key4biz dal 2002

L'ANALISI

Ascolta

Privacy e data protection tra GDPR e nuovo Codice Privacy. Il complesso quadro normativo italo-comunitario

Il GDPR sta diventando un legal benchmark globale. Dopo Giappone, Canada, Brasile e Singapore, anche negli Stati Uniti si va consolidando il consenso politico per nuove regole protettive per gli utenti digitali.

di **Emilio Tosi, Professore di Diritto Privato e Diritto delle Nuove Tecnologie Università di Milano Bicocca** | 31 ottobre 2018, ore 14:20

Dal 25 maggio 2018 – data di piena applicazione del *General Data Protection Regulation* della UE – il mondo sta lentamente cambiando: in meglio, parrebbe, ad avviso di chi scrive, almeno per quanto riguarda la tutela della riservatezza e della protezione dei dati personali.

Il GDPR sta diventando, infatti – è diventato potremmo forse già dire – un *legal benchmark* globale: dopo Giappone, Canada, Brasile e Singapore, tra i primi ad essersi allineati al nuovo standard normativo globale sulla falsariga di quanto stabilito dal nuovo quadro regolatorio comunitario, anche negli Stati Uniti si va consolidando il consenso politico per la definizione di nuove regole – non solo a livello statale ma soprattutto federale – protettive per gli utilizzatori di servizi e prodotti digitali che utilizzano dati personali.

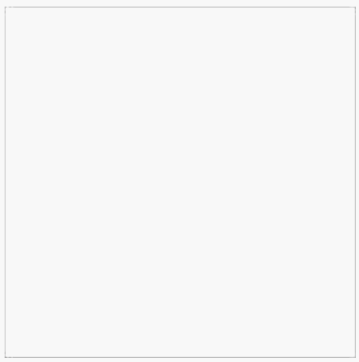
Il processo di armonizzazione globale è stato indubbiamente accelerato – ancor prima della piena applicazione del GDPR – lo scorso 10 aprile in occasione dell'audizione al Congresso degli Stati Uniti a Capitol Hill, Washington che ha interessato Mr. Zuckerberg, il CEO di **Facebook**: audizione in merito allo scandalo

LEGGI ANCHE

Carte di credito, la metà delle aziende non rispetta gli standard di sicurezza
27 settembre 2018

GDPR, allarme in Francia 'Dal 25 maggio denunce di violazioni in aumento del 64%'
26 settembre 2018

Video



Seminario FUB su Blockchain e servizi. L'intervento di Deborah Bergamini (Commissione Trasporti e Tlc)

globale di **Cambridge Analytica** che ha evidenziato la carenza di regole idonee a tutelare i cittadini dall'abuso dei loro dati da parte di soggetti non autorizzati dagli interessati.

Scandalo che ha travolto il mondo politico occidentale in quanto tale analisi massiva dei dati personali e degli orientamenti parrebbe aver influenzato – il condizionale è d'obbligo – l'esito del referendum pro-Brexit e la campagna vittoriosa delle ultime elezioni americane.

Quello che, invece, parrebbe un dato di fatto – tra *data breach* in senso lato e *breach of confidence* – è che sarebbero stati oggetto di profilazione occulta a CA, in quanto non resa nota né tantomeno assentita dagli interessati i dati contenuti nei profili personali Facebook di almeno 50 milioni di utenti poi divenuti 87 milioni per espressa ammissione del *social network*all'esito delle verifiche interne effettuate.

Segnalo, inoltre, che nei giorni scorsi Facebook è stata sanzionata dall'Autorità Inglese di protezione dei dati – **Information Commissioner's Office (ICO**) – con la sanzione più elevata all'epoca dei fatti – anteriormente al GDPR quindi – di 500.000,00 sterline inglesi. In base all'apparato sanzionatorio introdotto dal GDPR Facebook oggi rischierebbe molto di più: una sanzione pecuniaria sino al 4% del fatturato globale (art. 83 GDPR).

Per una volta nel contesto della regolamentazione digitale è la vecchia Europa a indicare la strada, in questo caso con riferimento alla *data protection,* agli Stati Uniti, in particolare alla californiana *Silicon Valley* sede dei grandi player globali, gli Over The Top digitali: **Google**, **Apple**, **Facebook**, **Amazon** per citare i principali.

Particolarmente significativo è, quindi, in questo mutato scenario regolatorio la recente legge dello Stato della California il*California Consumer Privacy Act of 2018* – che, però, entrerà in vigore solamente il 1° gennaio del 2020; segno tangibile che anche negli Stati Uniti si è avviato un lento ma inesorabile processo di allineamento al GDPR in attesa dell'auspicata legge federale sulla privacy.

Legge federale evocata e caldeggiata anche da **Tim Cook** in occasione della **40ma Conferenza Internazionale delle Autorità di Data Protection e Privacy –** che riunisce le Autorità di **115 Stati – quest'anno a Bruxelles coordinata dal Garante UE Giovanni Buttarelli;** il CEO di Apple – novello paladino della privacy ed inatteso estimatore del GDPR – dichiara:*"At Apple, we believe privacy is a fundamental human right".*

Certo, il percorso per una piena tutela della privacy a livello globale è appena iniziato e la strada irta di ostacoli: da ultimo, solo per citare alcuni fatti significativi, il furto dei token di Facebook, il bug di **Google plus** e l'annuncio della sua chiusura, infine, le denunce di **Clusit** sull'aumento del furto di credenziali usate per attacchi informatici.

"*Contro questi abusi* – osserva giustamente il Garante italiano **Antonello Soro**, sempre attento anche al contesto internazionale e non solo comunitario, in una recente intervista rilasciata a AGI 13 ottobre 2018 – *il nuovo Regolamento europeo rappresenta oggi un formidabile strumento per costringere gli Over The Top a gestire con maggiore trasparenza i dati personali dei loro utenti, a proteggerli con misure adeguate e a limitare in un perimetro chiaro gli usi che di questi dati essi possono fare. Prova ne sia il fatto che – proprio in base alle disposizioni del Regolamento – nel recente gravissimo caso di data breach che ha coinvolto 50 milioni di utenti, Facebook si sia affrettata a darne – come doveroso – immediata comunicazione al pubblico e alle autorità di protezione dati.*"

Non a caso il Garante Soro ha intitolato la Sua Relazione annuale del 10 luglio

2018 *'**Proteggere i dati per governare la complessità'*** rilevando, fra l'altro, che*: "Non possono essere i protocolli informatici o le condizioni generali di contratto, unilateralmente stabilite dai big tech, il codice normativo del digitale, su cui fondare diritti e doveri, nel contesto in cui più di ogni altro si dispiega la nostra esistenza.*

(...) Fake news, hate speech, cyberbullismo, eterna memoria della rete, ma anche minacce cibernetiche, algoritmi predittivi, uso massivo dei big data, persuasione occulta e social engineering funzionale ad attacchi informatici. Questi ultimi in Italia, nel solo mese di maggio, hanno toccato la soglia di 140 al giorno. Dal 25 maggio sono aumentate di oltre il 500% le comunicazioni di data breach al Garante, che hanno interessato, assieme a quelli notificati a partire da marzo, oltre 330.000 persone".

Dati ancora più aggiornati evidenziano che dal 25 maggio al 25 settembre **sono giunte** ben 2.547 segnalazioni, a fronte di 1.795 giunte nello stesso periodo dello scorso anno.

Crescente diffusione di prodotti e servizi ICT di nuova generazione basati sull'elaborazione massiva e sistematica di informazioni personali e non (Internet of Things, Big Data, Cloud computing e Smartphone), accrescono il ruolo strategico dei temi della privacy e della sicurezza dei dati raccolti con tali modalità pervasive.

Principio di sicurezza cristallizzato nell'art. 32 del GDPR in base al quale il Titolare del trattamento e il Responsabile del trattamento – tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche – mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

1. a)la pseudonimizzazione e la cifratura dei dati personali;
2. b)la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
3. c)la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
4. d)una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La centralità del principio di sicurezza del trattamento dei dati personali emerge, fra l'altro, anche dal considerando n. 83 del GDPR secondo cui:

"*Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale*".

Certo il complesso tema della tutela della privacy – che spazia dall'originario diritto alla riservatezza personale sino al diritto alla protezione dei dati personali di più recente tipizzazione normativa – non si esaurisce nella sicurezza dei dati ma va ben oltre; si pone, infatti, all'attenzione del giurista un quesito ineludibile: nell'economia attuale basata sul *data mining* – in cui il "nuovo petrolio" è costituito dallo sfruttamento massivo dei dati – è ancora possibile un'effettiva tutela di tali fondamentali diritti nella società dell'informazione o piuttosto si tratta di un singolare ossimoro dei tempi moderni?

Mai come oggi potremmo dire, a ragione, che la tutela della privacy e la protezione

dei dati personali costituiscono una vera e propria sfida regolatoria: **Social Network, Cloud Computing, Internet of Things, Smartphone e Big Data** sono solo alcune delle principali "temibili" variabili socio-economiche e tecnologiche che occorre disciplinare in modo equilibrato, bilanciando contrapposti interessi.

Privacy digitale: un vero e proprio ossimoro dei tempi moderni

E' stato da tempo avviato anche il processo di riforma della Direttiva 2002/58/CE (c.d. "**Direttiva ePrivacy**"), che dovrebbe uniformare l'attuale quadro normativo continentale in materia di circolazione dei dati personali nelle comunicazioni elettroniche – con un tentativo di disciplinare anche le comunicazioni *Machine to Machine* del nuovo fenomeno *IoT* – con l'introduzione, anche in questo caso, di un Regolamento direttamente applicabile negli Stati UE.

L'economia globale è ormai declinata digitalmente: le tecnologie dell'informazione e della comunicazione non costituiscono più un settore a sé stante, bensì il fondamento stesso di tutti i sistemi economici innovativi moderni.

Il **Digital Single Market (DSM)** è un mercato in cui è garantita la libera circolazione delle merci, delle persone, dei servizi, dei capitali – oltre che dei dati – in condizioni di concorrenza leale, livello elevato di protezione dei consumatori e dei dati personali.

La realizzazione del DSM consentirà all'UE di mantenersi tra i leader mondiali dell'economia digitale, sostenendo la crescita delle imprese europee su scala globale.

Il considerando n. 1 del GPDR ricorda che: *"La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale".* E ancora l'art. 1, comma 2 del GDPR statuisce che: *"Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali".*

Un pilastro fondamentale del DSM è, infatti, proprio quello costituito dalla costruzione europea di un nuovo quadro regolatorio armonizzato in materia di privacy e protezione di dati personali in attuazione del generale precetto contenuto nell'articolo 16, paragrafo 1, del **Trattato sul funzionamento dell'Unione europea** (TFUE) che poggia sulla duplice tutela della persona offerta dai seguenti referenti normativi contenuti nella **Carta dei diritti fondamentali dell'Unione Europea:**

- **art.7 Diritto al rispetto della vita privata e familiare** e
- **art.8 Protezione dei dati di carattere personale**

Un mercato efficiente, corretto e trasparente che non rinuncia, quindi, alla tutela dei diritti fondamentali della persona e dei soggetti più deboli dal punto di vista economico, informativo e negoziale. In particolare, si rammenta l'art.8 della Carta che statuisce: "*Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica*".

La protezione prevista dal Regolamento Generale – a differenza dell'**ePrivacy** che si applicherà anche alle persone giuridiche – si applica esclusivamente alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali.

Fra le tante novità del nuovo Regolamento – V*alutazione Impatto Privacy, Data Protection Officer, Diritto all'oblio, Diritto alla portabilità dei dati* e il robusto apparato sanzionatorio solo per fare alcuni cenni *ex multis* senza pretese di esaustività – si segnala **l'art. 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita,**rafforzamento di princìpi già noti anche mediante meccanismi di certificazione indipendente, che testimonia lo sforzo di arginare la potenziale pervasività tecnologica digitale *ab origine* e non solo *ex post.*

Menzione particolare, infine, non certo per importanza, merita il principio di applicazione territoriale esteso statuito dal nuovo art. 3 del GDPR che – al fine di disciplinare l'attività di trattamento dati dei grandi player multinazionali ma con sede oltre oceano, nella *Silicon Valley* – stabilisce che: "*Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*".

E ancora: "*Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*

1. *a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure*
2. *b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.*

Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico".

A questo nuovo quadro regolatorio comunitario si aggiunge ora anche il tassello dell'armonizzazione del Codice della Privacy italiano (D.Lgs. 196/03) che dopo essere stato novellato dal tanto atteso D.Lgs. 101/2018 a ragione può ben ora essere denominato *nuovo Codice della Privacy.*

Non è certo possibile dar conto di tutte le significative novità introdotte, fermo restando che i principi generali sono quelli stabiliti dal GDPR e che il nuovo Codice si è ritagliato uno spazio di operatività nei limiti consentiti dal nuovo Regolamento.

Merita di essere menzionata la norma che si propone di dare continuità applicativa alla poderosa produzione del Garante anteriore al GDPR.

Ecco allora che sino all'adozione dei corrispondenti provvedimenti generali di cui all'articolo 2-*quinquiesdecies* del nuovo*Codice in materia di protezione dei dati personali*, i trattamenti di cui al medesimo articolo, già in corso alla data di entrata in vigore del presente decreto, possono proseguire qualora avvengano in base a espresse disposizioni di legge o regolamento o atti amministrativi generali, ovvero nel caso in cui siano stati sottoposti a verifica preliminare o autorizzazione del Garante per la protezione dei dati personali, che abbiano individuato misure e accorgimenti adeguati a garanzia dell'interessato (art. 22, comma 3 nuovo *Codice Privacy*).

E ancora la fondamentale statuizione dell'art. 22 comma, 4 nuovo *Codice Privacy* secondo cui, a decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il GDPR e con le disposizioni del presente nuovo Codice Privacy.

Infine, non certo per importanza, l'art. 22 comma 13 del nuovo Codice Privacy stabilisce *che* per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie.

Non si tratta di una moratoria in senso stretto, come inizialmente ipotizzato, in quanto non vi è né sospensione delle attività ispettive né sospensione delle sanzioni. Più semplicemente si tratta in una circostanza attenuante *ex lege* fondata sulle difficoltà applicative del primo periodo successivo all'entrata in vigore – 8 mesi dal 19 settembre 2018 – di cui il Garante terrà conto.

Detta previsione, tuttavia, pare depotenziata in quanto il nuovo Codice novellato dal D.Lgs. 101/2018 non quantifica, come invece sarebbe stato forse opportuno per evitare conteziosi nella fase di applicazione inziale, la misura dell'attenuante

applicabile.

Il nuovo Codice, interviene, inoltre, sull'apparato sanzionatorio penale delineando il seguente nuovo quadro:

- Trattamento illecito di dati
- L'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala
- Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala
- Inosservanza dei provvedimenti del Garante

Si registra, inoltre, un rafforzamento dei poteri e dei compiti del Garante. In particolare, ai sensi dell'Art. 154–bis (Poteri) del nuovo Codice Privacy, il Garante ha il potere di:

1. *a)*adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento, anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento;
2. *b)*approvare le regole deontologiche.

Inoltre, in considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, come definite dalla raccomandazione 2003/361/CE, il Garante per la protezione dei dati personali, nel rispetto delle disposizioni del Regolamento e del presente Codice, promuove, nelle linee guida adottate a norma del nuovo Codice Privacy, modalità semplificate di adempimento degli obblighi del titolare del trattamento.

Norma che si ritiene di particolare importanza perché l'impianto complessivo del GDPR tradisce una struttura complessa, ispirata alle strutture articolate delle grandi imprese, nazionali e multinazionali, in cui si può agevolmente osservare il principio di *segregation of duties* fra le varie figure soggettive della filiera privacy (Titolare, Responsabile, DPO) e si possono investire ingenti budget e risorse umane all'adempimento dei nuovi precetti sia sotto il profilo organizzativo che della sicurezza dei dati.

Occorre, invece, fermi restando i principi fondamentali introdotti dal GDPR, semplificare significativamente gli adempimenti richiesti dal nuovo quadro normativo in relazione a studi professionali, micro, piccole imprese e medie imprese, distinguendo con nettezza tra chi tratta dati esclusivamente per svolgere la propria attività professionale o d'impresa nell'ambito di rapporti contrattuali di fornitura di servizi e beni, rispetto a chi svolge un attività d'impresa che coincide con lo sfruttamento commerciale dei dati raccolti.

Tuttavia, nonostante l'importante sforzo normativo che il GDPR esprime – ulteriormente rafforzato dal nuovo Codice Privacy italiano e in attesa del completamento, in corso d'opera, del tassello relativo alla privacy digitale comunitaria – non si può negare che la tutela della privacy e della protezione dei dati personali siano ancora elementi di uno scenario strategico globale, complesso e mutevole, non ancora giunto a un assetto regolatorio definitivo.

Anche se attualmente non si può più disconoscere che il virtuoso processo di allineamento globale al *legal benchmark*costituito dal GDPR UE – anche da parte dei principali attori dei mercati multinazionali, gli *over the top* della Silicon Valley californiana e più in generale degli Stati Uniti – è ormai positivamente avviato.

Da tali premesse discende l'iniziativa dello scrivente – **Direttore Esecutivo DNT "Diritto Nuove Tecnologie®-Studi Giuridici per l'innovazione"** – di promuovere in occasione del ventennale della fondazione dell'Università di Milano Bicocca insieme all'**Accademia della Guardia di Finanza di Bergamo** e con il patrocinio del **Garante per la Protezione dei Dati Personali**, di **American Chamber of Commerce** e di **Privacy Italia** – **mercoledì 31 ottobre p.v. ore 14.30 Aula Magna dell'Università di Milano Bicocca** – il Convegno-Tavola Rotonda *"Protezione dei dati personali tra GDPR UE e nuovo Codice Privacy: un primo bilancio applicativo"* che vedrà la partecipazione – oltre al **Dott. Antonello Soro Garante per la Protezione dei Dati Personali** – di

autorevolissimi Relatori che interverranno sui principali aspetti dell'importante riforma a quasi un semestre dalla sua piena applicazione.

Link Programma

PER SAPERNE DI PIÙ SU: DATA PROTECTION

ARTICOLO PRECEDENTE
Italtel partner del progetto 5GCity, primi test al Lucca Comics&Games 2018

ARTICOLO SUCCESSIVO
Lepida e CUP2000, approvato definitivamente il progetto di fusione

ALTRE NEWS IN "INTERNET"

Bonus Cultura, fondo alleggerito di 20 milioni di euro. Ancora in attesa i nati nel 2000

e-Fattura, le 2 semplificazioni per gli intermediari. Invio 'massivo' o 'puntuale' delle deleghe

Trump bannato da Facebook, Fox e NBC per contenuti razzisti. Account stranieri bloccati sui social per possibili interferenze nel voto

Vorticidigitali. Editoria, come può la radio monetizzazione la propria presenza online?

Finanza Agevolata. Contributo a fondo perduto fino al 35% a sostegno delle imprese audiovisive in Piemonte

News

INTERNET
MEDIA
TELECOMS
ENERGIA
CYBERSECURITY
SMART CITY
ROBOT
GAMES
MAPPAMONDO
HOTSPOT
BIBLIOTECH
RECENSITI
INFOGRAFICHE
PICS
WHO IS WHO

Rubriche

APP4ITALY
ASSETPROTECTION
BREAKINGDIGITAL
CDTI FORUM
COSA COMPRO
COSEDANONCREDERE
DIGITAL CUSTOMER EXPERIENCE
DIGILAWYER
DIGITAL CRIME
DIGITAL EDUCATION
DIGITANOMALIE
EMAIL MARKETING TIPS
ENTERPRISE 4.0
FINANZA AGEVOLATA

key4biz dal 2002

CHI SIAMO
COSA FACCIAMO
PARTNER
DAILYLETTER
PRIVACY POLICY
COOKIE POLICY
CONTATTI
Seguici