specifico di profitto (vantaggio o altra utilità) esclude lo scopo di danneggiare altri soggetti, prima presenti.

In particolare, quest'ultima circostanza fa sì che il testo come proposto rappresenti un'involuzione normativa, particolarmente inadeguata se si considera il contesto storico perché non idonea ad inglobare al suo interno i fenomeni fortemente lesivi dei diritti alla personalità sorretti dalla coscienza e volontà di trattare dati personali al fine di danneggiare terzi soggetti (si pensi al *revenge porn*).

Ne bis in idem

La sostanziale depenalizzazione di molte fattispecie punite nell'art. 167 non può trovare giustificazione nel considerando 149 del Regolamento generale[2]. Quest'ultimo, non dispone in alcun modo che il delitto di trattamento illecito debba essere abrogato o che non possa essere prevista una condotta che sia punita sia con la pena della reclusione, sia con la sanzione amministrativa.
Il recente orientamento della Corte di giustizia sul rapporto tra sanzione penale e quella amministrativa non è contrario alla sussistenza del *ne bis in idem*; il problema, poi, si pone solo quando il giudice ritiene che la sanzione amministrativa irrogata «assuma natura penale» e solo quando vi sia un *idem factum*[3].
La Corte di giustizia è di recente intervenuta nuovamente sul delicato problema delle limitazioni applicate al principio del *ne bis in idem*[4]. La Corte ha riconosciuto agli stati membri la facoltà di prevedere comunque il doppio binario, penale e amministrativo, per reprimere aspetti diversi di un medesimo fatto, quando «[...] tali procedimenti e sanzioni perseguano, ai fini del conseguimento di un simile obiettivo, scopi complementari riguardanti, eventualmente, aspetti diversi del medesimo comportamento illecito interessato, circostanza che spetta al Giudice del rinvio verificare».
Il doppio binario deve pur sempre garantire il rispetto del principio di proporzionalità ed assicurare che la severità dell'insieme delle sanzioni inflitte non ecceda la gravità del reato accertato.

Comunicazione, diffusione illecita e acquisizione fraudolenta di dati personali

A prescindere dal ricorso nuovamente al solo dolo specifico di profitto, non si comprende il riferimento, per una condotta grave come quella della diffusione, all'elemento costitutivo del reato caratterizzato dal fatto che i dati personali particolari (sensibili e giudiziari) trattati in violazione e fuori dai limiti previsti dalla legge per trattamenti di interesse pubblico (art. 2-*ter*) o necessari per motivi di interesse pubblico rilevante (art. 2-*sexies*) devono essere «riferibili ad un rilevante numero di persone».
Il ricorso a un criterio così indeterminato rischia di violare gravemente il principio di tassatività della norma penale. Piuttosto che a criterio quantita-

tivo, sarebbe stato più opportuno fare riferimento al solo criterio qualitativo del dato personale (sensibile e giudiziario) e collegare la condotta alla diffusione dei dati personali sensibili e giudiziari a prescindere dalla presenza di un rilevante numero di soggetti.
Si raccomanda, pertanto, un ulteriore processo di riflessione sulle norme in oggetto.

Affari pregressi
La norma che, all'articolo 19 del decreto, prevede la sostanziale cestinazione di tutti gli affari pregressi, dovrebbe essere più cautamente definita: occorrerebbe escludere i fatti di cui emerga già la gravità per evitare un condono occulto di quanto accaduto ed andrebbe meglio chiarito cosa si intende con il «di cui si è già esaurito l'esame» del comma 2.

Codici deontologici
La previsione dell'articolo 20 del decreto pare poi impraticabile. È proposta una clausola capestro che, entro l'irrealistico termine di sei mesi, potrebbe portare alla caducazione di due codici deontologici, in caso di inerzia delle categorie interessate. Queste ultime potrebbero avere interesse a sottrarsi alle previsioni attualmente integrative del codice, non formulando alcuna proposta entro sei mesi, o avanzando proposte che non possono essere approvate nei successivi sei mesi. La previsione di una revisione dei due codici è condivisibile, ma non dovrebbe essere formulata in questi termini.
È imperfetta anche la previsione relativa alla sorte degli altri codici deontologici, per i quali si pone un problema di aggiornamento e di verifica che va oltre il Regolamento europeo, ad esempio in materia di giornalismo. Inoltre, mentre è in principio giusta la loro revisione da parte delle categorie interessate, appare discutibile un intervento *ex officio* dell'Autorità che individui le norme incompatibili con il Regolamento. Un simile esercizio andrebbe fatto con le categorie interessate, trattandosi di codici deontologici.
In secondo luogo, è realmente necessario? Va precisato che, come fonti secondarie atipiche, esse varrebbero nella misura in cui restino compatibili con il Regolamento.

Disposizioni transitorie e finali

Maggiore evidenza è necessaria per il giusto principio contenuto nell'articolo 22, comma 10 del decreto, in riferimento alle micro piccole e medie imprese, che andrebbe esteso anche gli artigiani. In altre parole, il principio andrebbe collocato al di fuori delle norme puramente transitorie e finali.
Da ultimo, l'articolo 24 comma 1 risulta mal posto in quanto nessuna disposizione del decreto sostituisce le sanzioni penali con sanzioni amministrative.

Osservazioni finali

In relazione allo schema di decreto legislativo all'esame attuale, si auspica:

- l'introduzione di riferimenti più marcati alla necessità di rendere concreto il principio di *scalability* sotteso al Regolamento europeo, non potendosi trattare le piccole e medie entità al pari dei giganti dell'informatica. In questo senso, si auspica il ripristino dell'articolo 2 del Codice, che conteneva appunto alcuni principi cardine ai fini dell'applicazione in concreto del Regolamento, in tema di *scalability*, semplificazione e sburocratizzazione;
- il rafforzamento di incentivi a ricerca, innovazione, formazione professionale e start-up, anche attraverso, perché no, eventuali interventi di defiscalizzazione selettiva. La riforma intende del resto soffermarsi su ciò che è realmente necessario in termini di garanzie, eliminando ad esempio alcuni adempimenti formali che non si sono rivelati più necessari, come ad esempio la notificazione stessa. Occorre un lavoro che renda le norme più flessibili e adattabili, attraverso una *co-regulation* che da un lato continui a valorizzare l'esperienza dei codici deontologici, e dall'altro quella di misure complementari, e certo non sostitutive e non integrative, che potranno provenire dall'Autorità perché, ad esempio, non è possibile prevedere come il trattamento dei dati genetici e biometrici possa evolvere di qui ad alcuni anni;
- il mantenimento del Codice come impalcatura non di tutte le norme, ma di quelle più rilevanti in materia di tutela rispetto al trattamento dei dati personali;
- l'inclusione del testo del Regolamento europeo e del futuro Regolamento e-Privacy in allegato al codice.

In conclusione, si suggerisce alla Commissione di formulare parere positivo in quanto è necessario che un testo, sia pure in versione più ristretta, sia

adottato al più presto. In particolare, è necessario far partire un primo intervento che consenta al Garante di dotarsi degli strumenti necessari di cui ha bisogno, anche in termini di rafforzamento delle risorse umane e finanziarie[5]. Ciò è però condizionato all'adozione di una serie di modifiche che, a mio avviso, sono necessarie.
Sottolineerei l'importanza di un approccio non *partisan*, come del resto già accaduto nel 1996, nel 2001 e nel 2003, come pure in occasione dell'approvazione del pacchetto europeo di riforma, che ha visto il voto sostanzialmente unanime dei gruppi politici a livello italiano e europeo.
Consequenzialmente, è auspicabile che il nuovo governo si è impegnato ad adottare decreti correttivi per la riscrittura integrale e più armonica del Codice, utilizzando la già esistente previsione di delega, e includendovi anche il D.Lgs. 51/2018.
I lavori preparatori essere completati entro il mese di febbraio, in modo da poter includere anche il Regolamento e-Privacy e resto a disposizione per ogni contributo a riguardo.

Da ultimo, in riferimento alle brevi questioni poste oggi nel dibattito in Commissione, osservo in conclusione quanto segue.

Conservazione dei dati
La soluzione italiana soffre di un'insanabile e manifesta contrarietà rispetto al quadro europeo. La violazione dei princìpi è fragorosa e sonora. Il termine di sei anni per la conservazione dei dati di traffico non è contemplato nemmeno nei Paesi più marcatamente totalitari e non ha eguali in nessuno dei Paesi democratici. La Corte di giustizia ha fissato un limite assai più breve, e che l'ordinamento tedesco ha individuato in poche settimane. La Convenzione di Budapest prevede che ci possano essere tecniche sostitutive, come ad esempio il *freezing* dei dati. L'esperienza dimostra poi che l'investigazione si basa sempre di più su altre tecniche di indagine, ad esempio i *trojan horses.* Nel 95% dei casi, i dati richiesti riguardano gli ultimi sei mesi. Il fatto poi che tale modifica sia stata operata in un atto italiano che serviva a porre rimedio a eventuali infrazioni, rappresenta una rilevante contraddizione.

Piattaforma digitale nazionale dati
È condivisibile l'osservazione del Garante rispetto al tema di tale banca dati. La vecchia tendenza che ha interessato il Ministero dell'Interno con l'anagrafe della popolazione, poi l'amministrazione finanziaria con le banche dati dell'anagrafe tributaria, e ora ISTAT, a creare patrimoni informativi *multi-purposes*, ingenera problemi dal punto di vista del principio della compatibilità dello scopo, nonostante l'importante obiettivo che si vuole perseguire. Altro problema è se la soluzione prefigurata in quel testo abbia una sua concretezza. Si tratta probabilmente di un tema difficile da affrontare con questo primo decreto, ma potrebbe essere differito agli altri decreti correttivi previsti dall'odierna delega.

Età dei minori
Il mio personale avviso è quello di non modificare la soglia dei 16 anni, prevista dal Regolamento.

Minimo edittale
Si pone il problema del raccordo con la legge n. 689, nella quale è insito un rapporto di uno a sei tra la sanzione minima e quella massima. Cosicché, in caso di oblazione, il doppio del minimo corrisponde a un terzo del massimo. In altri Stati membri non si riscontra lo stesso approccio. Il tema è da approfondire.

Intervento al convegno
La legge delega sul coordinamento tra il Codice Privacy e il Regolamento UE 679/2016
https://www.youtube.com/watch?v=sTnqi5zsH3w&feature=youtu.be

Commissioni speciali congiunte Senato-Camera: audizioni - intervento del professor Buttarelli alla 3° ora e diciannove minuti
http://webtv.senato.it/4621?video_evento=91

NOTE

[1] *Opinion of the European Data Protection Supervisor on the data protection reform package*, Brussels, 7 March 2012, https://www.eerstekamer.nl/eu/documenteu/_opinion_of_the_european_data/f=/vixnjsqhwggb.pdf.

[2] Regolamento generale, considerando n. 149: «Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del *ne bis in idem* quale interpretato dalla Corte di giustizia».

[3] In tema di *ne bis in idem* e doppio binario in materia tributaria è legittimo sanzionare la società e punire il rappresentante legale per lo stesso fatto; Corte di giustizia UE, IV sezione, sentenza 5 aprile 2017, Orsi (C-217/15) e Baldetti (C-350/15).

[4] La sentenza verte sulla corretta interpretazione dell'art. 50 della Carta dei diritti fondamentali dell'Unione Europea, letto alla luce dell'art. 4, del protocollo n. 7 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950. Corte di giustizia UE, Grande Sezione, sentenza 20 marzo 2018, causa C-524/15.

[5] La media europea è di almeno il 25%, senza contare le modifiche apportate ai disegni di legge ancora in fase di adozione nei diversi Stati membri.

* Giovanni Buttarelli: Garante europeo per la protezione dei dati personali dal 2014, ha ricoperto, nella stessa sede, la carica di Garante aggiunto dal 2009 al 2014. È inoltre magistrato della Cassazione in servizio dal 1986. Buttarelli è stato inoltre segretario generale del Garante per la protezione dei dati personali dal 1997 al 2009. Dal 2016 è professore di Informatica giuridica presso la Facoltà di Giurisprudenza della LUISS 'Guido Carli' di Roma.

LA PROTEZIONE DEI DATI PERSONALI: DAL D.LGS. 196/2003 AL REGOLAMENTO UE 679/2016

Gianluigi Ciacci*

Dal 'right to privacy' al diritto alla protezione dei dati personali

Storicamente si inizia a parlare di questo interessante tema alla fine dell'Ottocento negli Stati Uniti in occasione della pubblicazione di un saggio (*The Right to Privacy*), sull'*Harvard Law Review* del 15 dicembre 1890, ad opera di due giuristi, Samuel D. Warren e Louis D. Brandeis: il diritto alla riservatezza venne inteso in origine come «right to be let alone», cioè «diritto di essere lasciato solo» (e quindi di escludere gli altri dalla propria sfera privata, in cui si facevano rientrare tutti quei valori dell'individuo che devono essere protetti da ingerenze esterne), quale contrappeso e limite dell'antitetico diritto di informare ed essere informato.

Negli anni successivi il concetto venne sviluppato in stretto collegamento con il diritto di informazione e l'evolversi della tecnologia: in particolare quando l'avvento dei computer, e la loro esponenziale diffusione, iniziò a realizzare la nascita di una nuova forma di potere, il c.d. 'potere informatico'. Potere che permette di conoscere ogni minimo aspetto della nostra vita privata, raccogliendo informazioni spesso a nostra insaputa, e quindi a far avvertire sempre più sentita l'esigenza di proteggersi dalla crescente, e tecnologicamente evoluta, ingerenza nella propria intimità.

Tale esigenza venne soddisfatta con due diverse modalità: da una parte, ad opera della dottrina giuridica, ampliando la portata del diritto alla riservatezza, non più 'passivo', finalizzato ad escludere gli altri, ma inteso come un diritto 'attivo', di controllare l'uso che altri fanno dei dati del soggetto interessato; dall'altra, emanando una serie di normative specifiche volte a disciplinare la delicata realtà, e quindi nella specie in materia di banche di dati personali.

Successivamente è ancora l'evoluzione tecnologica a far nuovamente mutare ambito e portata del diritto alla riservatezza: questo a causa dell'avvento del personal computer, che portò al passaggio dall'informatica accentrata, per pochi, all'informatica distribuita, per molti. E ancora di più quando nacque e si diffuse la 'Rete delle Reti' che, oltre a far diventare l'uso del computer veramente di massa, sollevò ulteriori e complicati problemi di protezione delle informazioni relative agli individui. Rendendo di conseguenza necessario giungere a una tutela che prescindesse dalla 'riservatezza', dalla 'delicatezza', dalla 'sensibilità' dei dati personali: e addirittura dalla stessa volontà di protezione della persona a cui l'informazione si riferisce, o dalla consapevolezza della sua necessità. Infatti le più recenti normative in materia non parlano più di 'diritto alla riservatezza', di privacy, o almeno non solo, ma di *diritto alla protezione dei dati personali*. Nuova impostazione che si concretizza con l'ultima generazione di leggi sull'importante argomento, che in Europa nascono dalla pubblicazione della direttiva 95/46/CE, e quindi dalla obbligatorietà del suo recepimento: realizzato nel nostro Paese dapprima con la legge 31 dicembre 1996, n. 675, e quindi con il decreto legislativo 30 giugno 2003, n. 196, dettato per correggere e semplificare tale legge.
Ultimo passaggio di questo racconto storico della complessa (ma affascinante) materia nasce non tanto dalla necessità di mutare nuovamente il modo di concepire la tutela della persona nei confronti dell'informazione, dell'informatica (che certo ha subito ulteriori sviluppi ed evoluzioni, si pensi all'enorme diffusione dei social network), sempre basata sul più ampio concetto di 'diritto alla protezione dei dati personali', ma da diverse considerazioni. Infatti, innanzitutto si rileva la difficoltà della disciplina normativa sulla materia, di non facile lettura e ricca di obblighi spesso avvertiti da chi li deve rispettare come inutili, e dunque percepita come ennesima espressione di una burocrazia vessatoria e come ennesimo impedimento allo sviluppo delle proprie attività; poi, a fronte della repentina evoluzione e diffusione dell'informatica e della telematica, oggi sempre più... *friendly* (cioè facile, economica, bella, e ricca di contenuti e possibilità, quindi alla portata di tutti) e di irrinunciabile interesse, nel nostro Paese si deve constatare una quasi totale assenza della cultura delle nuove tecnologie;

infine, è proprio l'evoluzione della tecnologia, il passaggio all'Internet 2.0, e il conseguente mutamento sociale realizzato dall'uso massivo della Rete e dei suoi servizi, a rendere necessario un aggiornamento della disciplina sulla protezione dei dati personali (si pensi che quando vennero emanate le prime leggi negli anni '90 non esistevano social network, tablet e app, e solo una minima parte della popolazione europea, intorno all'1%, usava Internet: in Italia erano circa 80.000, mentre oggi sono intorno ai 40 milioni). Tutto ciò, insieme alle mancanze o difetti dei testi normativi pubblicati nel settore, ha portato al Regolamento europeo 27 aprile 2016, n. 679: che ha come principale *mission* quella di rendere efficace la disciplina della protezione dei dati personali.
Applicabile direttamente in tutti i Paesi europei, tale fonte si propone dunque di assicurare un livello coerente di protezione, di garantire certezza e trasparenza nel trattamento delle informazioni, di offrire diritti azionabili e obblighi omogenei tra gli Stati, di assicurare un controllo e una cooperazione efficaci tra le autorità competenti. Finalità che cerca di raggiungere attraverso il rafforzamento dei diritti degli interessati, a fronte di una semplificazione degli adempimenti incombenti sui titolari del trattamento.
Per quanto riguarda l'*ambito di applicazione* della normativa comunitaria, secondo il criterio «materiale» stabilito dall'art. 2 la disciplina deve essere rispettata nel caso di trattamento interamente o parzialmente automatizzato di dati personali di persone fisiche. Mentre non si applica ai trattamenti effettuati dalle autorità per scopi di prevenzione, indagine, repressione di reati, sicurezza pubblica e politica estera, e ai trattamenti posti in essere da persona fisica per soli scopi esclusivamente personali.
Invece, secondo il criterio «territoriale» (art. 3), la nuova disciplina, rispetto all'attuale, è maggiormente pervasiva: questo in particolare perché al già presente principio di 'stabilimento' (in virtù del quale la normativa deve essere rispettata da chi tratta dati personali 'stabilito' all'interno dell'Unione) si aggiunge quello del *target*, secondo cui il Regolamento europeo si applica a chiunque utilizzi dati personali di cittadini UE da qualunque posto del mondo (nel caso in cui la finalità di tale utilizzo riguardi il monitoraggio del loro comportamento, oppure l'offerta di beni o la prestazione di servizi). Da ciò deriva un forte ampliamento del campo di applicazione della

normativa, strumentale a evitare la sua elusione a causa della nazionalità extra UE del titolare.
Con riferimento agli *obblighi* in capo a chi utilizza le informazioni, in generale cambia proprio l'impostazione dell'attività che si deve porre in essere per rispettare la disciplina in materia: non si deve più prestare attenzione solo ai singoli adempimenti da realizzare, nella specifica attività di trattamento della particolare tipologia di dati personali, ma si deve prendere in considerazione la complessiva realtà legata all'utilizzo delle informazioni personali nella propria struttura. Impostazione che si concretizza nei principi di *privacy by design* e *privacy by default*, nella valutazione di impatto privacy (non più limitata ai soli aspetti relativi alla sicurezza, ma estesa all'intera attività che viene realizzata sui dati), nella tenuta del Registro dei trattamenti, nella nomina del *Data Protection Officer* (DPO), cioè il 'responsabile della protezione dei dati personali', figura che ha suscitato grande interesse e sulla quale sono state riportate dai primi commentatori al Regolamento molte inesattezze), nel principio di *accountability*, cioè di 'responsabilizzazione': obbligo quest'ultimo che consiste, come già detto, nella predisposizione, da parte del titolare, di misure idonee ad esaminare preventivamente l'effetto che le attività svolte esercitano sul trattamento dei dati posto in essere, da cui poi far derivare gli specifici adempimenti, nella nuova versione stabilita nel Regolamento. Di questi, molti vengono ripresi dall'attuale disciplina, mentre si aggiungono, tra gli altri, l'obbligo di notificare eventuali *data breach* sia all'Autorità che agli interessati le cui informazioni abbiano subito un danno, o il potenziamento delle cautele nel caso di trasferimento di dati all'estero, o ancora la maggiore determinazione dell'obbligo del consenso e l'attenzione alla comprensibilità di quello di informativa.
Con riferimento alla nuova disciplina relativa ai *diritti dell'interessato*, viene ribadita proprio l'importanza dell'informativa (artt. 13 e 14), rispetto alla quale aumenta l'attenzione per la sua efficacia; si rafforza poi il consenso in caso di minore età, e si introduce la facoltà di richiedere la limitazione del trattamento ad alcune delle finalità perseguite dal titolare; l'art. 20 sancisce un nuovo diritto alla portabilità dei dati e, rispetto al c.d. diritto all'oblio (cioè il diritto alla cancellazione dei dati che non hanno più necessità o motivo di essere trattati), l'art. 17 estende la sua portata e il suo ambito di applicazio-

ne, seppur condizionato; infine, si stabiliscono procedure che consentono una maggiore facilità nel rivolgersi all'Autorità garante, permettendo quindi una più incisiva possibilità di tutela per l'interessato.
A tale proposito la figura del 'Garante per la protezione dei dati personali' viene confermata, e anzi potenziata, anche attraverso la previsione di un nuovo 'Comitato europeo della protezione dei dati personali': realtà che unisce le varie autorità dei diversi Paesi membri, imponendo una cooperazione fra le stesse, anche in occasione di eventuali attività di controllo congiunte. In tale ambito si introduce poi il meccanismo dello 'sportello unico', grazie al quale è possibile rivolgersi al Garante italiano anche per gestire pratiche negli altri Paesi UE.
Con riferimento alle *sanzioni*, il Regolamento rivede sostanzialmente la disciplina precedente, che viene semplificata ad iniziare dai parametri di commisurazione delle stesse: i nuovi importi non sono più legati ad una misura minima (scelta che permetterà una maggiore equità nelle situazioni in cui l'illecito rivesta una lieve importanza), ma allo stesso tempo si prevede un sensibile aumento del parametro massimo. Così, come visto, si stabiliscono due categorie di conseguenze pecuniarie: fino a 10 milioni di euro o, se impresa, fino al 2% del fatturato totale annuo dell'esercizio precedente, per alcuni tipi di inadempimenti; fino a 20 milioni di euro o, se impresa, fino al 4% del fatturato totale annuo dell'esercizio precedente, in ipotesi di violazioni più importanti.
Già dalla lettura di queste brevi note si può comprendere come l'applicazione del GDPR europeo richiede un sostanziale cambiamento nelle pratiche di trattamento: questo in particolare per quelle strutture che non avevano già implementato la precedente disciplina, che raggiungeranno così un livello effettivo di tutela dei dati personali utilizzati nella propria attività. Mentre per chi era già 'in regola' l'attività necessaria per conseguire lo stesso risultato sarà innanzitutto quella di adattare le procedure in essere, realizzate sulla base del D.Lgs. 196/2003, al Regolamento, in particolare nell'ottica di renderli 'efficaci', e quindi la protezione funzionante; andranno poi posti in essere i nuovi adempimenti, la cui principale difficoltà sarà soprattutto quella di allinearsi con il diverso approccio di sistema della disciplina europea.

Intervento al convegno
La protezione dei dati personali: dal D.Lgs. 196/2003 al Regolamento UE 679/2016

https://www.youtube.com/watch?v=m3WdxKdYg1A&feature=youtu.be

Commissioni speciali congiunte Senato-Camera: audizioni - intervento del professor Ciacci alla 4° ora e 58 minuti

http://webtv.senato.it/4621?video_evento=91

Link alle slide
gianluigi ciacci - la protezione dei dati personali

* Gianluigi Ciacci: docente di Informatica giuridica e di Diritto civile dell'informatica presso la Facoltà di Giurisprudenza della LUISS 'Guido Carli' di Roma. Dottore di ricerca presso l'Università degli Studi di Roma 'La Sapienza' in Informatica giuridica e Diritto dell'informatica. Avvocato in Roma specializzato in diritto delle nuove tecnologie.

LA RIVOLUZIONE GDPR

Giovanna Bianchi Clerici*

Il GDPR si propone di affrontare la sfida del bilanciamento tra le esigenze contrapposte della libertà di circolazione dei dati nell'odierno contesto digitale *infra* ed *extra* europeo e della contestuale massima tutela della loro protezione da una indiscriminata diffusione, che possa ledere i «diritti e le libertà delle persone fisiche».
A oltre vent'anni dal varo della prima direttiva europea sulla protezione dei dati personali (95/46/CE) – vent'anni in cui lo scenario tecnologico e sociale è mutato a una velocità irresistibile –, il GDPR è frutto della raggiunta consapevolezza dell'impossibilità per il legislatore di normare *a priori* nel dettaglio ogni futuribile fenomeno e invenzione. Occorreva una nuova prospettiva per disciplinare efficacemente e coniugare in maniera credibile l'interazione tra le nuove tecnologie, e la loro sempre più sofisticata capacità di conservazione e analisi di massa dei dati (il mitologico fenomeno dei *Big Data*) con il diritto fondamentale del singolo alla protezione delle informazioni sulla sua persona. Non era più possibile ridursi all'elencazione di prescrizioni tassative e indifferentemente valide per ogni tipo di trattamento indipendentemente dalla specifica tecnologia impiegata. Il GDPR procede per obiettivi: *in primis* il riconoscimento e il rispetto del diritto degli interessati, ma anche in questo caso occorre ampliare la visuale rispetto al passato. La nuova normativa è votata non più alla mera proclamazione teorica della tutela di un diritto del soggetto, ma punta alla disciplina organica dell'inevitabile impatto di un trattamento direttamente sulla persona.
Il Regolamento 2016/679/UE, inoltre, è direttamente applicabile in tutto il territorio dell'Unione. Obiettivo dichiarato: uniformità delle regole e coeren-

za nella loro applicazione in tutti gli Stati membri. Affinché i dati liberamente circolanti possano trovare identica garanzia ovunque, bisognava porre fine, all'interno dell'UE, al mosaico di normative diverse ed anche variabilmente stringenti. Non solo, il GDPR ha l'ambizione d'imporre la supremazia del diritto europeo sull'intero mondo digitale, senza confini. Il Regolamento si applica infatti a tutti coloro, anche stabiliti al di fuori dell'Unione, che trattano dati personali di cittadini europei.
Siamo stati abituati a pensare che la protezione dei dati personali si sostanziasse irriducibilmente nella trasparenza informativa e nel consenso dell'interessato, ma tra le basi giuridiche che rendono lecito il trattamento (elencate all'art. 6), il GDPR riconosce per la prima volta anche il legittimo interesse del titolare all'effettuazione di un trattamento, anche in assenza del previo consenso dell'interessato. Il titolare può giovarsi di tale base giuridica qualora, dopo un'attenta valutazione e operato il bilanciamento fra il proprio interesse (evidentemente economico od economicistico) al trattamento ed il diritto dell'interessato alla protezione dei propri dati, ritiene che il primo prevalga sul secondo, anche alla luce delle 'ragionevoli aspettative' dell'interessato medesimo in ragione del suo rapporto col titolare. In tale contesto, è meritevole di particolare attenzione il considerando 47, che giunge ad ammettere il legittimo interesse come valida base giuridica anche per il trattamento di dati personali per finalità di marketing diretto.
Questa è una delle più evidenti esemplificazioni del concetto di responsabilizzazione – *accountability* –, su cui poggia il GDPR, ed anche di quello dell'attenzione alla protezione dei dati personali fin dalla progettazione del trattamento – *privacy by design* –, intesa proprio come pianificazione dinamica, e non di tipo statico e comune a tutte le categorie di titolari. Si tratta di un approccio sostanzialista/realista e di un atteggiamento pro-positivo da parte del legislatore. A differenza di quanto abbiamo fatto fino ad oggi, con l'applicazione pedissequa delle regole stabilite dal Codice e la 'spunta' delle prescrizioni e linee guida imposte dal Garante, la nuova normativa impone ai titolari/responsabili un comportamento maturo e pro-attivo. Si passa da un regime autorizzatorio dall'alto a uno di responsabilizzazione dal basso: è un cambiamento culturale, in primo luogo.

All'operatività del mercato, in cui il titolare stabilisce finalità e modalità del trattamento a seconda di ciò che ritiene più adeguato al perseguimento del proprio utile, deve poter corrispondere l'operatività delle norme, per promuovere una nuova cultura dei dati: ove questi non hanno soltanto un mero valore economico, ma diventano anche elemento discriminante di competitività che distingue il titolare virtuoso dal titolare negligente, anche agli occhi dell'interessato che valuta come un valore il grado di attenzione del titolare alla protezione dei propri dati personali.
Si veda, ad esempio, come, con particolare riferimento ai trattamenti automatizzati – compresa la profilazione –, la logica di approccio dovrà essere preventiva e predisposta su misura. Poiché nessuno conosce ed ha interesse per il trattamento tanto quanto il titolare, la valutazione del rischio specifico è in capo a questo, chiamato a esaminare preventivamente gli effetti e le conseguenze del trattamento che pone in essere, progettandone fin dall'inizio le caratteristiche e valutandone l'impatto sui diritti e le libertà dell'interessato, in relazione all'obbligo di minimizzare il più possibile l'utilizzo di dati personali, anche grazie alle impostazioni predefinite (*privacy by default*). A maggiori libertà corrispondono maggiori responsabilità. Il Garante 'balia' va in soffitta: la valutazione in concreto del rischio spetta al titolare e il Garante diventa piuttosto il 'valutatore della sua valutazione'.
Ad alleviare il prevedibile scoramento di coloro che debbono nell'immediato fare i conti con la nuova normativa, vi è il fatto che sono confermati alcuni principi da tempo consolidati nell'ordinamento nazionale, a partire dalla garanzia del consenso specifico ed informato. Altri strumenti risulteranno di utilità: la compilazione del registro dei trattamenti, i modelli di nomina dei responsabili, la consultazione delle linee guida del Gruppo *ex* art. 29 e delle FAQ già pubblicate, la possibilità di consultare l'Autorità, il coinvolgimento delle associazioni di categoria.
Inoltre, il D.Lgs. 101/2018, adottato dopo un lungo e travagliato *iter*, prevede che il Garante promuova per le micro, piccole e medie imprese modalità semplificate di adempimento degli obblighi del titolare del trattamento, oltre a farne salvi per un periodo transitorio i provvedimenti adottati in passato, ove non incompatibili con il GDPR, e le autorizzazioni, oggetto di un successivo riesame. Non dovrebbero invece esservi modifiche alle attuali

disposizioni concernenti le comunicazioni elettroniche, in attesa del nuovo Regolamento c.d. e-Privacy, che detterà tutta la disciplina speciale (quindi prevalente sul GDPR) in questo settore, compresi profilazione e marketing, e ora in Consiglio dell'UE per la fase emendativa.
Il Regolamento impatta in modo significativo anche sul ruolo dell'Autorità, che diviene a tutti gli effetti organismo vigilante sull'applicazione diretta delle norme del GDPR. Ciò non significa una diminuzione dei compiti e poteri dell'Autorità. Al contrario: tra gli altri, fanno parte dei doveri del Garante l'adozione di clausole contrattuali standard per i contratti di designazione di un responsabile da parte del titolare; l'elencazione dei trattamenti soggetti o non soggetti al *Data Protection Impact Assessment* (DPIA) in quanto ad elevato rischio per i diritti e le libertà delle persone fisiche; è quindi prevista la consultazione preventiva del Garante nel caso in cui il titolare/responsabile, al termine della propria valutazione d'impatto, ritenga possa permanere un elevato rischio residuo (uno dei rari casi in cui il Garante, sollecitato, scende ad esaminare il dettaglio concreto dei trattamenti).
Tra i compiti più delicati, vi è anche l'elaborazione di codici di condotta, vincolanti per chi vi aderisca. Il Regolamento ripone molto affidamento su questi strumenti di auto-regolamentazione e co-regolazione (differenti e meno solenni dei Codici deontologici previsti dal nostro ordinamento), in quanto ritenuti prova di *compliance* e sufficienti garanzie di correttezza nelle modalità di trattamento ed un adeguato strumento di conformità. A ciò si affianca l'accreditamento degli organismi certificatori e di controllo degli stessi codici di condotta, ai quali il Garante 'delega' la certificazione, di durata triennale e revocabile.
Il Regolamento disciplina altresì le procedure di cooperazione tra le singole autorità nazionali, con la previsione dell'autorità capofila (quella del Paese dove è stabilito il titolare) e il meccanismo dello sportello unico (*one stop shop*), al fine di facilitare gli adempimenti dal lato delle persone fisiche e delle aziende. L'assistenza reciproca e le operazioni congiunte divengono prioritarie, nello spirito del GDPR, a vantaggio del cittadino o dell'impresa che ha il diritto di potersi rivolgere all'interlocutore a essi più prossimo in termini geografici e linguistici.

La nuova *governance* europea, il cosiddetto *Board* o Comitato europeo, composto da rappresentanti del 'vertice' di tutte le *Data Protection Authority* (DPA) e dell'*European Data Protection Supervisor* (EDPS), ha, tra gli altri, il compito di dirimere eventuali controversie tra autorità capofila e fornire pareri vincolanti, sul presupposto del meccanismo di coerenza. Questo organo di chiusura del sistema risulterà invero il produttore di quel *case law*, essenziale per autorità e operatori, nel dirimere dubbi applicativi non ancora sciolti, posta la difficoltà di interpretare un diritto non ancora pienamente messo alla prova e che ha avuto uno sviluppo ed una comprensione diversificati nei differenti Paesi dell'Unione.

Intervento al convegno
Il ruolo del Garante e del nuovo Comitato europeo della protezione dei dati personali
https://www.youtube.com/watch?v=IrWH2hwmNmA&feature=youtu.be

* Giovanna Bianchi Clerici: componente dell'Autorità garante dal 2012. Giornalista professionista, iscritta all'Ordine dei Giornalisti dal 1992. Dal 2005 al 2012 consigliere di amministrazione della Rai Radiotelevisione Italiana. Dal 1996 al 2005 deputato al Parlamento (XIII e XIV legislatura); capogruppo in Commissione VII (cultura, scienza e istruzione), dove si è occupata di istruzione, università e del sistema radiotelevisivo ed editoriale. È stata componente di diverse commissioni parlamentari.

LA CIRCOLARE AGID 2/2017 SULLE MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI

Daniela Intravaia*

La strategia europea per una crescita intelligente sostenibile e inclusiva del 2010[1] è all'origine dello sviluppo di un'agenda digitale europea e, all'interno di questa, di un unico mercato digitale[2].
Determinante in tal senso è il tema della sicurezza nell'utilizzo diffuso delle nuove tecnologie. Infatti, tra le remore che cittadini e imprese manifestano riguardo all'utilizzo di piattaforme informatiche e telematiche, sia per fruire di servizi pubblici, sia per scambiare merci o valori, vi è proprio la scarsa fiducia nell'affidabilità di tali strumenti sotto il profilo della sicurezza informatica in generale e della protezione dei dati in particolare[3].
Per tali motivi, oltre ad avere lanciato a partire dal 2010 una serie di azioni e progetti orientati ad elevare il livello di sicurezza delle reti e delle informazioni, l'Europa ha sempre incoraggiato gli Stati membri ad attivarsi anche al proprio interno per incrementare al massimo l'adozione di adeguate misure di sicurezza informatica e telematica.
L'Agenzia per l'Italia Digitale ha la responsabilità dell'attuazione dell'agenda digitale italiana e, nell'ambito di questa, ha compiti regolatori e di coordinamento delle azioni compiute da tutte le Pubbliche Amministrazioni (PA) italiane, anche in ambito di sicurezza informatica e di protezione da attacchi cibernetici.
L'agenda digitale italiana oggi si trova declinata nel Piano Triennale[4], attualmente in corso di aggiornamento. Il Piano è stato predisposto con la collaborazione del Team Digitale del commissario straordinario per l'agenda digitale e prevede l'adesione di tutte le pubbliche amministrazioni a una serie di piattaforme abilitanti, quali PagoPA, così come al sistema di autenticazione SPID

o al registro nazionale dei cittadini (Anagrafe Nazionale della Popolazione Residente - ANPR), che contribuiranno a realizzare interoperabilità e servizi digitali omogenei, anche transfrontalieri.
In tale contesto evolutivo, che metterà sempre più in correlazione i sistemi informativi degli uni e degli altri, la corretta gestione della sicurezza informatica diviene caposaldo per limitare i rischi di esposizione ad incidenti nei confronti di ciascuno degli attori in gioco, dove ad essere esposti a possibile danno o perdita sono i dati di cittadini e imprese, un tesoro che va protetto con ogni mezzo disponibile.
Lo schema che rispecchia il complesso degli ambiti di intervento del Piano Triennale e ne offre una visione sistemica è riportato nella figura 1.
Nel piano, sono numerosi i riferimenti alle politiche di sicurezza[5], così come è costante e continua l'azione di AgID per l'incremento della sicurezza delle infrastrutture che la stessa Agenzia gestisce, quali il *Computer Emergency Response Team* (CERT-PA), per la protezione dagli attacchi cibernetici rivolti alle pubbliche amministrazioni italiane.
Uno strumento che nel frattempo AgID ha reso disponibile all'intera platea delle amministrazioni, per far sì che a livello capillare si applichino misure preventive, è consistito nella emanazione di una serie di indicazioni, avvenuta con la pubblicazione delle misure minime di sicurezza affidate alla circolare 2/2017[6].
Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale, utili alle pubbliche amministrazioni per valutare il proprio livello di sicurezza informatica.
Le amministrazioni sono invitate ad applicare le misure minime descritte nella circolare, secondo il grado di complessità del proprio sistema informativo e tenendo in considerazione il contesto specifico; in particolare, le misure minime possono essere attuate in modo progressivo secondo *tre possibili gradi*:

1. *minimo*: è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme;
2. *standard*: è il livello, superiore a quello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e che rappresenta la maggior parte delle realtà della PA italiana;

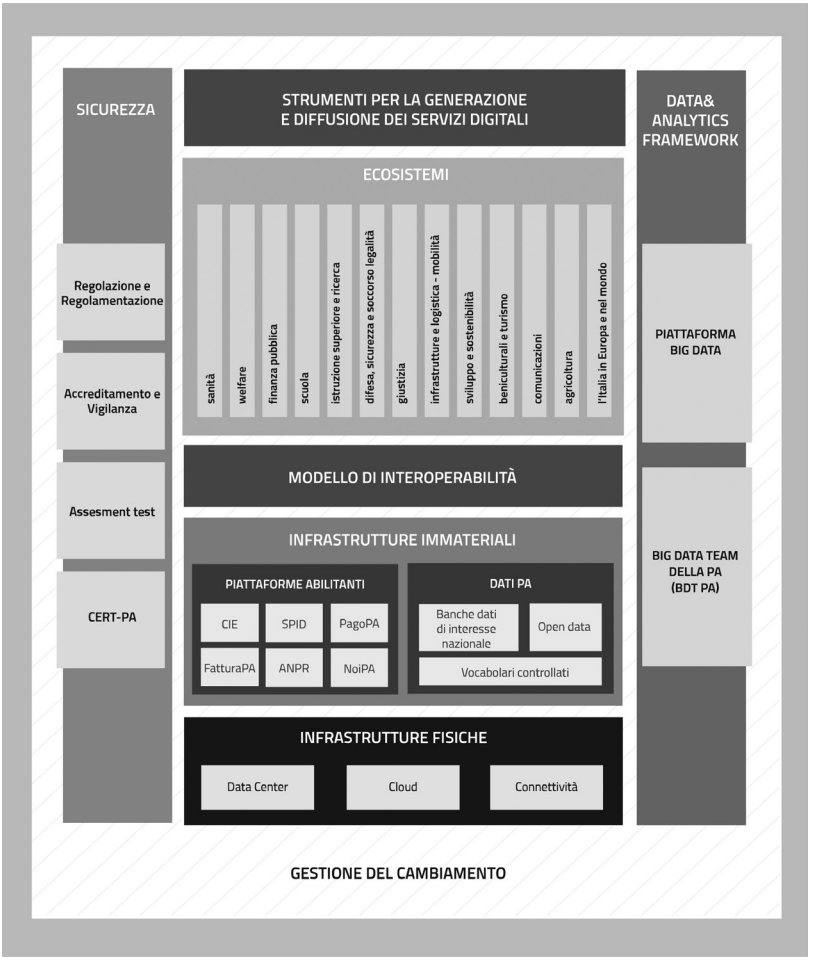

Figura 1. Ambiti di intervento del Piano Triennale di riferimento.

3. *avanzato*: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma può anche essere visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

Naturalmente, non è impedito alle imprese o ai professionisti di adottare le misure di sicurezza che AgID ha studiato guardando eminentemente alla propria platea di riferimento, che è quella del complesso delle amministrazioni pubbliche. Il livello minimo di cui al punto 1 ha caratteristiche di semplicità e di essenzialità tali da renderlo facilmente applicabile a qualsiasi contesto organizzativo.

Per predisporre tale documento, AgID ha preso le mosse dall'insieme di controlli noto come SANS 20, pubblicato dal Center for Internet Security, *CIS Critical Security Controls for Effective Cyber Defense* nella versione 6.0 di ottobre 2015.

La scelta è stata motivata dalla scalabilità e dalla correlata 'convenienza' organizzativa ed economica del citato sistema SANS 20. In particolare, i primi cinque tipi di controlli sono ritenuti indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni note.

AgID ha comunque effettuato una selezione delle regole SANS, individuandone complessivamente otto, caratterizzate da verbi come *inventariare*, *monitorare*, *valutare*, *proteggere*, che coprono sia un livello base di protezione da attacchi *cyber*, sia tematiche più generali della sicurezza informatica, quali la necessità di dotarsi di protezione da *malware* (codice malevolo) e di copie di sicurezza, nonché la protezione contro i rischi della c.d. esfiltrazione di dati.

In buona sostanza, la selezione delle famiglie di controlli, unita alla previsione di tre possibili livelli di sicurezza da perseguire, dovrebbe facilitare ogni e qualsiasi soggetto pubblico nell'aderire alla messa in atto delle misure stesse, sia per la semplicità di alcuni interventi, sia per la ragione che, quanto meno al livello minimo, non sono nemmeno richiesti investimenti consistenti.

Soprattutto, il pregio delle misure è correlato all'approccio organizzativo delle stesse: esse suggeriscono alle PPAA di mettere in atto nuovi processi di servizio, in passato non sempre adeguatamente considerati. Si tratta, ad

esempio, di avviare processi formativi (educativi) sulla gestione e sull'utilizzo degli strumenti tecnologici, che non si esauriscono mai nell'adozione di una misura *una tantum* e *per se*, ma al contrario vanno intesi come principio di un'azione costante e continua di prevenzione e monitoraggio.
Gli obiettivi di AgID nel redigere le misure minime di sicurezza ICT si possono sintetizzare come segue:

- *indirizzare* verso una politica della sicurezza tutte le amministrazioni, soprattutto quelle meno attrezzate, fornendo uno strumento operativo direttamente utilizzabile (una lista di raffronto, checklist), in vista di documenti evolutivi successivi;
- *stabilire una linea comune* di misure tecniche ed organizzative irrinunciabili ma semplici;
- *fornire alle amministrazioni uno strumento* per verificare lo stato corrente di attuazione delle misure di protezione contro le minacce informatiche, in vista di un percorso di miglioramento;
- *responsabilizzare* le amministrazioni sulla necessità di migliorare e mantenere *adeguato* il proprio livello di protezione cibernetica, ponendo il compito (e la relativa responsabilità) direttamente in capo al dirigente competente[7].

Le famiglie di controlli SANS 20 selezionate da AgID per l'applicazione alle PPAA sono di seguito indicate:

- ABSC 1 (CSC 1): inventario dei *dispositivi* autorizzati e non autorizzati;
- ABSC 2 (CSC 2): inventario dei *software* autorizzati e non autorizzati;
- ABSC 3 (CSC 3): proteggere le *configurazioni* di hardware e software sui dispositivi mobili, laptop, workstation e server;
- ABSC 4 (CSC 4): valutazione e correzione continua della *vulnerabilità*;
- ABSC 5 (CSC 5): uso appropriato dei *privilegi di amministratore*;
- ABSC 8 (CSC 8): difese contro i *malwares*;
- ABSC 10 (CSC 10): *copie* di sicurezza;
- ABSC 13 (CSC 13): *protezione dei dati*.

Soffermandosi in particolare sull'ultima delle famiglie previste, si potrà verificare una piena adesione alle logiche del General Data Protection Regulation (GDPR) UE 679/2016. Si tratta infatti di una famiglia di controlli orientati a definire processi interni e sistemi atti ad evitare l'esfiltrazione

dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti. Le misure principali consistono in:

- uso della crittografia;
- limitazioni dell'uso di dispositivi removibili;
- controlli sulle connessioni di rete/internet.

La scheda allegata alla circolare in relazione alla famiglia ABSC13 è piuttosto dettagliata, ma, in buona sostanza, raccomanda di effettuare un'analisi dei dati per individuare quelli che presentino particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali vada applicata la protezione crittografica, oltre al blocco di traffico da e verso URL presenti in una *blacklist*.
Alcune misure appaiono oggi di grande rilievo, se rilette alla luce della piena applicazione del GDPR e, forse, si potrebbe valutare se debbano essere portate dal c.d. livello *alto*, o avanzato, a quello *standard* (cioè, se non debbano essere previste quali indispensabili in ogni e qualsiasi trattamento informatizzato di dati).
Tra queste figurano, ad esempio, il monitoraggio puntuale del traffico uscente, l'impiego di crittografia non autorizzata e l'accesso ai siti che consentano lo scambio e la potenziale esfiltrazione di informazioni, oltre all'obbligo di periodiche scansioni attraverso sistemi automatizzati in grado di rilevare sui server la presenza di specifici *data patterns* significativi per l'amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.
Peraltro, la discussione sull'impianto evolutivo deve essere lasciata agli esperti di sicurezza di AgID, in dialogo con la comunità degli utenti, in una eventuale futura versione delle misure minime, tenendo sempre conto degli impatti organizzativi che ogni nuova prescrizione comporta, soprattutto sulle amministrazioni di piccole dimensioni (in termini di carico aggiuntivo e di necessarie risorse economiche e di personale dotato di competenze adeguate a gestire le misure eventualmente introdotte).
Deve comunque considerarsi che oggi occorre passare dalle regole minime al concetto di regole adeguate. In tal senso, è opportuno evidenziare che la valutazione sull'adeguatezza delle misure compete ai titolari, che soli possono disporre di tutte le informazioni per stabilire:

- natura
- ambito di applicazione
- contesto

- finalità del trattamento
- rischi per i diritti e le libertà delle persone fisiche.

Per tali motivi il GDPR (art. 24) pone in capo al titolare e non ad altri soggetti l'obbligo di mettere in atto «misure tecniche e organizzative adeguate» per assicurare e dimostrare che il trattamento sia effettuato conformemente al Regolamento.
In tal senso, anche dopo l'entrata in piena applicazione del GDPR, le misure minime della circolare 2/2017 conservano la propria efficacia, come primo livello di un processo che prosegue, con l'individuazione da parte del titolare di misure adeguate allo specifico trattamento in questione.
È importante considerare che si tratta di azioni che devono essere progressive e miranti all'obiettivo del miglioramento continuo, in parallelo con l'evoluzione tecnologica. Diversamente, l'esposizione a rischi per i dati di cittadini e imprese non sarà mitigata, con ciò non favorendo la fiducia nel mercato unico digitale, con il suo potenziale di crescita economica e di sviluppo sociale, due fattori certamente essenziali in questo momento storico, particolarmente per il nostro Paese.

Intervento al convegno
La circolare AgID n. 2/2017 sulle misure minime di sicurezza ICT ed impact assessment (DIPIA)
https://www.youtube.com/watch?v=FbJIr2BJ5Og&feature=youtu.be

Link alle slide
daniela intravaia - la circolare agid n. 2-2017

NOTE

[1] https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy_it.

[2] https://ec.europa.eu/commission/priorities/digital-single-market_it.

[3] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52010DC0245&from=IT, si veda in particolare par. 2.3, pp. 17-18: «Il diritto alla riservatezza e alla tutela dei dati personali è un diritto fondamentale nell'UE che deve essere fatto rispettare, anche online, con tutti i mezzi possibili: dall'applicazione generalizzata del principio di 'privacy by design' nelle TIC pertinenti fino ad arrivare, se necessario, ad azioni dissuasive».

[4] https://www.agid.gov.it/it/argomenti/piano-triennale.

[5] https://pianotriennale-ict.italia.it/sicurezza/.

[6] https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict.

[7] Da Corrado Giustozzi, consulente esperto di *cyber security* presso AgID.

* Daniela Intravaia: dirigente presso l'Agenzia per l'Italia Digitale, dal 2016 è responsabile dell'ufficio Coordinamento attività internazionali, responsabile Anticorruzione e trasparenza e dal 2017 referente per la piena applicazione del Regolamento 2016/679/UE e responsabile *ad interim* dell'ufficio Progettazione nazionale. Già responsabile del CISIA di Milano, ufficio territoriale della Direzione Generale Sistemi Informativi Automatizzati del Ministero della Giustizia (DGSIA-MinGiustizia) e dirigente generale DGSIA-MinGiustizia.

IL NUOVO 'DIRITTO ALL'OBLIO': TRA TUTELA DELL'IDENTITÀ PERSONALE ED ESIGENZE DI RISERVATEZZA

Andrea Sirotti Gaudenzi*

Premesse

«La storia non si cancella». In questo modo il Garante per la protezione dei dati personali aveva sintetizzato, nella propria *newsletter* del 21 giugno 2016, il senso del provvedimento con il quale era stata rigettata una domanda volta a far valere il «diritto all'oblio»[1]. Nell'occasione, l'Autorità evidenziava che elemento costitutivo di tale diritto è «il trascorrere del tempo rispetto al verificarsi dei fatti oggetto delle notizie rinvenibili attraverso l'interrogazione dei motori di ricerca e che, anche laddove sussista, tale elemento incontra tuttavia un limite quando le informazioni per le quali viene invocato risultino riferite a reati gravi, dovendo le relative richieste di deindicizzazione essere valutate con minor favore dalle Autorità di protezione dei dati pur nel rispetto, comunque, di un'analisi caso per caso»[2].

Il diritto all'oblio

Se è vero che il problema attuale è legato ai rapporti tra «memoria individuale e memoria sociale»[3], allora, come scritto da Stefano Rodotà, «il diritto all'oblio può pericolosamente inclinare verso la falsificazione della realtà e divenire strumento per limitare il diritto all'informazione»[4].
La questione del bilanciamento tra opposte esigenze sta alla base delle problematiche legate allo sviluppo di quella che il legislatore europeo ha chiamato per primo «società dell'informazione», in cui la comunicazione e la diffusione di qualsiasi tipo di 'sapere' assume un ruolo fondamentale per lo sviluppo degli individui e delle imprese.

Si è chiarito che «è sempre l'interesse pubblico che giustifica la violazione di quell'aspetto della dignità-riservatezza che è definito diritto all'oblio»[5]: così si è espressa la Suprema Corte di recente, richiamando l'«impostazione classica» che tende a collocare il diritto entro i confini di concetti noti e affermati come la dignità e la riservatezza e, più in generale, nell'alveo dei diritti della personalità[6], dovendosi riconoscere all'individuo il diritto di cambiare, di trasformarsi, di crescere[7], lasciandosi alle spalle un passato, anche pesante[8].
Di sicuro, se di diritto si dovesse parlare, non si potrebbe non cogliere quanto lo stesso rappresenti qualcosa di estremamente 'fluido', 'dinamico' e, naturalmente, in continua evoluzione[9].
Si deve evidenziare che due sono i significati attribuibili all'espressione «diritto all'oblio»[10]: se, da una parte, si potrebbe ritenere che il «diritto all'oblio» sia riconducibile al diritto del soggetto interessato alla cancellazione dei propri dati (di «diritto alla cancellazione» parla il nuovo Regolamento europeo in tema di dati personali[11]), da un'altra angolazione, con l'espressione 'diritto all'oblio' si potrebbe indicare la pretesa di un soggetto a non vedere riproposte notizie oramai superate[12] e in grado di arrecargli pregiudizio.

Questioni problematiche
Non è semplice dare una definizione di 'diritto all'oblio' (oggi tanto celebrato e oggetto di numerosi approfondimenti)[13]. A dire il vero, non è neppure così semplice affermare se l'oblio potesse essere considerato realmente un diritto sino a qualche anno fa[14], dato che – nonostante le 'aperture' espresse dalla giurisprudenza[15] – solo il recente Regolamento europeo sulla protezione dei dati personali 2016/679 (definitivamente applicabile in via diretta in tutti i Paesi membri a partire dal 25 maggio 2018) ha dato pieno riconoscimento al «diritto alla cancellazione» (già 'abbozzato' dalla direttiva 95/46/CE), facendo riferimento al «diritto all'oblio» sin nelle premesse (considerando 64 e 65)[16]. Infatti, all'art. 17, il Regolamento prevede che l'interessato abbia il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento abbia l'obbligo di cancellare sempre senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali 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 basa il trattamento e non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; d) i dati personali sono stati oggetto di trattamento illecito; e) i dati personali devono essere cancellati per adempiere un obbligo di legge previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione nel caso di minori.

Soluzioni giurisprudenziali

Uno dei più frequenti quesiti che gli esegeti si sono posti nel recente passato è stato legato al tentativo di 'agganciare' quello che da qualche anno viene comunemente e diffusamente chiamato 'diritto all'oblio' ai princìpi generali, collocandolo nell'alveo dell'impianto sistematico italiano[17]. La Suprema Corte, nel 2012, ebbe modo di chiarire che si dovesse riconoscere al soggetto a cui appartenessero i dati oggetto di trattamento un «diritto all'oblio», inteso come il «controllo a tutela della propria immagine sociale»[18], riconducendo questo diritto all'ambito della tutela dei dati personali. A tal proposito, si segnala che il Tribunale di Roma ha ritenuto il «diritto all'oblio» una sorta di «espressione del diritto alla riservatezza (*privacy*) e del legittimo interesse di ciascuno a non rimanere indeterminatamente esposto ad una rappresentazione non più attuale della propria persona derivante dalla reiterata pubblicazione di una notizia [...], con pregiudizio alla propria reputazione e riservatezza»[19].

Il Tribunale di Milano, in un provvedimento del 2013, ha posto l'attenzione sul fatto che il D.Lgs. 196/2003 avrebbe permesso l'introduzione di un «sistema informato al prioritario rispetto dei diritti e delle libertà fondamentali e della dignità della persona, e, in particolare della riservatezza e del diritto alla protezione dei dati personali nonché all'identità personale o morale del soggetto», cui viene attribuito rango costituzionale[20]. In un contesto come questo, «assume imprescindibile rilievo il bilanciamento tra contrapposti diritti e libertà fondamentali»[21]. Nell'occasione, si è evidenziato come si dovesse tener conto del rango di diritto fondamentale assunto dal diritto

alla protezione dei dati personali, tutelato dagli artt. 2 e 21 Cost., nonché dal diritto dell'Unione europea, quale diritto che «concorre a delineare l'assetto di una società rispettosa dell'altro e della sua dignità in condizioni di eguaglianza»[22]. Sul punto, è bene ricordare che si è progressivamente affermata la necessità che la notizia possa essere data solo in presenza di tre condizioni: a) verità (oggettiva o putativa), b) continenza e c) pertinenza[23]. Proprio il 'bilanciamento' tra opposte esigenze è alla base delle considerazioni di un *dictum* della Suprema Corte che, analizzando i rapporti tra diritto di cronaca e diritto alla riservatezza, ha affermato che il «diritto all'oblio» troverebbe limite nel diritto di cronaca, solo quando sussista un interesse effettivo ed attuale alla diffusione di dati[24]. Alle stesse conclusioni è giunta più recentemente la Corte di giustizia dell'Unione europea, nella celebre decisione della primavera del 2014 relativa al caso *Google Spain*[25], che viene da molti indicata come la *base giuridica* della disciplina del «diritto all'oblio»[26]. Sulla base dell'insegnamento espresso dai precedenti richiamati, si segnala anche un recente provvedimento della Cassazione che ha posto l'accento sulla necessità di procedere in un percorso di «*valutazione bilanciata* del diritto all'informazione ed alla cronaca giornalistica con i diritti fondamentali della persona, quale quello alla riservatezza»[27].

Intervento al convegno
Il nuovo diritto all'oblio: tra tutela dell'identità personale ed esigenze di riservatezza
https://www.youtube.com/watch?v=AAaOdFk5rBg&feature=youtu.be

Link alle slide
andrea sirotti gaudenzi - il nuovo diritto all'oblio

NOTE

[1] Autorità garante, provvedimento del 31 marzo 2016.

[2] *Ibidem*.

[3] S. Rodotà, *Il diritto di avere diritti*, Bari 2015.

[4] *Ibidem*.

[5] Cass. pen., sez. I, 8 gennaio 2015, n. 13941, in *CED*, 2015.

[6] Sul punto, sia permesso richiamare A. Sirotti Gaudenzi, *Diritto all'oblio e diritto all'informazione: un difficile equilibrio*, in *Corr. giur*., 2018, fasc. 8-9, pag. 1107.

[7] L. Rattin, *Il diritto all'oblio*, in *Arch. civ*., 2000, pag. 1069.

[8] In tal senso, di recente: Cass. civ., sez. I, 20 marzo 2018, n. 6919, in *Medialaws*, 2018, con nota di F. Paruzzo. Il provvedimento ha rilevato come l'opera di bilanciamento vada effettuata con riferimento a varie norme nazionali (art. 2 Cost., art. 10 c.c., art. 97 della L. 633/1941) ed europee (artt. 8 e 10, par. II CEDU, artt. 7 e 8 della Carta di Nizza), sulla base delle quali si ritiene che «il diritto fondamentale all'oblio può subire una compressione, a favore dell'ugualmente fondamentale diritto di cronaca, solo in presenza di specifici e determinati presupposti: 1) il contributo arrecato dalla diffusione dell'immagine o della notizia ad un dibattito di interesse pubblico; 2) l'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, peggio, meramente economico o commerciale del soggetto che diffonde la notizia o l'immagine; 3) l'elevato grado di notorietà del soggetto rappresentato, per la peculiare posizione rivestita nella vita pubblica e, segnatamente, nella realtà economica o politica del Paese; 4) le modalità impiegate per ottenere e nel dare l'informazione, che deve essere veritiera (poiché attinta da fonti affidabili, e con un diligente lavoro di ricerca), diffusa con modalità non eccedenti lo scopo informativo, nell'interesse del pubblico, e scevra da insinuazioni o considerazioni personali, sì da evidenziare un esclusivo interesse oggettivo alla nuova diffusione; 5) la preventiva informazione circa la pubblicazione o trasmissione della notizia o dell'immagine a distanza di tempo, in modo da consentire all'interessato il diritto di replica prima della sua divulgazione al grande pubblico». In assenza dei presupposti sopra indicati, «la pubblicazione di una informazione concernente una persona determinata, a distanza di tempo da fatti ed avvenimenti che la riguardano, non può che integrare [...] la violazione del fondamentale diritto all'oblio». In passato, si è sostenuto che «la lesione del diritto all'identità personale non può essere ravvisata in qualsiasi inesatta rappresentazione di vicende comunque collegate a una determinata persona, ma soltanto in quelle inesatte rappresentazioni della realtà comportanti una distorsione della personalità dell'interessato» (Trib. Milano, 7 ottobre 1993, in *Dir. ind*., 1994, pag. 791, con nota di S. Sandri). Il Tribunale della Capitale ha posto l'accento sul fatto che «[v]a prospettata non già la lesione del diritto all'identità personale, bensì del diritto alla reputazione qualora venga preso in considerazione il giudizio che altri daranno della propria persona a seguito della divulgazione di una certa raffigurazione, sì che risulti compromesso anche, e soprattutto, il valore della persona stessa» (Trib. Roma, 10 febbraio 1993, in *Foro it*., 1994, I, col. 1237).

[9] In particolare, sul punto, si rinvia a G. Finocchiaro, *La memoria della rete e il diritto all'oblio*, in *Dir. inf.*, 2010, pag. 392; F. Di Ciommo, R. Pardolesi, *Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la Rete, bellezza!*, in *Danno e resp.*, 2012, pag. 703.
[10] Cfr. G. Marchetti, *Diritto di cronaca on line e tutela del diritto all'oblio*, in AA.VV., *Da Internet ai social network*, Rimini 2013, pag. 71.
[11] Regolamento 2016/679, di cui si parlerà oltre.
[12] G. Marchetti, *Diritto di cronaca on line e tutela del diritto all'oblio*, cit., pag. 72.
[13] Il 'diritto all'oblio' non è espressamente previsto dalle fonti nazionali (peraltro, non vi erano norme espressamente dedicatevi nella direttiva 95/46/CE, a differenza di quanto avviene oggi con riferimento al nuovo regolamento dedicato al trattamento dei dati personali). Solo l'applicazione di princìpi ricavabili dalle norme fondamentali consente di dar vita a questo nuovo diritto. Se si volesse avviare un'analisi sistematica del *corpus* delle norme nazionali, si dovrebbe forse muovere dal diritto al pentimento nell'àmbito delle opere dell'ingegno. Difatti, la L. 633/1941 (l.d.a.) attribuisce all'autore un diritto personale e trasmissibile, che gli permette, qualora concorrano gravi ragioni morali, di ritirare l'opera dal commercio, «salvo l'obbligo di indennizzare coloro che hanno acquistati i diritti di riprodurre, diffondere, eseguire, rappresentare o spacciare l'opera medesima» (art. 142, comma I, l.d.a.). Naturalmente, la disposizione prevede la necessità di «gravi ragioni morali», come condizione all'esercizio del diritto e la cui presenza deve essere accertata dall'Autorità giudiziaria (Trib. Torino, 23 marzo 2006, in *Foro it.*, 2006, fasc. 7-8, col. 2081, con nota di G. Casaburi). L'ipotesi, pertanto, riguarda il «potere di ritirare dal commercio esemplari dell'opera pur lecitamente riprodotti» (Cass. civ., sez. I, 7 aprile 1999, n. 3353, in *Riv. dir. ind.*, II, pag. 83, con nota di L. Chimienti), a fronte di (fondati) motivi che possano spingere l'autore a far valere il proprio «cambiamento di corso artistico», che risulti eventualmente del tutto inconciliabile con il precedente. In fondo, come si sa, oggi il c.d. 'diritto all'oblio' viene fatto valere proprio per dare prova del fatto di «essere cambiati», di fronte a informazioni non più aggiornate o nelle quali il soggetto interessato non si riconosca più, invocando un diritto all'identità personale. Il D.Lgs. 196/2003, nell'introdurre un sistema informato al rispetto dei diritti e delle libertà fondamentali e della dignità della persona, e in particolare della riservatezza e del diritto alla protezione dei dati personali, nonché dell'identità personale o morale del soggetto ha sicuramente contribuito a legittimare richieste da parte di soggetti che avessero lamentato l'utilizzo di dati relativi alle proprie vicende, non ritenuto più pertinenti o attuali.
[14] In particolare, nel passato veder cancellare il proprio nome era tutt'altro che positivo. L'*abolitio nominis*, infatti, era la conseguenza della *damnatio memoriae* nella Roma antica: la sanzione comportava l'eliminazione di ogni traccia riconducibile alla persona condannata. La *damnatio memoriae* colpì imperatori come Caligola, Nerone e Domiziano, con condanne che imponevano di cancellare ogni traccia delle loro opere. E, forse, la fama dei primi due imperatori fu compromessa in maniera irreparabile proprio dalla condanna subìta. Ad esempio, di Caligola si sa che fosse folle o, più semplicemente bizzarro, perché fu proibito narrare le gesta di un imperatore che – probabilmente – aveva fatto anche qualcosa di buono e fu

consentito ai cronisti di narrare solo alcuni aneddoti inquietanti. Lo stesso Svetonio, che era uno storico di grande livello, preferì raccontare solo alcuni episodi raccapriccianti. Il resto lo fecero le cronache popolari prive di alcun riscontro degno di questo nome. Anche in età medievale la prassi proseguì. Solo per trarne spunto dalla storia dell'arte, si può ricordare che i mosaici della splendida chiesa di Sant'Apollinare Nuovo di Ravenna mostrano le tracce di una *damnatio memoriae* che colpì Teodorico e la sua corte, le cui effigi furono cancellate e sostituite da altre decorazioni, in quanto 'colpevoli' di riprodurre il ritratto del re goto di culto ariano, che aveva voluto che quel tempio fosse la sua cappella palatina. Si pensi poi ai processi postumi nella storia della Chiesa cattolica. Non a caso l'ordine di cancellare ogni riferimento alle opere di un uomo interessarono addirittura un pontefice: il papa Formoso, processato e condannato nell'anno 897, quando era già morto (per un inquadramento storico, sia consentito rinviare a: A. Sirotti Gaudenzi, *Il diritto all'oblio*: *responsabilità e risarcimento del danno*, Rimini 2017, pag. 12).

[15] Per esempio, si veda: Cass. civ., sez. III, 5 aprile 2012, n. 5525, in *Danno e resp*., 2012, fasc. 7, pag. 747.

[16] Si vedano: R. Pardolesi, *L'ombra del tempo e (il diritto al) l'oblio*, in *Questione giust.*, 2017, fasc. 1, pag. 76; A. Ricci, *I diritti dell'interessato*, in G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna 2017, pag. 179; S. Bonavita, R. Pardolesi, *GDPR e diritto alla cancellazione (oblio)*, in *Danno e resp*., 2018, fasc. 3, pag. 269. In particolare, è stato evidenziato che la direttiva ospita l'espressione «diritto alla cancellazione ("diritto all'oblio")», senza chiarire se si tratti di due locuzioni sovrapponibili o se la cancellazione debba essere ritenuto fenomeno diverso dall'oblio. Del resto, è stato anche dato particolare rilievo al fatto che la 'deindicizzazione' esprima una dimensione ulteriore dell'oblio (in tal senso S. Bonavita, *Le ragioni dell'oblio*, in *Ciberspazio & dir*., 2017, pag. 85).

[17] Nel tentativo di dare una impostazione sistematica allo studio dei diritti, è sembrato possibile ricondurre o, comunque, cercare di ricondurre quello che oggi chiamiamo «diritto all'oblio» nella categoria dei diritti della personalità, recuperando la nozione di diritti della personalità c.d. atipici (G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in AA.VV., *Internet e Diritto civile*, Napoli 2015, pag. 139).

[18] Cass. civ., sez. III, 5 aprile 2012, n. 5525, cit.

[19] Trib. Roma, 3 dicembre 2015, in *Corr. giur*., 2016, fasc. 8-9, pag. 1072, con nota di M. Rizzuti e in *Danno e resp*., 2016, fasc. 3, p. 299.

[20] Trib. Milano, 26 aprile 2013, in *Pluris*, 2013.

[21] Trib. Milano, 26 aprile 2013, cit.

[22] A tal proposito, si veda anche Cass. civ., sez. II, 4 gennaio 2011 n. 186, in *Giur. it*., 2011, fasc. 11, 2546, con nota di L. Gasso.

[23] *Ex pluribus*: Cass. civ., sez. I, 18 ottobre 1984, n. 5259, in *Arch. civ*., 1984, pag. 995; *Foro it*., 1984, I, col. 2711, con nota di R. Pardolesi; *Giust. civ*., 1984, I, p. 2941; *Not. giur. reg*., 1985, I, pag. 84; *Nuova giur. civ. comm.*, 1984, I, pag. 84, con nota di A. Fusaro; Cass. civ., sez. III, 14 ottobre 2008, n. 25157, in *CED*, 2008; Cass. civ., sez. III, 20 ottobre 2009, n. 22190, in *Mass. Giur. it*., 2009.

[24] Cass. civ., sez. III, 26 giugno 2013, n. 16111, in *Danno e resp.*, 2014, fasc. 3, pag. 271.
[25] Corte giust. 13 maggio 2014, n. C-131/12, *Mario Costeja Gonzalese e AEPD c. Google Spain e Google Inc.*, in *Corr. giur.*, 2014, fasc. 12, pag. 1471, con nota di G. Scorza, *Corte di giustizia e diritto all'oblio: una sentenza che non convince*.
[26] Si rinvia a M. Iaselli, *Come esercitare il diritto all'oblio in Internet*, Roma 2017, pagg. 28 e ss.
[27] Cass. civ., sez. I, 24 giugno 2016, n. 13161, in *Altalex*, 2016, con nota di M. Iaselli. Di 'bilanciamento' si è occupata di recente anche la Corte europea dei diritti dell'uomo, con sentenza datata 28 giugno 2018 (M.L. e W.W. contro Germania, ricorsi n. 60798 e n. 65599/10). Inoltre, con provvedimento del 5 novembre 2018 n. 28084, la terza sezione della Suprema Corte nazionale ha rimesso gli atti al Primo Presidente della Corte «per l'eventuale assegnazione alle Sezioni Unite della questione di massima di particolare importanza, concernente il bilanciamento del diritto di cronaca – posto al servizio dell'interesse pubblico all'informazione – e del c.d. diritto all'oblio – posto a tutela della riservatezza della persona – alla luce del quadro normativo e giurisprudenziale negli ordinamenti interno e sovranazionale».

* Andrea Sirotti Gaudenzi: avvocato cassazionista e docente universitario. Autore di numerose pubblicazioni, dirige collane e trattati giuridici. Patrocina davanti alla Corte europea dei diritti dell'uomo e alla Corte di giustizia dell'Unione europea, innanzi alle quali ha ottenuto alcuni significativi provvedimenti. Svolge attività di docenza presso varie università ed enti pubblici ed è formatore accreditato dal Ministero della Giustizia con riferimento alla materia della mediazione. Ha diretto il trattato *Proprietà intellettuale e diritto della concorrenza* (Utet) e coordina le collane *I Prontuari giuridici* e *ADR - Arbitrato - Processo civile* (Maggioli). Magistrato sportivo, è presidente della Corte d'appello federale della Federazione Ginnastica d'Italia. È responsabile scientifico di vari enti, tra cui l'Istituto Nazionale per la Formazione Continua (INFCON, Roma) e dell'Associazione di Diritto Informatico della Svizzera Italiana (ADISI, Lugano). È arbitro accreditato dal Registro del ccTLD '.it' ed è inserito nella lista dei saggi del Centro Risoluzione Dispute Domìni (CRDD). Collabora stabilmente con le testate del gruppo *Il Sole 24Ore*.

IL TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI NEL REGOLAMENTO UE *679/2016* E NEL NOVELLATO CODICE PRIVACY

Franco Cardin e Andrea Lisi*

Premessa

Come noto, il Codice Privacy[1] prevedeva regole distinte – con eccezione dell'ambito sanitario – per il trattamento dei cosiddetti dati personali sensibili[2] a seconda che lo stesso fosse effettuato da soggetti pubblici piuttosto che da soggetti privati ed enti pubblici economici.

Fermo restando il principio, previsto dal comma 4 dell'art. 18 del Codice Privacy – in base al quale i soggetti pubblici non dovevano richiedere il consenso dell'interessato – il successivo art. 20 stabiliva, infatti, che gli stessi fossero legittimati a effettuare il trattamento di dati sensibili solamente per finalità di rilevante interesse pubblico e a condizione che i tipi di dati che potevano essere trattati e le operazioni eseguibili con gli stessi fossero specificati da una disposizione di legge o, in mancanza, da un atto di natura regolamentare adottato in conformità del parere del Garante.

I soggetti privati e gli enti pubblici economici, viceversa, erano legittimati, come previsto dall'art. 26, comma 1, del Codice Privacy, a trattare dati sensibili solamente con il consenso scritto degli interessati e previa autorizzazione del Garante, salvo i casi di deroga all'obbligo di acquisire il consenso previsti espressamente nei commi 3 e 4 del medesimo articolo.

In altre parole, la scelta fatta dal nostro legislatore nel recepire la direttiva 95/46/CE – già con la L. 675/1996 e poi confermata con il Codice Privacy che l'ha sostituita – è stata caratterizzata, con riferimento al trattamento dei dati sensibili effettuato dai soggetti privati e dagli enti pubblici economici nonché, limitatamente all'ambito sanitario, anche dai soggetti pubblici, da un'impostazione che potremmo definire di tipo 'consenso-centrica'.

Il Regolamento UE 679/2016 (di seguito GDPR), diversamente, nel confermare l'impostazione già adottata con la direttiva 95/46/CE, non solo non prevede la separazione tra condizioni di liceità applicabili ai soggetti pubblici e ai soggetti privati [3]– che, come è stato sopra ricordato, costituiva una regola generale fondamentale del Codice Privacy – ma anche individua il consenso dell'interessato come una delle possibili condizioni di liceità per il trattamento di dati personali.

L'art. 9 del GDPR

Innanzitutto è opportuno sottolineare che l'art. 9 del GDPR, rubricato *Trattamento di categorie particolari di dati personali*, al paragrafo 1 elenca i tipi di dati che rientrano in questa categoria per i quali è previsto il divieto di trattamento. A ben vedere si tratta dei medesimi tipi di dati personali che il Codice Privacy definiva sensibili, ai quali sono stati aggiunti i dati genetici e quelli biometrici intesi a identificare in modo univoco una persona fisica.

Coerentemente con l'impostazione adottata dal legislatore europeo, di cui si è fatto cenno in premessa, nel successivo paragrafo 2 dell'art. 9 sono elencati i casi per i quali non si applica il predetto divieto e che, pertanto, rappresentano condizioni di liceità del trattamento dei dati personali particolari.

È opportuno ricordare che la maggior parte di questi casi coincidono sostanzialmente con quelli riportati nei commi 3 e 4 dell'art. 26 del Codice Privacy – per i quali i soggetti privati erano legittimati a trattare i dati sensibili anche senza il consenso dell'interessato – e che, pertanto, non dovrebbero rappresentare una novità sul piano operativo.

La prima condizione che rende lecito il trattamento di dati particolari, prevista nell'art. 9, paragrafo 2, lett. a) del GDPR è rappresentata dal consenso 'esplicito' dell'interessato e, pertanto, deve ritenersi non solo che lo stesso, per essere ritenuto valido, debba essere informato e libero, ma che sia anche escluso il comportamento concludente[4].

Gli altri casi elencati nel paragrafo 2 dell'art. 9 del GDPR, per i quali è lecito trattare i dati personali particolari, riguardano rispettivamente i trattamenti:

- necessari per adempiere agli obblighi ed esercitare i diritti specifici dei datori di lavoro, nella loro qualità di titolari del trattamento o dei dipen-

denti, in qualità di interessati, in ambito giuslavoristico e della sicurezza e protezione sociale (9.2.b);
- necessari per tutelare un interesse essenziale per la vita – comprese le situazioni di rischio per l'incolumità fisica o la salute – dell'interessato o di un terzo (9.2.c);
- effettuati nell'ambito della gestione dei rapporti intercorrenti tra le fondazioni e le associazioni senza scopo di lucro – che perseguono finalità politiche, filosofiche, religiose o sindacali – e i rispettivi soci, a condizione che i dati personali particolari di questi ultimi non siano comunicati all'esterno senza il loro consenso (9.2.d);
- riguardanti dati personali resi manifestamente pubblici dall'interessato (9.2.e);
- necessari per esercitare un diritto in sede giudiziaria, compresa la tutela in sede amministrativa e stragiudiziale (9.2.f);
- necessari per motivi di interesse pubblico rilevante (9.2.g);
- effettuati per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale, nonché per la gestione dei sistemi e sevizi sanitari o sociali (9.2.h), a condizione che i dati personali particolari siano trattati da un professionista soggetto al segreto professionale;
- effettuati nell'ambito del settore della sanità pubblica per motivi di interesse pubblico (9.2.i);
- necessari per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (9.2.j).

L'art. 2-*sexies* del novellato Codice Privacy

Con il D.Lgs. 101/2018 – entrato in vigore il 19 settembre 2018 – il Governo ha provveduto, in attuazione della delega conferita dall'art. 13 della legge 25 ottobre 2017, n. 163, ad adeguare il Codice Privacy, sia abrogando tutte le disposizioni ritenute incompatibili con quelle contenute nel GDPR, sia esercitando la facoltà di poter mantenere o introdurre disposizioni più specifiche per alcuni trattamenti, quali ad esempio quelli necessari per motivi di interesse pubblico rilevante di cui all'art. 9, paragrafo 2, lett. g) del GDPR.
Con l'art. 2 del predetto D.Lgs. 101/2018 è stato introdotto nel Codice Privacy

l'art. 2-*sexies*, il cui primo comma stabilisce che il trattamento delle categorie particolari di dati personali, necessario per motivi di interesse pubblico rilevante, è ammesso solamente se lo stesso è previsto dal diritto dell'Unione Europea oppure, nell'ordinamento interno, da norme di legge o, nei casi previsti dalla legge, di regolamento, che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili con gli stessi e le misure per tutelare i diritti dell'interessato.
Il secondo comma del predetto art. 2-*sexies* del novellato Codice Privacy elenca le materie nell'ambito delle quali il trattamento di categorie particolari di dati personali, da parte di soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, è considerato effettuato per motivi di rilevante interesse pubblico.

L'art. 2-*septies* del novellato codice

In attuazione della facoltà riservata dal paragrafo 4 dell'art. 9 del GDPR ai singoli Stati membri, di mantenere o introdurre ulteriori condizioni, relativamente al trattamento di dati genetici, biometrici o relativi alla salute, il D.Lgs. 101/2018, ha inserito nel Codice Privacy l'art. 2-*septies*, nel quale è stabilito che, fermo restando il divieto di diffusione di tali dati[5], gli stessi possono essere oggetto di trattamento in presenza di una delle condizioni alternative di legittimità di cui al paragrafo 2 dell'art. 9 del GDPR e in conformità alle misure di garanzia disposte dal Garante per la protezione dei dati personali con proprio provvedimento – il cui schema deve essere sottoposto a consultazione pubblica – da adottare con cadenza almeno biennale.
Con tale provvedimento l'Autorità garante dovrà individuare le misure di garanzia tenendo in considerazione non solo le specifiche finalità perseguite tramite il trattamento di ognuna delle predette categorie di dati personali, ma anche le linee guida e le raccomandazioni del Comitato europeo per la protezione dei dati e dell'evoluzione scientifica e tecnologica nel settore a cui tali misure sono rivolte.
Le predette misure di garanzia dovranno, tra l'altro, individuare le misure di sicurezza organizzative, quali ad esempio le modalità per l'accesso selettivo ai dati e per fornire le informazioni sulla salute agli interessati, nonché quelle tecniche quali la cifratura e la pseudonomizzazione.

Il Titolo V del novellato Codice Privacy

L'art. 6 del citato D.Lgs. 101/2018 ha apportato significative modifiche anche al Titolo V della parte II del Codice Privacy, contenente le regole specifiche per il trattamento delle categorie particolari di dati personali, quali ad esempio quelli idonei a rivelare lo stato di salute e quelli genetici in ambito sanitario, per finalità di tutela della salute dell'interessato o di terzi.

Particolare rilevanza assume il novellato art. 75, in quanto specifica che «Il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del Regolamento, dell'articolo *2-septies* del presente codice, nonché nel rispetto delle specifiche disposizioni di settore».

Coerentemente con quanto disposto dal novellato art. 75, pertanto, sono stati abrogati gli artt. 76 e 81 del Codice Privacy con la conseguenza che a partire dalla data di entrata in vigore del D.Lgs. 101/2018, i soggetti pubblici e privati e gli esercenti le professioni sanitarie possono trattare legittimamente i dati personali relativi alla salute dei loro pazienti, per le finalità sopra specificate, senza il loro consenso.

Per quanto riguarda, invece, il trattamento di dati genetici per finalità di cura si ritiene che nelle more dell'adozione delle misure di garanzia di cui all'art. *2-septies* del novellato Codice Privacy e tenuto conto di quanto previsto nel comma 11 dell'art. 22 del D.Lgs. 101/2018, contenente alcune disposizioni transitorie, questi particolari dati personali debbano essere trattati, nei soli casi e con le modalità e cautele previste nell'autorizzazione generale del Garante n. 8, senza il preventivo consenso del paziente.

Conclusioni: *accountability*, sicurezza e categorie particolari di dati personali

Come è noto, il principio dell'*accountability* – secondo il quale il titolare del trattamento deve essere in grado di dimostrare di aver adottato un processo complessivo di misure giuridiche, organizzative e tecniche per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi – pervade l'applicazione del GDPR (e quindi anche la sua attuazione nel nostro ordinamento).

L'*accountability*, quindi, comporta per il titolare la messa in atto di un processo di trasparenza informativa e documentata che deve animare a maggior ragione il trattamento dei dati personali più delicati e sensibili. Ovvio che la ragione di questa particolare attenzione è dovuta al maggiore rischio per i diritti e le libertà degli interessi in caso di violazioni nel loro trattamento. Tali rischi sono ben elencati e riassunti nel considerando 75 del GDPR:

- perdita del controllo dei dati personali;
- limitazione di diritti;
- discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- compromissione del segreto professionale;
- qualsiasi altro danno economico o sociale significativo alla persona fisica.

È innegabile, pertanto, che un percorso di *assessment* per il corretto e legittimo trattamento delle particolari categorie di dati personali deve preoccuparsi non solo di verificare le condizioni di liceità che ne consentano il trattamento, ma anche e soprattutto sviluppare un sistema di protezione trasparente e documentato che garantisca gli interessati di tali trattamenti. E non è per nulla banale predisporlo.

Intervento al convegno
Il trattamento di categorie particolari di dati personali
https://www.youtube.com/watch?v=CmOfxKLJpSk&feature=youtu.be

Link alle slide
andrea lisi - il trattamento di categorie particolari di dati personali

NOTE

[1] Ci riferiamo ovviamente al D.Lgs. 196/2003.

[2] Così definiti dall'art. 4, comma 1, lett. d) «i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale».

[3] Nel GDPR, infatti, le condizioni di liceità – contenute nell'art. 6 e nell'art. 9 per le categorie particolari di dati personali (sensibili nel Codice Privacy) – non fanno riferimento alla natura pubblica o privata del titolare del trattamento, quanto invece alla natura dell'attività nell'ambito della quale è necessario trattare dati personali come specificato nell'art. 6.1 lett. e) e nell'art. 9.2 lett. g).

[4] È opportuno ricordare a questo proposito che l'art. 7, paragrafo 1, del GDPR pone l'onere della prova della corretta acquisizione del consenso dell'interessato in capo al titolare del trattamento.

[5] Divieto già presente per i dati inerenti allo stato di salute nel Codice per la protezione dei dati personali.

* Franco Cardin: laureato in Scienze politiche, con indirizzo politico-economico, presso l'Università degli Studi di Padova, ha svolto per molti anni la funzione di dirigente amministrativo presso il Comune di Padova, assumendo dal 1992 al 1999 il ruolo di capo di gabinetto del sindaco. Dal 2000 al 2010 ha diretto il Dipartimento amministrativo interaziendale dell'Azienda Ospedaliera e dell'ULSS 16 di Padova. Promotore e coordinatore del progetto ARCHITRAVE nell'ambito del quale sono stati definiti i piani di classificazione e di conservazione dei documenti delle aziende sanitarie pubbliche del Veneto. Dal 2003 al 2010 coordinatore del gruppo interaziendale privacy e responsabile dell'applicazione della normativa in materia di protezione dei dati personali nell'Azienda Ospedaliera e nell'ULSS 16 di Padova. Dal 2011 esercita l'attività di consulente e di formatore in materia di protezione dei dati personali – con particolare riferimento al settore sanitario sia pubblico che privato – e di gestione elettronica dei documenti. Professore a contratto nell'ambito dei Master 'Archiviare il futuro: organizzazione e gestione dei documenti cartacei e digitali delle P.A.', anno accademico 2008/2009, e 'Management cultura digitale'. È membro del Consiglio direttivo di Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti (ANORC).

* Andrea Lisi: avvocato in Lecce, perfezionato in diritto comunitario ed esperto di ICT Law e Privacy. Consulente legale e strategico per i sistemi, i processi e i modelli di digitalizzazione documentale. È presidente della prima Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti (ANORC), vice-presidente di ANORC Professioni, segretario generale dell'Associazione Italiana Firma elettronica Avanzata biometrica e grafometrica (AIFAG). Docente dal 2009 di UniDOC - Progetto di formazione continua in materia di documentazione amministrativa, amministrazione digitale, delibere degli organi e documenti informatici - COINFO - Consorzio Interuniversitario sulla Formazione dell'Università degli Studi di Torino; docente dal 2009 nella Document Management Academy (DMA), SDA Bocconi di Milano, dal 2012 del MIS Academy (Management Information System), SDA Bocconi – IBM, e dal 2013 docente di ISLEGAL, SDA Bocconi; docente dal 2013 per ABI e ABI Lab; direttore scientifico della rivista *Document Management System - DMS* edita da Edisef.

ACCREDITAMENTO E CERTIFICAZIONI ALLA LUCE DEL NUOVO REGOLAMENTO PRIVACY: LE CERTEZZE, LE ATTESE

Filippo Trifiletti*

È, quella attuale, una società che ruota e si evolve attorno al valore collettivo del dato, risorsa strategica per lo sviluppo non solo economico ma anche culturale, e per la crescita della conoscenza.
Oggi, le nuove tecnologie informatiche e di telecomunicazione hanno un ruolo fondamentale per le attività umane, e la loro pervasività fa emergere priorità e aspetti critici, tra cui la protezione delle informazioni personali, ogni giorno rilevate, trattate e registrate da una moltitudine di soggetti, con strumenti diversi e su molteplici supporti. Spesso l'utente ignora quanti dati personali vengano archiviati, dove e soprattutto come proteggerli da usi impropri. Questo ha reso impellente, ancor più nel contesto globale dell'economia digitale, l'esigenza di norme comuni, per verificare la capacità dei fornitori dei servizi che gestiscono i dati, di assolvere anche a funzioni di tutela e protezione degli stessi, preservando al contempo i flussi informativi alla base del libero mercato.
A livello europeo, nel maggio 2016, è entrato in vigore il Regolamento UE 679/2016 (GDPR) sulla protezione e sulla libera circolazione dei dati personali, esecutivo dal 25 maggio 2018 in tutti i Paesi dell'Unione Europea. Il Regolamento, che in generale introduce regole più chiare in materia di informativa e consenso e limiti al trattamento automatico dei dati personali, nello specifico 'incoraggia' l'istituzione di meccanismi di certificazione della protezione dei dati, di sigilli e marchi, con l'obiettivo di attestare la conformità dei trattamenti effettuati dai titolari e dai responsabili del trattamento (art. 42). Vengono indicati sia i soggetti legittimati a rilasciare le certificazioni in modo indipendente che la differenza tra questi, con eventuale, autonoma,

distinta e concorrente facoltà di emettere certificazioni a norma. Le certificazioni possono quindi essere rilasciate (art. 43) da:

- organismi di certificazione, che devono essere accreditati dall'autorità di controllo competente o dall'ente nazionale di accreditamento designato ai sensi del Regolamento CE 765/2008 – in Italia Accredia – oppure da entrambi. La norma indicata come riferimento per l'accreditamento è la ISO/IEC 17065:2012 che disciplina il rilascio delle certificazioni di prodotto;
- l'autorità di controllo competente per lo Stato membro – in Italia il Garante per la protezione dei dati personali.

I 'criteri' di certificazione, genericamente richiamati dal GDPR, vengono approvati dall'autorità di controllo oppure dal comitato europeo per la protezione dei dati istituito dal Regolamento stesso.
Sono gli Stati membri a garantire che l'accreditamento degli organismi di certificazione sia affidato a uno solo o a entrambi i soggetti indicati nel Regolamento. L'autorità di controllo ha invece la funzione esclusiva di accreditare, in base alla valutazione di requisiti specificati nel Regolamento, i soggetti che verificano la conformità dei titolari o dei responsabili del trattamento che aderiscono a codici di condotta proposti da associazioni o altri organismi delle proprie categorie. L'adesione ai codici di condotta o a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.
Il provvedimento prevede che la Commissione europea potrà adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati, nonché le modalità per promuoverli e riconoscerli. Inoltre, accoglie gli indirizzi dell'Unione Europea sul dovere di attenzione speciale verso le micro, piccole e medie imprese, ma non stabilisce quali criteri adottare (prezzo, semplificazione, diversificazione degli schemi di certificazione). Pertanto, dovranno essere formulati indirizzi univoci per assicurare l'uniformità di trattamento dei soggetti che chiedono la certificazione.
La disciplina dell'accreditamento e della certificazione, introdotta da GDPR, lascia tuttavia altre questioni aperte. Oggetto di analisi sono tuttora gli aspetti legati all'attribuzione delle competenze e responsabilità tra l'autori-

tà di controllo e l'ente nazionale di accreditamento, a partire dalle funzioni che può assumere l'autorità di controllo: normazione, accreditamento, certificazione e vigilanza sull'applicazione dei meccanismi di controllo, se assunte contemporaneamente, configurano delle possibili incompatibilità che meritano attenzione. È da capire inoltre se la ISO/IEC 17065 debba essere applicabile anche alle autorità di controllo nel caso in cui queste certifichino.
E rimane da chiarire il fatto che gli schemi di valutazione della conformità potranno avere pesi e campi di applicazione diversi. Ai sensi del Regolamento 679/2016, infatti, gli schemi di accreditamento elaborati sulla base dei criteri approvati dal Comitato europeo diventano schemi validi a livello UE. Dal momento che la European co-operation for Accreditation (EA), l'infrastruttura europea di accreditamento, non valuta gli schemi regolamentati, spetta al Garante UE della protezione dei dati il ruolo di armonizzare tali schemi tra gli Stati membri. Inoltre, i requisiti di accreditamento aggiuntivi rispetto alla norma ISO/IEC 17065, che in base al GDPR le autorità di controllo degli Stati membri possono introdurre, non sarebbero coperti dagli accordi internazionali di mutuo riconoscimento EA MLA (*Multilateral Agreement*) e IAF (International Accreditation Forum) MRA (*Multilateral Recognition Arrangement*), con potenziali criticità, in particolare, per le aziende multinazionali.
Occorre anche valutare come si potrà conciliare l'attività degli enti di normazione, sugli stessi temi, con quella della Commissione europea e la diversa possibile valenza degli schemi basati su disciplinari proprietari, norme tecniche o documenti emessi dalla Commissione. Dovrebbe essere infine chiarita anche la valenza attribuita all'adesione ai codici di condotta, in relazione all'ottenimento di una certificazione, e alla loro spendibilità esimente ai fini della responsabilità d'impresa.
Su tali questioni aperte, il Garante per la protezione dei dati personali sta collaborando, a livello europeo, con le autorità competenti degli altri Stati membri per definire un quadro comune di criteri per l'accreditamento degli organismi e il rilascio delle certificazioni sul mercato. È terminata il 30 marzo scorso, e se ne attendono gli esiti, la consultazione pubblica sulle linee guida relative all'art. 43 del Regolamento 679, su cui ha lavo-

rato l'Article 29 Working Party, gruppo istituito in base all'art. 29 della direttiva 95/46/CE e organismo consultivo e indipendente, composto da un rappresentante delle autorità nazionali di protezione dei dati personali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione europea.
In Italia, Accredia, in qualità di ente unico nazionale di accreditamento, supporta il Garante per fornire tutta la sua esperienza in tema di accreditamento degli organismi di certificazione, al fine di garantire la corretta implementazione del Regolamento 679/2016 a livello nazionale. Infatti, il legislatore non ha ancora stabilito a chi spettino responsabilità e competenze per accreditare gli organismi di certificazione ai sensi del Regolamento.
In questo particolare contesto, Accredia e il Garante hanno dunque chiarito[1] che, fino a decisione del legislatore, le certificazioni di persone, e quelle rilasciate in materia di privacy o *data protection*, possono senz'altro rappresentare una garanzia e un atto di diligenza verso le parti interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, ma non possono definirsi 'conformi agli artt. 42 e 43 del Regolamento 679/2016'. Questo proprio perché devono ancora essere determinati i 'requisiti aggiuntivi' ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione.
A oggi Accredia ha accreditato lo schema proprietario conforme alla ISO/IEC 17065, gestito da un organismo che rilascia la certificazione ISDP©10003:2015 (https://is.gd/uEjCZp) dei processi per la tutela delle persone fisiche con riguardo al trattamento dei dati personali – Regolamento UE 679/2016. Schema suscettibile di opportuni adeguamenti, quando gli eventuali criteri integrativi di cui agli artt. 42 e 43 del Regolamento verranno rilasciati dal comitato o dall'autorità nazionale competente.
Una certificazione già attiva in materia di protezione dei dati personali è anche quella conforme alla norma ISO/IEC 27001, che riguarda i sistemi di gestione per la sicurezza delle informazioni, integrata con le linee guida ISO/IEC 27018[2]. Indirizzata *ai service providers* di *public cloud* che elaborano dati personali (*Personally Identifiable Information* - PII) e che agiscano in qualità di *data (PII) processor*, l'implementazione delle linee guida contribuisce a garantire il rispetto dei principi e delle norme privacy, da parte dei *pro-*

viders di *public cloud* che se ne dotano. Si tratta, tuttavia, di una certificazione di sistema di gestione che viene accreditata ai sensi della norma ISO/IEC 17021-1, e non della ISO/IEC 17065 indicata dal GDPR come riferimento.
È stata anche pubblicata la nuova prassi di riferimento UNI *Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 GDPR*, elaborata dal tavolo di lavoro 'Requisiti dei processi di gestione della privacy in ambito digitale' condotto da UNI con la partecipazione di Accredia e degli altri *stakeholders*. Articolata in due parti, una di supporto alla definizione e attuazione dei processi di trattamento dei dati personali, e l'altra contenente i requisiti per la conformità, la prassi si rivolge alle organizzazioni che trattano dati con strumenti informatici, con particolare attenzione alle PMI che possono giovarsi di uno strumento di guida standardizzato e coerente con il GDPR. La corretta implementazione di azioni efficaci per il trattamento dei dati con modalità IT può diventare uno strumento competitivo per le aziende che vogliono dimostrare la propria conformità, oltre che un metro di giudizio per le autorità competenti, con il valore aggiunto della certificazione di terza parte indipendente, secondo i requisiti della norma ISO/IEC 17065.
A breve inizieranno le attività di verifica ai fini dell'accreditamento.
Ma è sul fronte della definizione delle competenze del personale che il Regolamento 679/2016 trova un effettivo elemento complementare nella nuova norma (pubblicata nel novembre scorso) UNI 11697:2017 *Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza*. Il Regolamento prevede infatti la presenza del *Data Protection Officer* (DPO) in tutte le aziende pubbliche, in quelle dove il trattamento dei dati presenti rischi specifichi e quelle che trattano 'dati sensibili'. La competenza del DPO può quindi essere certificata sotto accreditamento, volontariamente, sulla base dei requisiti indicati nella norma UNI 11697, secondo le specifiche indicate da Accredia in apposita circolare[3].
Inoltre, l'ente ha coinvolto le parti interessate (inclusi UNINFO e il Garante) per definire regole e criteri comuni per tutti gli organismi di certificazione e si auspica che la norma venga promossa a livello europeo (Comitato Europeo di Normazione - CEN) per le figure professionali del responsabile

della protezione dati, manager Privacy, verificatore Privacy e specialist Privacy. Queste regole, già pubblicate da Accredia sotto forma di circolare, a breve verranno pubblicate anche come prassi di riferimento UNI (il tavolo dovrebbe finire i lavori in primavera).
A fronte di questa esperienza, e dato che l'Italia in materia di tutela della privacy risulta tra i Paesi capofila dell'Unione Europea, Accredia continua dunque a fornire al Garante e all'ente di normazione nazionale tutto il supporto tecnico possibile, garantendo il suo *know-how* in materia di accreditamento. L'accreditamento è sinonimo di garanzia e affidabilità per istituzioni, imprese e consumatori e le certificazioni accreditate assicurano la conformità di sistemi, processi, prodotti, servizi e persone ai requisiti fissati dalle norme e dagli standard internazionali. Inoltre, grazie agli Accordi di mutuo riconoscimento firmati dagli enti di accreditamento a livello europeo (EA MLA) e mondiale (IAF MLA), le certificazioni sono riconosciute a livello internazionale. Ci sono quindi tutte le premesse per garantire il cittadino e tutelare il suo diritto fondamentale alla sicurezza e alla protezione delle informazioni personali.

Intervento al convegno
Il valore dell'accreditamento per le certificazioni previste dal Regolamento 679/2016
https://www.youtube.com/watch?v=QhhxilesQHU&feature=youtu.be

Link alle slide
filippo trifiletti - il valore dell'accreditamento per le certificazioni previste dal reg. 679-2016

NOTE

[1] Cfr. Circolare ACCREDIA DC N° 30/2017 'Informativa in merito all'accreditamento prodotto (ISO/IEC 17065) delle certificazioni rilasciate in conformità allo schema ISDP 10003:2015 - Reg. EU 679/2016' in www.accredia.it/documenti.

[2] Cfr. Circolare ACCREDIA DC N° 13/2017 'Informativa in merito all'accreditamento per lo schema di certificazione ISO/IEC 27001:2013 con integrazione della linea guida ISO/IEC 27018:2014' in www.accredia.it/documenti.

[3] Cfr. Circolare ACCREDIA DC N° 3/2018 'Disposizioni in materia di certificazione e accreditamento per la conformità alla norma UNI 11697:2017 - Profili professionali relativi al trattamento e alla protezione dei dati personali' in www.accredia.it/documenti.

* Filippo Trifiletti: direttore generale di Accredia, l'ente italiano di accreditamento, ha partecipato a svariati organi collegiali, in ambito nazionale e internazionale, collaborando alla definizione e attuazione delle politiche dell'Unione Europea. Inoltre, nell'ambito dell'attività professionale, ha costantemente tenuto relazioni in convegni pubblici e docenze in attività corsuali, legate alle competenze. Dal 2007 al 2009 è stato direttore generale di SINCERT e, fino al 2007, direttore responsabile Area economica e internazionale (ultimo incarico ricoperto).

GDPR: SICUREZZA INFORMATICA E SPUNTI OPERATIVI

Alessandro Da Re*

Con il Regolamento UE 679/2016, il processo di *risk management*, e dunque la necessità e l'esigenza delle organizzazioni complesse di governare questioni che diversamente a lungo andare potrebbero creare danno, diviene a maggior titolo uno dei pilastri della privacy, così come la gestione degli incidenti di sicurezza informatica i quali, tuttavia, possono risultare per i meno preparati, tematiche davvero complesse.
La buona notizia è che nell'*Information Security Governance*, soprattutto nei Paesi anglosassoni il governo del rischio è un titolo che gode da lungo periodo di *framework* e modelli di riferimento maturi e ampiamente usati.
La domanda comunque è lecita: perché le regole sono cambiate? Non andavano bene quelle di prima? Perché il legislatore comunitario ha ritenuto utile estendere il pensiero nei confronti di un tema che di fatto va oltre i perimetri di frontiere sociali per divenire una logomachia planetaria? Forse perché a differenza di quanto si ritenesse in passato sono cambiati gli scenari e questo cambiamento segue regole matematiche asintotiche?
Ma che cos'è il rischio e come si può misurare? La risposta è 'dipende' e dipende davvero da molti fattori, tra cui lo scenario di riferimento, le minacce, le vulnerabilità, il valore del bene da difendere, l'impatto sull'organizzazione se violato, dal tipo di danno che ne deriva ovvero se economico, di immagine o entrambi.
Dipende anche dal rischio inerente – un istituto di credito ha un rischio inerente diverso da un ospedale –, ma soprattutto dipende se di quel rischio me ne sono preso cura.

Significa quindi evidenziare la necessità di proporre metodi consolidati per il trattamento del rischio, a partire dalla sua analisi per procedere verso la sua mitigazione accettandone il *residuo*, ovvero il suo trasferimento.
In linea di principio, il rischio può essere definito come probabile frequenza e probabile magnitudine di future perdite.
Scenari diversi quindi e presenza di elementi di *iperconnessione:* gli scenari IOT (*Internet of Things*) moderni dove l'esigenza del 'sempre connessi' porta a fattori di rischio non sottovalutabili e in alcuni casi difficilmente individuabili e mitigabili.
Definire il perimetro, ecco qual è il 'Santo Graal' nella gestione del rischio in un contesto in cui lo stesso risulta sempre più liquido; ben venga il Regolamento quindi, che, come dicevamo, pone nelle questioni di metodo, ancor prima di quelle giuridiche, il contenimento ed il trattamento di elementi che di fatto possono compromettere anche la sicurezza di una comunità.
Ne è esempio quanto avvenuto nelle zone sensibili di guerra in Medio Oriente: ideata come un'innocua app rivolta ai *runners*, scaricabile su uno smartphone o un braccialetto per il fitness, Strava Labs è tra le più utilizzate per monitorare i propri esercizi fisici, tracciare i percorsi di jogging e condividerli con altri atleti. Almeno questo è lo scopo per cui è stata studiata.
In realtà, si sta rivelando una pericolosa arma in grado di fornire informazioni potenzialmente sensibili sul personale militare americano e alleato in luoghi 'caldi' come Afghanistan, Iraq e Siria.
In modo inconsapevole, infatti, ha pubblicato una mappa costruita con i dati sull'attività fisica nel mondo. Mentre alcune basi sono ben note ai gruppi che vogliono attaccarle, la mappa mostra anche percorsi alternativi che potrebbero far supporre l'esistenza di basi segrete e quindi rivelare possibili obiettivi di attacco.
A lanciare l'allarme è stato su Twitter, Nathan Ruser, analista dell'Institute for United Conflict Analytics: «Strava ha rilasciato la mappa mondiale, 1,3 miliardi di localizzazioni Gps. È molto bella ma non buona per le operazioni segrete e le basi militari americane che sono identificabili».
Nella mia carriera di studioso di *cyber security* ho avuto l'onore di assistere ad una lezione magistrale dell'ex direttore generale dell'MI5 (i servizi

britannici di *intelligence* militare), Sir Lord Jonathan Evans, Baron Evans of Weardale, il quale, in modo molto sintetico ma efficace, elargiva dall'alto della sua indiscussa esperienza nella gestione dei rischi i seguenti sei comandamenti:

1. *La sicurezza non è una questione a buon mercato*. Sta a indicare il fatto che non solo è necessario definire e disporre di un conto economico che consideri nelle sue poste il *giusto* budget per la *cyber security*, ma ciò che deve cambiare è la *security posture*, ovvero la cultura di come nelle organizzazioni si affronta il tema, e organizzare il cambiamento di cultura, si sa, risulta spesso il costo più alto da sostenere, soprattutto se è il vertice che distoglie lo sguardo da un tema così delicato.
2. È *sicuramente costosa, ma lo è decisamente meno che gestire un disastro*. Purtroppo le organizzazioni immature nel nostro Paese sono numerose (anche tra le più blasonate) e se ne renderanno conto solamente dal momento in cui quel disastro avverrà davvero.
3. È *indispensabile un piano per rispondere agli incidenti e va provato*. Chiediamoci: quanti di noi hanno un piano di *continuità*, ovvero di resilienza, agli incidenti di sicurezza? Quanti hanno un piano di *ripristino* da disastro? E quanti soprattutto, ammesso che gli stessi siano consistenti e non si trasferiscano da qualcosa di copiato solo per il gusto di redigere in conformità al cogente, sono stati sottoposti a reali test periodici?
4. *Se non lo provi, sarai lento in caso di emergenza*. Immaginiamo solo per un attimo cosa accadrebbe se non ci fosse un protocollo di emergenza (c.d. *triage*) nei presidi di pronto soccorso, dal momento in cui avviene la segnalazione dell'incidente per poi continuare nel luogo del primo soccorso, durante il trasporto in ospedale e via via, o ancora in caso di disastro ambientale se la Protezione Civile non disponesse di protocolli studiati ed esercitati.
5. *Non lo potete fare da soli.* Tradotto ciò significa: assicuratevi il supporto dell'intera organizzazione, dall'apice a chi, con tutto rispetto, svuota i cestini e ancora lungo tutta la *filiera dell'informazione*, clienti e fornitori compresi.
6. *Sarete violati*. In realtà Lord Evans affermò «...you will be penetrated...», ma la traduzione letterale non mi pareva elegante.

Esistono diversi modi di gestire il rischio. Il primo è quello di un serio programma di *risk management*; quindi: analisi e applicazione delle contromisure; il secondo, meno consigliabile, è quello di gestire il rischio dopo che si sono verificati gli incidenti studiando di volta, in volta le contromisure.
Per quanto riguarda il contesto GDPR, risulta sicuramente fondamentale applicare contromisure e misure di sicurezza adeguate a governare il modo efficace ed efficiente il rischio, dove la comprensione del ciclo di vita del dato, il governo della profilatura delle abilitazioni (c.d *segregation of duty*), l'inventario delle risorse IT e la condivisioni delle politiche di sicurezza aziendali con le terze parti rappresentano i pilastri su cui poggiare le basi dell'*Information Security Governance*.
L'analisi di impatto, dal mio punto di vista va estesa non solo per quanto concerne le valutazioni in merito ai requisiti di cogente ovvero laddove viene compromessa la libertà del soggetto interessato al trattamento, ma anche e soprattutto nei confronti di tutte le informazioni trattate, anche quelle di business, facendo in modo che tutto ciò diventi 'cultura' per le aziende, dando loro la capacità di rappresentarsi più solide e competitive in un contesto internazionale complesso.
Fate attenzione ai principi base della sicurezza delle informazioni ai quali il legislatore si è ispirato – parliamo allora di *baseline security* –, ovvero cercate di comprendere se state camminando eretti, con la schiena diritta e in grado di schivare i pericoli oppure se state tentando di attraversare una superstrada a quattro corsie a gattoni, con occhi bendati e cuffiette con il *rock 'n' roll* che suona a palla.
A tal fine vi suggerisco alcuni *framework* da prendere seriamente in considerazione (cfr. considerando 90 del Regolamento):

- ISO/IEC 27002:2013 - *Information Technology - Security Techniques - Code of Practice for information security controls*, che vi permetterà di valutare la vostra 'postura' sull'*Information Security Governance*;
- ISO/IEC 31000:2018 - *Risk management - Guidelines*, che vi fornirà le linee guida per la gestione del rischio;
- ISO/IEC 31010:2009 - *Risk management - Risk Assesment Techniques*, che vi permetterà di misurarlo;
- ISO/IEC 29100:2011 - *Information Technology - Security Techniques*. È un

privacy framework appositamente studiato per i temi inerenti la privacy;
- ISACA CobIT 5 For Risk - con i suoi 111 esempi di scenari di rischio, offre esempi reali e deriva sia i controlli di sicurezza necessari, che le misure di efficacia sull'applicazione degli stessi.

Vanno certamente prese in esame le tecnologie per il rilevamento in tempo idoneo delle anomalie che concorrono al *data breach*, tenendo sempre a mente che spegnere il lumicino di una candela è sicuramente più facile che domare un incendio, ma rilevarne la luce a volte può essere davvero complesso.
In questo senso, la tecnologia sta sicuramente facendo passi da gigante in considerazione del fatto che oramai l'intelligenza artificiale o meglio i protocolli di *Machine Learning* concorrono a sostenere i requisiti di sicurezza negli scenari complessi di elaborazione, così come le infrastrutture di *Computer Emergency Response Team* (CERT) costituiscono un ottimo ausilio.
La necessità poi di far evolvere in modo considerevole la cultura sulla sicurezza delle informazioni a tutti i livelli rimane a mio modesto avviso, soprattutto nel nostro bel Paese, nel nostro operoso territorio, *il* problema, la questione centrale.
Secondo studi del Ponemon Institute, l'Italia è tra i Paesi che, a parità di investimenti sulla sicurezza delle informazioni, si colloca nelle ultime posizioni in relazione alla loro efficacia; la misura indica il valore degli investimenti in persone e tecnologie, ovvero la capacità di questi ultimi di essere al tempo stesso efficaci nella missione di fornire sicurezza utilizzando una quantità di risorse limitata. Il valore dell'Italia (negativo) indica che c'è tanto lavoro da fare, ed è un lavoro soprattutto di natura culturale. L'IT continua ad essere percepito dal business come un costo e non come un *asset* di valore per il raggiungimento degli obiettivi di business dell'azienda; fin tanto che questa tendenza non cambia, aumentare il livello di sicurezza delle nostre organizzazioni sarà difficile.
Mai come in questo contesto storico appare fondamentale ottenere l'*endorsement* a livello apicale per condividere strategie e obiettivi, governare il rischio, ottimizzare gli investimenti, essere sicuri e quindi conformi.

Intervento al convegno
Risk management: cinque brevi note per accelerare il processo di conformità al GDPR
https://www.youtube.com/watch?v=8kVA5J_olNk&feature=youtu.be

Link alle slide
alessandro da re - risk management

* Alessandro Da Re: ingegnere informatico, ha maturato la sua esperienza assumendo incarichi direzionali in progetti di governo della sicurezza delle informazioni, la gestione del rischio cyber, la conformità ai requisiti normativi nazionali e internazionali, l'analisi, definizione e implementazione di infrastrutture informatiche complesse nel ruolo di *Information Security Practice Manager*. Già consulente ministeriale, di importanti gruppi bancari e strutture ospedaliere nazionali e locali è tutt'ora in servizio presso il Gruppo Poste Italiane e un importante marchio del settore *fashion industries*. Studioso e cultore di modelli per la misura e la gestione del rischio informatico, è stato, nel merito, ideatore e co-autore di brevetto industriale nazionale. Relatore a sessioni di studio Associazione Italiana Information System Auditors (AIEA), il capitolo italiano dell'ordine professionale statunitense Information Systems Audit and Control Association (ISACA), che raggruppa più di 180.000 professionisti nel settore della sicurezza informatica su oltre centoquaranta Paesi), è co-relatore in convegni nazionali, organizzati dall'Associazione per lo Studio del Diritto, unitamente all'Agenzia per l'Italia Digitale (AgID), l'Autorità garante per la protezione dei dati italiana e l'Ufficio del Garante Privacy europeo. Nel tempo libero ama viaggiare, lo studio della sociologia e costruire chitarre classiche. È *associate platinum member* dell'ordine professionale ISACA e assiduo frequentatore degli eventi internazionali sulla sicurezza cibernetica (c.d. EURO CACS Conference). Ha conseguito le certificazioni professionali internazionali ISACA®: CRISC® (*Certified in Risk and Information System Control*), CSX® (*Cyber Security Nexsus*), CobIT Fundation® (*Control Objective for Information and Related Technolgy*).

La vignetta di Federico Cecchin

www.federicocecchin.com

ISSN 1825-9073

€ 10,00