

Come cambierà la privacy in vista del nuovo Regolamento Europeo

Rosaria Deluca

Istituto di Scienza e Tecnologie dell'Informazione

"A. Faedo" (ISTI-CNR)



Sommario

Introduzione

- 1. Le origini della privacy**
- 2. Evoluzione della privacy in Europa**
- 3. Evoluzione della privacy in Italia**
- 4. Il Regolamento Europeo sulla protezione dei dati personali: prospettive**
- 5. Confronto tra le novità della proposta e il testo emendato**
- 6. Riflessioni**

Introduzione

Il presente lavoro ha lo scopo di illustrare l'iter legislativo del Regolamento Europeo Privacy la cui approvazione è prevista nel maggio 2014. Il Regolamento Europeo, che diventerà immediatamente operativo per i 27 paesi dell'UE, introduce significative novità in tema di tutela dei dati personali e di sanzioni. E' quindi opportuno per tutti i soggetti pubblici e privati coinvolti farsi trovare pronti a recepirlo quando entrerà in vigore.

1. Le origini della privacy

La privacy trae origine tradizionalmente dall'ordinamento statunitense attraverso la diffusione del celebre saggio pubblicato nel 1890 da due giovani avvocati statunitensi *"The Right to be let alone"*, in cui viene richiesto che l'ordinamento protegga questo nuovo diritto. Il saggio ebbe il merito di dare inizio ad una sistematica discussione sul concetto stesso di privacy.

Con lo sviluppo delle tecnologie il concetto di privacy ha subito una trasformazione: Il *"diritto ad essere lasciato solo"* (Right to be alone) ha lasciato spazio ad una nozione più ampia del diritto alla propria privacy: da strumento passivo di difesa dalle intrusioni altrui, è divenuto strumento di libertà e partecipazione e, quindi, potere di controllo e conoscenza sulla circolazione dei propri dati personali. *"...Oggi è impossibile transitare senza lasciare tracce"* (R. Acciai, ex-Funzionario Garante Privacy).

2. Evoluzione della privacy in Europa

In Europa tali principi sono stati recepiti dalla Convenzione europea per i diritti dell'uomo e delle libertà fondamentali del 1950 che sanciva il *"diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza"* e nella Convenzione di Strasburgo del 1981 sulla *"protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale che lo riguardano"*.

Successivamente i principi sanciti dalla Convenzione di Strasburgo sono stati ripresi e sviluppati dalla direttiva europea 95/46/Ce relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

3. Evoluzione della privacy in Italia

Nell'ordinamento Italiano, il diritto alla riservatezza trova fondamento nella Costituzione, rispettivamente: nell'art 2 che sancisce il riconoscimento dei diritti inviolabili dell'uomo, nell'art. 3

che fonda il principio di uguaglianza e negli articoli 13-14-15 che sanciscono l'inviolabilità della libertà personale, del domicilio, della libertà e segretezza della corrispondenza e ogni altra forma di comunicazione.

L'attuale normativa italiana ha recepito quanto disposto dai principi contenuti nella direttiva comunitaria con la promulgazione della L. 675/96 che disciplina la tutela dei dati personali e il loro trattamento e che segna pertanto una pietra miliare nella tutela della privacy.

Successivamente con il D.P.R. 318/99 è stato istituito l'obbligo di adottare, per certi soggetti che effettuano trattamenti di particolare rilevanza, una serie di misure minime tra cui l'adozione di un documento programmatico sulla sicurezza (DPS).

Nel 2003 infine è stato emanato un testo unico (T.U. - D.Lgs. 196/03, denominato "Codice") con cui il legislatore ha provveduto ad uniformare l'intera disciplina, comprensivo sia delle norme relative al trattamento dei dati personali, sia degli obblighi relativi alle misure minime di sicurezza.

Dopo questa prima fase di sviluppo la normativa ha subito un processo di involuzione, in nome del concetto di "*semplificazione*", che ha dato avvio a una serie di disposizioni volte ad escludere l'applicazione dell'intero Codice alle persone giuridiche, agli enti e alle associazioni, a prescindere dalla natura del titolare, culminate infine con la soppressione del documento programmatico sulla Sicurezza.¹ (DPS).

Tali interventi normativi hanno destato subito forti preoccupazioni tra gli esperti della materia² poiché in contrasto con gli art.33-36 del Codice in materia di misure minime di sicurezza³ e con la L. 231/2001 in materia di responsabilità amministrativa delle persone giuridiche⁴ nonché in netta controtendenza rispetto alla nuova prospettiva comunitaria che cominciava a prendere forma.

¹ DL 138/2011 convertito in L. 148/2011, DL 70/2011 convertito nella L. 106/2011 e DL 201/2011 convertito nella L. 214/2011. Il DL 5/2012 convertito nella L. 35/2012.

² Lo stesso ex-Garante Privacy Pizzetti ha ribadito che "*le modifiche operate in maniera non organica rischiano di determinare difficoltà applicative e dubbi interpretativi tali da vanificare le stesse finalità di semplificazione che intendono perseguire*".

³ In particolare l'aggiornamento annuale del DPS, consentiva al Titolare di migliorare l'aspetto relativo alle misure di sicurezza e rappresentava uno strumento efficace di tutela di fronte ad eventuali controversie.

⁴ Il Decreto Legislativo n. 231 dell'8 giugno 2001 ha introdotto la disciplina della Responsabilità Amministrativa delle Società in base alla quale queste possono essere ritenute responsabili, e conseguentemente sanzionate, in relazione a taluni reati commessi o tentati nell'interesse o a vantaggio della società dagli amministratori o dai dipendenti. La responsabilità della Società viene esclusa se essa ha adottato ed efficacemente attuato, prima della commissione di reati, modelli di organizzazione, gestione e controllo idonei a prevenire i reati stessi e ha istituito un organismo preposto a vigilare sul funzionamento e sull'osservanza dei modelli.

4. Il Regolamento Europeo sulla protezione dei dati personali: prospettive

Il 25 gennaio 2012 è stato presentato dalla Commissione europea il testo della Proposta di Regolamento: era previsto un periodo di circa un anno per la conclusione dell'iter (approvazione da parte del Parlamento Europeo e del Consiglio) e l'entrata in vigore della nuova legislazione.

Il primo via libera si è avuto il 21 ottobre 2013, quando la Commissione competente del Parlamento europeo (Libe - Libertà civili, giustizia e affari interni) ha votato gli emendamenti al testo della proposta (49 SI – 3 NO – 1 ASTENSIONE). Attualmente il provvedimento, prima di essere approvato in via definitiva, deve ricevere il via libera del Consiglio e della Commissione, ma i tempi sembrano ormai restringersi⁵.

L'approvazione finale è prevista prima della scadenza della legislatura nel maggio 2014.

Il Regolamento che andrà a sostituire la direttiva del 1995 non dovrà essere recepito dai 27 paesi dell'UE, ma sarà pienamente operativo dal momento in cui verrà approvato dal Parlamento europeo e dal Consiglio ed interesserà direttamente le imprese sia europee, sia extra-UE. Resta a questo punto da definire il margine di autonomia decisionale che manterranno gli Stati Membri nell'applicazione di alcune regole specifiche sul proprio territorio. Saranno comunque conservate alcune norme nazionali che non potranno essere in contrasto con quanto stabilito a livello comunitario.

5. Confronto tra le novità della proposta e il testo emendato

Come possiamo osservare di seguito il testo emendato del Regolamento mantiene molte delle impostazioni della proposta originale della Commissione.

- 1) il principio dell'applicazione del diritto UE anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni o servizi ai cittadini UE o tali da permettere il monitoraggio dei comportamenti dei cittadini dell'Unione Europea (art.3).
- 2) Introduzione delle definizioni di *"dato genetico"* e *"dato biometrico"*.
- 3) Introduzione della categoria del trattamento dati per i minori per cui è prevista una tutela particolare e specifica (art.8).⁶
- 4) Viene attribuita maggiore rilevanza al consenso dell'interessato. Nel testo emendato il consenso della persona interessata deve essere "esplicito"⁷ anziché solo "inequivocabile" come nell'attuale direttiva 95/46 (art.4).

⁵ Fino al mese di settembre pendevano sulla proposta di regolamento, in seguito a una fortissima azione di *"lobby"*⁵, circa 4.000 proposte di emendamento, la commissione è riuscita a ridurli a soli 104, accelerando così di molto i tempi della votazione.

⁶ *"..il trattamento di dati personali di minori di età inferiore a tredici anni è lecito se e nella misura in cui il consenso è espresso o autorizzato dal genitore o dal tutore del minore"*.

- 5) Introduzione del diritto degli interessati alla portabilità del *dato "data portability"* da un provider all'altro, in formato neutro. Ad esempio, nel caso in cui l'interessato intenda trasferire i propri dati da un social network ad un altro (art.18).
- 6) Introduzione del *"diritto all'oblio"*, il quale consente ad ogni interessato di decidere e richiedere la rimozione di informazioni e dati personali, per motivi legittimi, dopo un determinato periodo di tempo. Nel testo emendato è stato trasformato in un diritto alla rettifica o alla limitazione del trattamento in forma rafforzata. Ad esempio, si potrà richiedere l'eliminazione dei propri dati in possesso di un social network. L'esercizio di tale diritto deve tuttavia rispettare alcune esigenze specifiche come quella della libertà di espressione o la possibilità di condurre ricerche storiche (art.17).
- 7) Tra le novità più rilevanti ricordiamo l'obbligo per talune aziende e per gli enti pubblici di nominare un *"data protection officer"*(art. 3). Nel testo emendato sono stati stabiliti criteri basati sulla tipologia di dati trattati piuttosto che sul numero dei dipendenti, come invece era previsto nella proposta.
- 8) Introduzione dell'obbligo di adottare misure tecnologiche *"privacy by design"* che riducano di default il trattamento dei dati personali al minimo necessario, anche riguardo al periodo massimo di conservazione e ai soggetti che possono avere accesso ai dati. Tale disposizione impone la previsione di misure a protezione dei dati già al momento della progettazione di un software o di un prodotto (art.23).
- 9) Introduzione del requisito del *"privacy impact assessment"*, vale a dire preventivare i rischi, adottare soluzioni preliminari che, già in sede di raccolta del primo dato, siano capaci di tutelarlo con una "anticipazione" di responsabilità già sulla parte di progettazione: ad esempio videosorveglianza, dati sanitari, dati biometrici ecc. (art. 33).
- 10) Introduzione di multe, che nella proposta potevano arrivare fino a un milione di euro o il 2% del fatturato. Il testo emendato prevede multe più pesanti: fino a 100 milioni di euro o fino al 5% del fatturato mondiale (art.79).
- 11) Introduzione della figura del *"joint Controller"*: due autonomi Titolari dovranno, per un medesimo trattamento di dati personali, concordare in un contratto le rispettive responsabilità privacy. Il loro accordo avrà valore anche in caso di controllo da parte dell'autorità giudiziaria o amministrativa (art. 24).

⁷ *"Qualsiasi manifestazione di volontà libera, specifica, informata ed esplicita con la quale l'interessato accetta, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento"*.

- 12) Introduzione di requisiti più stringenti per trasferire dati personali verso paesi terzi: è previsto l'obbligo di autorizzazione dei Garanti nazionali prima di inviare dati su richiesta di autorità giudiziarie o amministrative di paesi terzi.
- 13) Introduzione del principio della *"accountability"* (responsabilità verificabile) che comporterà l'onere, in capo al Titolare del trattamento di dimostrare l'adozione di tutte le prescrizioni privacy. Al fine di dimostrare l'osservanza di questo principio è stato introdotto il dovere di costituire e conservare un' apposita documentazione che attesti il *"modello organizzativo e di sicurezza privacy"*(art.28).
- 14) Introduzione dell'obbligo di notifica, in caso di violazione dei dati personali, all'autorità di controllo e in alcuni casi obbligo di comunicare l'accaduto anche all'interessato (art. 31-32). Viene superato l'istituto della Notificazione generica preventiva (art. 37 d.lgs n.196/2003).
- 15) Istituzione del comitato europeo per la protezione dei dati personali. Viene prevista una *"lead authority"* quando sono coinvolti più Stati membri (art. 64-72).

Inoltre il testo emendato ha rivisto il sistema delle sanzioni amministrative, che tutte le Autorità nazionali di controllo devono poter comminare, ma che sono libere di definire entro una soglia pecuniaria massima e nel rispetto di una griglia di criteri fissati nel testo.

Vanno segnalate anche le modifiche apportate alla proposta di Regolamento per quanto riguarda il meccanismo di *"one-stop-shop"* (sportello unico). Secondo il Parlamento, lo sportello unico deve permettere alle imprese multinazionali di dialogare con un unico interlocutore nell'Ue (l'Autorità privacy del Paese dove hanno il loro "stabilimento principale") ma, a differenza della proposta, il ruolo di questa Autorità (definita, appunto, "Autorità capofila") deve consistere nel coordinamento di un processo di co-decisione in cui tutte le Authority degli Stati membri interessati da un trattamento devono partecipare ed avere voce.

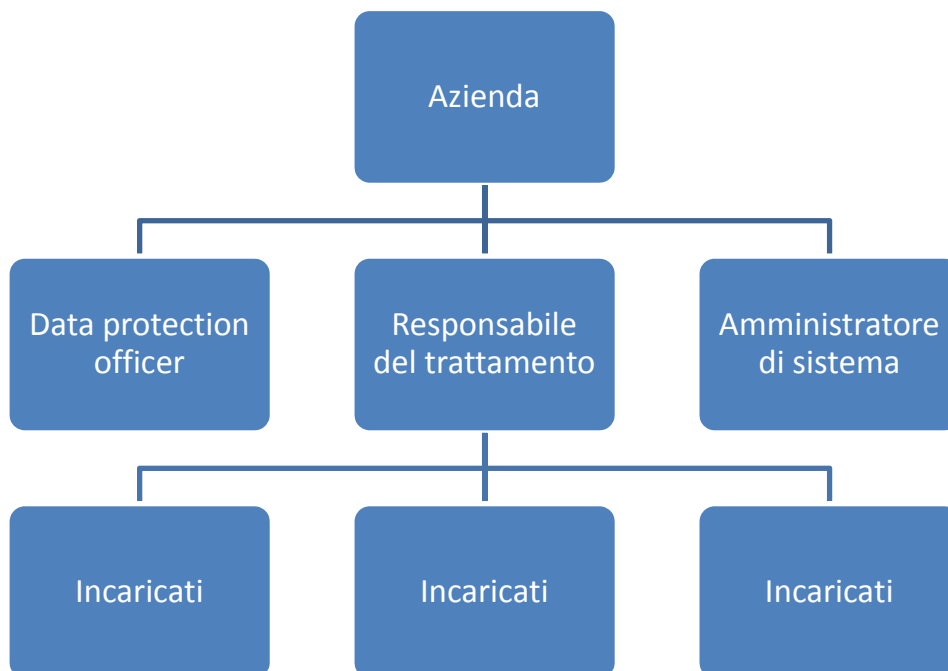
6. Riflessioni

Il commissario Ue alla giustizia, Viviane Reding, definisce l'approvazione del testo emendato da parte della commissione (Libe): *"un momento importante per la democrazia europea...un provvedimento che rafforza e uniforma il diritto europeo sulla materia e che consentirà di ridurre i costi per le imprese, nonché di aumentare la protezione dei nostri cittadini"*.

Anche il Garante Europeo per la protezione dei dati, Peter Hustinx, ha commentato positivamente gli ultimi sviluppi circa la normativa sulla data protection, affermando che: *"Il voto della commissione LIBE è un passo importante verso la protezione dei dati più forte ed efficace in*

Europa. Ci congratuliamo con il Parlamento europeo per come sta affrontando la sua responsabilità in questa fase essenziale ma complessa della legislazione”.

Il Garante europeo aggiunto Giovanni Buttarelli, facendo evidentemente riferimento alle ripetute modifiche apportate all'impianto normativo privacy dal Governo italiano, che hanno finito per ingenerare notevole confusione, sostiene che: *“occorre buonsenso...il nostro Legislatore nazionale deve riflettere sulla inopportunità in questo momento di fare scelte che vadano contro la linea di tendenza generale perché poi avremo dei contraccolpi rispetto alla loro attuazione. Quando si fanno delle novità normative su questa materia, poi ci vuole tempo per attuarle, e se poi cambiano le regole subito dopo, non è un buon segno per chi deve gestire le informazioni e per i cittadini stessi. Quindi, un po' di buonsenso dovrebbe prevalere per evitare qualche altra scelta come quelle fatte di recente⁸,...Il Regolamento europeo è una realtà vicina, per cui sarebbe bene non fare altri sbagli”.*



⁸ ...come peraltro aveva sottolineato lo stesso Garante Privacy, a seguito delle ultime semplificazioni.