Iusletter
informazione e aggiornamento giuridico

LaScala
STUDIO LEGALE

Focus on

LE NOVITÀ INTRODOTTE DAL REGOLAMENTO EUROPEO SULLA PRIVACY

Giugno 2016

www.lascalaw.com
www.iusletter.com

Milano | Roma | Torino | Bologna | Firenze | Ancona | Vicenza | Padova
redazione@lascalaw.com

Sommario

1. Introduzione

Lo scorso 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale UE il Regolamento «*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*» con cui l'Unione Europea si dota di una nuova legge che fa tesoro dell'esperienza maturata negli ultimi venti anni, da quando cioè fu adottata la prima direttiva in materia di privacy (direttiva 95/46/CE, ora abrogata).

L'obiettivo principale del Regolamento, che come tale si applica direttamente in tutti i Paesi dell'Unione, è quello di proseguire nel cammino di sensibilizzazione degli operatori e consapevolezza dei cittadini verso i temi della privacy tenendo conto che l'avvento delle tecnologie della comunicazione, e con esse la globalizzazione dei mercati, hanno lanciato nuove sfide che minacciano i diritti fondamentali dell'individuo ma, al tempo stesso, se affrontate per tempo con adeguate riforme normative, offrono incredibili opportunità di sviluppo.

La quantità di informazione creata nel mondo raddoppia ogni dodici mesi. Raddoppiava ogni 25 anni alla fine della Seconda Guerra Mondiale, e con l'avvento dell'*Internet delle cose* questa accelerazione esponenziale è prevista in crescita fino ad arrivare a raddoppiare addirittura ogni 12 ore[1].

Questa enorme mole di informazioni accompagna anche massivi trattamenti di dati personali attraverso cui compiere analisi predittive o estrarre informazioni nascoste da utilizzare in processi decisionali, anche senza intervento umano (*Big Data*).

Anziché evocare scenari da Grande Fratello, l'inevitabile prospettiva di un mondo governato dall'informatica, dove potenza di calcolo e banda larga saranno la nuova moneta, può essere compresa e domata, sottratta al potere di pochi e rivolta al benessere dell'umanità. Per questo, occorre un quadro normativo uniforme (il mercato è globale) che vada incontro al futuro senza sacrificare i diritti fondamentali dell'individuo faticosamente conquistati nel corso della storia e sanciti nelle dichiarazioni universali e nelle costituzioni liberali moderne.

[1] *The toxic terabyte, How data-dumping threatens business efficiency*, IBM UK Ltd., luglio 2006 (http://www-935.ibm.com/services/no/cio/leverage/levinfo_wp_gts_thetoxic.pdf).

2. Entrata in vigore e applicazione.

Il Regolamento entra in vigore il 24 maggio 2016, ma le sue disposizioni saranno vincolanti a decorrere dal 25 maggio 2018. I titolari del trattamento (ovvero coloro che trattano dati personali altrui per un fine commerciale proprio) hanno quindi due anni di tempo per mettersi in regola con le prescrizioni in esso contenute.

Questo periodo sarà utilizzato anche dai legislatori nazionali di ciascun Paese dell'Unione per emanare provvedimenti normativi integrativi che daranno concretezza ad alcune disposizioni generali adattandole agli strumenti e alle procedure interne dei singoli ordinamenti nazionali (ad esempio in tema di sanzioni amministrative e penali).

È bene tuttavia tenere presente che il Regolamento costituisce fonte primaria di diritto positivo e addirittura prevale sulle leggi ordinarie dello Stato le quali, quindi, in caso di scontro tra disposizioni nazionali ed europee incompatibili tra loro, si disapplicano. La lente attraverso cui leggere la normativa italiana di complemento, sarà pertanto sempre il Regolamento.

3. Ambito territoriale di applicazione (art. 3).

La nostra attuale legge in materia di protezione dei dati personali (il D.Lgs. 1986/2003, noto come Codice Privacy, che ha recepito la vecchia direttiva 95/46/CE), si applica ai trattamenti effettuati da chiunque è stabilito nell'Unione indipendentemente dal luogo in cui il trattamento è compiuto[2], ovvero a chiunque, anche non stabilito nell'Unione, utilizzi tuttavia strumenti di trattamento situati in uno Stato membro.

Il Regolamento amplia l'ambito applicativo rimuovendo quest'ultima condizione e assoggettando alla legge europea i trattamenti di dati personali compiuti da soggetti esteri che, pur non essendo stabiliti nell'Unione e pur non utilizzando strumenti di trattamento in essa situati, offrono, attraverso la rete o altri strumenti di

[2] Per tale intendendosi, per il diritto italiano, soggetti dotati di personalità giuridica e non semplici sedi secondarie o unità locali (Cass. 31 maggio 2006, n. 12980, in *Foro it.* 2007, 2, 1, 509). Sul concetto di *stabilimento* si è espresso anche il Gruppo dei Garanti Europei (WP 56 del 30 maggio 2002) chiarendo che esso è il luogo di effettivo e reale esercizio dell'attività economica mediante organizzazione stabile.

comunicazione a distanza, beni o servizi a soggetti che si trovano in un Paese comunitario.

Si è voluto così superare un limite applicativo della legge europea e ovviare ai dubbi che erano sorti in ordine all'efficacia della vecchia normativa allorché sembrava che il pervasivo trattamento di dati personali compiuto da colossi del web nordamericani (Google e Facebook *in primis*) potesse sfuggire alle tutele apprestate dalla normativa europea per il fatto che i servizi forniti fossero resi da soggetti non stabiliti nell'Unione che facevano uso solo di strumenti situati all'estero[3].

Oggi non si può più aggirare la normativa comunitaria in materia di trattamento dati stabilendo la sede in un Paese extra UE e lì collocare i server per l'accesso remoto via internet. Il solo fatto di offrire beni e servizi a soggetti presenti sul territorio europeo sarà sufficiente per applicare il Regolamento.

Occorre naturalmente stabilire quando un sito Internet si stia effettivamente rivolgendo a soggetti presenti nell'Unione escludendo i casi di mera accessibilità dal territorio europeo che, considerata la natura ubiquitaria della rete, è sempre possibile. Ebbene, in proposito si ricorre a criteri tra i più vari: la lingua utilizzata per le comunicazioni, la valuta indicata per le transazioni, l'espressa previsione di consegna di prodotti o fornitura dei servizi in un Paesi dell'Unione, l'indicazione di una legge o di un foro comunitari in caso di dispute, ecc.

4. Informativa agli interessati (artt. 13-15).

Il Regolamento interviene sul contenuto dell'informativa che deve essere resa ai soggetti interessati prima di compiere operazioni di trattamento sui loro dati o immediatamente dopo. L'obiettivo aggiuntivo che si è proposto il legislatore europeo rispetto alla vecchia direttiva, è quello di rendere edotto il soggetto interessato avendo riguardo anche alla sua età e tenendo presente il contesto in cui avviene la raccolta dei dati personali.

[3] Si veda sull'ampia nozione di «*stabilimento*» la Sentenza c.d. Google Spain nella causa C-131/12 (*Google Spain SL, Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*), nonché il dichiarato difetto di giurisdizione della corte di Vienna in uno dei round della lunga battaglia giudiziaria tra Max Schrems vs. Facebook (per cui ora la battaglia prosegue presso le corti irlandesi dove Facebook ha sede in Europa)

Rispetto a ciò che era previsto nella direttiva 95/46/CE, la nuova informativa dovrà indicare l'eventuale intenzione del titolare di trasferire i dati personali all'estero e le soluzioni contrattuali o normative sulla base delle quali attuerà tale trasferimento. Dovrà poi essere indicato il periodo di conservazione dei dati o i criteri per determinare tale periodo, il diritto di proporre reclamo al Garante Privacy, l'esistenza o meno di un processo decisionale o di profilazione automatizzato nonché la fonte da cui sono stati prelevati i dati (qualora non siano stati raccolti presso l'interessato). Non è invece più necessario indicare già con la prima informativa quali sono tutti i diritti dell'interessato (il diritto di opporsi al trattamento, di correggere o cancellare i dati o di limitarne il trattamento). Tali informazioni dovranno invece esser rese solo qualora l'interessato chieda al titolare o al responsabile la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano.

5. Diritto all'oblio (art. 17).

L'articolo in questione è rubricato «*Diritto alla cancellazione (diritto all'oblio)*». Tuttavia, al di là del titolo che molto anima la discussione, nulla aggiunge rispetto a quanto già recepito nella legge ed elaborato nelle corti europee.

Il diritto all'oblio è il diritto di un soggetto di opporsi al trattamento dei propri dati personali quando le ragioni di cronaca giornalistica che lo avevano dapprincipio legittimato, sono venute meno. È un vero e proprio *diritto di essere dimenticati* invocato da protagonisti di fatti (per lo più di carattere giudiziario) non più attuali e per i quali l'interesse pubblico ad essere informati è ormai assente.

Prima di internet, le lesioni del diritto all'oblio si verificavano in occasione di servizi giornalistici che riproponevano episodi di cronaca del passato a solo fine narrativo e di intrattenimento. Oggi, la *memoria infinita della rete*, per cui è sufficiente un clic su un motore di ricerca per rievocare il passato, ripropone con forza il tema del diritto all'oblio e, soprattutto, la domanda di quali soggetti siano tenuti ad attivarsi per garantirlo.

In proposito già rispondeva la direttiva del 1995 e, più puntualmente il Codice Privacy, che indica nel *titolare del trattamento* colui che deve provvedere alla cancellazione dei dati personali «*di cui non è necessaria la conservazione in*

relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati» (art. 7). Se allora, per via del tempo trascorso, non può più parlarsi di esercizio del diritto di cronaca, non sussistono più gli «*scopi per i quali i dati sono stati trattati*» e il soggetto interessato può legittimamente pretendere la loro cancellazione.

Il passo successivo lo ha compiuto nel 2014 la Corte di Giustizia dell'Unione Europea[4] chiarendo che titolare del trattamento non è solo il soggetto che pubblica la notizia che vìola il diritto all'oblio, ma anche il gestore del motore di ricerca che consente al pubblico di reperire quella notizia nel mare della rete. L'interessato può quindi rivolgersi direttamente al fornitore del servizio di ricerca per la deindicizzazione delle pagine web lesive del suo diritto.

La vera novità del Regolamento e piuttosto che non vi è alcun riferimento espresso al ruolo dei motori di ricerca e al diritto dell'interessato alla deindicizzazione dei risultati. Il diritto all'oblio, nella sostanza, rimarrà dunque tutelato per effetto dell'interpretazione evolutiva-adattativa compiuta dagli organi giurisdizionali europei.

6. Portabilità dei dati (art. 20).

Ai sensi di tale disposizione, il Regolamento ha introdotto il *diritto alla portabilità dei dati*, che si articola in due sottocategorie: il diritto dell'interessato di ricevere dal titolare i propri dati personali «*in un formato strutturato, di uso comune e leggibile da dispositivo automatico*», e il diritto di trasmettere tali dati ad un altro titolare del trattamento.

Si pensi ai siti *social* che molte persone usano come dei veri e propri diari di viaggio della propria vita su cui annotano ogni cosa.

Tutti questi dati non sono ostaggio del fornitore di servizi on line. Chi volesse chiudere il proprio account o migrare su altro fornitore, avrebbe oggi il diritto di portarsi con sé la propria storia e riprendere il cammino con un nuovo fornitore là dove lo aveva interrotto con il vecchio.

Bisogna tuttavia sottolineare che la portabilità riguarda solo i dati personali e non anche i contenuti multimediali eventualmente caricati dall'utente. Non sempre una

[4] Con la già citata sentenza nella causa C–131/12, *Google v. González*, (vedi precedente nota 3).

foto, un video o una conversazione, infatti, costituiscono (contengono) dati personali. Non è quindi scontato che, al di là della compatibilità dei formati elettronici e dei protocolli con cui i diversi operatori trattano i dati, la portabilità consenta veramente un passaggio di consegne senza perdita di informazioni da un provider all'altro.

7. Responsabilità del titolare (art. 24).

Il titolare non dovrà solo mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento compiuto sia conforme al Regolamento, ma dovrà anche essere in grado di dimostrare che tale misure sono in atto.

L'inadempimento, in questo caso, non è tanto costituito dal trattamento illegittimo, ma dalla incapacità del titolare di dimostrare di aver adottato idonee misure di sicurezza per garantire un trattamento legittimo.

Tale onere probatorio, può essere in parte assolto dal titolare con l'adesione a codici di condotta o ricorrendo al rilascio di certificazioni da parte di appositi organismi riconosciuti con provvedimento dell'Autorità Garante.

8. Progettazione del trattamento (art. 25).

Già prima di compiere una qualsiasi operazione di trattamento, il titolare deve verificare se le misure tecniche e organizzative che intende attuare sono adeguate avendo riguardo al tipo di dati trattati, al contesto in cui avviene il trattamento e alla finalità dello stesso, alla probabilità e gravità di eventuali attentati ai diritti e libertà degli interessati.

In altri termini, ogni buona operazione avente ad oggetto dati personali deve essere preceduta da una attenta progettazione delle singole fasi di trattamento nelle quali il titolare predispone i presidi e le procedure per minimizzare i rischi di perdita, alterazione o accesso non autorizzato ai dati personali apprestando le necessarie garanzie a protezione dei dati al fine di soddisfare i requisiti del Regolamento.

9. Impostazioni predefinite (art. 25).

Le impostazioni predefinite sono l'ambito, gli strumenti e le modalità del trattamento predisposte di *default* dal titolare. Esse devono essere contenute nei limiti del trattamento minimo necessario per il perseguimento del fine per cui i dati sono raccolti.

La maggior parte dei siti web, in special modo quelli che fanno networking, consentono di condividere e diffondere una gran quantità di informazioni, e non sempre con la piena consapevolezza dell'utente. Può accadere, infatti, che in automatico siano pubblicati contenuti (audio, video, foto), siano mostrati i gruppi di appartenenza o la propria attuale ubicazione, attivata la videocamera o mostrati dati relativi alla propria condizione sociale, professionale o di genere.

Tutte queste impostazioni, d'ora in poi, devono essere disabilitate alla prima registrazione (creazione account) rimettendo all'utente la scelta se attivarle o meno solo in un momento successivo selezionando le *opzioni privacy* a disposizione.

10. Registro delle attività di trattamento (art. 30).

Il titolare, ove abbia almeno 250 dipendenti o tratti dati sensibili o giudiziari, deve tenere un registro ove sono descritti tutti i trattamenti dati da esso compiuti con indicazione delle procedure e misure di sicurezza adottate.

Si tratta di una sorta di replica di quel documento in un recente passato noto come DPS (Documento Programmatico sulla Sicurezza) già previsto dalla nostra legge e poi abrogato con la riforma operata con il decreto legge n. 5 del 9 febbraio 2012 (il c.d. *decreto semplificazioni*).

Proprio come il DPS, anche il registro delle attività di trattamento deve contenere tutte le informazioni relative all'identità del titolare, ai soggetti responsabili, alle finalità del trattamento, alle categorie di soggetti a cui i dati vengono comunicati, ai termini di conservazione e cancellazione dei dati e, soprattutto, alle misure di sicurezza tecniche e organizzative adottate.

Anche il responsabile del trattamento (ovvero il soggetto terzo che per conto del titolare svolge alcune operazioni di trattamento dati) deve avere, al ricorrere delle medesime condizioni previste per il titolare (250 dipendenti o trattamento di dati

particolari), un proprio registro delle attività di trattamento con contenuto analogo e complementare a quello redatto dal titolare.

Vien da sé che tutte le grandi società di outsourcing informatico, per esempio, avranno entrambi i registri in quanto tratteranno dati propri in veste di titolari, e dati altrui in veste di responsabili.

11. Notifica di violazione (art. 33).

Nel caso di violazione dei dati personali il titolare deve senza ritardo, e comunque entro massimo 72 ore, darne comunicazione all'Autorità Garante a meno che non sia in grado di dimostrare che la violazione non costituisca un rischio per i diritti e le libertà delle persone fisiche. Oltre le 72 ore, la notifica deve essere corredata dalle ragioni del ritardo.

La nozione di «*violazione dei dati personali*» deve essere intesa in senso assai ampio. Essa senz'altro implica tutte le ipotesi di trattamento illegittimo compiuto in modo fraudolento o casuale da parte di un terzo che, aggirando le misure di sicurezza apprestate dal titolare, accede ai dati personali dal lui trattati. Ma la violazione ricorrere altresì nelle ipotesi di trattamenti illegittimi riconducibili ad una condotta del titolare stesso, anche omissiva.

Ciò implica la possibilità che il titolare si autodenunci nel caso in cui la *violazione dei dati personali* sia dovuta, per esempio, ad una sua mancata adozione di idonee misure di sicurezza o ad errata progettazione delle operazioni di trattamento.

Conseguentemente, qualora il legislatore italiano sanzioni il difetto di *notifica di violazione* con misure deterrenti significative, vorrà dire che ogni volta che un titolare non denunci egli stesso i propri trattamenti illegittimi, si troverà a dover prospettare l'ipotesi di essere sanzionato due volte, per la violazione del Regolamento in sé e – come una sorta di aggravante – per non aver denunciato la violazione.

In ogni caso, la mancata autodenuncia avrà sempre un rilievo. L'art. 83 del Regolamento, infatti, prescrive che i legislatori nazionali nello stabilire l'opportunità di infliggere una sanzione amministrativa e l'ammontare della stessa devono tenere in considerazione se il titolare o il responsabile hanno notificato la violazione.

12. Valutazione di impatto (art. 35).

Alla responsabilità del titolare si riconnette anche il suo obbligo di compiere una *valutazione di impatto* che il trattamento può avere sulla protezione dei dati personali (art. 35 del Regolamento). Tale valutazione (che consiste in un rapporto di analisi dei rischi dei trattamenti) va compiuta preliminarmente quando sono in uso nuove tecnologie o posso presentarsi rischi elevati per i diritti e le libertà delle persone fisiche.

In particolare, la valutazione d'impatto sulla protezione dei dati è richiesta nel caso in cui il titolare, attraverso trattamenti automatizzati, si propone di profilare persone fisiche per compiere decisioni che hanno effetti giuridici o che incidono in modo significativo su di loro.

Su questo punto, l'Autorità Garante interverrà nei prossimi mesi fornendo più precise indicazioni e pubblicando un elenco delle tipologie di trattamenti soggetti alla valutazione d'impatto.

13. Responsabile della protezione dei dati (art. 37).

Il Regolamento delinea i caratteri di una nuova figura professionale, il c.d. *responsabile della protezione dei dati* che deve essere nominato per i trattamenti compiuti da autorità o organismi pubblici, ovvero quando i trattamenti effettuati consistono nel monitoraggio regolare e sistematico degli interessati su larga scala oppure i dati oggetto di trattamento abbiano natura particolare (dati sensibili o dati relativi a condanne o reati penali).

Come recita il Regolamento, il responsabile della protezione dei dati deve sempre essere «*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*»; esso è quindi chiamato ad assumere un ruolo decisivo e centrale sia nell'ambito dei trattamenti compiuti da titolari che per quelli compiuti da responsabili del trattamento e non a caso deve essere sempre specificamente indicato nelle informative rese ai soggetti interessati, nei registri delle attività di trattamento (del titolare e del responsabile) e nelle eventuali notifiche all'Autorità Garante.

Tale figura, seppur possa trattarsi di un dipendente del titolare o del responsabile, deve disporre di una notevole libertà di mezzi e di giudizio. Prevede infatti il Regolamento che al responsabile della protezione dei dati siano fornite «*le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*» e che «*non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti*» né che possa essere «*rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti*».

Da tali brevi indicazioni, si evince che il responsabile della protezione dei dati, è destinato a diventare una sorta di *super* responsabile interno del trattamento, dotato di spiccate competenze specialistiche che nelle grandi aziende (anche riunite in gruppi) dovrà fungere da figura di riferimento verso l'interno (dipendenti e responsabili) e verso l'esterno (clienti e fornitori) per tutte le questioni di privacy, in grado di intervenire tempestivamente e con cognizione di causa per adeguare i trattamenti alle disposizioni del Regolamento e che possa interloquire per conto del titolare o del responsabile con l'Autorità Garante con idonea preparazione tecnica.

14. Sanzioni amministrative (art. 83).

Il Parlamento europeo e il Consiglio hanno voluto cogliere l'occasione della riforma per inasprire le sanzioni previste in tema di trattamento dei dati personali.

Gli Stati membri devono prevedere, secondo i propri ordinamenti, sanzioni amministrative pecuniarie fino a dieci milioni di euro oppure, nel caso in cui il trasgressore sia un'impresa, fino al 2% del fatturato mondiale annuo conseguito nell'esercizio precedente (alla data in cui è stata rilevata la violazione). Tali importi raddoppiano (venti milioni o il 4% del fatturato mondiale) nei casi di trattamenti più gravi (violazione delle condizioni per il rilascio del consenso informato, trattamento di dati giudiziari o sensibili, mancato riscontro al legittimo esercizio dei diritti dell'interessato, trasferimento dei dati verso paesi che non garantiscono livelli adeguati di tutela, violazione di un ordine dell'Autorità Garante, ecc.).

Trattandosi di soglie massime, non è escluso che le leggi integrative nazionali prevedano sanzioni inferiori e riduzioni di pena in caso di più violazioni compiute nell'ambito di un medesimo trattamento.

Il segnale forte tuttavia rimane. Soprattutto la previsione del 4% del fatturato mondiale costituirà un efficace deterrente per i colossi del web, primi fra tutti quelli statunitensi che, culturalmente lontani dalle regole europee in tema di privacy, non si sono mai conformati seriamente alle disposizioni della direttiva 95/45/CE e, in una analisi costi/benefici senz'altro a loro vantaggio, hanno fino ad oggi preso un po' sottogamba le conseguenze sanzionatorie e risarcitorie.

15. Conclusioni.

Il Regolamento sarà senz'altro oggetto di approfondita analisi nei prossimi mesi e il legislatore italiano, nel completare il quadro normativo, darà inevitabilmente degli indirizzi interpretativi.

C'è da aspettarsi, inoltre, che anche l'Autorità Garante fornisca alcuni chiarimenti, sia per replica a richieste provenienti da privati sia di sua iniziativa, come ha già fatto in tante occasioni, con grande limpidità e sinteticità espositiva.

Di contro, è altrettanto vero che si percepisce sempre più un'intenzione dei garanti europei, forti di oltre vent'anni di pratica, di assumere posizioni nette a difesa dei diritti degli interessati e di tenere sotto stretta osservazione i nuovi fenomeni e le realtà aggregative della società dell'informazione arginando il più possibile lo strapotere delle multinazionali, soprattutto nordamericane, poco inclini a doversi misurare con gli elevati standard europei di tutela della privacy.

Francesco Rampone – f.rampone@lascalaw.com