Il nuovo regolamento europeo in ambito privacy: Quali sono i punti di attenzione per le aziende italiane?

Antonio Piva - Attilio Rampazzo - Luca Spongano

"Il nuovo Regolamento Europeo della privacy sarà una riforma che andrà innanzitutto a beneficio delle persone fisiche, rafforzando i loro diritti alla protezione dei dati e la loro fiducia nell'ambiente digitale; semplificherà notevolmente il quadro giuridico per le imprese e il settore pubblico. Ciò dovrebbe stimolare lo sviluppo dell'economia digitale in tutto il mercato interno dell'Unione Europea ed oltre, in linea con gli obiettivi della strategia dell'Europa 2020 e dell'Agenda digitale europea. Infine, la riforma aumenterà la fiducia tra le autorità di contrasto e faciliterà gli scambi di informazioni e la cooperazione tra le autorità stesse nella lotta contro le forme gravi di criminalità, garantendo nel contempo alle persone fisiche un livello elevato di protezione"[1]

1. Introduzione

Se partiamo dalla concezione che sono dati personali tutte le informazioni riconducibili ad una persona, alla sua vita privata, professionale o pubblica come il nome, la foto, l'indirizzo e-mail, gli estremi bancari, i post nei social network o i referti medici, ci rendiamo conto dell'importanza di una normativa che garantisca e tuteli questo tipo di informazioni. La Carta dei diritti fondamentali dell'Unione europea afferma, infatti, che "ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano" in tutti gli ambiti della propria esistenza: a casa, al lavoro, quando fa acquisti oppure segue una cura medica, a scuola, su Internet. Nell'era digitale, poter raccogliere e conservare dati personali è diventato fondamentale e necessario anche per il

---

[1] *Comunicazione della Commissione UE: "Salvaguardare la privacy in un mondo interconnesso Un quadro europeo della protezione dei dati per il XXI secolo" (Bruxelles, 25.1.2012; COM(2012) 9 final).*

funzionamento dei sistemi stessi (si pensi, per esempio, all'utilizzo dei cookies[2]). In un mondo globalizzato, i trattamenti successivi alla raccolta, come la comunicazione fra imprese ed il trasferimento di dati a paesi terzi, sono diventati un fattore imprescindibile.

In questo contesto quasi tre anni fa, il 25 gennaio 2012, la Commissione europea ha ufficialmente presentato con un Regolamento Europeo[3], la proposta di aggiornamento della normativa concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati.

Il Regolamento in questione, non solo andrà a sostituire la direttiva 95/46/CE in materia di protezione dei dati personali - recepita dal legislatore italiano con la legge 675/96, successivamente sostituita dal D.Lgs. 196/03, il nostro attuale "Codice Privacy" - ma uniformerà ed armonizzerà a livello europeo la legislazione in materia di protezione dei dati personali, risalente ormai a quasi 20 anni fa. Le imprese europee saranno agevolate da un quadro legislativo comune, senza così dover far fronte a normative differenti in ciascuno stato membro.

Il Regolamento UE, come atto "self-executing" (ai sensi dell'art. 288 del Trattato sul funzionamento dell'Unione europea - TFUE), sarà direttamente ed immediatamente esecutivo e non necessiterà del recepimento da parte degli Stati membri, divenendo operativo dal momento in cui sarà approvato. In linea con l'approccio pragmatico scelto dalla Commissione UE, sarà lasciato agli Stati membri ed alle Autorità competenti in materia un certo margine per mantenere o adottare, in conformità al Regolamento, norme specifiche di settore.

L'ultima versione del Regolamento, approvato in prima lettura dal Parlamento Europeo, è del 12 marzo 2014[4], il cui testo è stato votato in maniera schiacciante (621 voti a favore, 10 contrari e 22 astensioni). Questo passaggio ha rappresentato un'importante impulso, formale e sostanziale, nel progresso dell'iter legislativo di approvazione. L'approvazione finale del documento - che secondo le ultime previsioni avverrà entro la prima metà del 2015 - spetterà al Parlamento Europeo attraverso la procedura legislativa ordinaria di co-decisione

---

[2] *I cookies sono piccoli file di testo che i siti visitati dall'utente inviano al suo terminale, dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita. Sono usati per eseguire autenticazioni informatiche, monitoraggio di sessioni e memorizzazione di informazioni degli utenti. Alcune operazioni non potrebbero essere compiute senza l'uso dei cookie, che in alcuni casi sono quindi tecnicamente necessari: a titolo esemplificativo, l'accesso all'home banking e le attività svolte sul proprio conto corrente online (visualizzazione dell'estratto conto, bonifici, pagamento di bollette, ecc.) sarebbero più complesse da svolgere e meno sicure senza la presenza di cookie in grado di identificare l'utente e mantenerne l'identificazione nell'ambito della sessione.*

[3] *Al riguardo si veda il Comunicato Stampa del Garante privacy, pubblicato il 7 Febbraio 2012.*

[4] *Il Testo emendato era stato già votato il 21 Ottobre 2013 dalla Commissione Libe (Libertà civili, giustizia e affari interni). È importante precisare che la bozza di Regolamento è stata e a tutt'oggi è, ancora, discussa in seno al Consiglio "Giustizia e affari interni" (GAI).*

con il Consiglio Europeo[5]. I Titolari del trattamento (imprese private, enti pubblici, studi professionali, etc.) avranno tempo due anni dalla pubblicazione del testo definitivo per mettersi in regola con gli adempimenti derivanti[6].

Campo di applicazione

Le norme interesseranno tutti quei soggetti (anche extraeuropei) che sono chiamati a trattare (in maniera automatizzata o meno) i dati relativi, per esempio, a clienti, dipendenti, studenti, utenti, fornitori. In sostanza, viene introdotto il principio dell'applicazione del diritto dell'Unione Europea anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni o sevizi a cittadini UE o tali da comportare il monitoraggio dei loro comportamenti.

Il Regolamento, come espressamente affermato anche nei relativi *considerando* al testo, si applicherà anche al trattamento di identificativi prodotti da dispositivi, applicazioni, strumenti e protocolli, quali gli indirizzi IP, i cookies e i tag di identificazione a radiofrequenza, salvo il caso in cui tali identificativi non si riferiscano a una persona fisica identificata o identificabile.

Le aziende e le istituzioni pubbliche dovranno, pertanto, adottare politiche ed attuare misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato sia conforme - fin dalla fase embrionale - a tutte le disposizioni del Regolamento.

Di importanza non secondaria, sarà l'impianto sanzionatorio. Al fine di rendere punibile chiunque, persona di diritto pubblico o di diritto privato, non ottemperi alle disposizioni del Regolamento, quest'ultimo richiederà agli Stati membri di garantire sanzioni efficaci, proporzionate e dissuasive e di adottare tutte le misure necessarie per la loro applicazione. L'Autorità di Controllo potrà arrivare ad imporre sanzioni amministrative pecuniarie fino a 100 milioni di Euro o fino al 5% del fatturato mondiale annuo (se superiore) nel caso di un'impresa.

Nella trattazione che segue viene fornita una sintesi, per punti distinti, delle principali e fondamentali novità derivanti dalla proposta di nuovo Regolamento Europeo.

Dovere di documentazione e di informazione

Sarà necessario elaborare un sistema documentale di gestione della privacy contenente tutti gli atti, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità al Regolamento. È l'applicazione operativa del principio di rendicontazione (o di "accountability"), secondo cui il Titolare del trattamento deve conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente - per ognuno di essi - una serie "nutrita" di informazioni, tali da assicurare e comprovare la conformità di

---

[5] *Si tratta del c.d. "trilogo", secondo il cui procedimento l'adozione definitiva di un Regolamento avviene a seguito della negoziazione congiunta tra Parlamento, Consiglio e Commissione Europea. Al riguardo si vedano, in particolare, gli articoli 288, 289 e 294 del TFUE (Trattato sul funzionamento dell'Unione europea).*

[6] *Si veda l'art. 91 del testo del Regolamento presentato dalla Commissione UE il 25.01.2012*

ciascuna operazione alle disposizioni del Regolamento (qualcosa di simile al Documento Programmatico sulla Sicurezza, ma di portata più ampia).

In tal senso, acquisirà ancora più importanza il principio di trasparenza e di informazione nei confronti dell'interessato, che il Titolare del trattamento farà valere sia attraverso l'adozione di politiche concise, trasparenti, chiare e facilmente accessibili, sia mediante la resa di informazioni e comunicazioni con un linguaggio semplice e chiaro (in particolare se le informazioni sono destinate ai minori). Ancora più rilevante diverrà l'obbligo di resa dell'informativa privacy e della acquisizione "granulare" dei consensi (specifici per ogni tipologia di trattamento), quando dovuti. Il Regolamento amplierà il contenuto da inserire nell'Informativa rispetto al dettato dall'art. 13 dell'attuale Codice Privacy (si veda la sintesi riportata nel riquadro sottostante)

Le informazioni da fornire all'interessato

L'informativa: D.Lgs. 196/03 e Regolamento Europeo

PRINCIPALI ADEMPIMENTI CODICE PRIVACY	PRINCIPALI NOVITA' DEL REGOLAMENTO EUROPEO
Finalità e **modalità** del trattamento	**Tabella sinottica "standard"** (art 13.bis)
Natura obbligatoria / **facoltativa** del conferimento	Informazioni concernenti la **sicurezza del trattamento**
Conseguenze di **rifiuto di rispondere**	Periodo di **conservazione** / criteri per determinarlo
Soggetti / categorie ai quali i dati possono essere **comunicati** o che possono venirne a conoscenza come Responsabili o Incaricati	Diritto di proporre **reclamo** all'Autorità di C. e sue coordinate
Ambito di **diffusione**	Intenzione, se del caso, di **trasferire** dati
Diritti di accesso e **altri diritti** (Art.7)	Informazioni, se del caso, sull'esistenza della **profilazione**
Estremi identificativi del Titolare / Rappr. nello Stato / Resp. del trattamento / Resp. riscontro all'interessato	**Ogni** altra **informazione necessaria** per garantire un trattamento equo
Sito / modalità per conoscere **elenco dei Resp**.	Informazioni, se del caso, su **trasmissione alle autorità pubbliche** durante gli ultimi 12 mesi consecutivi.

Valutazione d'impatto sulla protezione dei dati

I Titolari dovranno effettuare una Valutazione degli impatti privacy (*Data Protection Impact Analysis* – DPIA) fin dal momento della progettazione del processo aziendale e degli applicativi informatici di supporto, nei casi in cui il trattamento alla base degli stessi, per sua natura, oggetto o finalità, presenti rischi specifici per i diritti e le libertà degli interessati. In particolare, a titolo meramente esemplificativo e non esaustivo, la DPIA andrà realizzata per trattamenti quali: la valutazione sistematica di aspetti della personalità dell'interessato o quelli volti ad analizzarne la situazione economica, l'ubicazione, lo stato di salute, l'affidabilità o il comportamento, mediante un trattamento automatizzato; per trattamenti di dati concernenti la vita sessuale, la prestazione di servizi sanitari, lo stato di salute, la razza e l'origine etnica; o, ancora, per trattamenti di dati in archivi su larga scala riguardanti minori, dati genetici o dati biometrici, a sorveglianza di zone accessibili al pubblico, in

particolare se effettuata mediante dispositivi ottico-elettronici (video-sorveglianza).

Stando a quanto disposto dal Considerando n° 70 del Regolamento, verrà abolito l'obbligo di Notificazione di specifici trattamenti[7] all'Autorità di Controllo (il nostro attuale Garante Privacy). Tale adempimento è considerato dal Legislatore europeo come un obbligo che comporta oneri amministrativi e finanziari senza aver mai veramente contribuito a migliorare la protezione dei dati personali (in particolare per le piccole e medie imprese). È pertanto necessario (continua il testo del Regolamento) abolire tale obbligo generale di notificazione e sostituirlo con meccanismi e procedure efficaci che si concentrino piuttosto su quelle operazioni di trattamento che potenzialmente presentano rischi specifici per i diritti e le libertà degli interessati, per la loro natura, portata o finalità. In tali casi sarà necessaria una valutazione d'impatto sulla protezione dei dati, da effettuarsi prima del trattamento, che verta, in particolare, sulle misure, sulle garanzie e sui meccanismi previsti per assicurare la protezione dei dati personali e per comprovare il rispetto del Regolamento.

Designazione di un Data Protection Officer - DPO (o Privacy Officer)

Già nel 2006, il Presidente del Garante Privacy Francesco Pizzetti, affermava "*Vedo con molto favore l'istituzione della figura del Data Protection Officer (DPO) specialmente per le aziende e le corporation medie e grandi. La diffusione di questa figura non potrebbe che aiutare l'azione del Garante e la diffusione stessa della privacy nell'ambito delle strutture di impresa[8]*". Con l'avvento del nuovo Regolamento troverà previsione la nuova figura del "Responsabile per la protezione dei dati". Le categorie che dovranno adempiere saranno[9] tutte le autorità ed organismi pubblici e, in ambito privato, le imprese che trattino i dati di un certo numero di persone (c.d. interessati) o tipologie di dati che per natura, oggetto o finalità siano definite categorie "a rischio" dalla normativa.

Il DPO andrà designato per un dato periodo - quattro anni in caso di servizi esternalizzati in outsourcing – e in funzione delle qualità professionali, della

---

[7] *Si vedano al riguardo l'art. 37 del D.Lgs. 196/03 e i Provvedimenti emessi dal Garante Privacy in cui vengono individuati alcuni trattamenti (nell'ambito di quelli previsti dall'art. 37) che presentano minori rischi per i diritti degli interessati e sono pertanto esonerati dall'obbligo di notificazione [doc. web n. 852561; doc. web n. 993385; doc. web n. 996680; doc. web n. 1823225].*

[8] *Parole rilasciate nel 2006, in occasione dell'European Privacy Officers Forum – Epof (associazione che riunisce i Privacy Officers operanti all'interno di circa 35 società multinazionali con sede in Europa). Rif. Newsletter del Garante Privacy n. 278 del 19 giugno 2006.*

[9] *I casi di designazione necessaria del DPO sono, ad oggi, ambito ancora dibattuto in seno al Consiglio Giustizia e Affari Interni (GAI). In ambito privato, nel testo del 25 Gennaio 2012, l'obbligatorietà del DPO trova previsione per le imprese private di almeno 250 o più dipendenti; nella versione del 12 Marzo 2014, per le aziende che effettuano trattamenti di almeno 5.000 interessati in 12 mesi consecutivi. Si ricordi, comunque, che la designazione del DPO è obbligatoria nelle istituzioni dell'Unione Europea e, da alcuni anni, in diversi Stati Membri, in base all'art. 18 della Direttiva 95/46/CE. Con la continuazione delle discussioni del c.d. trilogo (rif. nota n.5) si svilupperà definitivamente il tema del DPO*

conoscenza specialistica della normativa. I Titolari del trattamento dovranno assicurarsi che ogni altra eventuale funzione professionale della persona che rivestirà il ruolo di DPO sia compatibile con i compiti e le funzioni dello stesso in qualità di DPO e non dia adito a conflitto di interessi (dovrà quindi essere autonomo, indipendente e non ricevere alcuna istruzione per l'esercizio delle sue attività).

Il DPO, il cui mandato potrà essere rinnovabile, potrà essere assunto oppure adempiere ai suoi compiti in base a un contratto di servizi. Il Titolare del trattamento, che a seconda della forma contrattuale, potrà essere datore di lavoro o committente, dovrà fornire al DPO tutti i mezzi inclusi il personale, i locali, le attrezzature e ogni altra risorsa necessaria per adempiere alle sue funzioni e per mantenere la propria conoscenza professionale. I principali compiti del DPO, il cui nominativo andrà comunicato all'Autorità di Controllo e al pubblico, saranno quelli di:

- sensibilizzare e consigliare il Titolare in merito agli obblighi (misure e procedure tecniche e organizzative) derivanti Regolamento;
- sorvegliare l'applicazione delle politiche compresa l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e l'effettuazione degli audit connessi;
- sorvegliare l'applicazione del Regolamento, con particolare riguardo alla protezione fin dalla progettazione, alla protezione di default, alla sicurezza dei dati, alle informazioni dell'interessato ed alle richieste degli stessi per esercitare i diritti riconosciuti;
- controllare che il Titolare effettui la Valutazione d'impatto sulla protezione dei dati (c.d. DPIA) e richieda all'Autorità di Controllo l'autorizzazione preventiva o la consultazione preventiva nei casi previsti;
- fungere da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento e consultarla, se del caso, di propria iniziativa;
- informare i rappresentanti del personale (es. rappresentanti sindacali) sui trattamenti che riguardano i dipendenti.

Si può quindi affermare, che si procede verso la creazione di una nuova categoria professionale che dovrà disporre di precise e specifiche competenze sia giuridiche che informatiche nell'ambito della protezione dei dati personali. In questa medesima direzione va inteso lo strumento di apprendimento e di verifica realizzato da AICA con il Modulo di Certificazione "Protezione dei dati personali – Privacy e Sicurezza" all'interno della Certificazione "Diritto e ICT".

Allo stato attuale non ci sono figure professionali specifiche che possano fregiarsi del titolo di DPO, né probabilmente ci saranno a breve specifiche certificazioni data la specifica volontà del legislatore europeo di affidare agli atti delegati della Commissione europea questa materia. Da una parte si può quindi affermare che non sono strettamente indispensabili (anche se, nella nostra opinione, vivamente consigliate) certificazioni per ricoprire il ruolo del DPO, quanto invece necessaria una "conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti".

Dall'altra parte, è probabile che le uniche certificazioni relative al DPO che avranno un valore nei prossimi anni - al fine della designazione del DPO - saranno solo e soltanto quelle già internazionalmente riconosciute e rilasciate da organismi che operano da anni nel settore come per esempio quelle riguardanti lo standard EUCIP, lo standard e-CF (European e-Competence Framework) ed e-CF*Plus*, ai quali hanno collaborato il Cepis ed AICA, o certificazioni rilasciate da ISACA[10] e da IAPP[11] (p.e. CISA, CISM, CIPP, CISPP e simili) poiché dirette a verificare competenze effettive e non certificazioni semplicemente formali. Certamente queste figure avranno necessità anche di un background tecnico, organizzativo e giuridico sulla protezione dei dati. In questa direzione può essere utilizzata la già citata certificazione "Protezione dei dati personali – Privacy e Sicurezza" di AICA.

Attuazione dei requisiti di sicurezza dei dati

L'attuale normativa privacy prevede, in capo ai Titolari del trattamento, l'adozione di differenti tipologie di misure di sicurezza: quelle minime (predefinite ed indicate nell'Allegato B al Codice Privacy); quelle idonee (individuate a seguito di analisi del rischio e in relazione alle conoscenze acquisite, al progresso tecnologico, alla natura dei dati ed alle specifiche del trattamento); quelle prescritte dal Garante Privacy (mediante i Provvedimenti generali e specifici). L'attuale testo del Regolamento affronta il tema della sicurezza dei dati in maniera generica, lascando aperta, come vedremo, la determinazione di dettaglio delle misure da adottare a futuri interventi da parte del Comitato europeo per la protezione dei dati[12] e della Commissione UE.

L'attuale testo del Regolamento richiede la messa in atto di misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento comporta. L'adeguatezza di tali misure deve derivare dai risultati della valutazione di impatto (*DPIA*), dall'evoluzione tecnica e dai costi di attuazione. Tale politica di sicurezza deve includere: a) la capacità di assicurare che sia convalidata l'integrità dei dati personali; b) la capacità di assicurare riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; c) la capacità di ripristinare la disponibilità e l'accesso ai dati in modo tempestivo, in caso di incidente fisico o tecnico che abbia un impatto sulla disponibilità, sull'integrità e sulla riservatezza dei sistemi e dei servizi di informazione; d) in caso di trattamento di dati personali sensibili, misure di sicurezza aggiuntive per garantire la consapevolezza dei rischi e la

---

[10] *ISACA - conosciuta come Information Systems Audit and Control Association, ora ISACA è solo un acronimo che identifica l'Associazione Internazionale che raggruppa un'ampia gamma di professionisti che operano nell' IT Governance.*

[11] *IAPP - International Association of Privacy Professionals.*

[12] *Il Comitato europeo per la protezione dei dati sostituirà il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito con direttiva 95/46/CE. Il comitato sarà composto dal responsabile dell'Autorità di controllo di ciascuno Stato membro e dal Garante europeo della protezione dei dati. Il Comitato contribuirà all'applicazione uniforme del Regolamento in tutta l'Unione Europea.*

capacità di adottare in tempo reale azioni di prevenzione, correzione e attenuazione, contro le vulnerabilità riscontrate o gli incidenti verificatisi, che potrebbero costituire un rischio per i dati; e) un processo per provare, verificare e valutare regolarmente l'efficacia delle politiche, delle procedure e dei piani di sicurezza attuati per assicurare la continua efficacia. Le misure appena citate devono come minimo: a) garantire che ai dati personali possa accedere soltanto il personale autorizzato agli scopi autorizzati dalla legge; b) proteggere i dati personali conservati o trasmessi dalla distruzione accidentale o illegale, dalla perdita o dalla modifica accidentale e dalla conservazione, trattamento, accesso o comunicazione non autorizzati o illegali; nonché c) assicurare l'attuazione di una politica di sicurezza in relazione con il trattamento dei dati personali. È assai probabile che l'adesione a codici di condotta (approvati ai sensi dell'articolo 38 del Regolamento) o un meccanismo di certificazione (approvato ai sensi dell'articolo 39 del Regolamento) possano essere utilizzati come elementi per dimostrare la conformità ai requisiti di sicurezza sopra elencati.

Sarà il Comitato europeo per la protezione dei dati l'ente deputato ad emettere orientamenti, raccomandazioni e migliori prassi, per le misure tecniche e organizzative, compresa la determinazione di ciò che costituisce l'evoluzione tecnica - per settori specifici e in specifiche situazioni di trattamento dei dati - in particolare tenuto conto degli sviluppi tecnologici e delle soluzioni per la protezione fin dalla progettazione e per la protezione di default.

Inoltre, se necessario, la Commissione UE potrà adottare atti di esecuzione per precisare i requisiti delle misure sopra elencate, in particolare per: a) impedire l'accesso non autorizzato ai dati personali; b) impedire qualunque forma non autorizzata di divulgazione, lettura, copia, modifica, cancellazione o rimozione dei dati personali; c) garantire la verifica della liceità del trattamento.

Privacy by design e Protezione di default

Si tratta dell'esplicitazione del principio dell'incorporazione della privacy fin dalla progettazione del processo aziendale e degli applicativi informatici di supporto, ovvero la messa in atto di meccanismi per garantire che siano trattati - di default - solo i dati personali necessari per ciascuna finalità specifica del trattamento (si tratta della riattualizzazione in chiave moderna del principio di necessità sancito dal Codice Privacy). I Titolari del trattamento dovranno, pertanto, prevedere meccanismi di protezione dei dati fin dalla progettazione delle attività e per l'intera gestione del ciclo di vita dei dati - dalla raccolta alla cancellazione - incentrandosi sistematicamente sulle garanzie procedurali in merito all'esattezza, alla riservatezza, all'integrità, alla sicurezza fisica ed alla cancellazione dei dati. Tali meccanismi andranno identificati sia nel momento in cui si definiscono le finalità e i mezzi del trattamento sia all'atto del trattamento stesso, tenuto conto dell'evoluzione tecnica (e dei costi di attuazione) delle migliori prassi (best pratices) internazionali e dei rischi del trattamento. A livello operativo vorrà dire sia fare in modo che la quantità dei dati raccolti e la durata della conservazione (o eventuale diffusione) non vada oltre il minimo necessario per le finalità perseguite, sia predisporre meccanismi che garantiscano che, di

default, non siano resi accessibili dati ad un numero indefinito di persone e che gli interessati siano in grado di controllarne il flusso. Questo avrà un forte impatto nello sviluppo di software destinati al trattamento di dati (es. CRM, ERP, gestionali aziendali) e sul rinnovamento del parco informatico delle amministrazioni, delle imprese e degli studi professionali.

Obblighi di segnalazione in caso di Violazione sui dati

Con la nozione di violazione dei dati personali (c.d. "personal data breaches"), si intende: la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati.

I Titolari del trattamento, in caso di una violazione come sopra descritta, dovranno mettere in atto due differenti azioni: la notificazione della violazione all'Autorità di controllo e la segnalazione al diretto interessato.

Nel primo caso, accertata la violazione, la relativa notificazione dovrà contenere una serie nutrita di informazioni: la natura della violazione medesima, le categorie e il numero di interessati coinvolti; l'identità e le coordinate di contatto del DPO; l'elenco delle misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione dei dati; la descrizione degli impatti derivanti; le misure proposte o adottate per porre rimedio alla violazione e attenuarne gli effetti.

Inoltre, l'Autorità di Controllo conserverà un registro pubblico delle tipologie di violazione notificate.

Nel caso in cui, poi, la violazione rischi di pregiudicare i dati, attentare alla vita privata, ai diritti o agli interessi legittimi dell'interessato, il Titolare, dopo aver provveduto alla notificazione, dovrà comunicare la violazione al diretto interessato senza ritardo. In mancanza l'Autorità di Controllo, considerate le presumibili ripercussioni negative della violazione, potrà obbligare il Titolare a farlo. La comunicazione all'interessato dovrà essere esaustiva e redatta in un linguaggio semplice e chiaro e descrivere la natura e le conseguenze della violazione, le misure raccomandate per attenuare i possibili effetti pregiudizievoli, i diritti esercitabili dall'interessato. La comunicazione non sarà richiesta quando il Titolare dimostrerà in modo convincente all'Autorità di Controllo di aver utilizzato le opportune misure tecnologiche di protezione (es. cifratura) e che tali misure sono state applicate, proprio, ai dati violati (es. furto tablet con dati sanitari cifrati). Queste misure tecnologiche di protezione devono rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

Riconoscimento di nuovi diritti

Il testo del Regolamento riconosce, sancendoli nel testo, nuovi diritti. In particolare si fa riferimento al Diritto all'oblio e Diritto alla portabilità del dato (rispettivamente, *right to be forgotten / right to erasure* e *data portability*).

Con Diritto alla portabilità del dato si intende il riconoscimento sia del diritto dell'interessato a trasferire i propri dati (es. quelli relativi al proprio "profilo utente") da un sistema di trattamento elettronico (es. Social Network) ad un altro

senza che il Titolare possa impedirlo, sia del diritto di ottenere gli stessi in un formato elettronico strutturato e di uso comune che consenta di farne ulteriore uso. Tale diritto dovrebbe trovare applicazione quando l'interessato ha fornito i dati al sistema di trattamento automatizzato acconsentendo al trattamento o in esecuzione di un contratto.

L'impulso alla base del diritto all'oblio nasce per regolare la diffusione del dato nella "rete"[13], in maniera tale che l'interessato abbia diritto di ottenere dal Titolare del trattamento la loro cancellazione totale e la rinuncia ad una loro ulteriore diffusione. Per rafforzare il "diritto all'oblio" nell'ambiente on-line, il Titolare che ha pubblicato dati personali, potrà essere obbligato ad informare i terzi (che trattano i medesimi dati), della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Per garantire tale diritto, sarà necessario che il Titolare del trattamento prenda tutte le misure ragionevoli, anche di natura tecnica, in relazione ai dati della cui pubblicazione è responsabile avendoli immessi per primo in rete. Il diritto all'oblio potrà, poi, permettere di gestire meglio i rischi connessi alla protezione dei dati online: si potrà richiedere, ottenendola, la possibilità di cancellare i propri dati se non sussistono motivi legittimi per mantenerli[14].

Conclusione

La rilevanza generale della proposta, come appare chiaro, ha una notevole portata. Non si tratterà di una semplice revisione, bensì di un intervento normativo a fronte dell'esperienza maturata negli ultimi anni su settori sino ad oggi solo sfiorati, che avrà effetti anche sulla concezione stessa della 'privacy', facendola calare sempre all'interno dei processi e dell'organizzazione aziendale non più come elemento/adempimento successivo ma presupposto ancillare e propedeutico già nelle fasi di progettazione dei processi.

Il fine primario del nuovo quadro giuridico sarà, poi, quello di apportare migliorie per le persone fisiche e per i Titolari del trattamento (aziende, imprese, enti pubblici), di dimostrarsi valido anche per i prossimi anni ed in grado di reggere gli impatti posti, in particolare, dall'avvento delle nuove tecnologie (pensiamo

---

[13] *La Corte di Giustizia dell'Unione Europea si è pronunciata, il 13 maggio 2014, in tema di diritto all'oblio su Google, nell'ambito della causa tra Google Spain e Google Inc., da una parte, e Agencia Española de Protección de Datos (AEPD) e il sig. González, dall'altra. L'Agenzia di protezione spagnola aveva accolto la denuncia depositata dal sig. González contro Google Spain e Google Inc., ordinando a quest'ultima di adottare le misure necessarie per rimuovere dai propri indici alcuni dati personali riguardanti l'interessato e impedirne il futuro accesso.*

[14] *Al riguardo si vede il servizio on-line messo a disposizione da Google attraverso il quale l'interessato può – se non ricopre nella vita pubblica un ruolo tale da giustificare l'ingerenza nei suoi diritti fondamentali con l'interesse preponderante del pubblico ad avere accesso all'informazione personale - richiedere che l'informazione che lo riguarda non venga più messa a disposizione del pubblico tramite indicizzazione sul motore di ricerca.*

per esempio alle sfide, in ottica privacy, derivanti dal Cloud Computing[15] o dall'Internet of Things - IoT).

Si può quindi affermare che si assisterà ad un passaggio da un sistema di tipo formalistico come quello attuale, ad uno di alta responsabilizzazione sostanziale in cui sarà richiesto un ruolo proattivo ai Titolari del trattamento.

In conclusione, una risposta efficace ed efficiente agli obblighi sopra descritti non potrà non passare dalla predisposizione e formalizzazione di un preciso organigramma privacy interno che "regoli il traffico" e vada a definire il "chi fa cosa", coerentemente alle mansioni aziendali[16]. Di non meno importanza sarà anche, da una parte la predisposizione, a livello contrattuale in caso di trattamenti esternalizzati, di precise clausole che prevedano la sottoscrizione di Service Level Agreement (SLA) o Privacy Level Agreement (PLA)[17], dall'altra la predisposizione di un "Sistema 231" (responsabilità amministrativa delle persone giuridiche), che si sostanzi sempre più in pratiche di controllo interno aziendale - anche secondo le schema PDCA: Plan, Do, Check, Act - per la protezione dell'organizzazione dalla commissione dei reati presupposto quali i reati informatici ed i trattamenti illeciti di dati (di cui, in particolare, all'art. 24 del D.Lgs. 231/2001).

Biografie

Antonio Piva, laureato in Scienze dell'Informazione, Vice Presidente dell'ALSI (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Ingegnere dell'Informazione, docente a contratto di diritto dell'ICT, qualità e comunicazione all'Università di Udine. Consulente su Governo Elettronico, Agenda Digitale ed innovazione nella PA locale, Auditor Sistemi informativi e 231, è consulente e valutatore di sistemi di qualità ISO9000, Privacy e Sicurezza presso Enti pubblici e privati. Ispettore AICA presso scuole ed enti di formazione. Membro del Consiglio Nazionale del Forum Competenze Digitali, è Presidente della Sezione Territoriale AICA del Nord Est.

Email: antonio@piva.mobi

---

[15] *Lo scorso agosto è stata pubblicata la ISO/IEC 27018:2014 Information Technology -- Security Techniques -- Code of Practice for Protection of Personally Identifiable Information (PII) in public clouds acting as PII processors Si tratta di un set di regole costruito sugli standards ISO 27001 e 27002 per garantire il rispetto dei principi e delle norme privacy da parte dei providers di public cloud che se ne dotano.*

[16] *Al riguardo si indica la norma ISO/IEC 29100:2011 Information Technology -- Security Techniques -- Privacy framework che fornisce i riferimenti per la gestione di un Sistema di Gestione della Privacy*

[17] *Nell'ambito della famiglia di norme ISO/IEC 27000 sono state pubblicate le seguenti norme che danno ottime linee guida sull'argomento:*

- *ISO/IEC 27036-1: 2014 - Information security for supplier relationships — Part 1: Overview and concepts*
- *ISO/IEC 27036-2: 2014 - Information security for supplier relationships — Part 2: Requirements*

ISO/IEC 27036-3:2013 - Guidelines for ICT supply chain security

Attilio Rampazzo, *CISA CRISC*, *C|CISO CMC* consulente di Sistemi Informativi e Sicurezza delle Informazioni in primaria azienda di Servizi Informatici italiana. Ha maturato un'esperienza pluriennale nello sviluppo e conduzione di progetti informatici in ambito bancario e finanziario, nei quali la qualità e la sicurezza hanno ricoperto un ruolo determinante. E' Vice Presidente di AICA sez. Nord Est e CISA Coordinator e Research Director in ISACA Venice chapter. Svolge attività come Valutatore di Sistemi di Sicurezza delle Informazioni e di Sistemi di Gestione dei Servizi (cert. AICQ Sicev) presso CSQA Certificazioni. Trainer accreditato APMG per ITIL, ISO 20000 e Cobit 5. Docente ai corsi per LA ISO/IEC 27001, LA ISO/IEC 20000-1, LA ISO 22301 riconosciuti AICQ Sicev. Socio AICA, AICQ, ISACA Venice chapter, ASSOVAL, ANIP.

Email: attilio.rampazzo@gmail.com

Luca Spongano, ha conseguito il Master in Diritto delle Nuove Tecnologie ed Informatica Giuridica presso l'Alma Mater Studiorum di Bologna - Facoltà di Giurisprudenza di Bologna (Cirsfid). Ha operato, tra gli altri, come esperto legale nel diritto delle nuove tecnologie e diritto dell'informatica, addetto alla gestione della normativa in ambito Protezione dei dati personali all'interno del Presidio Privacy della seconda Multiutility italiana, contribuendo alla definizione e mantenimento del Sistema di Gestione Privacy dell'intero Gruppo. È autore sulla rivista telematica informatico/legale Filodiritto. È membro del Gruppo Diritto ICT e Privacy nonché Consigliere della Sezione Territoriale AICA dell'Emilia Romagna. È curatore del "Privacy Blog" (www.lucaspongano.it/wordpress/) inerente le tematiche del diritto dell'informatica con un focus sulle tematiche Privacy. Svolge attività di assistenza e consulenza in ambito Privacy.

Email: lucaspongano@gmail.com