PORTOLANO
CAVALLO
studio legale

Privacy: cosa è successo nel 2012 e cosa aspettarsi nel 2013

8 febbraio 2013

Di Laura Liguroi e Federica De Santis

Nel corso dell'anno 2012 diversi interventi legislativi hanno profondamente inciso sul framework normativo in materia di tutela dei dati personali, così come delineato dal Codice in materia di protezione dei dati personali (D. Lgs. 30 giungo 2003, n. 196 – Codice Privacy).

Di seguito forniamo una rassegna delle principali novità in materia riferibili all'anno 2012, ed una selezione di trends che prevediamo possano caratterizzare l'anno 2013.

COSA È SUCCESSO NEL 2012

- **Definizione di dato personale e di interessato**

Per effetto del D.L. n. 201/2011, convertito in L. 214/2011 (c.d. decreto "Salva Italia"), le informazioni relative alle persone giuridiche, enti e associazioni non sono più considerate come dati personali ai sensi del Codice Privacy. Allo stesso modo, persone giuridiche, enti e associazioni sono stati esclusi dalla definizione di "interessati" del trattamento di dati personali.

In definitiva, la portata applicativa di tutte le disposizioni del Codice Privacy che riguardano gli interessati ovvero il trattamento di dati personali è stata limitata in via esclusiva alle persone fisiche e ai trattamenti di dati personali che vi si riferiscono.

Tuttavia tale intervento, dettato dalla necessità di ridurre gli oneri burocratici in materia di privacy per le imprese, ha suscitato alcuni dubbi interpretativi. In particolare, non era chiaro se le persone giuridiche dovessero ritenersi escluse del tutto dall'applicazione del Codice Privacy, o se invece residuasse uno spazio di tutela all'interno del Codice.

A tale riguardo il Garante Privacy, con provvedimento del 20 settembre 2012, ha chiarito che le disposizioni del Codice Privacy che riguardano i "contraenti" (nella specie, il capo I del Titolo X del Codice, dedicato ai "servizi di comunicazione elettronica") continuano ad applicarsi anche alle persone

giuridiche, enti e associazioni. Tra queste disposizioni, si segnalano in particolare quelle in materia di telemarketing e comunicazioni commerciali indesiderate.

Infatti, tali norme si rivolgono a destinatari individuati non in funzione della loro qualifica soggettiva (persone fisiche o giuridiche), bensì in funzione della loro qualifica di "contraenti", concetto che ricomprende ogni categoria di soggetti ed è pertanto applicabile tanto alle persone fisiche quanto a quelle giuridiche.

- **Cookies**

Con D. Lgs. 69/2012, dopo oltre un anno di ritardo, l'Italia ha dato attuazione alla Direttiva 2009/136/CE, che ha modificato la Direttiva e-Privacy 2002/58/CE, prevedendo espressamente il principio dell'"opt-in" (ovvero, del previo consenso) in tutti i casi in cui si accede a o si registrano cookies e altri strumenti analoghi (web beacon/web bug, clear GIF, ecc.) nei terminali degli utenti (pc, notebook, tablet, smartphone, ecc.)

Pertanto, affinché i cookies possano essere archiviati sul terminale dell'utente nel corso della sua navigazione in Internet, è necessario che l'utente stesso, sulla base di un'informativa chiara e completa in merito alle modalità e finalità del trattamento dei suoi dati, esprima un valido consenso, preliminare al trattamento.

Il consenso per l'uso dei cookies non è richiesto qualora questi ultimi siano cookies "tecnici", necessari, cioè, al fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica oppure per rispondere a specifiche richieste dell'interessato, ferma restando in ogni caso la necessità di fornire un'adeguata informativa in merito al trattamento dei dati.

A titolo esemplificativo – secondo alcuni chiarimenti forniti dal Gruppo europeo Articolo 29 per la protezione dei dati personali in un parere pubblicato il 7 giugno 2012 – sono cookies per i quali non è necessario acquisire il consenso preventivo dell'utente i cookie di sessione utilizzati durante le procedure di acquisto online, i cookies di autenticazione e quelli per contenuti multimediali tipo flash player se non superano la durata della sessione, i cookie di personalizzazione (ad esempio, per la scelta della lingua di navigazione), ecc.

Con provvedimento del 22 novembre 2012 il Garante Privacy ha avviato una consultazione pubblica diretta ai consumatori e ai principali operatori del settore, al fine di acquisirne le proposte e individuare idonee modalità per informare gli utenti con modalità semplificate, ovvero con messaggi che siano al tempo stesso chiari e snelli. La consultazione pubblica chiuderà il prossimo 19 marzo 2013.

- **Data breaches**

Il D. Lgs. 69/2012 ha introdotto alcuni obblighi per i fornitori di servizi di comunicazione elettronica accessibili al pubblico (ad esempio, servizi telefonici o di accesso a Internet) rispetto a violazioni di dati personali dei contraenti, quali violazioni di sicurezza che comportino la distruzione, la perdita, la diffusione non autorizzata o l'accesso ai dati personali (cd. data breaches).

In particolare, secondo le nuove disposizioni introdotte nel Codice Privacy (artt. 32-bis e seguenti), i fornitori di servizi di comunicazione elettronica accessibili al pubblico devono notificare senza ritardo eventuali violazioni di dati personali al Garante Privacy, nonché al contraente qualora la violazione rischi di arrecare pregiudizio ai dati o alla riservatezza del contraente stesso.

Il 26 luglio 2012 il Garante ha pubblicato delle linee guida relative alle circostanze in cui i fornitori hanno l'obbligo di comunicare le violazioni di dati personali, al formato applicabile alla comunicazione e alle relative modalità di effettuazione.

Contestualmente, si è svolta una consultazione pubblica in merito ad alcuni aspetti delle nuove disposizioni (tra cui, in particolare, le misure di sicurezza che i fornitori devono adottare e le modalità di notifica ai contraenti), i cui risultati non sono stati ancora pubblicati.

- **Misure di sicurezza**

Per effetto del D.L. 5/2012, convertito in legge 35/2012, è venuto meno l'obbligo, per coloro che trattano dati personali sensibili e giudiziari con strumenti elettronici, di redigere e aggiornare annualmente, entro il 31 marzo successivo, un "Documento programmatico sulla sicurezza" (DPS).

Il DPS doveva contenere, tra l'altro, una descrizione delle operazioni di trattamento dati effettuate e delle misure di sicurezza adottate. Inoltre, il riferimento all'avvenuta redazione o aggiornamento del DPS doveva essere riportato nella relazione sulla gestione degli amministratori, allegata al bilancio d'esercizio.

Nonostante l'abolizione del DPS, si ravvisa l'opportunità per le aziende di avere un documento relativo alle operazioni di trattamento effettuate e alle misure di sicurezza adottate, anche in funzione probatoria in caso di eventuali contestazioni per violazione della normativa a tutela dei dati personali.

- **Dati giudiziari**

Il D.L. 5/2012 ha ampliato le ipotesi di liceità del trattamento dei dati giudiziari (ad esempio, dati idonei a rivelare la qualità di indagato o imputato), non più limitato alle previsioni di legge o alla presenza di un'autorizzazione del Garante Privacy, ma esteso anche all'esistenza di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'Interno o con i suoi uffici periferici, previo parere del Garante Privacy.

COSA SUCCEDERÀ NEL 2013

- **Cookies**

La recente modifica alla disciplina in materia di cookies in Italia appare meno radicale rispetto al resto d'Europa. Già in precedenza vigeva, infatti, la regola dell'"opt-in" (ovvero, del previo consenso) per l'utilizzo dei cookies, ma soltanto per i cookie "tecnici". Ogni altro accesso ed ogni altra registrazione non autorizzati sul terminale dell'utente erano vietati.

Il principio dell'"opt-in", tuttavia, non è mai stato oggetto di interventi di enforcement da parte del Garante Privacy e l'"opt-out" tramite le impostazioni del browser dell'utente era (ed è tutt'ora) una pratica comune.

Il principio dell'"opt-in" per l'uso di cookies da parte degli operatori internet ha acceso un dibattito circa le modalità pratiche con cui ottenere dagli utenti un consenso preventivo per l'utilizzo di cookies.

Le indicazioni che il Garante Privacy fornirà all'esito della consultazione pubblica in corso aiuteranno gli operatori internet a conformarsi ai nuovi requisiti per l'utilizzo dei cookies?

- **Data breaches**

Il 2013 vedrà un'attenzione sempre crescente, da parte delle aziende, al tema della sicurezza nel trattamento dei dati personali degli utenti, al fine di prevenire spiacevoli incidenti legati alla sicurezza dei dati.

La sicurezza nel trattamento dei dati personali su dispositivi mobile costituirà uno dei temi principali oggetto di discussione.

- **Mobile advertising**

Le tecnologie di tracciamento e profilazione su dispositivi mobile, spesso impiegate ad insaputa degli utenti di tali dispositivi e delle loro applicazioni, porranno numerose questioni circa le modalità per tutelare la privacy online degli utenti.

- **Privacy by design e privacy by default**

I dispositivi mobili pongono delicate questioni relative alla tutela dei dati personali degli utenti che possono ritenersi proprie e specifiche del settore mobile. In tale scenario, i titolari dei trattamenti e sviluppatori di apps avvertiranno sempre più la necessità di adottare misure per la tutela dei dati personali sin dalla progettazione dell'app, secondo l'approccio indicato con i termini privacy by design e privacy by default.
Tale approccio sarà peraltro destinato a caratterizzare lo sviluppo di qualunque prodotto o software che implichi il trattamento di dati personali.

- **Cloud computing**

La crescente adozione su vasta scala di tecnologie cloud-based da parte delle aziende comporterà la necessità di affrontare alcuni temi, tra cui, ad esempio, la questione del controllo sui dati personali e sulle modalità, l'ubicazione e i soggetti che trattano i dati.

- **Binding corporate rules (BCR)**

Le BCR sono regole di condotta relative al trattamento di dati personali all'interno di un gruppo multinazionale che consentono, una volta approvate dalle Autorità nazionali per la protezione dei dati, di trasferire dati personali fra le società del gruppo con sede in UE e quelle situate in paesi terzi. I Garanti per la privacy dei paesi UE hanno approvato una apposita procedura che consente, a partire dal 1 gennaio 2013, la circolazione di dati personali da un'impresa multinazionale, nominata responsabile del trattamento, che offra servizi di trattamento dati in outsourcing ad altre aziende, con sede nell'UE.

Nei prossimi 12 mesi un numero sempre maggiore di multinazionali ricorrerà alle BCR per i trattamenti in outsourcing di dati personali.

- **Regolamento UE per la protezione dei dati personali**

Il framework normativo in materia di tutela dei dati personali è destinato a subire l'impatto del Regolamento UE sulla protezione dei dati proposto dalla Commissione europea il 25 gennaio 2012 allo scopo di garantire una maggiore armonizzazione in materia di privacy nell'intera UE. Il Regolamento, che al momento è ancora all'esame delle istituzioni UE, una volta approvato sarà direttamente applicabile in ciascuno degli Stati membri, i quali avranno due anni per conformarsi alle prescrizioni del Regolamento.
Le aziende che trattano dati personali si troveranno a dover considerare sin da subito i nuovi requisiti, in modo da preparare la propria struttura ed organizzare i propri rapporti contrattuali in vista dell'entrata in vigore del Regolamento.