doc. web n. 3881513]

Linee guida in materia di trattamento di dati personali per profilazione on line - 19 marzo 2015
(Pubblicato sulla Gazzetta Ufficiale n. 103 del 6 maggio 2015)

Registro dei provvedimenti
n. 161 del 19 marzo 2015

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

VISTA la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

VISTA la direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche;

VISTA la direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori;

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, di seguito Codice);

VISTO il decreto legislativo 9 aprile 2003, n. 70, di "attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico";

VISTO il decreto legislativo 28 maggio 2012, n. 69 "Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori";

VISTA la pronuncia della Corte di Giustizia dell'Unione europea, del 13 maggio 2014, nella causa C-131/12;

VISTO il provvedimento del Garante 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", pubblicato sulla Gazzetta Ufficiale n. 126 del 3 giugno 2014 (in www.garanteprivacy.it; doc. web n. **3118884**);

VISTO il provvedimento del Garante n. 353, del 10 luglio 2014, nei confronti di Google Inc. sulla "conformità al Codice dei trattamenti di dati personali effettuati ai sensi della nuova privacy policy" (doc. web n. **3283078**);

VISTI l'Opinion del WP 29 n. 04/2012 in materia di Cookie Consent Exemption, adottata il 7 giugno 2012, ed il Working Document del medesimo WP 29 n. 02/2013 providing guidance on obtaining consent for cookies, adottato il 2 ottobre 2013 (disponibili rispettivamente ai link **http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf** e **http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf**);

VISTA l'Opinion del WP 29 n. 2/2006 sugli aspetti di tutela della vita privata inerenti ai servizi di screening dei messaggi di posta elettronica adottata il 21 febbraio 2006 e disponibile al link **http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118_it.pdf**;

VISTA l'Opinion del WP 29 n. 10/2004 sulla maggiore armonizzazione della fornitura di informazioni adottata il 25 novembre 2004 e disponibile al link **http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_it.pdf#h2-11**;

VISTA l'Opinion del WP 29 n. 9/2014 sull'applicazione della Direttiva 2002/58/EC al device fingerptinting adottata il 25 novembre 2014 e disponibile al link **http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf** ;

VISTA la comunicazione del WP 29 del 23 settembre 2014 indirizzata a Google Inc. contenente l'indicazione delle possibili misure da implementare per rendere i trattamenti di dati effettuati dalla società conformi al quadro normativo europeo in materia di protezione dei dati personali, disponibile al link **http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy_appendix.pdf**;

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 del 28 giugno 2000;

RELATORE il dott. Antonello Soro;

PREMESSO

1. All'interno dell'attuale società dell'informazione operano diversi fornitori di servizi identificabili ai sensi dell'art. 2, d.lgs. 9 aprile 2003, n. 70, o altrimenti definibili come quei soggetti che comunque offrono servizi on line accessibili al pubblico attraverso reti di comunicazione elettronica.

Occorre innanzitutto considerare che, a differenza di quanto accade per quelli non stabiliti su territorio nazionale, con riguardo ai quali soltanto le più recenti tendenze interpretative espresse dalla Corte di Giustizia dell'Unione europea hanno statuito, al ricorrere di determinate condizioni, la piena applicabilità del quadro normativo in materia di protezione dei dati personali sia europeo sia nazionale, i fornitori dei servizi della società dell'informazione, stabiliti su territorio nazionale, già risultano tenuti, proprio in virtù della diretta applicabilità del principio di stabilimento di cui agli artt. 4 della direttiva 95/46/CE, nonché 5, comma 1, del Codice, al pieno rispetto delle prescrizioni e degli obblighi derivanti dalla menzionata disciplina.

Per questa ragione, considerate anche le esigenze di tutela della competitività all'interno del mercato di riferimento, di uniformità di trattamento tra tutti i soggetti tenuti agli adempimenti di specie, nonché la loro complessità, soprattutto in un settore, quale quello in questione, nel quale le soluzioni adottabili sono funzione anche dei rapidissimi sviluppi delle diverse tecnologie applicabili, l'Autorità si è determinata all'adozione delle presenti "Linee guida in materia di trattamento dati personali per profilazione on line" (di seguito Linee guida) con l'intento di armonizzare, semplificandole, le diverse modalità attraverso le quali è possibile garantire il rispetto dei principi applicabili in materia di protezione dei dati personali nell'espletamento delle attività che caratterizzano la fornitura di servizi on line.

L'Autorità intende cioè fornire, con le presenti Linee guida, regole di condotta uniformi che attuino quei canoni e quei principi di semplificazione i quali costituiscono uno degli obiettivi dell'azione istituzionale del Garante.

2. La gamma dei servizi offerti, sul mercato ed in base alla tecnologia attuale, è certamente ampia.

Le diverse funzionalità cui si fa riferimento possono infatti variare dal motore di ricerca sul web alla posta elettronica, dalle mappe on line alla commercializzazione di spazi pubblicitari, dai social network alla gestione di pagamenti on line, dai negozi virtuali per l'acquisto di applicazioni, musica, film, libri e riviste, alla ricerca, visualizzazione e diffusione di filmati, da servizi di immagazzinamento, condivisione e revisione di testi, a software per la visualizzazione di immagini o per la gestione di agende e calendari, da funzionalità per il controllo e la gestione dei profili dell'utente, all'immagazzinamento (servizi cloud/storage), a strumenti di analisi statistica e di monitoraggio dei visitatori di siti web e così via.

Si tratta, per lo più, di funzionalità offerte a titolo gratuito agli utenti finali, dal momento che il modello imprenditoriale delle società coinvolte nella prestazione di tali servizi si fonda spesso su modelli di business che valorizzano gli introiti ad esse derivanti dalla pubblicità.

In un numero considerevole di casi, i dati raccolti vengono utilizzati per finalità di profilazione, cioè per l'analisi e l'elaborazione di informazioni relative a utenti o clienti, al fine di suddividere gli interessati in "profili", ovvero in gruppi omogenei per comportamenti o caratteristiche sempre più specifici, con l'obiettivo di pervenire all'identificazione inequivoca del singolo utente (cd. single out) ovvero del terminale e, per il suo tramite, anche del profilo, appunto, di uno o più utilizzatori di quel dispositivo.

La menzionata categorizzazione è generalmente strumentale sia alla messa a disposizione di servizi sempre più mirati e conformati sulle specifiche esigenze dell'utente, sia alla fornitura di pubblicità personalizzata, che pertanto abbia un grado di probabilità di successo (ma, al tempo stesso, anche un livello di pervasività) molto più elevati rispetto a messaggi promozionali generici, sia all'analisi e monitoraggio dei comportamenti dei visitatori dei siti web, sia allo sfruttamento commerciale dei profili ottenuti, i quali possono avere un significativo valore di mercato in ragione della loro capacità di fornire indicazioni sulle propensioni al consumo di beni e servizi.

Gli utenti delle funzionalità prese in considerazione possono essere distinti a seconda che dispongano di un account creato a seguito di una procedura di registrazione per l'accesso "autenticato" ai servizi (cd. utenti autenticati, ad esempio per il servizio di posta elettronica), ovvero che utilizzino le medesime funzionalità in assenza di previa autenticazione (cd. utenti non autenticati).

Le indagini di carattere istruttorio condotte dall'Ufficio, nonché il quadro complessivo oggetto di approfondimento, hanno consentito di identificare diversi ambiti, con riferimento ai quali pare opportuno richiamare i soggetti coinvolti - sia quelli già presenti ed operanti sul mercato, sia quelli che intendano intraprendere un'attività di trattamento dati connessa alla fornitura di servizi on line - ad un puntuale rispetto delle disposizioni di legge in materia di trattamento dei dati, pur considerate le specificità dei contesti nei quali tali soggetti operano e, dunque, prendendo in considerazione possibili, particolari modalità idonee a garantire la necessaria tutela degli utenti.

Tra essi:

A) modalità e contenuto dell'informativa resa agli interessati, anche in relazione all'esplicitazione delle diverse finalità e alle modalità del trattamento dei loro dati personali (art. 13 del Codice);

B) richiesta del consenso degli interessati per finalità di profilazione, nonché rispetto del diritto di opposizione degli interessati (artt. 7, 23, 24 e 122 del Codice).

La profilazione in questione può essere effettuata essenzialmente 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;

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) ad eccezione dell'utilizzo dei cookie (per i quali si fa espresso richiamo, oltre alla disciplina di legge, alle prescrizioni rese dall'Autorità con il 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", in Gazzetta Ufficiale n. 126 del 3 Giugno 2014), utilizzo di 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);

C) rispetto del principio di finalità nella conservazione dei dati personali degli utenti (art. 11, comma 1, lett. e), del Codice).

3. Quanto alla lettera A) del paragrafo che precede, relativa agli obblighi di cui all'art. 13 del Codice, l'Autorità intende porre l'accento sulla circostanza che l'informativa che deve essere resa agli utenti, e dunque la loro preventiva consapevolezza circa i possibili impieghi delle informazioni loro riferibili, costituisce l'ineludibile presupposto per consentire agli interessati medesimi di esprimere o meno il proprio consenso ai trattamenti di dati che li riguardano, a seguito della necessaria e personale valutazione sull'impatto che tali trattamenti potranno avere sul proprio diritto alla protezione dei dati personali.

È opportuno pertanto ricordare a tutti i soggetti titolari che costituisce un preciso obbligo ed una condizione necessaria di conformità alla disciplina di legge garantire che l'informativa da rendere ai propri utenti sia facilmente accessibile, ad esempio con un solo click dalla pagina del dominio cui l'utente accede, formulata in modo chiaro, completo ed esaustivo.

Al pari è necessario che, a fronte di eventuali aggiornamenti o modifiche di tale documento, gli interessati siano posti nella condizione di comprendere e valutare i cambiamenti apportati, anche mediante raffronto tra le diverse versioni dell'informativa eventualmente susseguitesi nel tempo.

Al riguardo, e con particolare riferimento ai requisiti di accessibilità ed efficacia dell'informativa, i soggetti tenuti potranno conformarsi alle raccomandazioni espresse dal WP 29 nell'Opinion n. 10/2004 sulla maggiore armonizzazione della fornitura di informazioni, adottata il 25 novembre 2004, e strutturarla su più livelli, in quanto: "Le avvertenze multistrato possono contribuire a migliorare la qualità delle informazioni sulla tutela dei dati; ciascuno strato privilegia le informazioni necessarie alla persona per capire la propria posizione e assumere decisioni. In caso di spazio/tempo di comunicazione limitato, i formati multistrato possono migliorare la leggibilità delle avvertenze".

È bene tuttavia precisare che una tale architettura dovrebbe essere comunque configurata evitando un'eccessiva frammentazione in un numero troppo elevato di livelli, pena la dispersione delle informazioni rese che ovviamente ne comprometterebbe la fruibilità. Nel caso, pertanto, in cui venga utilizzata una struttura dell'informativa su più livelli, il Garante ritiene opportuno che le informazioni siano distribuite in accordo con il seguente criterio:

- un primo livello immediatamente accessibile (con un solo click dalla pagina visitata) all'interno del quale ospitare tutte le informazioni di carattere generale di maggiore importanza per gli utenti, relative tra l'altro ai trattamenti di dati personali effettuati, alle tipologie di dati personali oggetto di trattamento, anche per categorie (ad es., se del caso, 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 ed ai relativi estremi identificativi, nonché l'indicazione degli eventuali responsabili e di un indirizzo presso cui gli utenti possano esercitare in modo agevole i propri diritti.

In questo primo livello di informativa è inoltre necessario sia riportata almeno l'indicazione della finalità di profilazione perseguita, a seconda dei casi, attraverso le diverse modalità utilizzate dal titolare.
In linea con l'indicazione della menzionata finalità di profilazione e delle modalità attraverso cui il titolare la persegue, il primo livello dovrà inoltre indicare dettagliatamente le modalità di acquisizione del consenso al trattamento, ove necessario. Sul punto si tornerà nel prosieguo.

- Il secondo livello, accessibile dal primo, può essere invece destinato a contenere l'informativa relativa alle specifiche funzionalità ovvero diversi esempi per chiarire le modalità del trattamento delle informazioni personali. In questo secondo livello potrebbero anche essere archiviate le eventuali precedenti versioni dell'informativa, 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.

Le regole che determinano l'efficacia e la correttezza dell'informativa resa all'utente devono applicarsi in modo identico per ciascun tipo di terminale (mobile, tablet, desktop computer, dispositivi portatili e TV plug-in) e per ogni applicazione resa disponibile agli utenti.

4. Quanto alla lettera B) del paragrafo 2, è necessario preliminarmente richiamare il principio di carattere generale di cui all'art. 23 del Codice, ai sensi del quale "Il trattamento di dati personali da parte di privati … è ammesso solo con il consenso espresso dell'interessato"; inoltre tale consenso è valido solo "se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13". Il successivo art. 24 disciplina, poi, una serie di presupposti considerati equipollenti al consenso, al ricorrere dei quali il trattamento può essere pertanto effettuato anche in assenza di esso. Tra questi, a titolo esemplificativo,

l'adempimento di obblighi di legge, l'esecuzione di obblighi contrattuali, il perseguimento di un legittimo interesse del titolare o di un terzo destinatario dei dati etc.

La portata generale di questo principio trova poi specificazione nella disposizione dell'art. 122 contenuto nella parte speciale del Codice, ai sensi del quale "L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con le modalità semplificate di cui all'articolo 13, comma 3. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio".

4.1. Se si esamina la specifica attività di fornitura del servizio di posta elettronica per l'inoltro e la ricezione di messaggi, di cui al caso a), lettera B), del paragrafo 2) che precede, se ne trae che i fornitori di tale funzionalità effettuano attività di trattamento, in modalità automatizzata, dei dati personali degli utenti autenticati che utilizzano il servizio; e ciò per il conseguimento di diverse finalità. Alcune di esse, anche di carattere strettamente tecnico, sono direttamente riconducibili alla fornitura del servizio in questione secondo specifiche modalità, quali 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 questo caso, il trattamento dei dati degli interessati per le richiamate finalità - effettuato verosimilmente in modo automatizzato e dunque senza alcun intervento umano -, come pure per salvaguardare la sicurezza dei servizi offerti all'utente, è, ai sensi delle direttive 95/46/CE e 2002/58/CE prima, e del Codice poi, sottratto all'obbligo della preventiva acquisizione del consenso, dal momento che rientra nell'ipotesi di deroga che attiene l'esecuzione di obblighi derivanti dal contratto di fornitura del servizio di posta elettronica.

Per il conseguimento, invece, di eventuali finalità di profilazione, 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, è invece necessario che i titolari provvedano ad acquisire il preventivo ed informato consenso dei propri utenti.

A tale riguardo, si richiamano anche le conclusioni del WP 29 nel parere n. 2/2006 sugli aspetti della vita privata inerenti ai servizi di screening dei messaggi di posta elettronica, del 21 febbraio 2006 che, nell'indagare proprio il delicato bilanciamento tra le esigenze di tutela della riservatezza delle comunicazioni e quelle della fornitura di servizi connessi all'utilizzo della posta elettronica, ed in linea con il dichiarato obiettivo di "promuovere tecnologie che integrino i requisiti di protezione dei dati e tutela della privacy nella realizzazione di infrastrutture e sistemi di informazione, ivi comprese le apparecchiatura terminali", ha espressamente invitato gli operatori del settore a "progettare e mettere a punto sistemi rispettosi della vita privata, riducendo al minimo il trattamento di dati personali e limitandolo a quanto strettamente necessario e proporzionato alle finalità del trattamento". Nella medesima Opinion il Gruppo si è, peraltro, espresso anche in ordine alla possibilità di ricercare una linea di demarcazione tra le attività di trattamento dei dati effettuate per finalità di gestione del servizio o di sicurezza delle reti, che non necessitano di essere preventivamente autorizzate dall'interessato, e quelle tese invece al conseguimento di finalità ulteriori, stabilendo peraltro che quando il trattamento non trova legittimazione nella necessità del provider di salvaguardare la sicurezza del servizio, in forza dell'art. 5, paragrafo 1 della direttiva e-privacy, deve intendersi fatto divieto ai provider di procedere in altre operazioni del trattamento "senza il consenso degli utenti".

Così delineato il quadro giuridico di riferimento se ne induce allora che, per le attività di profilazione 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, è necessario, lo si ribadisce, che il titolare ne acquisisca il preventivo ed informato consenso.

Con riferimento all'utilizzo della specifica funzionalità di posta elettronica, l'Autorità si riserva comunque l'adozione di ogni iniziativa ritenuta opportuna a tutela degli interessati.

4.2. Con riguardo a quanto indicato sub b), lettera B) del paragrafo 2) che precede, occorre considerare la possibilità che i titolari procedano all'incrocio dei dati personali degli interessati anche relativi all'utilizzo di più funzionalità diverse tra quelle messe a disposizione.

Anche tale condotta deve essere valutata alla luce del quadro giuridico di riferimento e, in questa prospettiva, deve essere chiarito che le operazioni di trattamento tese alla profilazione dell'utente realizzate anche attraverso l'incrocio di dati raccolti in relazione a funzionalità diverse, non rientrando in alcuno dei casi di esonero dall'obbligo di acquisizione del consenso di cui all'art. 24 del Codice, possono essere effettuate soltanto previa espressa manifestazione di volontà dell'utente stesso.

Né è sufficiente, a tal fine, la sola menzione di questa finalità tra quelle oggetto dell'informativa resa agli interessati per esimere i titolari dall'obbligo di acquisirne un valido consenso.

4.3. Con riferimento, poi, alle attività poste in essere dai titolari e richiamate sub c), lettera B), del paragrafo 2) che precede (utilizzo di altri identificatori diversi dai cookie quali credenziali di autenticazione, fingerprinting etc.), si osserva che il ricorso

a tali tecniche di identificazione si basa sul trattamento, da parte dei titolari, 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 del terminale (cd. single out) e, per il suo tramite, anche del profilo di uno o più utilizzatori di quel dispositivo. Tale tecnica, denominata fingerprinting, utilizzata per il conseguimento delle medesime finalità di profilazione, risulta anch'essa disciplinata, al pari dell'impiego dei cookie, dall'art. 122 del Codice; con ogni riflesso in ordine all'obbligo di acquisizione del consenso preventivo dell'interessato, tranne i casi di esenzione previsti (nella specie, trasmissione di una comunicazione su una rete di comunicazione elettronica o erogazione del servizio su richiesta dell'utente).

La sola differenza apprezzabile, sulla quale l'Autorità intende comunque porre l'accento, tra l'impiego dei cookie e del fingerprinting, consiste nel fatto che mentre nel primo caso 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 definitiva, appare allora evidente che, affinché i trattamenti di dati effettuati per finalità di profilazione, anche realizzata con diverse modalità, soddisfino i requisiti degli artt. 23, 24 e 122 del Codice, è necessario il consenso dell'interessato. Tale consenso deve inoltre rispondere, ai fini della sua validità, ai requisiti di legge e pertanto 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 al pari necessario, in tal senso, che la sua espressione costituisca una inequivoca manifestazione di volontà da parte dell'interessato.

5. I destinatari del presente provvedimento, nella loro autonomia imprenditoriale e nella qualifica di titolari del trattamento cui competono, tra l'altro, proprio "le decisioni in ordine alle … modalità del trattamento di dati personali" (art. 4, comma 1, lett. f) del Codice), possono scegliere in ordine ai criteri ed alle misure da adottare per assicurare la necessaria conformità alla legge dei trattamenti di dati degli utenti volti alla loro profilazione, comunque effettuata.

Considerata tuttavia la specificità dei servizi offerti da tali soggetti, il Garante propone comunque, anche in linea con le richiamate finalità di semplificazione, una soluzione di acquisizione del consenso on line idonea a soddisfare i menzionati requisiti previsti dalle disposizioni vigenti, segnatamente dagli artt. 7, 23 e 122 del Codice, sul presupposto naturalmente che tale consenso non sia stato già altrimenti acquisito sulla base di modalità più tradizionali (ad es. coupon, form on line, moduli cartacei etc.).

In questa prospettiva, si ritiene che debba necessariamente sussistere uno stadio ovvero un momento, nel corso dell'esperienza di navigazione dell'utente e ovviamente preliminare rispetto alla fruizione delle funzionalità, nel quale gli sia appunto consentito scegliere tra più, diverse alternative.

Considerata d'altro canto la distinzione, richiamata in premessa, tra utenti autenticati e non autenticati, le forme di acquisizione di tale consenso potranno, di riflesso, essere diversificate proprio in relazione alla tipologia di utente considerata.

5.1. In tal senso, con specifico riguardo agli utenti non autenticati, occorre indagare se in un determinato momento della fruizione di una o più diverse funzionalità esista uno spazio, fisico ovvero virtuale, idoneo a consentire loro, da un lato, di esprimere un eventuale consenso al trattamento come più sopra identificato; dall'altro e allo stesso tempo al titolare di prendere atto e tenere traccia delle scelte manifestate.

In caso di risposta negativa, sarà dunque necessario che il titolare implementi un tale meccanismo, ad esempio facendo sì che l'utente non autenticato, accedendo alla home page (o ad altra pagina) del sito web, visualizzi immediatamente in primo piano un'area di idonee dimensioni, ossia di dimensioni tali da costituire una percettibile discontinuità nella fruizione dei contenuti della pagina web che sta visitando, contenente almeno le seguenti indicazioni:

i) che il sito effettua attività di trattamento dei dati per finalità di profilazione mediante trattamento dei dati personali degli utenti secondo le specifiche modalità prescelte (ad es. tramite incrocio dei dati tra funzionalità diverse ovvero utilizzando altri identificatori diversi dai cookie 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 o anche, per gli utenti autenticati, in relazione all'utilizzo del servizio per l'inoltro e la ricezione di messaggi di posta elettronica etc.);

ii) il link all'informativa, ove vengono fornite tutte le indicazioni di cui al paragrafo 3);

iii) il link ad una ulteriore area dedicata nella quale sia possibile negare il consenso alla profilazione ovvero, se del caso, 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;

iv) 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.

La menzionata area deve essere parte integrante di un meccanismo idoneo a consentire l'espressione di una azione positiva nella quale si sostanzia la manifestazione del consenso dell'interessato. In altre parole, essa deve determinare una discontinuità, seppur minima, dell'esperienza di navigazione: il superamento della presenza dell'area visualizzata deve cioè essere possibile solo mediante un intervento attivo dell'utente (appunto attraverso la selezione di un elemento contenuto nella pagina sottostante l'area stessa).

Ed è di tutta evidenza che, sia da un punto di vista giuridico, sia da un punto di vista tecnico, non sarà possibile attribuire il medesimo significato né all'azione, alternativa, che si sostanzia nell'accesso all'ulteriore area nella quale modulare le scelte né alla selezione, per il tramite dell'apposito link, della pagina che contiene l'informativa.

È opportuno sottolineare che ciascuna delle possibili azioni nella disponibilità dell'utente genera uno specifico evento informatico il quale, per le descritte caratteristiche, è dunque inequivocamente riconoscibile dal fornitore del servizio che può pertanto agevolmente tenerne traccia.

Nel caso l'utente abbia acconsentito all'utilizzo dei propri dati per la finalità esplicitata, tale operazione soddisferà allora pienamente il requisito dell'art. 23 del Codice il quale esige che l'avvenuto consenso sia "documentato per iscritto".

La presenza di tale "documentazione" dell'avvenuta acquisizione del consenso dell'interessato consentirà poi al fornitore di servizi di non riproporre alcuna forma di discontinuità nella navigazione alle ulteriori visite dell'utente, che utilizzi il medesimo terminale, sul ovvero sui domini nella propria titolarità, ferma restando naturalmente la possibilità per quest'ultimo di negare il consenso e/o modificare, in ogni momento e in maniera agevole, le proprie opzioni (cfr. art. 7, comma 4, del Codice). Per consentire, proprio, l'effettività di tale diritto di autodeterminazione, è allora altresì necessario che tutte le pagine web eventualmente riconducibili al titolare rechino un collegamento all'area dedicata all'interno della quale l'utente potrà esercitare compiutamente i propri diritti.

Nel caso in cui, invece, l'utente si sia limitato a selezionare il collegamento all'informativa, proprio per ricevere maggiori informazioni al fine di compiere scelte ancor più consapevoli, il meccanismo in discussione gli dovrà essere riproposto alla prima azione successiva a tale presa visione, per consentirgli di esprimere il proprio consenso o diniego al trattamento.

Qualora, infine, abbia scelto di accedere all'area dedicata all'eventuale modulazione delle scelte, poiché anche questa azione, al pari della selezione del link all'informativa - lo si è anticipato - non equivale ancora a consenso, il fornitore dovrà registrarla, integrando poi questa informazione con quelle, ulteriori, relative alle specifiche scelte poste in essere dall'utente, anche in modo dettagliatamente analitico.

Per realizzare il tracciamento delle azioni e delle scelte, anche di dettaglio (espressione ovvero negazione, in tutto o in parte, del consenso, come pure esercizio del diritto di opposizione alla profilazione) rimesse all'interessato, il titolare potrebbe avvalersi o di appositi cookie tecnici (in tal senso, si veda anche il considerando 25 della direttiva 2002/58/CE), oppure di altri identificatori diversi dai cookie.

Con l'ovvia, ulteriore avvertenza tuttavia che, qualora la menzionata "documentazione" sia stata effettuata mediante utilizzo di cookie, se l'utente scegliesse, come è nella sua disponibilità, di rimuovere tutti quelli installati sul proprio dispositivo, incluso il menzionato marcatore "tecnico", poiché questa operazione, non coinvolgendo il titolare, non equivale all'esercizio del diritto di opposizione, questi dovrebbe nuovamente, anche in questo caso, far ricorso al meccanismo di acquisizione del consenso sopra rappresentato.

Qualora, invece, ci si sia avvalsi di altri identificatori diversi dai cookie, e dunque non archiviati all'interno del dispositivo nella disponibilità dell'utente, bensì presso i server nella disponibilità del fornitore, al mutare delle preferenze espresse dall'interessato, essenzialmente sempre revocabili, non si dovrà fare ulteriormente ricorso al meccanismo di riproposizione della discontinuità, bensì procedere all'aggiornamento, proprio, delle indicazioni già registrate.

5.2. Il meccanismo descritto intende realizzare uno spazio fisico ovvero virtuale deputato alla raccolta ed alla gestione del consenso degli utenti non autenticati.

Anche agli utenti autenticati dovranno, naturalmente, essere garantite le stesse tutele; ed è opportuno che, con l'obiettivo di assicurare la medesima fruibilità dell'esperienza di navigazione (user experience), coloro che dispongono di un account ovvero siano già registrati come utenti dei servizi di uno specifico fornitore siano posti nella condizione di utilizzare i meccanismi di espressione, negazione e revoca del consenso già descritti a proposito degli utenti non autenticati. Le principali differenze tra le menzionate tipologie di interessati consistono nella diretta ovvero indiretta riconducibilità delle scelte effettuate a soggetti appartenenti all'una ovvero all'altra categoria, essendo l'utente autenticato, per così dire, già pienamente identificato in re ipsa, nonché nella possibilità di fruire di tutti o solo di alcuni dei servizi offerti, considerato che appunto alcuni di essi (ad esempio la posta elettronica) sono necessariamente riservati in via esclusiva agli utenti che dispongono di uno specifico account.

Occorre considerare inoltre che anche gli utenti autenticati - sia chi si accinga a creare un nuovo account sia chi già ne disponga e si appresti, nella prima sessione utile, a fruire delle funzionalità mediante autenticazione e relativa digitazione delle proprie credenziali - devono necessariamente attraversare una fase della navigazione nella quale, appunto preliminarmente rispetto alla creazione dell'account oppure all'accesso autenticato alle funzionalità, non sono ancora riconoscibili dal sistema. Pare allora opportuno che, appunto in tale fase preliminare, ad essi, al pari dei non autenticati, venga proposto il medesimo meccanismo di acquisizione del consenso come sopra ipotizzato; con la differenza, tuttavia, che se tali utenti accettano di proseguire nella navigazione e dunque esprimono il proprio consenso superando la discontinuità artificialmente indotta per approdare, alternativamente, o alla pagina di creazione dell'account (per i nuovi autenticati) ovvero a quella nella quale viene visualizzata la schermata in cui digitare le credenziali di autenticazione (per

quelli che già dispongono di un account), questa fase della navigazione, che è il momento tipico nel quale il sistema è in grado, in modo diretto ed inequivoco, di attribuire comportamenti e scelte a soggetti determinati, non venga gravata di ulteriori complessità.

Anche in linea con il principio di finalità disciplinato dal Codice, si ritiene pertanto che nella delineata situazione l'ulteriore passaggio oggetto di descrizione, configurandosi come specificazione del precedente, possa essere gestito annettendo prioritaria rilevanza alle scelte già consapevolmente manifestate dall'utente non autenticato e dunque estendendo la validità di quelle stesse volontà anche al momento, logicamente e cronologicamente successivo, nel quale questi subisca un mutamento di status, da non autenticato ad autenticato; alla duplice, rigorosa condizione, tuttavia, che da un lato l'utente sia reso pienamente edotto della modalità, come indicata, di conferma delle manifestazioni di volontà già espresse in qualità di utente non autenticato e del fatto che, essendo talune funzionalità riferibili esclusivamente ad un utente autenticato, le relative scelte sono dunque nell'esclusiva disponibilità di quest'ultimo. Dall'altro lato, che gli siano sempre pienamente garantiti sia il diritto di revoca (del consenso o del diniego espressi in precedenza) sia quello di integrare le proprie preferenze anche con riguardo alle funzionalità fruibili solo da un utente autenticato (ad esempio, la posta elettronica); e ciò mediante la predisposizione di apposito e ben visibile link all'area dedicata in cui esercitare tali diritti, anche in maniera esaustivamente analitica; includendo, pertanto, in tale area anche l'elencazione delle funzionalità che, essendo appunto utilizzabili solo previa sottoscrizione dell'account, possono costituire oggetto della scelta del solo utente autenticato.

Resta inteso che le scelte in ordine al trattamento dei propri dati per finalità di profilazione espresse da un utente non autenticato, proprio perché non riconducibili ad un account, avranno validità esclusivamente con riferimento allo specifico dispositivo utilizzato, tanto nella prima quanto nelle successive sessioni, fino ad una eventuale revoca; non altrettanto può dirsi, invece, per la manifestazione di volontà espressa dall'utente autenticato, la quale, per l'essenziale, menzionata caratteristica di diretta riconducibilità delle scelte ad un soggetto individuato in re ipsa, è destinata ad estendere la propria validità anche nell'ipotesi nella quale l'utente autenticato fruisca delle funzionalità e dei servizi mediante utilizzo di più, diversi dispositivi.

In altri termini, mentre la documentazione delle scelte espresse dall'utente non autenticato è efficace soltanto con riferimento al dispositivo utilizzato, quella relativa alle scelte di chi dispone di un account permane, anche se tale utente faccia uso di più di un dispositivo.

Pur ribadendo la facoltà per i fornitori di adottare la procedura tecnica che ritengono preferibile per assicurare la conformità dei trattamenti di dati personali effettuati alla disciplina applicabile, l'Autorità ritiene, anche tenute presenti le più volte richiamate esigenze di semplificazione, che la soluzione illustrata sia qualificabile come quella che presenta, a tecnologia vigente su internet, il minor livello di discontinuità nell'esperienza di navigazione dell'utente.

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi dell'art. 154, comma 1, lett. h), del Codice, delibera di adottare le presenti Linee guida affinché tutti i fornitori dei servizi della società dell'informazione di cui all'art. 2, decreto legislativo 9 aprile 2003, n. 70, nonché tutti i soggetti che comunque offrono ai propri utenti servizi on line accessibili al pubblico attraverso reti di comunicazione elettronica, con specifico riguardo ai trattamenti di dati personali relativi all'utilizzo delle funzionalità offerte, tengano conto delle indicazioni e delle semplificazioni illustrate; segnatamente, per quanto concerne:

- l'informativa agli interessati di cui all'art. 13 del Codice (secondo quanto indicato al paragrafo 3 delle presenti Linee guida);

- il consenso preventivo degli utenti, sia autenticati che non autenticati, in relazione al trattamento, per finalità di profilazione on line, delle informazioni che li riguardano, anche derivanti, a seconda dei casi, dal 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, tramite incrocio dei dati personali raccolti in relazione alla fornitura ed al relativo utilizzo di più funzionalità tra quelle messe a disposizione, nonché per l'utilizzo di altri identificativi diversi dai cookie, ai sensi degli artt. 23 e 122 del Codice (secondo i criteri e le modalità indicate al paragrafo 4);

- il rispetto del diritto di opposizione di cui all'art. 7 del Codice;

- l'adozione di una policy di data retention conforme al principio di finalità di cui all'art. 11 del Codice.

Si dispone la trasmissione di copia delle presenti Linee guida al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la loro pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 19 marzo 2015

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia