Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 3-20

Il Regolamento europeo sulla protezione dei dati: specificità e risvolti economici

Giorgio Caridi*, Livio Milano**

Sommario: 1. I diritti degli interessati. – 2. Gli obblighi nell'elaborazione dei dati personali. – 3. Gli obblighi del responsabile del trattamento. – 4. I risvolti economici del GDPR.

1. *I diritti degli interessati*

Il diritto di opporsi è conferito a tutti gli interessati dal Regolamento generale sulla protezione dei dati dal momento che possono sussistere motivi relativi a situazioni particolari delle persone i quali giustificano l'esercizio di questo diritto in relazione al trattamento dei loro dati personali. Questo è il caso di quando il trattamento sia necessario per l'esecuzione di adempimenti di interesse pubblico, o sia richiesto nell'esercizio dell'autorità ufficiale da parte dei responsabili del trattamento dei dati, o quando tale trattamento debba essere effettuato ai fini degli interessi legittimi perseguiti dal controllore o da terze parti.

Il diritto di obiettare esiste anche quando ci sono attività di profilazione svolte in queste situazioni. Fare appello a questo diritto impedisce ai responsabili del trattamento di elaborare ulteriormente i dati personali. Tuttavia, essi possono continuare a elaborare tali informazioni se è possibile dimostrare la sussistenza di motivi legittimi validi per il trattamento in modo da ignorare gli interessi, i diritti e le libertà degli interessati. Lo stesso vale anche quando vi sono validi motivi legittimi per l'istituzione, l'esercizio o la difesa di rivendicazioni legali.

Ciò che è altamente rilevante per tutti noi, al giorno d'oggi, è il fatto che questo diritto può essere esercitato anche quando i dati personali degli individui vengono elaborati nel contesto del marketing diretto o

* Dottore di Ricerca in "Comunicazione, interculturalità ed organizzazioni complesse", cultore della materia, LUMSA Roma.

** Avvocato in Roma.

della profilazione relativa a tale marketing. Può essere fatto in qualsiasi momento, e quando gli interessati si oppongono, i loro dati personali non possono più essere elaborati per il marketing diretto. Al momento della prima comunicazione con gli interessati, l'esistenza del diritto di opporsi, come indicato in precedenza, deve essere indicata a questi ultimi in modo chiaro e separatamente dalle altre informazioni. Questo diritto può essere esercitato dagli interessati quando si utilizzano i servizi di società dell'informazione con mezzi automatizzati, tramite specifiche tecniche. È importante sottolineare che il diritto di opporsi esiste anche quando i dati personali degli individui vengono elaborati per scopi di ricerca scientifica o storica o per fini statistici. Questo, tuttavia, non avviene se il trattamento viene effettuato per motivi di interesse pubblico.

Infine, il GDPR stabilisce il diritto alla restrizione dell'elaborazione.

Gli interessati hanno il diritto di ottenere dai controllori una restrizione dell'elaborazione quando si verifica una delle seguenti condizioni. Innanzitutto, gli interessati contestano l'accuratezza dei dati personali per un periodo che consente ai responsabili del controllo di verificarne l'esattezza. In secondo luogo, il trattamento è illecito e gli interessati sono contrari alla cancellazione dei propri dati personali e richiedono invece la limitazione del loro utilizzo. In terzo luogo, i responsabili del trattamento non hanno più bisogno di dati personali ai fini del trattamento, ma tali dati sono richiesti dalle persone interessate per l'istituzione, l'esercizio o la difesa di rivendicazioni legali. In quarto luogo, gli interessati sono contrari all'elaborazione in attesa della verifica, indipendentemente dal fatto che i motivi legittimi dei controllori prevalgano su quelli degli interessati.

Altri due diritti significativi degli interessati dal GDPR sono il diritto alla cancellazione e il diritto alla portabilità dei dati. Il diritto alla cancellazione è talvolta noto come il diritto all'oblio o ad essere dimenticati, sebbene questa denominazione non sia del tutto corretta. «In estrema sintesi tale disposizione prevede il diritto all'oblio e alla cancellazione, rafforzando il diritto alla cancellazione di cui all'art. 12 lett. B) Direttiva 95/46, nonché l'obbligo per il titolare del trattamento che abbia divulgato dati personali di informare i terzi della richiesta dell'interessato di cancellare tutti i link verso tali dati, le loro copie o riproduzioni»[1].

[1] Cfr. G. Resta, V. Zeno-Zencovich, *Il diritto all'oblio su internet dopo Google Spain*, Roma, RomaTre-Press, 2015, pp. 245-246.

Il Regolamento europeo sulla protezione dei dati: specificità e risvolti economici

L'Articolo analizza i diritti e gli obblighi scaturenti dal GDPR, con un focus su quelli propri del Responsabile del trattamento. In seguito, viene proposta anche un'analisi dell'impatto che la normativa EU può avere sulle PMI italiane, dal punto di vista economico ed organizzativo.

General Data Protection Regulation: peculiarities and economic implications

The article analyzes the rights and obligations arising from the GDPR, with a focus on the responsibilities of the DPO. Then it will analyze the impact that this EU legislation will have on Italian SMEs, from an economic and organizational point of view.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 21-38

Le nuove sfide del diritto europeo nell'era dei big data

Giulia Mercadante*

Sommario: 1. Privacy e tutela della dignità della persona. – 2. Big data: funzionamento e tecnologia. – 3. GDPR e strumenti per la privacy-by-design. – 4. Il conflitto istituzioni-aziende digitali su scala globale.

1. *Privacy e tutela della dignità della persona*

Le nuove sfide sociali imposte dalla complessità del reale contemporaneo, segnato dall'evoluzione che dalla fine degli anni Novanta a oggi ha interessato Internet e i servizi da esso derivati, investono giocoforza le istituzioni giuridiche e politiche, imponendo al legislatore una presa di coscienza profonda delle dinamiche derivanti dalle tecnologie a disposizione e dalla loro diffusione. Considerando anche solo superficialmente questi meccanismi, è evidente come questo tipo di trasformazione tecnologica ci abbia portato a vivere in un contesto in cui il trattamento digitalizzato dei dati coinvolge grandissima parte delle relazioni interpersonali che non avvengono fisicamente. È oggi necessario superare la visione dualistica tra realtà digitale e realtà "reale" a favore di una prospettiva che tenga conto di una realtà complessiva formata da entrambe le componenti, nella quale non si può parlare di progresso equo e libero senza avere chiaro che avanzamento tecnico-tecnologico e necessità di garantire i diritti fondamentali delle persone sono intimamente legati. Inoltre, solo le società e le istituzioni che hanno contezza delle potenzialità, del funzionamento e dei rischi delle tecnologie di cui dispongono sono in grado di elaborare una strategia politico-economica del loro utilizzo e di inserirsi nel delicato equilibrio geopolitico che caratterizza questa fase storica.

La tutela della libertà della persona, nel suo senso privato, economico, sociale, politico e religioso, è nei sistemi a matrice democratica il

* Dottoressa magistrale in linguistica all'Università di Pisa, ora studentessa di informatica umanistica, corso magistrale.

valore fondamentale dei diritti universali dell'uomo nel quale possiamo trovare un punto di ancoraggio per rifondare una contemporaneità priva di riferimenti, sia politici, sia valoriali ben delimitati. Il suo senso ultimo risiede nel rispetto della dignità della persona, presupposto cardine sul quale poggia il diritto alla riservatezza e alla protezione dei dati personali. La garanzia di una sfera personale sottratta alle intrusioni di terzi, e l'assicurazione che determinate informazioni resteranno private, proteggono infatti l'individuo da eventuali discriminazioni e gli assicurano la possibilità di godere del diritto al pieno sviluppo della persona umana: è chiara la relazione biunivoca che intercorre tra individuale e sociale nella contemporanea società del *web 2.0* e la necessità di soluzioni che mirino a un'ottimale convivenza tra i due aspetti. A partire dall'Articolo 8 della Carta di Nizza, il quale richiede il rispetto del principio di leale cooperazione per la regolamentazione sul trattamento dei dati personali, la limitazione del trattamento alle sole finalità coperte dal consenso e la vigilanza di un'autorità indipendente, si deduce che l'Unione Europea individua nella protezione dei dati personali un vero e proprio diritto fondamentale da mantenere e a aggiornare tramite intervento legislativo.

Il General Data Protection Regulation (da qui in poi abbreviato in GDPR) soddisfa questa esigenza, ponendosi l'obiettivo di conciliare la protezione dei cittadini europei con lo sviluppo delle possibilità offerte dal digitale, funzionali sia al miglioramento dei servizi disponibili, sia alla sopravvivenza e alla competitività degli Stati del Vecchio Continente all'interno degli equilibri politici ed economici mondiali.

Il risultato è una legislazione realista che prende atto dell'inarrestabilità e della non reversibilità del processo evolutivo della tecnologia e del fatto che il mondo e la politica debbano ormai costruire il proprio futuro sull'uso sempre più sofisticato dei dati.

2. *Big data: funzionamento e tecnologia*

Come è implicito, la prospettiva evolutiva dell'Internet 2.0 porta la necessità di un aggiornamento in senso legislativo che tenga conto delle problematiche legate ai trattamenti big data.

Il GDPR non contiene norme specifiche in materia di big data, ma fornisce di fatto gli strumenti per disciplinarli, ribadendo il principio di

Le nuove sfide del diritto europeo nell'era dei big data

Nell'epoca della frenetica evoluzione tecnologica e della sovrabbondanza di dati utilizzati per molteplici scopi, si pongono con sempre più forza gli interrogativi riguardanti la protezione della *privacy* dei cittadini e della sicurezza sociale, ma soprattutto dell'effettiva possibilità che esse siano compiute. Poiché neanche il General Data Protection Regulation è esente dal rischio di diventare un palliativo utile al mero rispetto della forma, vogliamo qua mettere in luce gli aspetti che lo rendono capace di adattarsi al rapido cambiamento dei mezzi a disposizione per il trattamento dei dati. Si sottolineano inoltre le soluzioni e la tutela strutturale che esso offre per gestire il flusso di dati prodotti dal web in prospettiva big data e i loro possibili utilizzi, e si indagano i suggerimenti da esso forniti per una opportuna applicazione. L'attenta osservazione di queste caratteristiche ci mostra che il GDPR può diventare un valido strumento con il quale l'UE può proporre un modello di protezione dati che coniughi i diritti delle persone con le esigenze del mercato.

New challenges of European law in big data era

In this period of fast technological evolution and overabundance of data used for various purposes, the questions about citizens privacy protection and social security necessarily stand out. Since the General Data Protection Regulation is not exempt from the risk of becoming a stopgap measure to merely accomplish the legal procedure, our purpose is to highlight the aspects that make this regulation adaptive to data processing tools changes. Furthermore, we would like to a) underline the solutions and the structural protection that it offers to manage big data flow and their possible employments, b) investigate the suggestions it provides for an appropriate compliance. The careful observation of these characteristics leads us to believe that the EU could propose the GDPR as a valuable tool and a positive model of data protection, combining people rights and market requirements.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 41-58

«Nessuno può mettere il GDPR in un angolo». Breve storia comparata del consenso per il marketing nell'era globale

Tania Orrù*

Sommario: 1. Introduzione – 2. Il caso pratico. – 3. Il consenso marketing "globale" e il trasferimento transfrontaliero dei dati. – 4. Il GDPR e gli altri ordinamenti: una relazione da approfondire. Breve panoramica comparata su consenso marketing e trasferimento dei dati all'estero: a. Stati Uniti; b. Giappone; c. Russia; d. Repubblica Popolare Cinese. – 5. Conclusioni.

1. *Introduzione*

Nell'economia globale e nell'era digitale, dove, per dirla col nostro Garante «confini e distanze si fanno permeabili ai nostri dati, soprattutto in formato digitale, ed il nuovo spazio telematico rende labili i riparti di giurisdizione»[1], il Regolamento Europeo 2016/679 (in seguito, GDPR)[2], inteso come "fronte comune" europeo, non può che trovarsi costantemente a confronto con i principi e le regole vigenti in materia negli altri ordinamenti. Il presente Articolo, partendo da un caso pratico, si propone di offrire alcune indicazioni utili per i professionisti privacy inclu-

* Avvocato. Dopo alcune esperienze in ambito aziendale quale giurista d'impresa, a marzo 2011 entra a far parte, costituendone il primo nucleo, dell'Ufficio Affari Legali e Societari di una nota *maison* italiana quotata in Borsa, che opera nel settore della moda di lusso. Specializzata in data protection law, dal 9 maggio 2013 ricopre il ruolo di privacy officer e dal 10 maggio 2018 è data protection officer di tale società.

[1] Le parole riportate sono di G. Bianchi Clerici (Garante), "Privacy: il Garante italiano incontra l'Autorità giapponese", Comunicato stampa Garante 22 novembre 2017, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7187436.

[2] Cfr. Regolamento EU 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati e abrogazione della Direttiva 95/46/EC (General Data Protection Regulation).

se le principali normative di riferimento e qualche spunto di riflessione in merito alla coesistenza dei diversi ordinamenti internazionali, dei loro principi, delle loro regolamentazioni e quanto disposto in Europa dal GDPR, con particolare riguardo alla disciplina del consenso marketing e al trasferimento transfrontaliero dei dati da paesi terzi verso l'Unione Europea.

2. *Il caso pratico*

Il presente scritto nasce dalla difficoltà pratica di rintracciare pubblicazioni o manuali operativi di diritto privacy "internazionale comparato" che pongano direttamente a confronto la regolamentazione europea GDPR e gli altri ordinamenti.

Poniamo in particolare il caso di un operatore (inteso come qualsiasi professionista specializzato in data protection law (che sia esso consulente, privacy officer, data protection officer) che debba assistere un'azienda avente sede all'interno dell'Unione Europea, la quale, oltre a commercializzare i propri prodotti attraverso un suo sito e-commerce, li distribuisce e commercializza, in paesi dell'Unione e in paesi extra-UE, tramite una rete di negozi gestiti da società locali (appartenenti al medesimo Gruppo) dalla stessa controllate in qualità di Capogruppo. In particolare, si noti che la raccolta e il trattamento dei dati dei clienti finali dei negozi (vale a dire dati anagrafici, dati di contatto, ecc.) vengono acquisiti tramite la compilazione, da parte dei clienti finali, delle consuete schede clienti nelle quali è previsto il rilascio di consensi specifici e informati al trattamento dei dati forniti per le seguenti finalità (che si potrebbero definire "classiche" per le aziende) ovvero: la prestazione di servizi di assistenza e cura del cliente sia sul piano amministrativo che con riguardo al rapporto di vendita, inclusa l'attività di marketing diretto e analisi degli acquisti effettuati mediante l'applicazione di parametri geografici, di età, di ripetitività, di interesse merceologico e gusto, di controvalore economico; i suggerimenti per acquisti futuri; l'invio di comunicazioni promozionali e di marketing attraverso strumenti automatizzati e non, incluse ricerche di mercato personalizzate in base alla profilazione dei dati dei clienti; l'analisi del comportamento di acquisto (nonché del comportamento di navigazione). Il tutto riconciliando e incrociando in un sistema di *Customer*

«Nessuno può mettere il GDPR in un angolo». Breve storia comparata del consenso per il marketing nell'era globale

L'Articolo, partendo da un caso pratico, si propone di offrire alcune indicazioni utili, le normative di riferimento e qualche spunto di riflessione per gli operatori in ambito data protection in merito alla coesistenza fra i diversi ordinamenti internazionali, i loro principi, le loro regole e quanto disposto in Europa dal GDPR, con particolare riguardo per la disciplina del consenso marketing e per il trasferimento transfrontaliero dei dati da paesi terzi verso l'Unione Europea; il tutto attraverso una breve panoramica comparata con alcuni ordinamenti esteri (Stati Uniti, Giappone, Russia, Repubblica Popolare Cinese). Al termine dell'analisi discenderanno alcune considerazioni sulla potenziale "trasversalità" internazionale dei principi alla base del GDPR e sul valore di spinta propulsiva che quest'ultimo potrebbe rivestire per gli ordinamenti esteri che già guardano alla regolamentazione europea uniforme con notevole interesse.

Nobody can put the GDPR in a corner. A short comparative story of marketing consent in the global era.

The aim of this Article, starting from a practical case, is to provide to the data protection operators with some useful indications, reference regulations and some food for thought on the coexistence between the different international legal systems, their principles, their rules, in comparison with the GDPR provisions in Europe, with particular regard to the regulation of marketing consent and the cross-border transfer of data from third countries to the European Union; all through a brief overview compared with some foreign jurisdictions (United States, Japan, Russia, People's Republic of China). At the end of the analysis there will be some considerations on the potential international "transversality" of the principles underlying the GDPR and on the value of propulsive thrust that the latter could have for foreign jurisdictions that already look at the uniform European regulation with considerable interest.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 59-76

Le "icone": un nuovo strumento a tutela dei dati personali

Roberto Pusceddu*

Sommario: 1. Oggetto d'indagine. – 2. Il dominio della parola: il c.d. logocentrismo. – 3. La disposizione normativa. – 4. Il "Legal Design": un approccio "nuovo" al diritto. – 5. La funzione informativa dell'icona nel documento giuridico. – 6. L'esempio delle Creative Commons. – 7. Una prima proposta: la standardizzazione delle "icone". – 8. Critica: l'impossibilità di semplificare un linguaggio complesso. – 9. Conclusioni.

1. *Oggetto d'indagine*

Il presente contributo ha ad oggetto il Regolamento UE n. 679/2016 e si sofferma, in particolare, sull'utilizzo del disegno (nella forma di "icone") con riferimento alle misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intellegibile e facilmente accessibile mediante l'utilizzo di un linguaggio semplice e chiaro.

Ciò che si pone in rilievo nel presente elaborato è il particolare rapporto che intercorre tra il disegno ed il diritto e, nello specifico, si indagherà la funzione, o le funzioni, che le icone svolgono nella tutela e nella protezione dei dati personali.

In altri termini, l'interessato deve essere messo nella condizione di poter comprendere sempre come dovranno essere trattati i suoi dati personali.

Il presente elaborato impone, dunque, di soffermarsi sul particolare rapporto tra il "diritto" ed il "disegno".

* Avvocato, Cultore di materia in Filosofia del Diritto e Teoria Generale del diritto, Dottorando di Ricerca in Scienze Giuridiche presso l'Università degli Studi di Cagliari.

Giova precisare che "Il disegno nel diritto" è una tematica studiata, infatti, sotto molteplici sfaccettature da David Howes (Concordia University), Margaret Hagan (Stanford University), nell'ambito del Laboratorio "Lawbydesign", Richard K. Shering (New York Law School), Volker Boehme- Neßler (Carl von Ossietzky Universität Oldenburg) e, nell'ambito dell'Università di Cagliari, da Giuseppe Lorini, Stefano Moroni e Patrick Maynard (i quali, in particolare, hanno indagato le norme disegnate ed i disegni normativi).

2. *Il dominio della parola: il c.d. logocentrismo*

È bene domandarsi, in primo luogo, quali funzioni vengano assolte dalle immagini nel diritto. A riguardo, occorre sottolineare che il rapporto tra il diritto ed il disegno non può certo definirsi pacifico. Nel diritto, storicamente, infatti, non vi sono immagini che impongano o descrivano norme.

Il diritto si avvale, di regola, di testi formulati linguisticamente. È agevole affermare che il diritto sia governato dal c.d. logocentrismo[1].

Cosi come ha affermato Volker Boehme-Neßler Volker in "Pictorial law. Modern law and the power of pictures" (2011), il diritto moderno non si avvale di immagini e nei confronti delle stesse conserva un atteggiamento scettico. Questo generale atteggiamento scettico nei confronti delle immagini è il risultato di un evoluzione storica[2].

Nel mondo del diritto, ad oggi, l'immagine si colloca sul piano dell'eccezione alla regola.

La regola è, infatti, rappresentata dal testo formulato linguisticamente (dotato di una formulazione verbale). Si pensi al testo contenuto in una disposizione codicistica ovvero ad una sentenza emessa da un qualsivoglia giudice.

Qualsivoglia documento giuridico – sia esso un atto processuale sia esso un mero atto amministrativo – conterrà degli enunciati formulati linguisticamente. Pur tuttavia, in alcuni ambiti del diritto, è riconosciuto

[1] Cfr. V. Boehme-Neßler, *Pictorial law. Modern law and the power of pictures*, Berlino- Heidelberg, Springer, 2011, p. 107.

[2] *Ivi*, p. 101.

Le "icone": un nuovo strumento a tutela dei dati personali

Il presente contributo ha ad oggetto il Regolamento UE n. 679/2016 e si sofferma, in particolare, sull'utilizzo del disegno (nella forma di "icone') con riferimento alle misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intellegibile e facilmente accessibile mediante l'utilizzo di un linguaggio semplice e chiaro. Ciò che si pone in rilievo nel presente elaborato è il particolare rapporto che intercorre tra il disegno ed il diritto e, nello specifico, si indaga la funzione che le icone svolgono nella tutela e nella protezione dei dati personali. In altri termini, l'interessato deve essere messo nella condizione di poter comprendere sempre come dovranno essere trattati i suoi dati personali.

"Icons": a new instrument to protect personal data

This paper concerns the EU Regulation no. 679/2016 and focuses, in particular, on the use of the Design (in the form of "icons') with reference to appropriate measures to provide the data subject with all the information and communications relating to the treatment in a concise, transparent, intelligible and easily accessible through the use of simple and clear language.
The main objective in this paper is to emphasize the particular relationship between design and law and, in particular, investigates the function that icons play in the protection of personal data. In other words, the holder of interests must have the possibility to understand how his personal data will be processed.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 77-97

Il silenzio della memoria: la tutela del diritto all'oblio dalla sentenza *Google Spain* al Regolamento UE 2016/679

Ilaria Rivera*

Sommario: 1. La giurisprudenza della Corte di giustizia sul "diritto all'oblio": il caso c.d. *Google Spain*. – 2. Il diritto all'oblio e il ruolo di Internet. – 3. Il nuovo quadro normativo europeo: l'Articolo 17 del Regolamento UE 2016/679. – 4. Il diritto all'oblio come forma di tutela dell'identità digitale. – 5. Alcune conclusioni: il silenzio della memoria nell'era digitale.

1. *La giurisprudenza della Corte di giustizia sul "diritto all'oblio": il caso c.d. Google Spain*

Una delle novità più rilevanti del Regolamento europeo 2016/679[1] è certamente la tutela del diritto all'oblio[2].

Il cammino che ha portato alla previsione espressa si snoda in diversi passaggi, che hanno sollecitato l'attenzione nel dibattito scientifico sulle criticità connesse alla diffusione dei dati personali mediante soprattutto gli strumenti digitali.

Nel tentativo di individuare plasticamente i confini della materia, il passaggio da cui occorre partire (e forse quello maggiormente indagato) è

* Assegnista di ricerca in *Juridical Sciences* - Luiss Guido Carli.

[1] Si tratta del Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Sul diritto all'oblio come diritto fondamentale, cfr. E. Stradella, "Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare, e, infine, cui prodest?", «Rivista AIC», n. 4, 2016, pp. 26 ss.

[2] Nella vasta letteratura, per un approfondimento, si vedano E. Gabrielli (a cura di), *Il diritto all'oblio. Atti del Convegno di Studi del 17 maggio 1997*, Napoli, 1999; F. Pizzetti (a cura di), *Il caso del diritto all'oblio*, Torino, 2013; M. Mezzanotte, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009; G. Finocchiaro, "Il diritto all'oblio nel quadro dei diritti della personalità", «Il Diritto dell'informazione e dell'informatica», 2014, pp. 591 ss.

quello della pronuncia della Corte di giustizia dell'Unione europea sul caso Google Spain (causa C-131/12) del 13 maggio 2014[3]. La vicenda è nota e ciò che si intende qui evidenziare è l'interazione tra giudici – nazionale ed europeo – nella risoluzione della questione sottesa alla controversia.

Volendo sintetizzare, nella pronuncia il giudice di Lussemburgo conclude nel senso di ritenere che la disciplina della Direttiva CE 46/95 sulla protezione dei dati personali[4] si applica anche al motore di ricerca Google Inc., in quanto Google Spain rappresenta una succursale[5] stabilita nel territorio spagnolo e, come tale, è soggetta alle norme del suo ordinamento; in secondo luogo – e questo costituisce il cuore del ragionamento – il motore di ricerca Google Spain non potrebbe interpretarsi come mero vettore di dati poiché l'attività posta in essere di rinvenimento delle informazioni, di indicizzazione e di memorizzazione ma costituisce "trattamento dei dati personali"[6], ai sensi dell'art. 2, lett. b) della sopra citata Direttiva[7].

[3] Cfr. Corte Giustizia UE, 13 maggio 2014, C 131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. La questione pregiudiziale è stata proposta dall'autorità giudiziaria spagnola, a seguito dell'accoglimento da parte del Garante della privacy spagnolo del reclamo presentato da un soggetto nei confronti di Google Spain e Google inc., perché, digitando il proprio nome sul motore di ricerca, apparivano i link a pagine del giornale risalenti al marzo 1998, ove si dava pubblicità a una vendita all'asta di immobili a lui pignorati, chiedendo quindi al gestore del motore di ricerca di eliminare i riferimenti alle proprie vicende personali. A seguito della pronuncia, peraltro, Google ha adottato un modulo che può essere presentato dai singoli per richiedere la cancellazione dei propri dati.

[4] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[5] «Il trattamento di dati personali realizzato per le esigenze di servizio di un motore di ricerca come Google Search, il quale venga gestito da un'impresa con sede in uno Stato terzo ma avente uno stabilimento in uno Stato membro, viene effettuato «nel contesto delle attività» di tale stabilimento qualora quest'ultimo sia destinato a garantire, in tale Stato membro, la promozione e la vendita degli spazi pubblicitari proposti dal suddetto motore di ricerca, che servono a rendere redditizio il servizio offerto da quest'ultimo» (p.to 55).

[6] In senso contrario si attestava l'Avvocato generale, sostenendo l'inapplicabilità del ruolo di titolare del trattamento, sulla base della considerazione che «Il fornitore di servizi di motore di ricerca su Internet che offre semplicemente uno strumento di localizzazione delle informazioni non esercita alcun controllo sui dati personali contenuti in pagine web di terzi».

[7] «Trattamento di dati personali» («trattamento»): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati

Il silenzio della memoria: la tutela del diritto all'oblio dalla sentenza Google Spain al Regolamento UE 2016/679

Le nuove tecnologie digitali hanno importato cambiamenti in materia di protezione dei dati personali, con la conseguente necessità di garantire il corretto utilizzo dei dati in considerazione della valida espressione del consenso del soggetto interessato. Il diritto all'oblio si giustificherebbe, in tal senso, laddove il trattamento dei dati non sia più necessario in relazione alle finalità che lo hanno giustificato; d'altra parte, tale diritto non sarebbe legittimo, secondo quanto stabilito dal Regolamento UE 2016/679 (art. 17), ad esempio per garantire l'esercizio della libertà di espressione e di informazione.

The silence of the memory. The protection of the right to be forgotten from Google Spain to Regulation (EU) 2016/679.

The new technologies have brought new challenges for the protection of personal data and so it is the necessity to guarantee the right to the correct use of the personal data in consideration of the data subject's consent. A data subject should have the "right to be forgotten' where the retention of such data is no longer necessary in relation to the purposes for which these data are collected or otherwise processed but, for example, this right shouldn't be lawful where it is necessary, in accordance with the art. 17 of Regulation EU 2016/679, to protect the right of freedom of expression and information.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 99-120

Le nuove frontiere del digital marketing: dalla profilazione alla manipolazione online nell'ambito politico alla luce del GDPR

Irene Rizzuto*

1. *Uso dei dati in ambito politico. Cambridge Analytica, le elezioni presidenziali USA e Brexit*

È già noto da tempo come la politica abbia risposto alla necessità di trovare nuovi strumenti in grado di coinvolgere i cittadini e di realizzare più efficaci campagne elettorali attraverso l'utilizzo delle nuove tecnologie, realizzando campagne mirate di comunicazione pubblicitaria a carattere politico-elettorale.

Di questo uso dei big data e delle conseguenti implicazioni e rischi per le «libertà nelle democrazie tradizionali»[1] ha avuto una forte eco il caso "Cambridge Analytica", del quale si è di recente occupato l'intero giornalismo internazionale, e che ha coinvolto sia il referendum su Brexit nel Regno Unito che la campagna elettorale statunitense del 2016[2].

* Avvocato del foro di Milano, presta la propria attività nell'ambito del diritto civile e della data protection e si occupa di corsi rivolti alle aziende. È stata General Counsel per un'azienda multinazionale del settore e-commerce. Appassionata classicista, ha collaborato con l'Università degli studi di Milano e di Bergamo come assistente alla cattedra di diritto romano e diritto greco.

[1] Cfr. F. Pacifico, "Caso Cambridge Analytica. Il Garante Soro: «Così è a rischio la libertà di scelta», Intervista ad Antonello Solo, Presidente del Garante per la protezione dei dati personali", «Il Mattino», 20 marzo 2018.

[2] Il Garante italiano ha dichiarato che anche nel nostro paese sono in corso valutazioni per l'apertura di un'istruttoria volta ad indagare i rapporti tra alcuni partiti politici italiani e la SCL, casa madre dell'affiliata Cambridge Analytica.

Da quel che risulta dalle inchieste condotte dai quotidiani «The New York Times»[3] e «The Guardian»[4], Cambridge Analytica pare aver sviluppato un sistema di microtargeting comportamentale[5], attraverso l'uso di un metodo sviluppato da Kosinski e Stilwell, ricercatori dell'Università di Cambridge[6].

Questi ultimi hanno infatti elaborato una tecnica per mappare i tratti della personalità in base ai like lasciati dagli utenti su Facebook. In particolare, i ricercatori avevano corrisposto agli utenti piccole somme di denaro per scaricare un'app (MyPersonality), attraverso la quale avevano raccolto alcune informazioni private dai profili dei partecipanti, avevano registrato una media di 170 like per utente ed avevano somministrato test psicometrici[7]. L'obiettivo della ricerca è stato, dunque, quello di dimostrare la capacità predittiva dei like lasciati dagli utenti di Facebook rispetto ad attributi personali come l'orientamento sessuale, la religione, la personalità, l'intelligenza e l'uso di sostanze stupefacenti. Secondo un

[3] M. Rosenberg, N. Confessore, C. Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions", «The New York Times», 17 marzo 2018.

[4] Cfr. C. Cadwalladr, E. Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", «The Guardian», 17 Mar 2018.

[5] Si tratta di una strategia di digital marketing che utilizza i dati dei consumatori e la demografia per identificare gli interessi di specifici individui o di gruppi molto ristretti con idee simili e per influenzarne i pensieri o le azioni. Si veda meglio *infra*.

[6] Cambridge Analytica è una società di consulenza londinese che utilizza il data mining, l'analisi di dati e la comunicazione strategica applicandoli al campo del marketing commerciale ed elettorale. La stessa, per svolgere la propria attività, acquista big data dai cosiddetti "broker di dati", società che raccolgono informazioni sulle abitudini e i consumi degli utenti. Queste società utilizzano le innumerevoli tracce che ciascun utente lascia nel web e generalmente le fornisce in maniera aggregata o anonima. Tali dati vengono poi elaborati da Cambridge Analytica attraverso l'uso di modelli e algoritmi al fine di creare profili degli utenti, utilizzando l'approccio della psicometria, campo della psicologia che si occupa della classificazione dei processi psichici e della personalità di un individuo. I dati psicografici riguardano le credenze, i valori, gli interessi, le aspirazioni e le attitudini delle persone e sono ormai da tempo utilizzati nel marketing.

[7] I test somministrati si basano sul c.d. modello del Big Five. La teoria propone una classificazione formata da cinque fattori: apertura, coscienziosità, estroversione, piacevolezza e stabilità emotiva. La combinazione tra le cinque dimensioni del modello *OCEAN* (*openness, consciousness, extroversion, agreeableness, neuroticism*), costituisce la configurazione di personalità di ogni individuo. Numerose ricerche hanno dimostrato che conoscere il profilo della personalità di una persona consente di prevederne il comportamento in maniera piuttosto attendibile (ad esempio la performance lavorativa, la qualità della vita coniugale, ecc.).

Le nuove frontiere del digital marketing: dalla profilazione alla manipolazione online nell'ambito politico alla luce del GDPR

L'articolo analizza la sempre maggiore difussione di pratiche di profilazione avanzate, attraverso l'uso dei big data in combinazione con la scienza comportamentale, pratiche il cui uso non è più ormai limitato al marketing commerciale, ma si è propagato al cosiddetto marketing politico.
Accennando al celebre caso "Cambridge Analytica", si passa a esaminare il parere 3/2018 del Garante europeo, pubblicato pochi giorni dopo le inchieste giornalistiche con lo scopo di approfondire il tema della circolazione di informazioni false o ingannevoli aventi il fine di influenzare il dibattito politico e le elezioni, attraverso il fenomeno del microtargeting politico e della manipolazione online.
Il Garante, richiamate le tutele in tema di marketing e di profilazione introdotte dal GDPR, ribadisce l'importanza che l'Unione europea si muova nell'ottica di rinforzare ulteriormente la protezione di alcune categorie speciali di dati personali e i principi di trasparenza, di limitazione delle finalità e di minimizzazione, ponendo migliori salvaguardie contro profilazioni e decisione automatizzate illecite.

New frontiers of digital marketing: from profiling to online manipulation in the political context in the lights of GDPR

This article examines the ever greater diffusion of advanced profiling practices, by making use of big data combined with behavioural science, practices whose use is no longer limited to commercial marketing, but has spread to the so-called "political marketing".
By mentioning the well-known "Cambridge Analytica case", this article proceeds examing the EDPS Opinion 3/2018, published few days later the journalists' investigations in order to deepen the issue of the circulation of false or misleading information served influence political campaign and elections, through the phenomenon called "political microtargeting" and "online manipulation".
The EDPS, cited the legal safeguards introduced by GDPR, underlines the importance that the EU institutions act in order to reinforce protection of special categories of data, the principles of transparency, purpose limitation and data minimization, and safeguards against unlawful profiling and automated decision-making.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 123-139

L'impatto del Regolamento europeo in materia di protezione dei dati personali sull'attività giurisdizionale

Sara Conti*, Ginevra Peruginelli**

1. *Il contesto: il nuovo Regolamento e il sistema giudiziario*

Negli ultimi anni, si assiste nel settore giudiziario ad un forte interessamento verso il tema della protezione dei dati personali. Se da un lato l'uso delle tecnologie della società dell'informazione rappresenta un elemento fondamentale per il miglioramento dell'amministrazione della giustizia, dall'altro esso apre nuovi scenari e questioni delicate per la tutela effettiva dei dati personali.

L'utilizzo di strumenti informatici è essenziale per garantire un efficiente funzionamento dell'attività giurisdizionale: ciò si ripercuote in un effettivo accesso alla giustizia per i cittadini, in procedure più snelle e semplici in caso di violazione della legge e infine in una più stretta ed efficace cooperazione delle autorità giudiziarie nazionali tra di loro e tra i diversi paesi dell'Unione europea.

La disponibilità di strumenti che utilizzano web services e sistemi di archiviazione elettronica, la possibilità di scambiare elettronicamente

* Tecnologo presso l'Istituto di Teoria e Tecniche dell'Informazione Giuridica del CNR (ITTIG) e dottoranda di ricerca presso il Dipartimento di Ingegneria dell'Informazione dell'Università degli Studi di Firenze.

** Ricercatrice presso l'Istituto di Teoria e Tecniche dell'Informazione Giuridica del CNR (ITTIG).

documenti e atti giuridici, nonché l'avvio dei processi telematici mirano sicuramente a supportare coloro che operano nel settore della giustizia, incrementando l'offerta di adeguati servizi per il cittadino e per un'efficiente e trasparente amministrazione della giustizia. Tuttavia, in tale contesto vengono raccolti, trattati e conservati grandi quantità di dati personali, creando situazioni di estrema ambiguità. Il settore della giustizia dei diversi Stati membri si è trovato fino ad oggi di fronte ad un frammentato panorama normativo in materia di protezione dei dati personali, caratterizzato da differenti approcci nazionali, nonché da diverse procedure relative alla raccolta, gestione e conservazione dei dati personali che comportano, ad esempio, attività autorizzate in uno Stato membro e non permesse in un altro.

Il primo tentativo di regolamentare la protezione dei dati è stata la Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Questo atto legislativo stabilisce le norme minime sulla protezione dei dati in tutta Europa per raggiungere un livello equivalente di protezione dei diritti e delle libertà delle persone riguardo al trattamento dei dati in tutti gli Stati membri. L'obiettivo era quello di eliminare le divergenze tra le legislazioni nazionali degli Stati membri in modo da garantire una regolamentazione coerente e uniforme del flusso di dati personali. Nonostante l'ambizioso proposito, a livello pratico la Direttiva non ha impedito la frammentazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione che le operazioni online, in particolare, comportassero rischi per la protezione delle persone fisiche. Trattandosi, com'è noto, di un atto comunitario non direttamente applicabile negli Stati membri ma suscettibile di trovare attuazione attraverso l'adozione di apposite misure nazionali, le divergenze tra i vari Stati membri nell'attuazione e nell'applicazione della Direttiva hanno contribuito a creare diversi livelli di protezione. Tali criticità in riferimento soprattutto all'effettività della tutela giuridica offerta dalla Direttiva hanno portato il legislatore europeo ad affidare la disciplina di un settore così articolato come quello del trattamento dei dati personali ad un differente strumento normativo, vale a dire il regolamento.

Nel dicembre 2015 è stato completato il processo per concordare una nuova serie di norme volte a riformare il quadro giuridico per garantire il diritto alla protezione dei dati dei cittadini dell'UE. Questo pro-

L'impatto del Regolamento europeo in materia di protezione dei dati personali sull'attività giurisdizionale

Il Regolamento generale per la protezione dei dati personali n. 2016/679 è la normativa di riforma della legislazione europea in materia di protezione dei dati. Il Regolamento, rafforzando le tutele poste a salvaguardia dei dati personali e i diritti degli individui, si adatta al nuovo contesto sociale ed economico, caratterizzato da un costante sviluppo tecnologico e da modalità sempre più pervasive di scambio e sfruttamento di dati. In particolare, questo breve contributo si propone di offrire alcuni strumenti per "leggere" la riforma del Regolamento e di individuare le novità contenute in questo atto, rilevanti per il settore giudiziario, che solitamente non è specificatamente considerato da parte della dottrina che analizza tale normativa. In tale contesto si colloca il progetto europeo INtroduction of the data protection reFORM to the judicial system – INFORM, che si occupa di promuovere la corretta conoscenza della nuova normativa europea in materia di protezione dei dati personali esclusivamente in ambito giudiziario.

The impact of the General Data Protection Regulation on judicial activity

The General Data Protection Regulation n. 2016/679 is the European legislation reform on data protection. The Regulation, reinforcing the safeguards placed to protect personal data and the rights of individuals, is well suited to the new social and economic context, characterized by constant technological development and by increasingly pervasive ways of exchanging and exploiting data. In particular, this brief contribution aims to offer some tools to "read" the reform of the European regulation and to identify the novelties contained in this act, relevant to the judiciary sector, which is usually not specifically considered by the doctrine that analyzes this legislation. In this context the European project INFORM – INtroduction of the data protection REfORM to the judicial system – INFORM, promotes the accurate knowledge of the new European legislation on the protection of personal data in the judicial system.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 141-158

Il GDPR negli enti pubblici fra opportunità e difficoltà operative

Diego Giorio*

Sommario: 1. Premessa. – 2. I principi. – 3. I diritti – 4. Le figure coinvolte. – 5. Le incombenze. – 6. Privacy e trasparenza. – 7. Conclusioni.

1. *Premessa*

Gli enti pubblici, centrali e locali, raccolgono ed elaborano miriadi di dati: l'anagrafe gestisce i cittadini residenti e ne segue gli spostamenti, lo stato civile registra le tappe principali dell'esistenza, gli uffici tecnici raccolgono dati sull'edilizia e sul traffico, le Aziende sanitarie attendono alla salute pubblica, per menzionare i primi esempi che possono venire alla mente da una lista pressoché infinita. Enti pensionistici, uffici scolastici di ogni ordine e grado, Agenzie Regionali per l'Ambiente, Agenzia delle Entrate, Motorizzazione Civile sono collettori di dati di tutti i tipi, consentendo, potenzialmente, di conoscere ogni aspetto della vita pubblica e parte della vita privata di ogni cittadino. Oltre alla naturale informatizzazione, il percorso delle grandi banche dati pubbliche è caratterizzato da un crescente centralismo e da una sempre maggiore interconnessione. Pensiamo, ad esempio, all'Ufficio del Registro e al Catasto urbano, poi divenuto Agenzia del Territorio, confluiti entrambi nell'Agenzia delle Entrate. Oppure pensiamo alle anagrafi, finora gestite a livello comunale, quindi distribuite sui circa 8000 comuni italiani, e ora in fase di aggregazione nell'ANPR, l'Anagrafe Nazionale della Popolazione Residente[1].

* Servizi demografici del Comune di Villanova Canavese – Autore e membro del Consiglio di Redazione per SEPEL Editrice. Le opinioni nel presente articolo sono espresse a titolo puramente personale.

[1] Art. 62 D.Lgs. 7 marzo 2005, n. 82, come modificato dall'Art. 2, c. 1, del D.L. 18 ottobre 2012, n. 179, convertito dalla L. 17 dicembre 2012, n. 221.

Da un lato ci sono innegabili vantaggi, dato che non è ragionevole, nell'era dei big data, che per il Catasto una persona risulti proprietaria di una villa, per la Motorizzazione guidi una fuoriserie e all'Agenzia delle Entrate appaia nullatenente. D'altro canto, qualunque concentrazione di dati è dannosa per la privacy e l'eccesso di controllo è pericoloso per la democrazia e le libertà individuali; di conseguenza occorre bilanciare con estrema attenzione diritti e doveri, controllo e riservatezza, trasparenza e protezione, in quell'eterno «gioco di pesi e contrappesi»[2] fra valori contrapposti e spesso degni di pari tutela.

Purtroppo non è sempre immediato, in situazioni dai contorni a volte sfumati, definire i limiti e conciliare correttamente privacy e trasparenza: norme a volte contraddittorie o con troppe aree grigie, sentenze talvolta in contrasto fra loro, difficoltà di bilancio e vincoli che limitano la formazione del personale sono ostacoli contro i quali le Pubbliche Amministrazioni combattono ogni giorno.

L'implementazione del GDPR negli enti pubblici è quindi caratterizzato da alcune peculiarità e difficoltà, da esaminare almeno nei termini generali del problema. Ogni ente avrà poi le sue specificità, sia in termini di tipologia – una biblioteca o un ospedale devono adottare approcci diversi – sia in termini di dimensione, stante il fatto che un piccolo Comune o una grande metropoli hanno a disposizione strumenti diversi e affrontano difficoltà differenti durante il percorso di adeguamento.

In queste righe ci si riferisce alle Pubbliche Amministrazioni con un'accezione più ampia rispetto alla lista contenuta nel D.Lgs. 30 marzo 2001, n. 165, ricomprendendo qualunque servizio dello Stato, centrale o locale. In termini di trattamento dei dati personali, l'apparto giudiziario, per gli aspetti non regolati da altre norme, quale la Direttiva (UE) 2016/680, nonché i gestori di pubblico servizio, ricadono certamente nell'ambito di applicazione di gran parte dei principi espressi dal Regolamento (UE) 2016/679 e si possono dunque estendere anche ad essi le considerazioni generali riferibili ad altri enti dello Stato, come anche suggerito dal WP29 nelle linee guida per la designazione del DPO[3].

[2] Cfr. R. Imperiali, *Codice della Privacy*, Milano, IlSole24Ore, 2005, p. 102.

[3] Cfr. Garante Privacy, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287 (15 maggio 2018).

Il GDPR negli enti pubblici fra opportunità e difficoltà operative

Lo Stato, attraverso i suoi enti, centrali e locali, raccoglie e gestisce una quantità immensa di dati, che gli consente di conoscere tutti gli aspetti della vita pubblica e molti aspetti della vita privata dei suoi cittadini.
L'implementazione del Regolamento europeo è quindi particolarmente importante e delicata negli uffici pubblici, che si trovano a gestire grandi quantità di dati, spesso particolarmente sensibili.
Se il percorso di adeguamento al GDPR rappresenta un grosso sforzo organizzativo ed economico, la revisione dei processi è però una preziosa occasione per guadagnare in efficienza, modernizzare i sistemi informatici, migliorare la propria immagine e rendere ai cittadini un servizio adeguato ai tempi.
In questo articolo si analizzano gli aspetti principali della normativa, alla luce delle peculiarità e delle difficoltà del processo di implementazione nella realtà di un'Istituzione pubblica.

State agencies and GDPR: opportunities and operational difficulties

The State, through its central and local agencies, collects and manages an immense amount of data, which allows it to have access to all aspects of public life and many aspects of the private behavior of its citizens.
The implementation of GDPR is therefore a particularly important and complex issue for public offices, which manage large amounts of data, most of which is particularly sensitive.
On one hand, the process of adaptation to the GDPR represents a major organizational and economic effort; on the other hand, review of the processes may be seen as a valuable opportunity to gain efficiency, modernize IT systems, to improve positive perception and to offer citizens a service appropriate for our times.
This article analyzes the main aspects of the GDPR legislation in light of peculiarities and difficulties in the implementation process given the reality of conditions in public institutions.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 159-176

DNA e anonimizzazione: i possibili effetti negativi di un intervento legislativo sulla Ricerca medica

Paola Aurucci*, Paolo Pinto**

1. *1. Introduzione*

Il Regolamento Europeo sulla Protezione dei Dati[1] fornisce delle chiare prescrizioni sull'utilizzo del DNA a scopo di ricerca scientifica, richiedendo la pseudonimizzazione dei dati, ovvero la rimozione dei riferimenti anagrafici del soggetto.

Il Governo Italiano ha ritenuto di estendere la tutela della Privacy in questo settore, imponendo l'anonimizzazione.

La procedura di anonimizzazione comprende quella di pseudonomizzazione e la estende, imponendo delle modifiche ai dati, che vengono resi meno precisi attraverso varie tecniche.

Il criterio fondamentale è che anche ove qualcuno si procurasse fraudolentemente i nominativi dei soggetti non sarebbe in grado di reidentificarli, ovvero collegare a ciascuno il suo DNA o svolgere altre

* Ricercatrice (Ph.D). Borsista presso l'Università di Torino. Ricercatrice e data protection expert presso Center for advanced technology in health and wellbeing dell'Ospedale San Raffaele.

** Data Scientist (Ph.D). Consulente in tema di Data Driven Marketing e Privacy Compliance.

[1] Regolamento (UE) 2016/679.

operazioni lesive della sua Privacy, tra cui dedurre ulteriori parti del suo DNA a partire da un frammento.

Purtroppo queste modifiche sono tali da danneggiare seriamente la sfruttabilità scientifica del dato.

In letteratura è generalmente accettato che la procedura di anonimizzazione man mano che viene approfondita provochi una diminuzione di utilità dei dati superiore a quella della reidentificabilità[2].

Inoltre le severissime linee guida per l'anonimizzazione suggerite dalla Comunità Europea nel Parere 05/2014[3] si basano su presupposti scientifici[4] che a loro volta in letteratura sono oggetto di contestazioni[5].

Il presente studio si pone i seguenti obiettivi

Una disamina delle prescrizioni del Regolamento in merito all'utilizzo del DNA per scopi di ricerca

Un approfondimento sull'intervento in merito del Governo Italiano

Una descrizione delle procedure di anonimizzazione così come suggerite dalle Linee Guida del Working Party Art 29

Una descrizione del DNA come dato personale

[2] J. Brickell, V. Shmatikov, "The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing", «Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining», 2008, pp. 70-78. Cfr. anche: T. Li, N. Li, "On the tradeoff between privacy and utility in data publishing", KDD '09 Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining, 2009, pp. 517-526.

[3] Parere 05/2014 – WP 216; "Parere 05/14 sulle tecniche di anonimizzazione" Gruppo di Lavoro Ex Art. 29 , adottato il 10 Aprile 2014.

[4] L. Sweeney, "K-anonymity: A model for protecting privacy", «International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems», vol 10, 2002, pp. 557-570, https://doi.org/10.1142/S0218488502001648; A. Solomon, R. Hill, E. Janssen, S.A. Sanders, J.R. Heiman, "Uniqueness and how it impacts privacy in health-related social science datasets", «Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium», 2012, https://doi.org/10.1145/2110363.2110422; D. Butler, "Data sharing threatens privacy", «Nature», 2007, https://doi.org/10.1038/449644a; Y.A. de Montjoye, C.A. Hidalgo, M. Verleysen , V. Blondel, "Unique in the crowd: The privacy bounds of human mobility", «Nature Scientific Reports», vol. 3, 2013, https://doi.org/10.1038/srep01376; A. Narayanan, V. Shmatikov, "Robust de-anonymization of large sparse datasets", «Security and Privacy», IEEE Symposium, 2008, pp. 111-125.

[5] D. Barth-Jones, "The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now", «Worjing Paper», 2012, disponibile su SSRN: https://ssrn.com/abstract=2076397 o http://dx.doi.org/10.2139/ssrn.2076397.

DNA e anonimizzazione: i possibili effetti negativi di un intervento legislativo sulla Ricerca medica

La Ricerca medica sul DNA potrebbe incontrare delle difficoltà a seguito dell'entrata in vigore del GDPR e in particolare dei regolamenti attuativi nazionali.
In particolare in Italia è stata proposta una forma di attuazione che nella forma originale prevedeva l'anonimizzazione dei dati utilizzati in tale ambito anziché la semplice pseudonomizzazione.
Nel presente articolo si illustrano le peculiarità del DNA come dato e si mostra come esso sia particolarmente difficile da anonimizzare senza compromettere l'affidabilità dei risultati della Ricerca.
Si descrive infine un orientamento emergente in Letteratura che potrebbe consentire un soddisfacente trattamento dei dati, sempre che non intervengano a livello nazionale sbarramenti legislativi ulteriori rispetto a quanto previsto dal GDPR.

DNA and Anonymization: possible negative effects of legislative intervention on medical

Medical Research on DNA could meet some problems after the adoption of DGDPR and especially, of national implementing decrees.
In particular, in Italy is currently pending a proposed actuation decree, which in the original form prescribed anonymization of DNA data in lieu of simple pseudonimyzation.
This paper illustrates some peculiarities of DNA as high dimensional data and shows why it is especially difficult to anonymize it without compromising Research results.
An emerging trend in Literature is described, which could allow a satisfying data treatment, provided no further barriers beyond those posed by GDPR are created at a national legislative level.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 179-196

Blockchain, decentralizzazione e privacy: un nuovo approccio del diritto

Lorenzo Piatti*

Sommario: 1. La tecnologia decentralizzata e il Diritto. – 2. GDPR e blockchain. – 3. Blockchain e GDPR. – 4. Conclusioni.

1. *La tecnologia decentralizzata e il diritto*

Blockchain, il registro decentralizzato su cui sono sviluppate applicazioni distribuite come Bitcoin, sta rivoluzionando il modo di immaginare il disegno dei servizi informatici dei prossimi anni. Chiaramente non è questa la sede per parlare della concretezza – o meno – dei progetti, start-up e ICO che sono spuntati come funghi digitali da qualche anno a questa parte: tuttavia, per dare un senso a questo contributo, è necessario avere la consapevolezza che la tecnologia blockchain, e in generale la *Distributed Ledger Technology* (DLT), sta impattando con prepotenza la comunità e la cultura informatica degli ultimi anni[1].

Le conseguenze dell'approccio distribuito delle risorse informatiche, siano essi applicazioni o servizi veri e propri, sono – a parere di chi scrive – ancora limitate allo strato più alto dell'architettura delle comunicazioni e di Internet: la DLT di cui si parla nelle prossime pagine rap-

* Consulente nei processi di dematerializzazione e normativa digitale. Le opinioni espresse sono a titolo personale.

[1] Bitcoin e blockchain sono stati oggetto di diversi studi, ma per avere un'introduzione analitica al tema si consiglia l'approccio di S. Capaccioli, *Criptovalute e bitcoin. Un'analisi giuridica*, Milano, Giuffrè, 2015. Altri spunti sul tema, in particolare sugli *smart contracts*, possono essere trovati anche in questa rivista: S. Capaccioli, "Smart contracts: traiettoria di un'utopia divenuta attuabile", «Ciberspazio e Diritto», Vol. 17, n. 55, 2016, pp. 25-45; L. Piatti, "Dal Codice Civile al codice binario: blockchain e smart contracts" «Ciberspazio e Diritto»», Vol. 17, n. 56, 2016, pp. 325-344; N. Busto, "Bitcoin tra disintermediazione e iper-intermediazione", «Ciberspazio e Diritto», Vol. 17, n. 56, 2016, pp. 309-323.

presenta oggi (solo) un'aggiunta allo strato di trasporto TCP/IP[2], senza scendere nei livelli più profondi dell'architettura della rete. Il risvolto tecnico non è banale e ha – chiaramente – impatti giuridici sia per il modo con cui il legislatore regola la rete, sia per le logiche con cui la rete – e la blockchain – può aiutare il legislatore.

L'analisi che segue fa riferimento a questo strato superficiale di codice, senza potersi spingere – per ora – nel profondo cambio di paradigma che sta rivoluzionando l'idea stessa della gestione di Internet, portando l'evoluzione della rete da una struttura centralizzata a una struttura profondamente decentralizzata e distribuita. Mi riferisco alla tendenza – ancora embrionale ma comunque attuale[3] – di certi ricercatori e comunità di riappropriarsi dell'Internet nel suo livello più basso – quello delle infrastrutture – passando da un approccio centralizzato, basato su prestatori di rete e servizi (ISP) accentrati ed esterni alla propria realtà, a un approccio decentralizzato, basato sulla creazione di una propria rete Internet, sia fisica che software.

Il tentativo di questi esperimenti è di riportare la struttura del web alla sua idea originaria, fortemente libertaria e autoregolamentata.

Ad ogni modo, anche la decentralizzazione – chiamiamola – di "primo livello" porta con sé delle conseguenze sul piano giuridico: per comprendere la complessità di approcciare da un punto di vista normativo un sistema decentralizzato è utile ripercorrere brevemente l'esponenziale importanza del diritto all'interno del panorama informatico, partendo dal 1996. In quell'anno veniva pubblicata online la Dichiarazione d'Indipendenza del Ciberspazio[4], in cui J.P. Barlow ammoniva i pensatori e i legislatori del mondo fisico a guardarsi bene dal cercare di regolare la

[2] Come noto, semplificando il più possibile, gli strati della rete sono oggi 5: uno applicativo (che consiste in diversi protocolli, tra cui HTTP e FTP), due di network e trasporto (TCP/IP), un quarto di connessione (Ethernet oppure protocolli di comunicazione senza fili) e infine lo strato fisico (I cavi di Internet). *Blockchain* si inserirebbe in cima alla catena, tra lo strato di trasporto e quello applicativo. Cfr. P. De Filippi, A. Wright, *blockchain and the law,* Londra, Harvard University Press, 2018.

[3] Si vedano ad esempio i progetti nelle comunità americane come *Detroit Technology Community Project* (https://www.alliedmedia.org/dctp sito web consultato e online il 24 maggio 2018), gli spagnoli di "Guifi" (https://guifi.net/en sito web consultato e online il 24 maggio 2018) nonché gli italiani di "Ninux" (http://ninux.org sito web consultato e online il 24 maggio 2018).

[4] J.P. Barlow, "A Declaration of the Independence of Cyberspace", https://www.eff.org/it/cyberspace-independence (sito web consultato e online il 24 maggio 2018).

Blockchain, decentralizzazione e privacy: un nuovo approccio del diritto

La regolamentazione di Internet per come la conosciamo, compreso il nuovo Regolamento in tema di protezione dei dati (GDPR), è stata pensata e scritta per una rete accentrata, dove i prestatori e i fruitori dei servizi sono – almeno – identificabili, e dove la coercizione della normativa è – oggi – effettiva. Il cambio di paradigma imposto da Bitcoin, blockchain e DLT obbliga a ripensare l'approccio normativo e, nel frattempo, ad adattare le regole attuali ad una tecnologia nuova. Questo articolo tenta brevemente di capire come il GDPR – in attesa dell'emanazione della Direttiva e-privacy – possa trovare applicazione nel contesto del Mondo nuovo della *Decentralized Ledger Technology* (DLT).

Blockchain, decentralization and privacy: a new legal approach

The Internet regulation as we know it, including the European General Data Protection Regulation (GDPR), has been written for a centralized web, where the service provider and the users are – at least – identifiable, and where the law enforcement is – today – effective. The disruption brought by Bitcoin, Blockchain and DLT imposes a new regulatory approach and, in the meantime, it force to adapt the current rules to a totally new technology. This article tries to briefly understand how the GDPR – waiting for the e-privacy Directive – may find a concrete application in the Brave New World of the Decentralized Ledger Technology (DLT).

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 197-208

Blockchain e Protezione dei Dati Personali alla luce del nuovo regolamento europeo GDPR

Andrea Razzini[1]

Sommario: 1. Introduzione. – 2. Analisi di conformità tra GDPR e blockchain. – 3. Recenti piattaforme blockchain con requisiti di privacy. – 4. Possibili abusi. – 5. Conclusioni.

1. *1. Introduzione*

L'avvento della tecnologia blockchain promette un futuro in cui gli utenti avranno a disposizione una nutrita schiera di applicazioni evitando qualunque forma di controllo sulle operazioni che avvengono nella rete. La ben nota denuncia nel 2013 dei programmi di sorveglianza di massa attuati all'insaputa degli utenti di Internet, poi la più recente notizia sulla profilazione nascosta a scopi elettorali, hanno seriamente messo in dubbio le nostre capacità di difesa contro la manipolazione dei dati. Il controllo operato dai grandi operatori di servizi digitali ha reso Internet un luogo dove la privacy dei navigatori è a rischio. Sembra invece possibile, con la blockchain, restituire agli utenti il pieno controllo su tutto quello che faranno all'interno di questa tecnologia, ma se mettiamo a confronto questo principio con le regole sulla protezione dei dati, vale a dire con il nuovo regolamento Europeo in materia di trattamento dei dati personali, vengono alla luce molti aspetti di contrasto più che di compatibilità riguardo i diritti che ognuno di noi potrà esercitare sui propri dati.

[1] L'autore si è laureato in Ingegneria Elettronica al Politecnico di Milano e in Fisica all'Università degli Studi di Milano. Possiede una lunga esperienza maturata in multinazionali in ambito Telecomunicazioni di cui una decina di anni nel settore Sicurezza Informatica. Possiede diverse certificazioni come ad es. CISSP, CEH e CCSK e lavora attualmente come consulente per attività sia di Threat Assessment e Risk Assessment che di Vulnerability Analyses e Penetration Testing. Le idee espresse rappresentano opinioni personali.

Prima di passare in rassegna in modo puntuale i principali articoli del regolamento sulla protezione dei dati e metterli a confronto con le caratteristiche proprie della blockchain, elencheremo le rispettive caratteristiche su cui porre maggiormente l'attenzione.

Il regolamento generale sulla protezione dei dati personali (GDPR, General Data Protection Regulation- Regolamento UE 2016/679) è un Regolamento con il quale la Commissione europea intende regolare la protezione dei dati personali di cittadini dell'Unione Europea nonché dei residenti nell'Unione Europea, sia all'interno che all'esterno dei suoi confini. Il testo, pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, inizierà ad avere efficacia il 25 maggio 2018. Ecco di seguito gli elementi fondamentali di questo regolamento:

- Raccolta e consenso al trattamento dei dati (artt. 7, 13, 14, 21);
- Diritto alla cancellazione (artt. 17, 13, 14);
- Diritto di limitazione (artt. 18, 19);
- Diritto alla portabilità dei dati (art. 20);
- Sicurezza e obbligo di notifica incidenti (artt. 32, 33, 34);
- Responsabilità del trattamento (artt. 19, 24, 30);
- Privacy by design e privacy by default (artt. 25, 29).

Impropriamente definita talvolta come nuova legge privacy, riguarda più da vicino la protezione dei dati in senso lato, partendo dalla risk analyses, proseguendo sulla Data Protection Impact Analyses ed istituendo un vero e proprio ciclo di vita del trattamento e analisi dei rischi.

Il GDPR è insomma una disposizione unitaria, mirante a rafforzare, unificare e applicare la protezione dei dati personali in tutto il territorio dell'Unione Europea. Una volta applicato, il regolamento imporrà alle imprese di ottenere il consenso attivo dei clienti per l'utilizzo delle loro informazioni personali, consentendo nel contempo agli utenti il diritto di rimuovere i dati da qualsiasi banca dati.

Questa ricerca dei "diritti digitali" nasce già negli anni "90, attraverso il concetto di Cyberspace, ovvero il luogo di tutte quelle informazioni mediate dall'utilizzo di un computer L'evoluzione dei sistemi elettronici verso una decentralizzazione atta a preservare questi diritti di privacy e libertà, raggiunge il suo culmine nel 2008 con la pubblicazione del già citato articolo di S. Nakamoto sulla nascita del sistema di pagamento

Blockchain e Protezione dei Dati Personali alla luce del nuovo regolamento europeo GDPR

«We implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it».
Con queste parole, nel 2008, Satoshi Nakamoto, inventore del protocollo Bitcoin, in un articolo di sole 9 pagine, pose le basi per una nuova rivoluzione digitale che prenderà il nome di Blockchain. La Blockchain è la tecnologia dirompente che nei prossimi anni vedrà nascere numerose applicazioni in svariati campi: dagli Smart Contracts, alle ICO *(Initial Coin Offering),* alle operazioni distribuite di storage, oltre naturalmente al diffondersi dei pagamenti elettronici con diversi mezzi e opzioni.
Allo stesso tempo, alla luce dell'entrata in vigore del Regolamento Generale sulla Protezione dei Dati Personali (GDPR), è necessario cercare di evidenziare le problematiche di compatibilità tra questi 2 mondi in apparenza distaccati.

Blockchain and Personal Data Protection under the GDPR framework

«We implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it».
Through these words, in the year 2008, Satoshi Nakamoto, the inventor of the Bitcoin protocol, in his article of 9 pages only, created a new digital revolution that will soon assume the name of Blockchain. Blockchain is a disruptive technology that in the coming years will be used for several applications in different fields: from smart contracts to the ICOs (Initial Coin Offering), to the storage distributed operations and electronic payments via different means.
At the same time, given the next General Data Protection Regulation (GDPR), it is necessary to try to highlight the compatibility problems between these 2 worlds.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 211-224

Il principio di responsabilizzazione: la vera novità del GDPR

Rosanna Celella*

Sommario: 1. Premessa. – 2. L'*accountability*: il "principio dei principi". – 3. Misure di sicurezza e garanzie di *accountability*. – 4. L'implementazione del principio di *accountability*. – 5. La privacy, da costo a risorsa.

1. *Premessa*

La necessità di emanare un Regolamento europeo per la protezione dei dati personali è nata dalla continua evoluzione del concetto di protezione dei dati personali, dovuta principalmente alla diffusione del progresso tecnologico.

La tecnologia attuale consente alle imprese private e alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Da qui la necessità di instaurare un quadro giuridico più solido e coerente in materia di protezione dei dati personali che, affiancato a efficaci misure di attuazione, consentirà lo sviluppo dell'economia digitale nel mercato interno, garantirà la tutela dei dati personali delle persone fisiche e rafforzerà la certezza giuridica e operativa per i soggetti economici e le autorità pubbliche che operano nel settore.

Il presente elaborato si focalizzerà sulla disamina del principio di *accountability*. Tale principio, di cui all'Articolo 5.2 del Regolamento europeo, rappresenta un'evidente novità e può essere definito come il "principio dei principi", la cui osservanza garantisce il rispetto di tutti gli altri principi generali.

* Laureata in Giurisprudenza presso la LUISS Guido Carli, ha conseguito un Master di II livello in diritto dell'informatica presso La Sapienza e un *Executive Master* in diritto europeo per la protezione dei dati personali presso la LUISS Guido Carli; attualmente *trainee lawyer* specializzata in diritto digitale, privacy e cybercrime, lavora anche come *Data Protection Officer* presso aziende ed enti locali.

Il principio di *accountability* fa sorgere in capo al titolare del trattamento una serie di obblighi di *compliance*, rendendolo la figura centrale del Regolamento europeo, la cui prospettiva non è più centrata sui diritti dell'interessato, ma sugli obblighi del titolare.

Lo scopo del presente elaborato è quello di verificare se tale principio possa essere considerato un mero obbligo cui conformarsi oppure un'opportunità per l'azienda.

Si vorrà, in tal modo, tentare di dimostrare che l'esigenza di protezione dei dati personali e l'adeguamento alla normativa non deve per forza scontrarsi con gli interessi delle grandi aziende che fanno dei dati personali la loro ricchezza; al contrario è auspicabile una sana e proficua collaborazione, al fine di garantire sia il progresso tecnologico che la tutela degli individui e dei loro dati.

2. *L'accountability: il "principio dei principi"*

Il principio di responsabilizzazione si concretizza nel rispetto degli altri principi[1] di cui all'Articolo 5.1 e nella capacità del titolare di dimostrare di averli osservati.

L'Articolo 24 del Regolamento prevede che «Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario».

L'*accountability*, infatti, combina due aspetti: l'adozione da parte del titolare di misure adeguate ed efficaci e la capacità di dimostrare la conformità delle attività di trattamento con le disposizioni del GDPR.

Si tratta di una grande novità nella materia della protezione dei dati, in quanto viene affidato ai titolari il compito di decidere autonomamente modalità, garanzie e limiti del trattamento dei dati personali, nel rispetto della normativa.

[1] Cfr. L. Bolognini, E. Pelino, C. Bistolfi, *Il Regolamento Privacy Europeo*, Milano, Giuffrè, 2016.

Il principio di responsabilizzazione: la vera novità del GDPR

Il presente elaborato si focalizza sulla disamina del principio di *accountability* previsto dal Regolamento UE 2016/679 (GDPR) che pone in capo al titolare del trattamento una serie di obblighi di *compliance*, facendolo diventare la figura centrale della nuova normativa europea. Esaminando prima teoricamente le varie misure di *accountability* e poi analizzando in che modo sono state implementate da una grande azienda come Google, si tenterà di dimostrare se la *compliance* può essere considerata non solo una mera imposizione normativa, ma anche opportunità per le aziende in termini di vantaggio competitivo.

Accountability principle, the real novelty of the GDPR

This paper focuses on the examination of the Accountability Obligations under the General Data Protection Regulation 2016/679 (GDPR), which places a series of compliance obligations on the data controller, making him the central figure of the new European legislation. By first examining the several accountability measures and then analysing how they have been implemented by a large company like Google, we will try to demonstrate whether "compliance" can be considered not only a mere regulatory imposition, but also opportunities for companies.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 225-244

Analisi e studio di una soluzione innovativa a complemento del GDPR per promuovere la cultura della sicurezza informatica in Europa

Mauro Alberto Brignoli*

1. *Sicurezza informatica in Europa*

1.1. *Ecosistema europeo delle imprese*

In Europa oltre il 90% del mercato[1] è rappresentato dalle piccole e medie imprese (PMI) e nel dominio cibernetico le PMI sono ancora più dominanti. Per questa ragione, esse dovrebbero essere la spina dorsale dell'economia europea partecipando a programmi di ricerca e sviluppo che possano migliorare la ulteriormente la competitività globale, innalzando il livello qualitativo e quantitativo delle soluzioni di sicurezza informatica necessarie per soddisfare la domanda del mercato. Tuttavia,

* Laureato in Ingegneria Informatica presso il Politecnico di Milano con un Master di II livello in sicurezza dell'informazione e informazioni strategiche presso l'Università la Sapienza di Roma. IT Professional esperto di cybersecurity, intelligence e data protection. Responsabile della protezione dei dati personali (DPO) norma UNI 11697:2017.

[1] Cfr. P. Muller, J. Julius, D. Herr, L. Koch, V. Peycheva, S. McKiernan, "Annual Report on European SMEs 2016/2017", Disponibile a: https://ec.europa.eu/docsroom/docu ments/26563/attachments/1/translations/en/renditions/native (Maggio 2018).

l'esperienza degli ultimi anni mostra che le PMI europee innovano prevalentemente internamente oppure collaborando con altre aziende su progetti di ricerca e sviluppo e in progetti orientati al mercato. Tipicamente questo si verifica quando mancano risorse e capacità organizzative. Nella sostanza, queste mancanze pongono delle barriere difficili da superare per poter contribuire attivamente quando si sviluppano nuove catene di valore che attraversano settori industriali trasversali come lo sono i prodotti di sicurezza informatica. Le PMI hanno bisogno di un supporto per poter competere nella sfida e l'Europa deve trovare una soluzione se vuole essere un leader nel mercato globale.

Ostacoli essenziali che impediscono la penetrazione nel mercato europeo della sicurezza informatica sono in prima istanza la difficoltà di accesso ai consumatori al mercato. Il problema della mancanza di scalabilità è una sfida molto impegnativa per le PMI. Normalmente queste avviano attività con proprie forze nel mercato nazionale, trovando in seguito seri ostacoli all'internazionalizzazione dovuti ai vari costi come quelli connessi ad un mercato frastagliato, imputabili alla presenza di normative, lingue, culture diverse. Attualmente il mercato europeo della sicurezza informatica è dominato da società non europee, tipicamente multinazionali. Le PMI europee sono costrette a competere in un ambiente ostile e gli sforzi di esportazione sono troppo impegnativi, poiché i grandi operatori della sicurezza IT, beneficiando della loro forte presenza nel mercato, proteggono le loro nicchie da nuove minacce esterne e dai concorrenti. Come conseguenza le imprese più piccole sono confinate nei mercati locali e ancora dipendenti dagli appalti pubblici nel loro paese d'origine.

1.2. *Riforma europea della cybersecurity*

Nel suo discorso[2] sullo "stato dell'Unione" del 2017, Jean-Claude Juncker, presidente della Commissione europea, ha sottolineato che "il commercio riguarda l'esportazione dei nostri standard, siano essi norme sociali o ambientali, protezione dei dati o requisiti di sicurezza alimentare" con il chiaro obiettivo di aumentare le esportazioni europee da un lato e garantire un commercio equilibrato dall'altro. La consapevolez-

[2] Cfr. J. Junker, "Discorso sullo stato dell'Unione 2017", disponibile a: http://europa.eu/rapid/press-release_SPEECH-17-3165_it.htm (maggio 2018).

Analisi e studio di una soluzione innovativa a complemento del GDPR per promuovere la cultura della sicurezza informatica in Europa

Il documento offre una panoramica della sicurezza informatica in Europa, focalizzando l'attenzione sul mercato europeo delle imprese. Presenta i contenuti della riforma europea in materia di cyber security, analizzando le principali componenti della sicurezza e la responsabilità delle persone per determinare il valore economico degli incidenti informatici. Si concentra sulle opportunità e le sfide in tema di sicurezza e privacy soprattutto quelle derivanti dall'introduzione del GDPR. Analizza l'impatto dal punto di vista dei cambiamenti attesi nelle organizzazioni che dovranno introdurre la figura del "Data Protection Officer" – DPO, prevista dal regolamento. Analizza il ruolo e responsabilità delle persone coinvolte nella gestione della sicurezza e della privacy aziendali. Infine illustra una possibile soluzione innovativa per promuovere la cultura della sicurezza e della privacy in Europa con le persone al centro della strategia. È considerata l'introduzione di una nuova figura il "Cybersecurity Awareness Officer" – CAO.

Analysis and study of an innovative solution to complement the GDPR to promote the cyber security culture in Europe

The document provides an overview of cyber security in Europe, focusing on the European business market. Presents the contents of the European reform on cyber security, analysing the main security components of and the responsibility of people to determine the economic value of cyber incidents. It focuses on the opportunities and challenges regarding security and privacy, especially those arising from the introduction of the GDPR. It analyses the impact of the expected changes in the organisations that will have to introduce the figure of the "Data Protection Officer" - DPO, provided for in the regulation. It analyses the role and responsibility of the people involved in the management of corporate security and privacy. Finally, it illustrates a possible innovative solution to promote the culture of security and privacy in Europe with the people at the centre of the strategy. The introduction of a new figure the "Cybersecurity Awareness Officer" – CAO is considered.

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 245-263

Luci ed ombre del regime delle diverse tipologie di certificazione previste dal GDPR – General Data Protection Regulation

Giovanna Raffaella Stumpo*

Sommario: 1. Premessa. – 2. Il SGP: Sistema di Gestione Privacy e rilevanza della certificazione. – 3. Significato, tipologie e iter di certificazione: cosa non dice il Regolamento. – 3.1. La certificazione di sistema ed informazioni esplicative nel Regolamento. – 4. La certificazione delle competenze: il disposto del Regolamento e la norma tecnica UNI 11007. – 4.1. I requisiti di qualificazione tecnica della figura del DPO (*Data Protection Officer*).

1. *Premessa*

Dal 25 maggio il GDPR (General Data Protection Regulation) – Regolamento del Parlamento europeo e del Consiglio 27 aprile 2016 n. 697 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) (anche solo il Regolamento) – è vincolante ed efficace per i 28 Stati Membri (SM) dell'Unione Europea, con efficacia abrogativa della Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

In virtù della sua diretta applicabilità, il Regolamento comporta per tutti i diversi Operatori di mercato dell'UE (Aziende, P.A. e Studi) che, nell'esercizio del business ed in particolare nell'attività di produzione / erogazione di beni /servizi trattano dati personali di interessati – persone fisiche – con ricorso in tutto/in parte a strumenti elettronici e non (cfr. Capo I art. 2 comma 1 del Regolamento), e con impatto in ambito UE (cfr. Capo I, art. 3 del Regolamento) e che si qualificano quali titolari del trattamento ai sensi dell'art. 4, punto 7) della normativa UE, l'obbligo di realizzare un SGP "Sistema di Gestione Privacy", in linea previsionale certificabile a cura di Ente terzo accreditato.

* Avvocato del Foro di Milano, Giornalista pubblicista, Formatore, Esperto in discipline strumentali all'esercizio della professione forense, Auditor SGQ e Certificazione ISO 9001 e Auditor M.O.G. ex D.Lgs. n. 231/2001.

Sul punto, è infatti chiaro il disposto del "considerando 100" del Regolamento, a norma del quale «al fine di migliorare la trasparenza ed il rispetto del presente Regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli e marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi».

Il meccanismo di certificazione preso in considerazione dal Regolamento rimanda pertanto al mondo delle c.d. norme internazionali e tecniche sui sistemi di gestione, come parametro su cui impostare un SGP - Sistema di Gestione Privacy per l'allineamento organizzativo e tecnico ai suoi precetti, e con possibile relativa certificazione a cura di Ente terzo accreditato, utile a fini di trasparenza informativa e per l'onere della prova imposto al titolare, di conformità alla c*ompliance* normativa.

Sotto diverso profilo – e quanto al diverso tema della "certificazione delle competenze", il meccanismo rileva per la non meno importante dimostrazione che il titolare deve fornire rispetto a "formazione, capacità e competenza" prescritte dal Regolamento, in relazione ad alcune figure rilevanti dell'"Organigramma privacy".

Vediamo meglio di cosa stiamo parlando, individuando anche le principali lacune previsionali del Regolamento sul sistema delle certificazioni.

2. *Il SGP: Sistema di Gestione Privacy e rilevanza della certificazione*

Salve le eccezioni espressamente previste per alcuni adempimenti (in particolare per le PMI) per previsione del Regolamento, a chi, all'interno dell'Organizzazione effettua le determinazioni circa "finalità e mezzi del trattamento" – e, quindi, conseguentemente si qualifica quale titolare-, è fatto obbligo "di responsabilizzazione" (cfr. Capo II, art. 5 comma 2 del Regolamento); con onere di un comportamento attivo, che sul piano organizzativo, tecnico e di metodo, deve rispondere ai seguenti principi ispiratori:

- *accountability* (i.e. necessità di dimostrare l'adozione di politiche privacy e misure adeguate alla tutela dei diritti dell'interessato, in conformità al dettato regolamentare);

Luci ed ombre del regime delle diverse tipologie di certificazione previste dal GDPR – General Data Protection Regulation

Al fine di migliorare la trasparenza ed il rispetto delle regole sulla tutela del dato, il Regolamento UE 697/2016 vincolante per il 28 SM dal 25 maggio 2018 incoraggiata l'istituzione di meccanismi di certificazione, sigilli e marchi di protezione che consentano agli interessati di valutare rapidamente il livello di protezione dei dati oggetto di trattamento. Tali sistemi, che richiamano gli standard tecnici ed internazionali ISO, rilevano a favore del titolare, nel fornire la prova di aver adottato "misure tecniche ed organizzative adeguate" al contenimento ed alla gestione dei rischi collegati ad ogni trattamento ed anche di essersi dotato di un "organigramma privacy" – con figure di ruolo adeguatamente formate, competenti e capaci, rispetto ai compiti ed agli adempimenti imposti dallo stesso Regolamento.

Standards ISO and different certification mechanisms according to the Regulation UE 697/2016

To enhance transparency and compliance with the rules on personal data protection the Regulation UE 697/2016, in force and binding the 28 European Member States since May 25, encourages the establishment of certification mechanisms, data protection seals and marks, in order to allow data subjects to quickly assess the level of protection relating to data processings.
Certification mechanisms, based on international and technical standards ISO, play an important role in the scope of the Regolation, as they support the Data Controller in the evidence of appropriate technical and organisational measures prescripted, to ensure and to demonstrate that processings are performed in accordance with the rules established, and also that data processors and people authorised to process in the organization, are fully and correctly trained, prepared and competent to operate in compliance with the Regulation.