PILLS n. 3 – 2017

4/2017

Privacy: il nuovo pacchetto di normativa europea per la protezione dei dati personali

Avv. Claudia Recchia e Avv. Fabio Scorzelli

KEY WORDS: Privacy; Codice Privacy; Regolamento (UE) n. 679/2016; Direttiva (UE) 2016/680.

Premessa

Il termine "*privacy*" rientra ormai nell'uso comune e sta ad indicare il diritto alla riservatezza degli aspetti, comportamenti e atti della sfera privata della persona; tale diritto è invocato quando si vuole tutelare la riservatezza dell'individuo rispetto a qualsiasi tipo di intromissione o divulgazione da parte di terzi, in assenza di un'autorizzazione in tal senso.

In Europa con l'emanazione del Regolamento (UE) n. 2016/679 e della Direttiva (UE) n. 2016/680 la "*privacy*" si rinnova. In particolare, il 4 maggio 2016, è stata pubblicata nella Gazzetta Ufficiale Europea la menzionata legislazione (Regolamento e Direttiva), che si inserisce nel cosiddetto "Pacchetto europeo di protezione dati" con l'obiettivo, da un lato, di adeguare la protezione dei dati personali all'evoluzione tecnologica e, dall'altro, di garantire un'uniforme circolazione dei dati all'interno dell'Unione Europea.

Storia ed evoluzione

Il diritto alla riservatezza nasce come diritto ad essere lasciato solo ("*to be let alone*") negli Stati Uniti d'America nel 1890 ed entra nel dibattito italiano nella seconda metà del '900, come generico diritto alla libera determinazione nello svolgimento della personalità dell'individuo.

In Europa i primi riferimenti alla *privacy* risalgono all'art. 12 della Dichiarazione Universale dei diritti dell'uomo, secondo cui è diritto di ciascun individuo essere tutelato dalla legge contro le interferenze o lesioni arbitrarie della propria vita privata. L'art. 8 della Convenzione europea dei diritti dell'uomo (CEDU), successivamente, sancisce il diritto al rispetto della vita privata e familiare; a riguardo, la Corte europea dei diritti dell'uomo interviene fornendo un'interpretazione estensiva del diritto alla riservatezza ed evidenziando come la tutela prevista dal citato art. 8 CEDU si estenda fino a ricomprendere il diritto di ciascuno a sviluppare rapporti sociali al riparo da qualsiasi forma di discriminazione, in modo tale da garantire il pieno godimento della vita privata.[1]

Nell'ambito della nostra Carta Costituzionale il diritto alla riservatezza non è disciplinato direttamente, ma è possibile ricavare dal testo costituzionale una tutela di tipo indiretto negli articoli 14, 15 e 21 concernenti, rispettivamente, il domicilio, la libertà e la segretezza della corrispondenza e la libertà di manifestare liberamente il proprio pensiero. Sul punto è intervenuta, in particolare, la sentenza n. 38 del 1973 della Corte Costituzionale, che ha ricondotto la *privacy* tra i diritti inviolabili dell'art. 2

[1] Corte europea dei diritti dell'uomo, *Information Note on the Court's case-law 67*, August-September 2004, "*Sidabras and Džiautas v. Lithuania*" - 55480/00 and 59330/00 Judgment 27.7.2004 [Section II].

della Costituzione, richiamando nella motivazione l'art. 12 della Dichiarazione Universale dei diritti dell'uomo e l'art. 8 della CEDU.

In tale scenario, sono dapprima intervenute la Direttiva 95/46/CE (a cui si è data attuazione in Italia con il Codice Privacy, D.lgs. n. 196/2003), relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione dei dati, e la Direttiva 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della sita privata nel settore delle comunicazioni elettroniche, e, in un secondo momento, la proposta del gennaio 2012 della Commissione europea (c.d. "Pacchetto europeo protezione dati"). Tale proposta è oggi sfociata:

(i) nel Regolamento (UE) n. 2016/679, efficace in tutto il territorio dell'Unione Europea a partire dal 25 maggio 2018, che abroga la Direttiva 95/46/CE;

(ii) nella Direttiva (UE) n. 2016/680, che deve essere recepita dagli Stati membri entro il 6 maggio 2018 p.v. e che sostituisce ed integra la decisione quadro 977/2008/CE, sulla protezione dei dati scambiati dalle autorità di polizia e giustizia (mai attuata in Italia).

Le principali novità normative

Il Regolamento (UE) n. 2016/679, "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*" (di seguito il "Regolamento"), ha un ambito di applicazione materiale e territoriale, e in dettaglio si applica: (i) al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi (ambito materiale); (ii) al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento (dove per stabilimento si intende l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile) di un Titolare del trattamento o

Responsabile del trattamento, indipendentemente dal fatto che il trattamento avvenga all'interno dell'Unione Europea (ambito territoriale).

Il Regolamento attribuisce nuovi compiti alle figure del Titolare e del Responsabile del trattamento, rispetto alla normativa attuale. In particolare, il Titolare ha il compito di mettere in atto misure tecniche e organizzative volte a garantire e dimostrare che il trattamento avvenga in misura conforme al Regolamento[2] ed ha l'obbligo di effettuare una valutazione d'impatto del trattamento, con annessi obblighi di revisione, qualora quest'ultimo possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche[3] (le tipologie di trattamenti soggetti alla valutazione di impatto sono contenute in un pubblico elenco redatto dall'autorità di controllo). Riguardo nello specifico il ruolo del Responsabile del trattamento, si prevede che l'attività di questi sia disciplinata da un contratto o da altro atto giuridico conforme al diritto dell'Unione Europea; il Responsabile, infatti, tratta i dati personali per conto del Titolare, previa autorizzazione scritta. Sia il Titolare che il Responsabile hanno obblighi di comunicazione inerenti l'avvenuta violazione dei dati personali; in particolare, il Responsabile deve informare, senza ritardo, il Titolare, il quale dovrà notificare la violazione all'autorità di controllo[4] (in Italia, il Garante per la protezione dei dati personali). Titolare e Responsabile debbono, ancora, tenere un registro delle attività di trattamento in forma scritta, ad eccezione di quelle organizzazioni che abbiano meno di 250 dipendenti.[5]

Al fine di tutelare in maniera più intensa i diritti dell'interessato a fronte di un costante sviluppo di nuove tecnologie, il Regolamento introduce i principi di *privacy by design* e di *privacy by default*: (i) la *privacy by design* prevede che il Titolare attui misure di tipo

[2] Cfr. artt. 24 e 43 del Regolamento.
[3] Cfr. art. 35 del Regolamento.
[4] Cfr. artt. 33 e 34 del Regolamento.
[5] Cfr. art. 30 del Regolamento.

tecnico-organizzativo a tutela dei principi di protezione dei dati, dalla progettazione fino all'esecuzione del trattamento; (ii) la *privacy by default* richiede, invece, nella fase operativa del trattamento, misure volte a garantire l'utilizzo dei soli dati personali necessari per ogni specifica finalità di trattamento.[6]

Una delle novità di maggior rilievo, introdotta dal Regolamento, è la figura professionale del *Data Protection Officer* (DPO)[7]; le autorità pubbliche e le imprese che svolgono talune operazioni a rischio di trattamento dei dati devono, infatti, designare un "Responsabile della protezione dei dati" (DPO). Il DPO deve obbligatoriamente essere presente all'interno delle aziende pubbliche ed in quelle ove i trattamenti dei dati presentino rischi specifici, quali le aziende in cui si trattano dati sensibili o nelle quali sia richiesto un monitoraggio su larga scala regolare e sistematico degli interessati. Il DPO ha il compito di garantire il rispetto della disciplina e può incorrere in sanzioni, fino all'ammontare di € 20 milioni o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'ultimo esercizio. Tale figura può essere sia un dipendente della società, titolare del trattamento, sia un soggetto esterno che svolge le proprie funzioni sulla base di un contratto di servizio. Tra le competenze del DPO, in particolare, si richiamano: (i) gli obblighi di informazione nei confronti del titolare, del responsabile del trattamento e dei dipendenti, (ii) gli obblighi di verifica e vigilanza, (iii) le attività di punto di contatto tra Titolare e Garante per la protezione dei dati personali.

Altra novità del Regolamento, meritevole di attenzione, è l'accrescimento degli obblighi di trasparenza alla quale il legislatore europeo dedica un'apposita Sezione.[8] Riguardo le modalità di trattamento dei dati, si prevede che all'interessato, specie se minore,

[6] Cfr. art. 25 del Regolamento.
[7] Cfr. art. 37 del Regolamento.
[8] Cfr. Sezione I, Capo III, del Regolamento.

siano rese le informazioni in un linguaggio semplice e comprensibile e in forma scritta, salvo richiesta contraria da parte dello stesso interessato qualora sussista la possibilità di provare la sua identità in altro modo. Tali informazioni devono indicare il periodo di conservazione dei dati, il diritto di reclamo all'autorità di controllo e la volontà, eventuale, del Titolare di trasferire i dati ad un paese terzo.[9]

Merita un cenno anche il nuovo diritto alla portabilità dei dati che, diversamente dal diritto di accesso, consente agli interessati del trattamento di ricevere gratuitamente dal Titolare i loro dati personali in maniera strutturata e leggibile da un elaboratore (pertanto, non in formato cartaceo); ciò al fine di semplificare l'eventuale trasferimento online dei dati ad un altro Titolare.

La Direttiva (UE) 2016/680, "*relativa alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali*" (di seguito la "Direttiva"), si applica al trattamento dei dati personali da parte delle autorità competenti per le finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.[10]

Un punto cardine della Direttiva è rappresentato dall'agevolazione della libera circolazione dei dati personali tra le forze dell'ordine e le autorità giudiziarie competenti dei diversi Paesi membri, per scopi di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché per la salvaguardia da qualsiasi minaccia alla sicurezza pubblica.[11] Allo stesso modo, viene tutelato il diritto alla privacy dei cittadini europei, evitando di trattare in maniera

[9] Cfr. artt. 5 e 12 del Regolamento.
[10] Cfr. artt. 1, c. 1 e 2, c. 1 della Direttiva.
[11] Cfr. il Considerando 4 e l'art. 1 della Direttiva.

automatizzata quei dati personali che minaccino di pregiudicare la sfera personale dell'individuo.