Recenti provvedimenti del Garante della protezione dei dati personali in tema di regole privacy applicabili (i) alla profilazione *online*, (ii) all'uso dei *cookies* e (iii) ai *mobile remote payment*

Contenuti

1. Decisione Google: il Garante chiarisce le regole per la profilazione *online*

Il Garante per la protezione dei dati personali, al termine di approfondita istruttoria condotta a livello europeo e nazionale iniziata nel 2012, con il recente ***"Provvedimento prescrittivo nei confronti di Google Inc. sulla conformità al Codice dei trattamenti di dati personali effettuati ai sensi della nuova privacy policy"*** (il "**Provvedimento del 10 luglio 2014**") emesso in data 10 luglio 2014, ha individuato le regole per assicurare maggiore trasparenza e garanzie nel trattamento dei dati personali degli utenti delle diverse funzionalità offerte da Google, individuando dettagliate modalità per rendere agli utenti l'informativa *online* e acquisirne il consenso.

Specifico riferimento è fatto alle attività di c.d. "profilazione", consistenti in particolar modo nella visualizzazione di pubblicità comportamentale personalizzata ed analisi e monitoraggio dei comportamenti dei visitatori di siti *web*, non solo attraverso l'uso di *cookie* e altri identificatori (es. *fingerprinting*), ma anche mediante l'incrocio dei dati personali degli utenti raccolti in relazione alla fornitura e utilizzo di più funzionalità diverse tra quelle mese a disposizione dalla società.

Più dettagliatamente, le prescrizioni imposte dal Garante riguardano:

- **Obbligo di informativa.** Google dovrà predisporre un'informativa completa, chiara, nonché facilmente accessibile agli utenti, mediante un **sistema di struttura su più livelli** ma comunque idonea ad evitarne un'eccessiva frammentazione (c.d. "avvertenze multistrato") in modo da fornire in un primo livello generale le informazioni più rilevanti, quali le tipologie di dati personali trattati, la qualifica di titolare e relativi estremi identificativi, i *link* alle specifiche *policy* delle singole funzionalità, le eventuali modalità di acquisizione del consenso, nonché l'indicazione delle modalità e finalità di profilazione tesa sia alla visualizzazione di pubblicità comportamentale personalizzata e all'analisi e monitoraggio dei comportamenti degli utenti web, che alla raccolta di dati personali con tecniche più sofisticate che non i semplici *cookie*, come ad esempio il c.d. *fingerprinting*, idoneo a raccogliere i dati archiviandoli direttamente presso i *server* della società.

- **Acquisizione del consenso dell'interessato e opposizione al trattamento.** Per le finalità ulteriori rispetto a quelle strettamente inerenti all'esecuzione delle specifiche funzionalità, ed in particolare per le finalità di profilazione dell'utente, il Garante prescrive a Google la necessaria acquisizione del **consenso espresso ed esplicito degli utenti, non essendo sufficiente la sola menzione di tale finalità tra quelle oggetto dell'informativa resa agli interessati**. Sarà invece necessario che la società implementi un meccanismo che garantisca la visualizzazione, da parte dell'utente, in primo piano nella *home page* (o altra pagina) del sito *web*, di un'area di dimensioni tali da costituire una "*percettibile discontinuità*" nella fruizione dei contenuti della pagina *web* visitata, contenente almeno: (i) l'indicazione delle finalità di profilazione e relative modalità di attuazione (es. incrocio dei dati tra funzionalità diverse, *cookie*, *fingerprint*, ecc.); (ii) *link* alla *privacy policy* completa; (iii) *link* ad un'ulteriore area dedicata in cui l'utente abbia la possibilità di **negare il consenso alla profilazione o selezionare le eventuali finalità o modalità attraverso cui sceglie di essere profilato**; (iv) indicazione che la prosecuzione della

navigazione mediante accesso o selezione di un elemento sottostante o comunque esterno all'area in primo piano comporta la prestazione del consenso alla profilazione: il consenso sarà manifestato pertanto mediante l'**espressione di un'azione positiva da parte dell'utente**.

- **Conservazione dei dati.** Google dovrà provvedere a definire tempi di conservazione dei dati compatibili con le disposizioni generali del Codice *Privacy*, che dispone che i dati debbano essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi della raccolta. A tale proposito il Garante prescrive che, nel caso di dati mantenuti sui sistemi c.d. attivi, la società dovrà provvedere alla cancellazione dei dati personali su richiesta dell'interessato **entro il termine massimo di due mesi**. Il termine è fissato in **sei mesi dalla richiesta**, invece, per i dati archiviati nei sistemi di *back-up* della società. Il Garante, al momento, si astiene inoltre dal dettare prescrizioni in relazione alle richieste di cancellazione in esercizio del diritto all'oblio avanzate con riguardo ai risultati delle ricerche rinvenibili nel *web* attraverso la funzionalità del motore di ricerca Google, in ragione della complessità nonché estrema novità della materia, riservandosi eventuali interventi futuri anche al consolidarsi di orientamenti più definiti tra le autorità europee competenti.

Le misure prescritte dal Garante dovranno essere adottate da Google entro e non oltre il termine di 18 mesi dalla data di notifica alla società del Provvedimento del 10 luglio 2014, pubblicato lo scorso 10 luglio.

Il Provvedimento del 10 luglio 2014 presenta aspetti di interesse generale, in quanto rappresenta uno dei primi interventi concreti, in tutta Europa, in grado di fornire delle vere e proprie linee guida tecniche a tutte le imprese *web* che operano nell'ambito del *behavioural advertising* raccogliendo i dati personali degli utenti (siti *web* preferiti, eventuali acquisti *online*, gusti e preferenze, ecc.) per finalità di profilazione e pubblicità mirata, anche mediante l'integrazione ed il raffronto con le diverse funzioni e servizi offerti all'utente.

Le stesse, infatti, qualora operino trattamenti di dati personali degli utenti con modalità e finalità analoghe a quelle adottate dal colosso americano, potrebbero essere suscettibili di sanzioni in caso di mancata adozione di misure che assicurino un livello di tutela degli utenti almeno pari a quello prescritto dal Garante a Google.

2. Il Garante detta le regole per l'uso dei *cookies*

I *web cookies* consistono in stringhe di testo che registrano e memorizzano le scelte di navigazione degli utenti, permettendo per esempio di individuarne i siti *web* preferiti, gusti e preferenze (anche a fini pubblicitari e di *marketing* diretto, c.d. *cookies di profilazione*). Il D.Lgs. 69/2012, in attuazione delle direttive 2009/136/CE e 2009/140/CE (cc.dd. "*Cookies Law*"), ha modificato l'articolo 122 del Codice *Privacy* imponendo ai fornitori di comunicazioni elettroniche e gestori di siti *web* requisiti di preventiva informativa e consenso.

Il Garante per la protezione dei dati personali, al termine di una consultazione pubblica iniziata nel novembre 2012, con il provvedimento dell'8 maggio 2014 (il "**Provvedimento dell'8 maggio 2014**"), ha chiarito la portata delle regole sull'utilizzo dei *cookies*, individuando altresì modalità semplificate per l'informativa e la raccolta del consenso.

Mentre sino ad oggi la prassi più diffusa per l'utilizzo dei *cookies* prevedeva un meccanismo di *opt-out*, consentendo al gestore un libero utilizzo dei *cookies* fino al momento del dissenso manifesto dell'utente attraverso la disabilitazione degli stessi, con l'entrata in vigore della *Cookie Law* i gestori sono obbligati a rendere articolata informativa agli utenti in merito al trattamento dei dati personali e a raccogliere espresso consenso, ove necessario.

Le misure prescritte dal Garante, e che dovranno essere adottate entro un anno dalla pubblicazione del Provvedimento dell'8 maggio 2014 (avvenuta in data 3 giugno 2014) sono differenziate a seconda della finalità del *cookie* utilizzato: l'obbligo di acquisire il consenso preventivo è limitato all'utilizzo di *cookies* per finalità diverse da quelle meramente tecniche.

Mentre per i ***cookies tecnici*** (vale a dire quelli utilizzati al solo fine di effettuare la trasmissione sulla rete di comunicazione o di fornire un servizio esplicitamente richiesto dall'utente) e i ***cookies analitici*** - assimilati a quelli tecnici se utilizzati direttamente dal gestore del sito per raccogliere informazioni aggregate sull'utilizzo del sito – non occorre il consenso, per quanto riguarda i ***cookies* di profilazione** e i ***cookies* analitici di terze parti** (ovvero *cookies* installati da un sito diverso tramite il sito del gestore) il Garante ha stabilito che sulla pagina di accesso di ogni sito debba immediatamente comparire un *banner* ben visibile, in cui sia indicati chiaramente che il sito utilizza *cookies* analitici di terze parti ovvero *cookies* di profilazione per inviare messaggi pubblicitari mirati, e che proseguendo nella navigazione (ad es., accedendo ad un'altra area del sito o selezionando un'immagine o un *link*) si presta il consenso all'uso di tali *cookies*.

Il *banner* dovrà essere immediato, comparire in primo piano e presentare dimensioni sufficienti da permettere l'attiva percezione da parte dell'utente. Il *banner* dovrà anche contenere un *link* a un'informativa estesa, con le indicazioni sull'uso dei *cookie* inviati dal sito, dove sia possibile negare il consenso alla loro installazione direttamente o collegandosi ai vari siti nel caso dei *cookie* di terze parti. I gestori dei siti, perciò, avranno l'obbligo di garantire a chi naviga *online* la possibilità di decidere in maniera libera e consapevole se far usare o no le informazioni raccolte tramite i diversi tipi di *cookies* di profilazione.

3. Le implicazioni *privacy* dei *mobile remote payment*

Il Garante per la protezione dei dati personali, con il **"Provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di *mobile remote payment*"** del 22 maggio 2014 (G.U. n. 137 del 16 giugno 2014) (il "**Provvedimento del 22 maggio 2014**"), ha individuato le regole per la fornitura dei servizi di *mobile remote payment*, che consentono di effettuare gli acquisti ed i conseguenti pagamenti di beni e servizi tramite un terminale mobile. In particolare, detti servizi si concretizzano nell'offerta, da parte dei fornitori di reti e servizi di comunicazione, di prodotti e di servizi che l'utente può pagare utilizzando il proprio *smartphone*, *tablet* e PC, attraverso apposita piattaforma tecnologica che gestisce il pagamento tramite l'addebito sul conto telefonico.

Il Provvedimento del 22 maggio 2014, basato sulle direttive 2007/64/CE, c.d. PSD ("*Service Payment Directive*") nonché 2009/110/CE ("*e-Money Directive*"), risponde all'esigenza di determinare in maniera esaustiva le misure *privacy* da implementare, individuando i possibili ruoli dei vari soggetti coinvolti. Nello specifico, il Provvedimento del 22 maggio 2014 si rivolge non solo agli operatori di reti e servizi di comunicazione elettronica che offrono il servizio di pagamento tramite dispositivo mobile, ma anche ai c.d. aggregatori (vale a dire, i gestori della piattaforma tecnologica che fa da interfaccia all'acquisto e successivo pagamento), ai *merchant* (le aziende fornitrici dei contenuti digitali disponibili), nonché a tutti gli eventuali soggetti che, tramite applicazioni proprie o di terzi, offrono agli utenti la possibilità di acquistare prodotti o servizi tramite l'uso del credito telefonico. Ciò in quanto l'erogazione dei servizi di *mobile remote payment* implica il trattamento di una serie di dati personali dell'utente, non solo di carattere identificativo, quali ad esempio i dati relativi alla numerazione telefonica, i dati anagrafici, la data e l'ora dell'operazione effettuata, l'identificativo di sessione e l'indirizzo IP dell'utente ed eventualmente il suo indirizzo di posta elettronica, ma anche, potenzialmente, dati di natura sensibile, quali quelli legati alla tipologia e descrizione del servizio o del prodotto digitale richiesto, nonché allo storico degli acquisti effettuati.

Tutti i soggetti coinvolti nel trattamento sono tenuti entro 180 giorni dalla data di pubblicazione (16 giugno) all'adozione delle misure indicate dal Provvedimento del 22 maggio 2014:

- **Informativa.** Sia l'operatore che il *merchant*, ciascuno per i profili di propria competenza (l'operatore per utilizzo del sistema di pagamento, il *merchant* in relazione alle vendita del bene o servizio), dovranno rendere agli utenti un'informativa chiara e completa: oltre alla chiara identificazione dei dati personali e/o sensibili raccolti e all'esplicitazione delle finalità di erogazione del servizio, l'informativa dovrà specificare se i dati personali dell'utente saranno trattati anche per scopi ulteriori, ad esempio per finalità di *marketing* e invio di comunicazioni promozionali, specificando altresì i canali di comunicazione utilizzati (modalità tradizionali o automatizzate), o eventuale profilazione, chiarendo che dette attività possono svolgersi solo previa acquisizione del consenso dell'utente, espresso e specifico per ciascuna finalità. Parimenti dovranno essere indicate le modalità di esercizio da parte dell'utente dei diritti dell'articolo 7 del Codice *Privacy*, nonché l'identità del titolare del trattamento e dei responsabili, fra cui nello specifico gli aggregatori, gestori della piattaforma per conto dell'operatore e del *merchant*. L'informativa deve essere rilasciata al momento della sottoscrizione dell'utente ai servizi erogati: in considerazione delle dimensioni degli schermi dei dispositivi utilizzati, il Garante chiarisce che una prima informativa breve possa essere predisposta adottando l'approccio c.d. *layered*, per poi rimandare, tramite apposito *link*, ad un'informativa completa disponibile nella pagina dell'operatore.
- **Consenso.** Il consenso dell'utente non è necessario per finalità strettamente collegate all'erogazione del servizio; al contrario l'operatore e il *merchant* (e anche l'aggregatore, nel caso in cui agisca quale titolare del trattamento per proprie finalità) dovranno acquisire il preventivo consenso dell'utente nel caso in cui i dati dello stesso, riferibili agli acquisti effettuati, vengano utilizzati per finalità di *marketing* diretto, profilazione e/o comunicati a soggetti terzi; tali consensi dovranno essere specifici e distinti per ciascuna finalità, ad esempio come diversi *flag* da selezionare in una specifica casella nella pagina *web* dell'operatore al momento dell'acquisto. Nel caso, invece, di trattamento di dati sensibili, per i quali il Codice *Privacy* richiede il consenso in forma scritta, il Provvedimento del 22 maggio 2014 prevede che

Milano

Daniele Vecchi
Tel. +39 02 763741
dvecchi@gop.it

Melissa Marchese
Tel. +39 02 763741
mmarchese@gop.it

lo stesso possa prestarsi con modalità telematiche equiparabili allo scritto: firma elettronica qualificata o digitale, certificato elettronico, o misure alternative che potranno essere sottoposte alla valutazione dell'Autorità in sede di verifica preliminare.

- **Misure di sicurezza logiche ed organizzative.** Oltre alle ordinarie misure di sicurezza previste dal Codice *Privacy* e dall'Allegato B, operatori, aggregatori e *merchant* saranno tenuti ad adottare ulteriori cautele, tra cui: (a) comunicazioni "neutre" tra l'operatore e il *merchant* con riferimento all'esito delle operazioni di acquisto prevedendo, nel messaggio di "*ok*" o "*ko*" che l'operatore trasmette al *merchant* a seconda che l'operazione sia andata o meno a buon fine, evitando qualsiasi indicazione di eventuali cause ostative diverse da quelle tecniche, legate all'indisponibilità od insufficienza di credito telefonico dell'utente; (b) per gli addetti di *customer care* dell'operatore che, per finalità di assistenza alla clientela, visualizzano lo storico delle operazioni di acquisto effettuate dal numero telefonico dell'utente, i riferimenti temporali ed i relativi importi, nonché la categoria merceologica del prodotto o servizio acquistato, accesso a tali dati potrà avvenire solo con *strong authentication* basata su *token* e *account* nominale "*operatore di customer care*", nonché tracciamento analitico e dettagliato degli accessi al sistema. Misure analoghe per gli incaricati dell'aggregatore rispetto ai dati raccolti dalla piattaforma tecnologica da essi gestita; (c) tabelle interne di classificazione che prevedano criteri di codifica dei prodotti e servizi basati non sul loro specifico contenuto ma esclusivamente sull'individuazione di classi e/o genere (ad es. video sportivo, cronaca ecc.); (d) nel caso di attività di profilazione compiute dagli operatori sui dati di consumo/traffico telefonico e dati relativi alla fornitura di altre tipologie di beni digitali diversi da quelli oggetto di *mobile payment* (ad esempio relativi alla c.d. Tv interattiva), utilizzo di appositi "meccanismi di rotazione" che consentano di applicare allo stesso utente chiavi di codifica differenti, destinate a mascherare i dati all'interno dei diversi sistemi dedicati alle attività di profilazione che l'operatore può svolgere, al fine di evitare analisi incrociate delle abitudini, dei gusti e delle preferenze di consumo della clientela nei diversi ambiti di fornitura individuati; (e) conservazione dei dati per un periodo massimo di 6 mesi, salvo prolungamento per fini di giustizia e contestazioni giudiziali. L'indirizzo IP invece dovrà essere cancellato immediatamente dopo l'erogazione del servizio.
- **Notifica dei data *breach*.** Gli operatori di comunicazioni elettroniche accessibili al pubblico, in presenza di violazioni di dati personali dei propri utenti, dovranno notificare tali violazioni, come disposto dal nuovo articolo 32 *bis* del Codice *Privacy*.