

**La conformità dei servizi Google al Codice della privacy italiano: il Garante privacy adotta il primo provvedimento generale prescrittivo in Europa.**

*di:*

*Prof. Avv. Alessandro del Ninno*  
*Studio Legale Tonucci & Partners*  
[adelninno@tonucci.com](mailto:adelninno@tonucci.com)

---

## Indice

§ 1. *Introduzione: breve inquadramento del Provvedimento prescrittivo del Garante.*

§ 2. *Le misure obbligatorie prescritte dal Garante a Google: contenuti dell'informativa privacy agli interessati e modalità pratiche di rilascio.*

§ 2.1 *Segue: acquisizione del consenso degli utenti per i trattamenti di profilazione svolti mediante servizi e funzionalità Google.*

§ 2.2 *Segue: le prescrizioni del Garante a Google in materia di conservazione dei dati e le politiche di data retention e data deletion.*

§ 3. *Conclusioni: alcuni dubbi e note critiche sul Provvedimento Google.*

---

## **§ 1. Introduzione: breve inquadramento del Provvedimento prescrittivo del Garante.**

Ancora non è sopito il dibattito sulla recente sentenza della Corte di Giustizia UE sul c.d. *diritto all'oblio* nel caso Google che ecco che il gigante di Mountain View (che sta attraversando un delicato momento per i vari fronti aperti in Europa, dalla fiscalità - con lo spinoso dibattito sulla *web tax* o "*Google tax*" - al copyright, ai sospetti di abuso di posizione dominante che hanno di recente risvegliato l'Antitrust UE) è nuovamente al centro dell'attenzione a seguito del recente provvedimento dell'Autorità per la protezione dei dati personali italiana che - prima fra i Garanti privacy europei - ha emanato una serie di vincolanti prescrizioni sul trattamento dei dati personali degli utenti nell'ambito della fornitura e fruizione dei vari servizi Google.

Con il provvedimento n. 353 del 10 Luglio 2014 intitolato *Provvedimento prescrittivo nei confronti di Google Inc. sulla conformità al Codice dei trattamenti di dati personali*

effettuati ai sensi della nuova *privacy policy* (di seguito, per brevità, il “Provvedimento”) – il Garante ha preso spunto dall’esame di conformità al Codice della *privacy* italiano della nuova *privacy policy* di Google (che dal 1° Marzo 2012 ha unificato in un solo documento le circa 70 diverse *policies* fino ad allora in vigore) per prescrivere una serie di regole a tutela degli utenti italiani fruitori di servizi Google. Tale Provvedimento si può considerare l’esito italiano di una istruttoria nazionale avviata dal Garante il 2 aprile 2013 (al pari di almeno altre cinque autorità europee per la protezione dei dati) comunque collegata ad una istruttoria europea condotta (tramite il Garante *privacy* francese a ciò delegato, la CNIL) dalle Autorità di protezione dei dati nazionali riunite nel cosiddetto *Working Party* previsto dall’art. 29 della Direttiva 46/95 sulla protezione dei dati personali e tesa ad un controllo sulla liceità e correttezza dei trattamenti effettuati dalla Google ai sensi della nuova *privacy policy*.

L’esame ha avuto per oggetto la conformità alla normativa italiana sulla protezione dei dati di cui al Codice della nuova *privacy policy* di Google con riferimento ai trattamenti degli utenti svolti nell’ambito della fornitura della molteplicità di servizi e funzionalità offerti da Google, e che variano dal motore di ricerca sul web (Google search) alla posta elettronica (Gmail), dalla commercializzazione di spazi pubblicitari (DoubleClick) al browser (Google Chrome), dal social network (Google+) alla gestione di pagamenti online (Google Wallet), dal negozio virtuale per l’acquisto di applicazioni, musica, film, libri e riviste (Google Play) alla ricerca, visualizzazione e diffusione di filmati (YouTube); dai servizi di immagazzinamento, condivisione e revisione di testi (Google Docs e Google Drive) al software per la visualizzazione di immagini satellitari (Google Earth); dalla gestione di agende e calendari (Google calendar) a funzionalità per il controllo e la gestione dei profili dell’utente (Google Dashboard), da strumenti di analisi statistica e di monitoraggio dei visitatori di siti web (Google Analytics) fino alle mappe online con il servizio Street View su Google Maps. Su quest’ultimo servizio – tra l’altro – è opportuno ricordare che proprio di recente – il 18 Dicembre 2013 – il Garante italiano ha comminato una sanzione a Google di circa un milione di Euro per inidonea informativa (la sanzione ha riguardato il passato poichè ad oggi il Garante ritiene l’informativa del servizio Street View idonea); una sanzione assai elevata se raffrontata ad analoghe sanzioni applicate a Google per il servizio Street View per motivi ben più gravi, come ad esempio la sottrazione di dati sull’accesso alle connessioni wi-fi non protette degli utenti: in Francia la sanzione fu di 100 mila euro, in Germania di 145 mila euro, solo 25 mila negli Stati Uniti (in totale, per quella vicenda, Google ha pagato in vari paesi circa 7 milioni di dollari).

Ancora, con riferimento invece al servizio You Tube, è interessante notare come nel Provvedimento il Garante ha sottolineato che Google omette di informare con chiarezza gli utenti circa la propria identità di titolare del trattamento dei dati personali raccolti anche attraverso l’uso di You Tube e successivamente incrociati con quelli relativi ad altre funzionalità ed ha prescritto che tale indicazione sia espressa in modo visibile sia nella *privacy policy*, sia nelle pagine di fruizione di YouTube.

A seguito della istruttoria il Garante italiano ha ravvisato le criticità di seguito elencate, per risolvere le quali ha poi imposto a Google Inc. l'adozione delle conseguenti misure organizzative e tecniche:

1. l'informativa resa da Google agli interessati è inidonea e non conforme all'art. 13 del Codice della privacy, sia per le modalità con le quali viene resa agli utenti, sia per i contenuti informativi sia per l'insufficiente esplicitazione delle diverse finalità e modalità del trattamento dei dati personali degli utenti;
2. Google omette poi di richiedere (ai sensi degli articoli 23 e 122 del Codice) lo specifico, separato e consapevole consenso degli interessati per finalità di profilazione e successivo invio di comunicazioni commerciali mirate o basate sulla analisi ed il monitoraggio dei comportamenti degli utenti sul web; sul punto il Garante ha rilevato come la profilazione avvenga mediante a) trattamento, in modalità automatizzata, dei dati personali degli utenti autenticati in relazione all'utilizzo del servizio per l'inoltro e la ricezione di messaggi di posta elettronica veicolati attraverso Gmail; b) incrocio dei dati personali raccolti in relazione alla fornitura ed al relativo utilizzo di più funzionalità diverse tra quelle messe a disposizione dell'utente; c) utilizzo di *cookie* e altri identificatori (credenziali di autenticazione, *fingerprinting* etc.), necessari per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso delle funzionalità offerte (*pattern*);
3. Google non ha adottato idonee procedure per consentire agli utenti di esercitare i propri diritti privacy, come ad esempio il diritto di opporsi al trattamento;
4. Google non rispetta i principi in materia di tempi massimi di conservazione dei dati (art. 11 del Codice).

Gli "interessati" presi in considerazione dal Provvedimento (a fini della predisposizione delle misure a loro tutela) sono ascrivibili poi a tre categorie:

- gli utenti che dispongono di un account Google creato a seguito di una procedura di registrazione per l'accesso "autenticato" ai servizi di Google (cd. utenti autenticati);
- gli utenti che utilizzano le medesime funzionalità in assenza di previa autenticazione (cd. utenti non autenticati);
- gli utenti i cui dati, pur non utilizzando tali soggetti direttamente le funzionalità di Google, possono comunque essere acquisiti dalla società, come nel caso in cui navighino all'interno di siti di terze parti ove vengono installati, tra gli altri anche i cookie di Google (cd. *passive users*).

## § 2. Le misure obbligatorie prescritte dal Garante a Google: contenuti dell'informativa privacy agli interessati e modalità pratiche di rilascio.

Prima di analizzare e commentare le misure prescrittive di cui al Provvedimento appare opportuno ricordare che il Garante - *“consapevole delle difficoltà tecnico-operative connesse all'implementazione delle misure cui Google è tenuta ai fini dell'adempimento delle prescrizioni di cui al presente provvedimento, in quanto si tratta di modifiche relative ad una molteplicità di funzionalità rese disponibili su una pluralità di piattaforme tecnologiche e sistemi operativi, peraltro di non trascurabile complessità tecnica”* - ha dato a Mountain View termine di 18 mesi per l'adeguamento. In questo periodo, in ogni caso, il Garante si è riservato di valutare lo stato di avanzamento delle misure (Google proporrà all'Autorità italiana entro il 30 Settembre 2014 un apposito protocollo di verifica volto a disciplinare le modalità ed i tempi relativi allo scambio di documentazione tra Google e l'Autorità, nonché le modalità di attuazione e, appunto, dei riscontri che l'Autorità effettuerà nel corso dei 18 mesi).

Passando all'esame delle misure prescrizioni, e con riferimento alla prima criticità - cioè l'inidoneità dell'attuale informativa che Google rilascia agli utenti sul complesso dei propri servizi - il Garante ha indicato le seguenti soluzioni, soffermandosi in particolare (più che sui contenuti) sulle modalità tecniche con le quali Google dovrebbe rilasciare l'informativa agli utenti. In primo luogo il Garante ha difatti disposto (pur lasciando libera Google di adottare altre soluzioni tecniche, purché le stesse determinino i medesimi effetti di conformità al Codice delle soluzioni suggerite dall'Autorità) che l'informativa sia facilmente accessibile, ad esempio con un solo click dalla pagina del dominio cui l'utente accede. Con riferimento ai contenuti essa deve essere formulata in modo chiaro, completo ed esaustivo e - a fronte di eventuali aggiornamenti o modifiche - gli interessati devono essere posti nella condizione di comprendere e valutare i cambiamenti apportati, anche eventualmente mediante raffronto tra le diverse versioni della *privacy policy* susseguitesisi nel tempo.

Assai interessante la parte del provvedimento nella quale il Garante italiano suggerisce a Google - quale modalità idonea di fornitura delle informazioni a fronte di una molteplicità di servizi e funzionalità complesse - l'adozione del meccanismo delle cosiddette *“avvertenze multistrato”*. Tale meccanismo (che ragionevolmente ed analogicamente potrebbe ritenersi applicabile anche ad altri fornitori - es: Facebook - e ad analoghi servizi) è ripreso da una delle soluzioni tecniche raccomandate dal Gruppo dei Garanti europei nel Parere n. 10/2004 *sulla maggiore armonizzazione della fornitura di informazioni*. In sostanza, partendo da tale meccanismo, il Garante suggerisce di rilasciare all'interessato una informativa strutturata su più livelli, secondo i seguenti criteri:

- un primo livello deve fornire all'utente tutte le informazioni di carattere generale di maggiore importanza, relative ad esempio ai trattamenti di dati

personali effettuati, alle tipologie di dati personali oggetto di trattamento, anche per categorie (ad es. dati di localizzazione dei terminali degli utenti e dei punti di accesso wi-fi, indirizzi IP, MAC address, dati relativi a transazioni finanziarie e così via), alla qualifica di titolare che compete a Google ed ai suoi estremi identificativi, nonché l'indicazione del rappresentante designato nel territorio dello stato e di un indirizzo presso cui gli utenti possano esercitare in modo agevole ed in lingua italiana i propri diritti. In questo primo livello di informativa è inoltre necessario per il Garante riportare i link alle specifiche *policies* delle singole funzionalità, ove esistenti, nonché almeno l'indicazione della finalità di profilazione di alcuni trattamenti che Google comunque effettua (visualizzazione di pubblicità comportamentale personalizzata, analisi e monitoraggio dei comportamenti dei visitatori di siti web, perseguita nelle modalità anche automatizzate che più sopra sono state elencate). Oltre a dover indicare in questo primo livello dell'informativa la finalità di profilazione e le relative modalità Google deve inoltre indicare dettagliatamente le modalità di acquisizione del consenso al trattamento, ove necessario;

- il secondo livello può essere invece destinato - a parere del Garante - a contenere la policy relativa alle specifiche funzionalità ovvero diversi esempi per chiarire le modalità del trattamento delle informazioni personali. In questo secondo livello potrebbero poi anche essere archiviate le precedenti versioni della privacy policy, ancorché non più in vigore, l'indicazione dei rischi specifici che possono derivare per gli interessati dall'utilizzo dei servizi (ad esempio in caso di scelta di password non sufficientemente sicure poiché di agevole identificazione etc.) e tutte le altre indicazioni di dettaglio idonee a consentire il più efficace esercizio dei diritti riconosciuti agli utenti.

Altra prescrizione rilevante del Garante - infine - è che le soluzioni in materia di informativa che siano conformi - come suggerito - al Codice devono applicarsi in modo identico indipendentemente dal tipo di terminale con il quale l'utente accede ai servizi o alle funzionalità Google: ciò significa e implica che agli utenti dei servizi e delle funzionalità Google dovrà essere rilasciata l'informativa con le modalità indicate indipendentemente dal fatto che tali utenti accedano via mobile, tablet, desktop computer, dispositivi portatili o TV plug-in e per ogni applicazione resa disponibile.

## **§ 2.1 Segue: acquisizione del consenso degli utenti per i trattamenti di profilazione svolti mediante servizi e funzionalità Google.**

In primo luogo il Garante richiama i principi generali del Codice della privacy sulla previa acquisizione del consenso dell'interessato (ove obbligatorio) ai sensi dell'articolo 23 (che dispone che il trattamento di dati personali da parte di privati è ammesso solo con il consenso espresso, libero, specifico e informato

dell'interessato), sui casi in cui non è necessario acquisire alcun consenso (elencati dall'art. 24 del Codice) e sulle modalità di espressione del consenso in caso di cookies di profilazione (ex art. 122 del Codice). In tale delineata prospettiva l'Autorità specifica nel Provvedimento che Google non è tenuta a richiedere alcun consenso agli interessati quando - ad esempio - nella prestazione del servizio Gmail di posta elettronica tratta automaticamente i dati degli utenti registrati per finalità di carattere tecnico come ad esempio l'impiego di filtri antispam, la rilevazione di virus, la possibilità, garantita all'utente, di effettuare ricerche testuali, utilizzare il controllo ortografico, far ricorso all'inoltro selettivo di messaggi o di risposte automatiche in caso di assenza, gestire le preferenze e la creazione di regole per l'assegnazione del messaggio a cartelle determinate in base al suo contenuto, fare uso di flag per marcare messaggi segnati da carattere di urgenza, consentire la lettura vocale dei messaggi per soggetti non vedenti, la conversione delle e-mail in entrata in messaggi di testo per telefoni cellulari etc.

In questi casi il trattamento è finalizzato al perseguimento di finalità contrattuali di fornitura del servizio email richiesto dall'utente e quindi si applica una delle tipiche esimenti del consenso previste dall'art. 24 del Codice (esecuzione di obblighi derivanti da un contratto).

Diverso è il caso dei trattamenti svolti da Google che perseguono finalità di profilazione dell'utente: per il conseguimento di tali finalità ulteriori rispetto a quelle direttamente e strettamente inerenti la messa a disposizione della specifica funzionalità del servizio di posta elettronica, ed in particolare per la visualizzazione, da parte dell'utente autenticato, di messaggi di testo tesi alla fornitura di pubblicità comportamentale personalizzata, il Garante prescrive a Google di acquisire il preventivo ed informato consenso dei propri utenti, mai fino ad ora richiesto nello specifico.

Google procede poi alla profilazione degli utenti anche mediante incrocio dei dati personali degli interessati relativi all'utilizzo di più servizi e funzionalità Google: ma lo fa senza chiedere il prescritto consenso obbligatorio ai sensi del Codice (e ovviamente non è sufficiente menzionare nell'informativa la possibilità che sia svolto un tale trattamento per considerare acquisito il consenso).

Infine Google procede alla profilazione degli utenti dei suoi servizi mediante l'utilizzo di *cookie* e di altri identificatori quali credenziali di autenticazione e *fingerprinting* (cioè la tecnica di identificazione basata sul trattamento di dati personali ovvero anche di informazioni o parti di informazioni - che non sono o non sono ancora dati personali ma che, poste in associazione tra loro ovvero con altre informazioni, possono diventarlo - con l'obiettivo di pervenire all'identificazione inequivoca - cd. *single out* - del terminale e, per il suo tramite, anche del profilo di uno o più utilizzatori di quel dispositivo). Anche in quest'ultimo caso il Garante ha rilevato l'assenza nella *policy* Google di idonei meccanismi di acquisizione del necessario consenso specifico

alla profilazione e l'insufficienza di meccanismi – che non possono essere equiparati al consenso espresso - basati su comportamenti concludenti degli utenti come la passiva accettazione delle condizioni d'uso, il cd. *further browsing* (cioè la prosecuzione della navigazione all'interno del sito) e similari.

Appare assai interessante notare come il Garante sottolinei nel Provvedimento la maggiore rischiosità – in termini di possibile violazione dei diritti privacy degli utenti di Google – della tecnica del fingerprinting rispetto alla normale operatività dei cookies: difatti – sottolinea il Garante – *“l'utente che non intenda essere profilato, oltre alle tutele di carattere giuridico connesse all'esercizio del diritto di opposizione, ha anche la possibilità pragmatica di rimuovere direttamente i cookie, in quanto archiviati all'interno del proprio dispositivo; con riguardo al fingerprinting il solo strumento nella sua disponibilità consiste nella possibilità di rivolgere una specifica richiesta al titolare, confidando che essa venga accolta. Ciò in quanto il fingerprinting non risiede nel terminale dell'utente, bensì presso i sistemi del provider, ai quali l'interessato non ha, ovviamente, alcun accesso libero e diretto.”*

In ogni caso, per tutti i casi di trattamento di profilazione degli utenti svolto da Google nelle varie modalità sopra elencate e con le finalità illustrate il Garante fissa un ineludibile principio: il trattamento può essere effettuato solo previo consenso dell'interessato; tale consenso deve rispondere, ai fini della sua validità, ai requisiti di legge e pertanto esso deve essere libero, acquisito in via preventiva rispetto al trattamento medesimo, riferibile a trattamenti che perseguono finalità esplicite e determinate, informato e documentato per iscritto. È dunque necessario, in tale prospettiva, che la sua espressione costituisca una inequivoca manifestazione di volontà da parte dell'interessato.

Proprio in tale ottica – e ferma restando in capo a Google la libertà di attuare i principi in materia di acquisizione consenso con l'implementazione di meccanismi e tecniche di sua scelta, purchè rispondenti al dato ed ai principi normativi richiamati – il Garante propone alcune soluzioni per raccogliere il consenso di utenti non autenticati e autenticati (per i cosiddetti *passive users* – cioè i soggetti che non utilizzano direttamente le funzionalità di Google, ma i cui dati possono tuttavia comunque essere da essa acquisiti ad esempio perché navigano su siti di terze parti ove sono installati anche cookie di Google, l'Autorità richiama espressamente le prescrizioni già emanate nel provvedimento n. 229, dell'8 maggio 2014, relativo alla *"Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie"* il quale ha stabilito che, in tale situazione, sarà il gestore del sito ove avviene la navigazione a raccogliere il consenso anche per l'installazione dei cookie da parte di Google ed a farsi carico di acquisire, già in fase contrattuale, il collegamento (link) alla o alle pagine web contenenti le informative e i moduli per l'acquisizione del consenso relativo ai cookie di Google).

Il Garante raccomanda a Google di implementare meccanismi che diano luogo, all'atto dell'accesso alla *home page* (o ad altra pagina) del sito web da parte di un utente non registrato (o perché non ancora autenticato e riconosciuto dai sistemi Google, o perché non registrato e privo di *account*) alla immediata visualizzazione in primo piano di un'area di idonee dimensioni, ossia di dimensioni tali da costituire una percettibile discontinuità nella fruizione dei contenuti della pagina web che l'utente sta visitando, contenente almeno le seguenti indicazioni:

- a) che il sito effettua attività di trattamento dei dati per finalità di profilazione sia mediante trattamento, in modalità automatizzata, dei dati personali degli utenti autenticati in relazione all'utilizzo del servizio per l'inoltro e la ricezione di messaggi di posta elettronica veicolati attraverso Gmail, sia tramite incrocio dei dati tra funzionalità diverse, sia utilizzando cookie o altri identificatori anche al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente stesso nell'ambito dell'utilizzo delle funzionalità e della navigazione in rete nonché allo scopo di effettuare analisi e monitoraggio dei comportamenti dei visitatori di siti web; il link alla *privacy policy*, ove vengono fornite tutte le indicazioni;
- b) il *link* ad una ulteriore area dedicata (che il Garante specifica deve essere presente in tutte le pagine web Google) nella quale sia possibile negare il consenso alla profilazione ovvero selezionare, in modo esaustivamente analitico, soltanto la oppure le funzionalità e le modalità in relazione all'utilizzo delle quali l'utente sceglie di essere profilato;
- c) l'indicazione che la prosecuzione della navigazione mediante accesso o selezione di un elemento sottostante o comunque esterno all'area in primo piano (ad esempio, di un form di ricerca, di una mappa, di un'immagine o di un link) comporta la prestazione del consenso alla profilazione.

L'utente manifesterà il proprio consenso alla profilazione - valido ai sensi dell'art. 23 del Codice (di cui Google dovrà registrare e conservare traccia informatica, anche mediante specifico cookie tecnico, in modo tale da non ripresentare al medesimo utente il meccanismo o l'area) - ponendo poi in essere una azione positiva che implichi una discontinuità, seppur minima, dell'esperienza di navigazione: per esempio equivale a consenso espresso dell'utente il fatto che l'area visualizzata scompaia o si chiuda a seguito di una sua specifica azione attiva, come la selezione di un elemento contenuto nella pagina sottostante l'area stessa. In tale ottica - al contrario - non equivale ovviamente a manifestazione di consenso l'azione dell'utente che accede alla specifica area nella quale modulare le scelte oppure clicca sul *link* della pagina che contiene la *privacy policy*.

L'unica differenza, dal rilevante impatto pratico, tra utenti registrati e non registrati in merito ai sopra illustrati meccanismi di acquisizione del consenso alla profilazione è rappresentata - come chiarisce il Garante - dal fatto che le scelte in ordine al



trattamento dei propri dati per finalità di profilazione espresse da un utente non autenticato, proprio perché non legate ad un *account*, avranno validità esclusivamente con riferimento allo specifico dispositivo utilizzato, tanto nella prima quanto nelle successive sessioni, fino ad una eventuale revoca; invece la manifestazione di volontà dell'utente autenticato essendo espressa da un soggetto individuato *in re ipsa* varrà anche nell'ipotesi nella quale l'utente autenticato fruisca delle funzionalità e dei servizi Google mediante utilizzo di più e diversi dispositivi.

## **§ 2.2 Segue: le prescrizioni del Garante a Google in materia di conservazione dei dati e le politiche di *data retention* e *data deletion*.**

Con riferimento ai tempi di conservazione dei dati da parte di Google (ed alle connesse politiche di cancellazione) il Garante ha svolto l'esame di conformità della *privacy policy* di Google sulla base del fondamentale principio contenuto nell'art. 11 del Codice della privacy, che dispone che i dati possono conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. Si tratta del principio di finalità che deve essere a base - come specifica il Garante - di ogni *data retention policy*.

Tuttavia - e del tutto correttamente - il Garante ha inteso specificare nel Provvedimento che le misure in merito alle politiche di conservazione e cancellazione dei dati - per la loro ovvia interferenza con l'esercizio del diritto all'oblio sul quale è intervenuta la recente sentenza della Corte di Giustizia UE - sono state prescritte esclusivamente alla luce dell'art. 11 del Codice e per i soli utenti di Google registrati dotati di account che richiedano la cancellazione e non si applicano comunque al servizio di *web search* di Google inteso quale motore di ricerca Internet (fruibile anche da utenti non registrati ai servizi Google). In altri termini il Garante sottolinea che alcuna misura in merito alle modalità di esercizio e rispetto del diritto all'oblio degli utenti non autenticati è stata volutamente considerata nel Provvedimento, in attesa che il Gruppo dei Garanti europei (che all'uopo si è riunito il 3 Giugno scorso) adotti specifiche Linee Guida per supportare (anche Google) nella corretta implementazione pratica dei principi espressi dalla Corte UE (come è noto, comunque, Google ha già attivato un form *on line* per ricevere le richieste di esercizio del diritto all'oblio: sono state inoltrate più di 70.000 richieste che riguardano 250.000 pagine web e dall'Italia sono giunte 6000 richieste).

Il Garante ha rilevato che Google, in tutti gli atti istruttori, non ha fornito informazioni certe e definitive sulla tempistica di conservazione dei dati degli utenti, specificando solo il tempo di archiviazione della cd. *search history* (indefinitamente o fin quando l'utente stesso non rimuova i dati della cronologia in caso di utenti non registrati e fino a 180 giorni per quelli registrati; 9 mesi per la conservazione degli indirizzi IP prima dell'anonimizzazione e 18 mesi per quella dei cookie). Inoltre,

Google appare non cancellare o anonimizzare mai definitivamente i dati: anche quando rimossi o dissociati dall'account utente, restano nella sua disponibilità per non meglio identificate ragioni di miglioramento dei servizi e per un tempo potenzialmente illimitato.

Sul punto il Garante - richiamando le due modalità di cancellazione dei dati - una relativa all'esaurimento dei termini legittimi di conservazione, l'altra che prende invece in considerazione la scelta (e la conseguente azione positiva, ovvero la richiesta) dell'interessato di ottenere, a determinate condizioni, la cancellazione dei dati personali che lo riguardano (cd. *data deletion policy*) - ha prescritto a Google quanto segue:

- nel caso le informazioni si trovino sui sistemi Google cd. attivi o *live-serving* Google dovrà provvedere alla cancellazione dei dati personali su richiesta dell'interessato autenticato (cioè dotato di account) entro il compimento del 63° giorno decorrente dalla richiesta (e comunque nel periodo preliminare dei primi 30 giorni dalla ricezione della richiesta Google dovrà non cancellare ma solo disattivare i dati a tutela dell'utente, onde a prevenire cancellazioni accidentali o fraudolente dei suoi dati personali);
- qualora, invece, i dati siano stati archiviati nei sistemi di *back-up*, il tempo massimo per procedere alla relativa cancellazione sarà pari a sei mesi dalla richiesta dell'utente autenticato, quantificabili in 180 giorni solari e dunque entro il compimento del 181° giorno. Durante questo periodo la sola operazione consentita sui dati potrà essere il recupero di informazioni perse e tali informazioni dovranno comunque essere protette da accessi non autorizzati mediante utilizzo di idonee tecniche di cifratura o, se del caso, di anonimizzazione dei dati stessi in base a quanto previsto dal Parere dei garanti europei n. 05 del 10 Aprile 2014 *sull'impiego delle tecniche di anonimizzazione*;
- Google dovrà infine adottare una *policy di data retention* conforme al principio di finalità fissato dall'art. 11 del Codice della privacy.

\* \* \* \*

### § 3. Conclusioni: alcuni dubbi e note critiche sul Provvedimento Google.

Una prima conclusione che si può formulare sul Provvedimento riguarda alcuni dubbi sulla sua diretta applicabilità ai sensi delle stesse regole italiane che appunto chiariscono e delimitano l'ambito di applicazione del Codice della privacy. Il Provvedimento, difatti, prescrive un insieme di regole obbligatorie "*a Google Inc., con sede in Mountain View, USA, con specifico riguardo ai trattamenti di dati personali relativi all'utilizzo delle funzionalità offerte per il tramite del sito web [www.google.it](http://www.google.it) e di tutte le altre pagine web in lingua italiana comunque riconducibili alla società*".

Orbene, l'articolo 5 del Codice della privacy (*"Oggetto ed ambito di applicazione"*) dispone – ai primi due commi – che:

1. *Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.*
2. *Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.*

Google Inc. sicuramente tratta e detiene all'estero dati personali *"tramite il sito web [www.google.it](http://www.google.it) e tutte le altre pagine web in lingua italiana"*, ma non è certo un soggetto *"stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato"*. Non avrebbe altrimenti senso la nomina di Google Italy (tra l'altro solo a partire dal 2010) quale proprio rappresentante in Italia ai sensi e per gli effetti dell'art. 5 del Codice *"in relazione all'applicazione del Codice privacy e alla normativa sulla tutela dei dati personali"*. E' difatti lo stesso Garante a ricordare in apertura del Provvedimento la natura dei rapporti tra Google Inc. e Google Italy: Google, per il tramite della propria controllata Google International LLC, ha sottoscritto con la società Google Italy S.r.l. con unico socio, costituita nel 2002 e - soprattutto - dotata di personalità giuridica autonoma, un *"marketing and service agreement"* per la promozione e commercializzazione e vendita di spazi pubblicitari generati sul sito web [www.google.it](http://www.google.it) e su tutte le altre pagine web in lingua italiana comunque riconducibili alla società.

La titolarità dei servizi Google è in capo alla società USA. Ma se alla società USA non è applicabile il Codice della privacy ai sensi dell'art. 5.1 (in quanto titolare del trattamento estero non stabilito sul territorio dello Stato), allora l'unico presupposto è rappresentato dal *"trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea che impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici"*. Se è verificato – appunto ai sensi dell'art. 5.2 del Codice – questo presupposto oggettivo rappresentato dalla presenza di strumenti situati nel territorio dello Stato impiegati per il trattamento, allora il titolare estero non stabilito dovrà procedere alla designazione di *"un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali"*. Ciò che effettivamente ha fatto Google Inc. (designando Google Italy S.r.l.), sia pure a partire dal 2010 (e si tralasciano in tale sede le altre considerazioni che sul punto emergerebbero per il passato).

Il dubbio che sorge è che la stessa Google – proprio nel famoso processo penale subito dai suoi rappresentanti nel noto caso Vivi Down (la pubblicazione su You Tube di un video in cui un ragazzo disabile veniva vessato da alcuni compagni, conclusosi con assoluzione dei dirigenti Google in Cassazione, con la sentenza 3672 del 3 febbraio 2014) – ha provato che nessun dato è trattato in Italia per la fornitura dei propri servizi, in quanto i *server* sono tutti all'estero (Google si avvale di 10 data center dove ospita circa 900 mila servers: 6 sono negli USA, 2 in Europa e 2 in Asia). Ci si chiede allora quali siano e se vi siano gli “strumenti impiegati per il trattamento” situati nel territorio italiano (che dovrebbero inoltre essere – a stretto rigore – gestiti direttamente dal titolare estero non stabilito e non certo dal rappresentante, la cui designazione ha solo l'effetto – diciamo – di “intermediazione” formale nell'applicazione diretta delle regole privacy italiane al titolare estero). In sostanza, può effettivamente sorgere il dubbio – al di là della formalistica nomina da parte di Google Inc. di Google Italy S.r.l. quale rappresentante in Italia a fini privacy – che a disciplina privacy vigente non vi siano i presupposti di applicabilità diretta a Google Inc. di un provvedimento italiano che è tutto incentrato sulla titolarità dei trattamenti in capo a soggetto estero non stabilito nel territorio dello Stato e che appare anche privo di strumenti di gestione propria e diretta impiegati in Italia per il trattamento dei dati degli utenti.

Una seconda nota – piuttosto critica - riguarda ciò che il Provvedimento del Garante non dice. Al di là delle questioni sulla diretta applicabilità a Google Inc. ed anche volendo riconoscere che Google Inc. deve sottoporsi alle prescrizioni dettate dall'Autorità privacy italiana, appare allora poco logico e conseguente che se all'esito dell'istruttoria italiana il Garante ha rilevato (per lo meno a far data dal 1° Marzo 2012, data di entrata in vigore della nuova privacy policy di Google) tra l'altro che:

- a) Google non ha mai richiesto il consenso obbligatorio degli utenti alla profilazione;
- b) Google non ha fornito una informativa idonea sui trattamenti dei dati degli utenti;
- c) Google non rispetta termini di conservazione dei dati raccolti in conformità al Codice della privacy;

lo stesso Garante non abbia proceduto (ne se ne sia riservato – come spesso fa - un successivo approfondimento) a sanzionare Google in via diretta in sede amministrativa (es: art. 161 del Codice per informativa inadeguata) o penale (art. 167 del Codice per trattamento illecito di dati personali a seguito della violazione dell'art. 23 sul consenso), come ad esempio aveva deciso in sede di valutazione del servizio Street View.

Infine, una considerazione conclusiva attiene alla possibilità che - dopo il Provvedimento Google - sia possano aprire analoghe istruttorie sulle *privacy policies* e in generale sui trattamenti svolti da altri colossi del web. Tra i Big Data - ad esempio - un candidato perfetto in tale prospettiva appare Facebook. In una delle ultime *privacy policy* del 2013 Facebook, nel nuovo accordo che fa firmare ai suoi utenti, si ascrive il diritto di usare le informazioni dei profili e le immagini dei suoi iscritti per fare campagne pubblicitarie agli amici senza chiedere alcun consenso agli interessati. Ciò ha ingenerato una nuova battaglia legale (al momento negli USA) avviata dalle sei principali organizzazioni americane che difendono la privacy. I legali delle associazioni hanno infatti inviato una lettera alla *Federal Trade Commission*, l'ente governativo per la protezione dei consumatori, e ai politici degli Stati Uniti sostenendo che i recenti cambiamenti fatti dal colosso dei social network violano i termini di un accordo del 2012 siglato da Facebook con la stessa *Federal Trade Commission*. Secondo le associazioni l'accordo stipulato prevede che Facebook non possa condividere informazioni dei suoi utenti senza chiedere ogni volta il permesso in modo esplicito e senza pagare per l'uso dei dati. Presupposti che, nelle nuove regole, sono invece del tutto assenti.

In ogni caso, al di là delle iniziative formali delle Autorità privacy, deve comunque ritenersi che alcune prescrizioni pratiche sul trattamento dei dati degli utenti che il Garante italiano ha prescritto a Google nel proprio Provvedimento (la cui violazione è sanzionabile con una sanzione da 30 mila a 180 mila Euro) abbiano una portata generale (es: l'informativa multi-livello; le prescrizioni su *data retention* e *data deletion*, etc) e in quanto tale possano ragionevolmente ed analogicamente applicarsi anche ad altri fornitori di analoghi servizi.