

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DELIBERA 10 giugno 2021.

Linee guida cookie e altri strumenti di tracciamento.
(Provvedimento n. 231).

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzone, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il dott. Fabio Mattei, segretario generale;

Vista la direttiva 2002/21/CE del 7 marzo 2002, del Parlamento europeo e del Consiglio, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (c.d. direttiva quadro), come successivamente modificata e integrata;

Vista la direttiva 2002/58/CE del 12 luglio 2002, del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (c.d. direttiva *ePrivacy*), come modificata dalla direttiva 2009/136/CE del 25 novembre 2009, del Parlamento europeo e del Consiglio;

Visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

Visto il Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al citato regolamento;

Visto il decreto legislativo 28 maggio 2012, n. 69 recante «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»;

Visti il parere del Gruppo di lavoro «art. 29» (di seguito WP29) n. 04/2012 in materia di *Cookie Consent Exemption*, adottato il 7 giugno 2012, ed il *Working Document* del medesimo WP29 n. 02/2013 *providing guidance on obtaining consent for cookies*, adottato il 2 ottobre 2013, nonché le linee guida del WP29 sul consenso ai sensi del regolamento (UE) 2016/679 adottate il 10 aprile 2018, ratificate dal Comitato europeo per la Protezione dei dati personali (di seguito, EDPB) il 25 maggio 2018 e sostituite, da ultimo, dalle *Guidelines 05/2020 on consent under Regulation 2016/679* adottate il 4 maggio 2020;

Visto il parere dell'EDPB n. 05/2019 del 12 marzo 2019 sulle interrelazioni tra la direttiva *e-Privacy* ed il regolamento, con particolare riguardo alle competenze, ai compiti ed ai poteri delle autorità di protezione dati;

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 nella *Gazzetta Ufficiale* della Repubblica italiana - Serie generale del 3 giugno 2014, n. 126, del 3 giugno 2014;

Viste le FAQ in materia di informativa e consenso per l'uso dei *cookie* del 3 dicembre 2014 ed i «Chiarimenti in merito all'attuazione della normativa in materia di *cookie*» del 5 giugno 2015, pubblicati dall'autorità nel proprio sito web www.Garanteprivacy.it

Visto il provvedimento del Garante n. 161, del 19 marzo 2015, recante le «linee guida in materia di trattamento di dati personali per profilazione *on-line*», pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana - Serie generale, n. 103 del 6 giugno 2015;

Vista la deliberazione del Garante n. 255 del 26 novembre 2020 (doc.web n. 9498472) con la quale è stato adottato uno schema di «linee guida sull'utilizzo di *cookie* e altri strumenti di tracciamento» (allegato 1, doc. web 9501061) nonché l'unità scheda di sintesi (allegato 2, doc. web 9501097), con contestuale avvio, mediante pubblicazione del relativo avviso nella *Gazzetta Uffi-*



ziale della Repubblica italiana - Serie generale, n. 307 dell'11 dicembre 2020, di una consultazione pubblica sulle misure ivi indicate;

Visti gli esiti di tale consultazione pubblica, tesa ad «acquisire osservazioni e proposte riguardo alle predette linee guida»;

Considerati, in particolare, i contributi pervenuti, nel previsto termine di trenta giorni, da diverse associazioni di categoria, dagli operatori e da soggetti appartenenti al mondo imprenditoriale, da associazioni di consumatori, rappresentanti dell'accademia e singoli interessati;

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 l'avv. Guido Scorza;

Premesso

1. Considerazioni preliminari

Le presenti linee guida hanno innanzitutto una funzione ricognitiva in relazione al diritto applicabile alle operazioni di lettura e di scrittura all'interno del terminale di un utente, con specifico riferimento all'utilizzo di *cookie* e di altri strumenti di tracciamento, nonché l'obiettivo di specificare, al riguardo, le corrette modalità per la fornitura dell'informativa e per l'acquisizione del consenso *on-line* degli interessati, ove necessario, alla luce della piena applicazione del regolamento (UE) 2016/679 (di seguito, regolamento).

Il quadro giuridico di riferimento è infatti, ad oggi, costituito tanto dalle disposizioni della direttiva 2002/58/CE (c.d. direttiva *ePrivacy*) e successive modifiche, come recepita nell'ordinamento nazionale all'art. 122 del decreto legislativo 30 giugno 2003, n. 196 (di seguito codice), quanto dal regolamento, per ciò che concerne specificamente la nozione di consenso di cui agli artt. 4, punto 11) e 7 e al considerando 32, come da ultimo interpretati dalle linee guida del WP29 adottate il 10 aprile 2018, ratificate dal Comitato europeo per la Protezione dei dati personali (di seguito, EDPB) il 25 maggio 2018 e sostituite, da ultimo, dalle *Guidelines 05/2020 on consent under Regulation 2016/679* adottate il 4 maggio 2020.

In proposito il Garante, come è noto, ha già adottato un provvedimento (n. 229, dell'8 maggio 2014), volto ad «individuare le modalità semplificate per rendere l'informativa online agli utenti sull'archiviazione dei c.d. *cookie* sui loro terminali da parte dei siti internet visitati», come pure a «fornire idonee indicazioni sulle modalità con le quali procedere all'acquisizione del consenso degli stessi, laddove richiesto dalla legge», le cui indicazioni necessitano ora di essere integrate e precisate, in particolare con riferimento a taluni, specifici aspetti (al fine di agevolare i titolari del trattamento nella corretta applicazione del citato quadro regolamentare come specificato dal richiamato provvedimento del maggio 2014 e dalle presenti linee guida, si allega a queste ultime una tabella riassuntiva delle indicazioni contenute in entrambi i provvedimenti).

Da un lato deve essere infatti considerato che il regolamento, come precisato all'art. 95, «non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE», la quale espressamente prevede, all'art. 1, paragrafo 2, che «le disposizioni della presente direttiva precisano e integrano [il regolamento (EU) 2016/679] ...».

D'altro canto, non può essere sottovalutato come il regolamento abbia inteso ampliare e rafforzare il potere dispositivo e di controllo della persona riguardo al trattamento delle sue informazioni personali, in particolar modo integrando la definizione di consenso contenuta nella precedente direttiva 95/46/CE, chiarendo che la manifestazione di volontà dell'interessato al trattamento dei suoi dati personali deve essere, oltre che - come appunto già nel vigore della direttiva - libera, specifica ed informata, anche «inequivocabile» (1) ma pure esigendo che l'obiettivo della concreta ed efficace attuazione dei principi di protezione dati venga conseguito sin dalla progettazione e attraverso impostazioni predefinite (*cd. privacy by design e by default*).

L'esigenza di un nuovo intervento del Garante è dovuta al lungo intervallo di tempo trascorso, alle novità normative frattanto intervenute e al monitoraggio che, anche per il tramite dei numerosi reclami, segnalazioni e richieste di pareri, l'autorità ha effettuato sulla concreta e talvolta non corretta implementazione delle regole menzionate - in particolare considerando gli effetti riscontrabili sull'esperienza di navigazione, sui diritti e sulle tutele degli interessati, come pure sulla operatività delle imprese e dei fornitori di servizi di comunicazione elettronica - nonché alla sempre crescente diffusione di nuove tecnologie caratterizzate da crescenti livelli di potenziali pervasività.

Infine, deve essere tenuta in considerazione l'evoluzione comportamentale degli stessi utenti della rete, sempre più orientati alla moltiplicazione delle proprie identità digitali come risultanti dall'accesso a plurimi servizi e funzioni disponibili e, in primo luogo, ai *social network*. Tale fenomeno comporta infatti il rischio che le informazioni personali oggetto di trattamento siano raccolte proprio incrociando i dati anche relativi all'utilizzo di funzionalità e servizi diversi, ai quali è possibile accedere utilizzando molteplici terminali (*cd. enrichment*), con l'effetto della creazione di profili sempre più specifici e dettagliati. Si impone, di conseguenza, la necessità di un quadro rafforzato di tutele maggiormente orientate a favorire e a rendere effettivo il controllo sulle informazioni personali oggetto di trattamento e, in definitiva, la capacità di autodeterminazione del singolo.

(1) V. considerando 32 del regolamento e il raffronto tra l'art. 2, lettera h) della direttiva 95/46/Ce e l'art. 4, punto 11) del regolamento)



2. La funzione dei *cookie*

Il considerando 30 del regolamento espressamente afferma che «Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (*cookies*) o identificativi di altro tipo, quali i *tag* di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai *server*, possono essere utilizzate per creare profili delle persone fisiche e identificarle».

Come è noto, i *cookie* sono di regola stringhe di testo che i siti *web* (cd. *Publisher*, o «prime parti») visitati dall'utente ovvero siti o *web server* diversi (cd. «terze parti») posizionano ed archiviano - direttamente, nel caso dei *publisher* e indirettamente, cioè per il tramite di questi ultimi, nel caso delle «terze parti» - all'interno di un dispositivo terminale nella disponibilità dell'utente medesimo.

I terminali cui ci si riferisce sono, ad esempio, un computer, un tablet, uno smartphone, ovvero ogni altro dispositivo in grado di archiviare informazioni. Già oggi, e ancor più in futuro, tra essi occorre annoverare anche i cd. dispositivi IoT (*Internet of Things*, o *Internet* delle cose), i quali sono progettati per connettersi alla rete e tra loro per fornire servizi di varia natura, non necessariamente limitati alla mera comunicazione.

I *software* per la navigazione in internet e il funzionamento di questi dispositivi, ad esempio i *browser*, possono memorizzare i *cookie* e poi trasmetterli nuovamente ai siti che li hanno generati in occasione di una successiva visita del medesimo utente, mantenendo così memoria della sua precedente interazione con uno o più siti *web*.

Le informazioni codificate nei *cookie* possono includere dati personali, come un indirizzo IP, un nome utente, un identificativo univoco o un indirizzo *e-mail*, ma possono anche contenere dati non personali, come le impostazioni della lingua o informazioni sul tipo di dispositivo che una persona sta utilizzando per navigare nel sito.

I *cookie* possono dunque svolgere importanti e diverse funzioni, tra cui il monitoraggio di sessioni, la memorizzazione di informazioni su specifiche configurazioni riguardanti gli utenti che accedono al *server*, l'agevolazione nella fruizione dei contenuti *on-line* etc. Possono ad esempio essere impiegati per tenere traccia degli articoli in un carrello degli acquisti online o delle informazioni utilizzate per la compilazione di un modulo informatico.

Se da un lato è tramite i *cookie* che è possibile consentire, tra l'altro, alle pagine *web* di caricarsi più velocemente, come pure instradare le informazioni su una rete - in linea dunque con adempimenti strettamente connessi alla operatività stessa dei siti *web* -, sempre attraverso i *cookie* è possibile anche veicolare la pubblicità comportamentale (c.d. «*behavioural advertising*») e misurare poi l'efficacia del messaggio pubblicitario, ovvero conformare tipologia e modalità dei servizi resi ai comportamenti dell'utente oggetto di precedente osservazione.

3. Altri strumenti di tracciamento

Il medesimo risultato può essere conseguito anche mediante l'utilizzo di altri strumenti (la totalità dei quali può essere distinta tra i c.d. «identificatori attivi», come appunto i *cookie*, e «passivi», questi ultimi presupponendo la mera osservazione), che consentono di effettuare trattamenti analoghi a quelli sopra indicati.

Tra gli strumenti «passivi» è ricompreso il *fingerprinting*, ossia quella tecnica che permette di identificare il dispositivo utilizzato dall'utente tramite la raccolta di tutte o alcune delle informazioni relative alla specifica configurazione del dispositivo stesso adottata dall'interessato. Tale tecnica può essere utilizzata per il conseguimento delle medesime finalità di profilazione tesa anche alla visualizzazione di pubblicità comportamentale personalizzata ed all'analisi e monitoraggio dei comportamenti dei visitatori di siti *web*, ovvero per conformare tipologia e modalità dei servizi resi ai comportamenti dell'utente oggetto di precedente osservazione. Per tali ragioni, il *fingerprinting* e gli ulteriori strumenti di tracciamento devono dunque essere ricompresi nell'ambito di applicazione delle presenti linee guida.

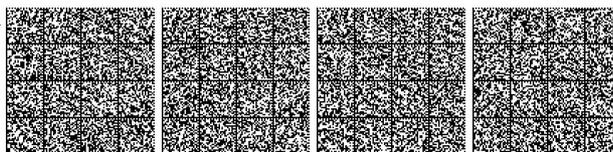
Sussiste tuttavia una non trascurabile differenza, sulla quale l'autorità intende porre l'accento, tra l'impiego di una tecnica attiva quale quella relativa ai *cookie* ed una passiva, come quella relativa al *fingerprinting*.

Nel primo caso, infatti, l'utente che non intenda essere profilato, oltre ovviamente a poter rifiutare il proprio consenso, o a ricorrere alle tutele di carattere giuridico connesse all'esercizio dei diritti di cui al regolamento, ha anche la possibilità pratica di rimuovere direttamente i *cookie*, in quanto archiviati all'interno del proprio dispositivo.

Diversamente, con riguardo al *fingerprinting* e agli altri identificatori «passivi», l'utente non dispone di strumenti autonomamente azionabili, dovendo necessariamente far ricorso all'azione del titolare. Ciò in quanto quest'ultimo fa uso di una tecnica di lettura che non presuppone l'archiviazione di informazioni all'interno del dispositivo dell'utente, bensì la mera osservazione delle configurazioni che lo contraddistinguono rendendolo identificabile, ed il cui esito si sostanzia in un «profilo» che resta nella sola disponibilità del titolare, cui l'interessato non ha, ovviamente, alcun accesso libero e diretto e del quale potrebbe, prima ancora, non avere neppure consapevolezza.

4. La classificazione di *cookie* ed altri strumenti di tracciamento

I *cookie* e, in buona misura, gli altri strumenti di tracciamento possono avere caratteristiche diverse sotto il profilo temporale e dunque essere considerati in base alla loro durata (di sessione o permanenti), ovvero dal punto di vista soggettivo (a seconda che il *publisher* agisca autonomamente o per conto della «terza parte»).



E tuttavia la classificazione che risponde alla *ratio* della disciplina di legge e dunque anche alle esigenze di tutela della persona, è quella che si basa, in definitiva, su due macro categorie:

i *cookie* tecnici, utilizzati al solo fine di «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» (cfr. art. 122, comma 1 del Codice);

i *cookie* di profilazione, utilizzati per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso delle funzionalità offerte (*pattern*) al fine del raggruppamento dei diversi profili all'interno di *cluster* omogenei di diversa ampiezza, in modo che sia possibile al titolare, tra l'altro, anche modulare la fornitura del servizio in modo sempre più personalizzato al di là di quanto strettamente necessario all'erogazione del servizio, nonché inviare messaggi pubblicitari mirati, cioè in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete.

Analogamente, anche gli altri identificatori possono essere catalogati secondo criteri diversi, dei quali il principale resta, tuttavia, la finalità per la quale vengono utilizzati: di natura «tecnica» o di natura «non tecnica», dovendosi intendere quest'ultima categoria in senso ampio, dal momento che l'attuale disciplina di legge, di cui in appresso, tesa alla tutela della confidenzialità delle comunicazioni elettroniche oltre che delle informazioni di carattere personale, è inequivocamente formulata secondo lo schema di una generale proibizione di trattamento dei dati degli interessati, salvo eccezioni rigorosamente e restrittivamente codificate, insuscettibili di estensione analogica.

5. Normativa applicabile

Per l'utilizzo di *cookie* e degli altri identificatori tecnici, in virtù della funzione assoluta e nei limiti ed alle condizioni richiamate, il titolare del trattamento sarà assoggettato al solo obbligo di fornire specifica informativa, anche eventualmente inserita all'interno di quella di carattere generale, rientrando il loro impiego in una ipotesi codificata di esenzione dall'obbligo di acquisizione del consenso dell'interessato; i *cookie* e gli altri strumenti di tracciamento per finalità diverse da quelle tecniche potranno, invece, essere utilizzati esclusivamente previa acquisizione del consenso, comunque informato, del contraente o utente. E ciò in base alla norma tuttora applicabile alla fattispecie, ossia l'art. 122 del codice, ai sensi del quale:

«1. 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 modalità semplificate. 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. Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente.

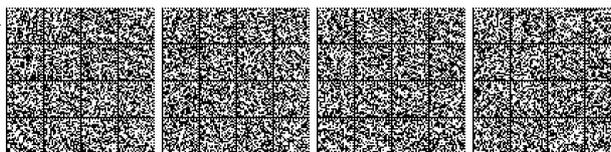
2. Ai fini dell'espressione del consenso di cui al comma 1, possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente.

2-bis. Salvo quanto previsto dal comma 1, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente».

Questa disposizione è stata introdotta nell'ordinamento nazionale a seguito del recepimento della direttiva *ePrivacy*, precedente rispetto alla data della piena operatività degli effetti del regolamento. Tale direttiva, al pari delle norme di diritto interno che la recepiscono, è tuttora applicabile allo specifico settore che riguarda i trattamenti di dati effettuati nell'ambito delle comunicazioni elettroniche (v., in proposito, il considerando 173 del regolamento secondo cui «È opportuno che il presente regolamento si applichi a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo, di cui alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio ...», nonché l'art. 2, lettera l), della direttiva quadro 2002/21/CE che ricomprende anche la direttiva *ePrivacy* nel novero delle «direttive particolari»).

La successiva entrata in vigore del regolamento impone tuttavia una indagine, innanzitutto tesa a ricercare il coordinamento tra le regole poste. Ad esclusione delle fattispecie disciplinate in via esclusiva ed esaustiva dalla direttiva *ePrivacy*, molte attività di trattamento devono infatti essere ricondotte all'ambito di applicazione tanto della direttiva quanto del regolamento (2), con l'avvertenza tuttavia che, per la parte di potenziale sovrapposizione - in virtù del rapporto di *genus a species* sussistente tra le due discipline e di quanto disposto dall'art. 1, par. 2, della direttiva *ePrivacy*, il quale chiarisce proprio come le norme di questa precisino e integrino quelle del regolamento - ogniqualvolta la direttiva renda più specifiche le prescrizioni del regolamento, essa, in quanto *lex specialis*, dovrà essere applicata e prevarrà sulle (più generali) disposizioni del regolamento. Queste ultime re-

(2) Così la Corte di Giustizia, che nella sentenza *Wirtschaftsakademie* (C-210/16 del 5 giugno 2018) ha applicato la direttiva 95/46 nonostante il caso si riferisse a operazioni di trattamento rientranti nell'ambito di applicazione materiale della direttiva *ePrivacy*; lo stesso è accaduto nella sentenza resa nel caso *Fashion ID* (C-40/17 del 29 luglio 2019)



stano invece applicabili per tutte quelle fattispecie non specificamente previste dalla direttiva nonché per offrire, alle norme di questa, la cornice regolatoria di carattere generale entro cui collocarne i precetti (3)

Ad esempio, è nella direttiva *ePrivacy* che, nei casi previsti, si rinviene l'obbligo di acquisizione del consenso all'impiego di *cookie* e altri strumenti di tracciamento; ma è nel regolamento che andranno ricercate le specifiche caratteristiche di quel consenso ai fini della sua validità e conformità alla disciplina generale.

Dalla ricostruzione normativa effettuata si trae una prima, importante conclusione: la disciplina di carattere speciale applicabile alla specie non contempla ulteriori basi giuridiche che rendano legittimo il trattamento se non in presenza del consenso dell'interessato ovvero al ricorrere di una delle ipotesi di deroga rispetto all'obbligo della sua raccolta previste proprio da tale disciplina speciale. In nessun caso sarà pertanto possibile invocare ad esempio, come è stato invece osservato nel corso delle verifiche effettuate su diversi siti *web*, la scriminante del legittimo interesse del titolare per giustificare il ricorso a *cookie* o altri strumenti di tracciamento.

6. Le modalità per l'acquisizione del consenso on-line alla luce di alcuni opportuni chiarimenti e nuove raccomandazioni

6.1 Il c.d. «*scrolling*» e il *cookie wall*

Il Garante ritiene che l'impianto teso alla individuazione della modalità tecnica per l'acquisizione del consenso *on-line* per il tracciamento a mezzo *cookie* (ovvero anche realizzato per il tramite di altri strumenti) illustrato nel menzionato provvedimento del maggio 2014 sia da ritenersi tuttora valido, pur nel mutato assetto normativo che privilegia ed impone ai titolari di agire in ossequio al nuovo regime di *accountability* (art. 5, paragrafo 2, del regolamento) consentendo loro, se del caso, anche l'adozione di modalità diverse attraverso cui assicurare la conformità alle regole e la tutela degli interessati.

Si reputa, tuttavia, opportuno fornire taluni chiarimenti in relazione all'utilizzo del c.d. *scrolling* ai fini della raccolta del consenso all'installazione e all'utilizzo di *cookie* ed altri strumenti di tracciamento nonché all'utilizzo del c.d. *cookie wall*.

Al riguardo, deve essere innanzitutto ricordato che, secondo il considerando 32 del regolamento, «Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito *web*, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto.

(3) In senso conforme, con specifico riguardo alle interrelazioni tra le discipline, si veda anche il parere dell'EDPB n. 5/2019 del 12 marzo 2019, richiamato in premessa.

Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso».

L'EDPB ha, inoltre, chiarito (parere n. 5/2020, del 4 maggio 2020) che il semplice *scrolling* non è mai idoneo, di per sé, ad esprimere compiutamente la manifestazione di volontà dell'interessato volta ad accettare di ricevere il posizionamento, all'interno del proprio terminale, di *cookie* diversi da quelli tecnici e, dunque, non equivale, in sé considerato, al consenso «in nessuna circostanza» (4)

Il Garante condivide naturalmente l'opinione dell'EDPB: il semplice «*scroll down*» del cursore di pagina è inadatto in sé alla raccolta, da parte del titolare del trattamento, di un idoneo consenso all'installazione e all'utilizzo di *cookie* di profilazione ovvero di altri strumenti di tracciamento.

Non pare potersi escludere, tuttavia, che lo *scrolling* possa intervenire nella procedura di acquisizione del consenso e costituire non la sola, bensì una delle componenti di un più articolato processo che consenta comunque all'utente di segnalare al titolare del sito, con la generazione di un preciso *pattern*, una scelta inequivoca e consapevole, che sia al tempo stesso registrabile e dunque documentabile, volta a prestare il proprio consenso all'uso dei *cookie* o di altri strumenti di tracciamento, come richiesto dalle norme vigenti.

Tale conclusione risulta d'altro canto coerente, oggi, con il richiamato approccio regolamentare teso alla valorizzazione dell'*accountability*; pertanto, ed analogamente a quanto affermato con riferimento al potere di autonomia del titolare nell'identificazione delle soluzioni più appropriate per conseguire la conformità alle regole dei trattamenti di dati personali effettuati, il Garante invita i titolari a valutare con estremo rigore ogni possibile soluzione, anche di carattere tecnico, idonea ad essere interpretata e registrata come una forma di consenso espresso dall'utente per l'installazione dei *cookie* o per l'impiego di altri strumenti di tracciamento.

Affinché lo stesso risulti acquisito legittimamente, il medesimo titolare dovrà inoltre far sì che eventuali modalità alternative rispetto a quelle proposte nelle presenti linee guida di espressione del consenso *on-line* siano realizzate in modo tale da rendere inequivoco anche per l'utente l'effetto della propria azione, equivalente alla manifestazione del consenso stesso. Ciò, allo scopo di limitare l'incidenza dei c.d. «falsi positivi», ossia di er-

(4) “Based on recital 32, actions such as scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action: such actions may be difficult to distinguish from other activity or interaction by a user and therefore determining that an unambiguous consent has been obtained will also not be possible. Furthermore, in such a case, it will be difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it” (cfr. punto 86).



ronee interpretazioni di azioni casuali come espressioni consapevoli della volontà dell'utente.

Qualora invece, nel caso concreto, all'azione dell'utente non corrisponda alcun evento informatico inequivoco, documentabile e dotato delle menzionate caratteristiche anche sotto il profilo della consapevolezza per lo stesso utente, allora in nessun modo sarà possibile attribuire a tale azione la validità del consenso ai sensi della normativa vigente.

Ulteriori chiarimenti appaiono opportuni con riferimento al cd. *cookie wall*, intendendosi con tale espressione un meccanismo vincolante (cd. «*take it or leave it*»), nel quale l'utente venga cioè obbligato, senza alternativa, ad esprimere il proprio consenso alla ricezione di *cookie* ovvero altri strumenti di tracciamento, pena l'impossibilità di accedere al sito.

Tale meccanismo, non consentendo di qualificare l'eventuale consenso così ottenuto come conforme alle caratteristiche imposte dal regolamento, e segnatamente al suo art. 4, punto 11 con particolare riferimento al requisito della «libertà» del consenso, è da ritenersi illecito, salva l'ipotesi da verificare caso per caso nella quale il titolare del sito offra all'interessato la possibilità di accedere ad un contenuto o a un servizio equivalenti senza prestare il proprio consenso all'installazione e all'uso di *cookie* o altri strumenti di tracciamento.

E ciò alla irrinunciabile condizione della conformità dell'alternativa proposta ai principi del regolamento codificati al suo art. 5, paragrafo 1, ed innanzitutto a quello di cui alla lettera *a*), che esige che i dati personali siano trattati in modo lecito, corretto e trasparente (principio di «liceità, correttezza e trasparenza»); in difetto, il *cookie wall* non potrà essere reputato in linea con la disciplina vigente.

6.2 La reiterazione della richiesta di consenso in presenza di una precedente mancata prestazione dello stesso

Ancora con riferimento alle modalità di acquisizione del consenso, l'osservazione del comportamento dei siti *web* e le segnalazioni pervenute hanno evidenziato l'ulteriore problematica della spesso ridondante ed invasiva riproposizione, da parte dei gestori dei siti *web*, del meccanismo basato sulla presentazione del *banner* ad ogni nuovo accesso dell'utente al medesimo sito anche quando quest'ultimo abbia liberamente scelto. Una implementazione che, se da un lato compromette la fluidità della *user experience*, non trova ragione negli obblighi di legge ed ha contribuito sin qui ad una probabile sottovalutazione del valore del contenuto con esso proposto.

L'eccessiva riproposizione del *banner* ai fini dell'acquisizione del consenso, laddove l'utente l'abbia in precedenza negato, appare suscettibile di lederne la libertà inducendolo a prestarlo pur di proseguire nella navigazione libero dalla comparsa del *banner* contenente l'informativa breve e la richiesta di prestazione del consenso.

In tale contesto, quindi, nel caso in cui l'utente mantenga le impostazioni di *default* e dunque non acconsenta all'impiego di *cookie* o altri strumenti di tracciamento, così come nel caso in cui abbia acconsentito solo all'im-

piego di alcuni *cookie* o altri strumenti di tracciamento, tale scelta dovrà essere debitamente registrata e la prestazione del consenso non più nuovamente sollecitata se non quando ricorra uno dei seguenti casi:

quando mutino significativamente una o più condizioni del trattamento e dunque il *banner* assolva anche ad una specifica e necessaria finalità informativa proprio in ordine alle modifiche intervenute, come nel caso in cui mutino le «terze parti»;

quando sia impossibile, per il gestore del sito *web*, avere contezza del fatto che un *cookie* sia stato già in precedenza memorizzato sul dispositivo per essere nuovamente trasmesso, in occasione di una successiva visita del medesimo utente, al sito che lo ha generato (ad esempio nel caso in cui l'utente scelga di cancellare i *cookie* legittimamente installati nel proprio dispositivo senza che il titolare abbia modo, dunque, di tenere traccia della volontà di mantenere le impostazioni di default e dunque di proseguire la navigazione senza essere tracciati);

quando siano trascorsi almeno sei mesi dalla precedente presentazione del *banner*.

7. La *privacy by design e by default* in relazione ai *cookie* ed agli altri strumenti di tracciamento

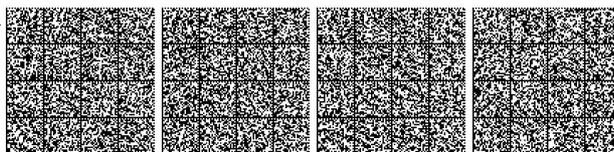
7.1 Il meccanismo di acquisizione del consenso

È opinione del Garante che il meccanismo di acquisizione del consenso *on-line* tramite presentazione di un *banner*, come lo si è analiticamente descritto nel provvedimento del maggio 2014, mantenga, ad oggi, una sua sostanziale validità. È tuttavia necessario, anche in questo caso, valutare l'opportunità di aggiornamenti o migliorie alla luce del mutato assetto normativo.

Al riguardo, occorre prendere in considerazione la portata innovativa del regolamento e i nuovi equilibri che esso tratteggia nelle relazioni tra titolare e interessato con specifico riferimento al suo art. 25, il quale dispone, al secondo paragrafo, che «Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ...».

In adempimento di tale obbligo, di carattere generale poiché applicabile a qualsiasi trattamento di dati, il titolare dovrà garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari in relazione a ciascuna specifica finalità del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non eccedano il minimo necessario per il conseguimento delle finalità perseguite, in modo che l'utilizzo di informazioni per l'accesso ad un sito sia inizialmente limitato al minimo indispensabile per consentire la fruizione e che sia rimesso interamente all'interessato un effettivo, concreto potere di scelta in ordine alla possibilità di consentire o meno un utilizzo eventualmente più ampio dei suoi dati.

Il rispetto di tali regole impone dunque che, per impostazione predefinita, al momento del primo accesso



dell'utente a un sito *web*, nessun *cookie* o altro strumento diverso da quelli tecnici venga posizionato all'interno del suo dispositivo, né che venga utilizzata alcuna altra tecnica attiva o passiva di tracciamento.

Questo risultato costituisce un obbligo espressamente codificato il cui mancato adempimento è sanzionabile ai sensi del regolamento. Nella propria autonomia imprenditoriale e in ossequio all'*accountability*, ciascun titolare può naturalmente adottare le modalità ritenute più idonee per assicurarne il rispetto.

Tuttavia, e considerato pure che occorre assicurare anche la libertà di scelta di chi invece intenda accettare di essere profilato, il Garante suggerisce l'adozione dello specifico modello, di seguito illustrato, da reputarsi in linea con i menzionati obblighi. Qualora i gestori dei siti *web* decidano di conformarvisi, dovranno implementare un meccanismo in base al quale l'utente, accedendo per la prima volta alla *home page* (o ad altra pagina) del sito *web*, visualizzi immediatamente un'area o *banner* le cui dimensioni siano, al tempo stesso, sufficienti da costituire una percettibile discontinuità nella fruizione dei contenuti della pagina *web* che sta visitando, ma anche tali da evitare il rischio che l'utente possa far ricorso a comandi e dunque compiere scelte indesiderate o inconsapevoli; con l'effetto che l'adeguatezza e la congruità delle dimensioni del *banner* dovranno essere valutate anche in relazione ai diversi dispositivi di possibile utilizzo da parte dell'interessato.

Tale *banner* dovrà essere parte integrante di un meccanismo che, pur non impedendo il mantenimento delle impostazioni di *default*, permetta anche l'eventuale espressione di una azione positiva nella quale deve sostanziarsi la manifestazione del consenso dell'interessato.

Qualora l'utente scegliesse, com'è nella sua piena disponibilità, di mantenere quelle impostazioni di *default* e dunque di non prestare il proprio consenso al posizionamento dei *cookie* o all'impiego di altre tecniche di tracciamento, dovrebbe dunque limitarsi a chiudere il *banner* mediante selezione dell'apposito comando usualmente utilizzato a tale scopo, cioè quello contraddistinto da una X posizionata di regola, e secondo prassi consolidata, in alto a destra e all'interno del *banner* medesimo, senza essere costretto ad accedere ad altre aree o pagine a ciò appositamente dedicate. Tale comando dovrà avere una evidenza grafica pari a quella degli ulteriori comandi o pulsanti negoziali idonei ad esprimere le altre scelte nella disponibilità dell'utente, di cui si dirà in appresso. Le modalità di prosecuzione nella navigazione senza prestare alcun consenso dovranno, in altre parole, essere immediate, usabili e accessibili quanto quelle previste per la prestazione del consenso.

Mediante il ricorso a questo meccanismo si garantirebbe che, appunto *by default*, l'interessato che non intenda esprimere il proprio consenso non sia in alcun modo tracciato o profilato conseguendo, al tempo stesso, l'ulteriore risultato di generare un evento informatico riconoscibile e registrabile da parte del titolare. Esso, esprimendo la volontà dell'interessato di non prestare il proprio consenso

all'utilizzo di *cookie* o altri strumenti di tracciamento diversi da quelli tecnici, impedirebbe al sito la reiterazione della presentazione del *banner* in occasione di successivi accessi dell'utente, fatte salve le eccezioni descritte al paragrafo precedente e, comunque, per un periodo di tempo non inferiore a sei mesi.

In altri termini, il consenso potrà intendersi come validamente prestato soltanto se sarà conseguenza di un intervento attivo e consapevole dell'utente, opportunamente riscontrabile e dimostrabile, che consenta di qualificarlo come in linea con tutti quei requisiti (libero, informato, inequivoco e specifico, cioè espresso in relazione a ciascuna diversa finalità del trattamento) richiesti dal regolamento.

Tale *banner* dovrà allora contenere, oltre alla X in alto a destra di cui è stata già illustrata la funzione, almeno le seguenti indicazioni ed opzioni:

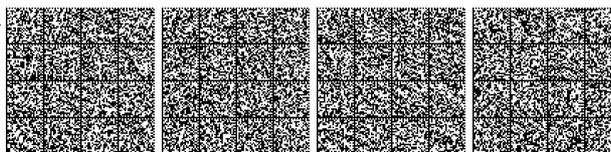
i) l'avvertenza che la chiusura del *banner* mediante selezione dell'apposito comando contraddistinto dalla X posta al suo interno, in alto a destra, comporta il permanere delle impostazioni di *default* e dunque la continuazione della navigazione in assenza di *cookie* o altri strumenti di tracciamento diversi da quelli tecnici;

ii) una informativa minima relativa al fatto che il sito utilizza - se così è ovviamente - *cookie* o altri strumenti tecnici e potrà, esclusivamente previa acquisizione del consenso dell'utente da prestarsi con modalità da indicarsi nella medesima informativa breve (*cf.* punto iv che segue), utilizzare anche *cookie* di profilazione o altri strumenti di tracciamento al fine di inviare messaggi pubblicitari ovvero di modulare la fornitura del servizio in modo personalizzato al di là di quanto strettamente necessario alla sua erogazione, cioè in linea con le preferenze manifestate dall'utente stesso nell'ambito dell'utilizzo delle funzionalità e della navigazione in rete e/o allo scopo di effettuare analisi e monitoraggio dei comportamenti dei visitatori di siti *web*;

iii) il *link* alla *privacy policy*, ovvero ad una informativa estesa posizionata in un *second layer* - che sia accessibile con un solo click anche tramite un ulteriore *link* posizionato nel *footer* di qualsiasi pagina del dominio cui l'utente accede - ove vengano fornite in maniera chiara e completa almeno tutte le indicazioni di cui agli artt. 12 e 13 del regolamento, anche con riguardo ai predetti *cookie* o altri strumenti tecnici (*cf.*, al riguardo, il successivo paragrafo 8);

iv) un comando attraverso il quale sia possibile esprimere il proprio consenso accettando il posizionamento di tutti i *cookie* o l'impiego di eventuali altri strumenti di tracciamento;

v) il *link* ad una ulteriore area dedicata nella quale sia possibile selezionare, in modo analitico, soltanto le funzionalità, i soggetti cd. terze parti - il cui elenco deve essere tenuto costantemente aggiornato, siano essi raggiungibili tramite specifici *link* ovvero anche per il tramite del *link* al sito *web* di un soggetto intermediario che li rappresenti - ed i *cookie*, anche eventualmente rag-



gruppati per categorie omogenee, al cui utilizzo l'utente scelga di acconsentire.

In quest'ultima ipotesi, quando cioè i *cookie* siano raggruppati per categorie omogenee, qualora si verificassero successive modifiche nel novero delle terze parti corrispondenti ai *link* posizionati in questa area e dunque ulteriori soggetti terze parti venissero aggiunti alla lista, è rimessa alla prima parte, cioè al gestore del sito, la loro accurata selezione, come pure la necessaria attività di vigilanza per assicurare che l'ingresso di tali soggetti ed il trattamento che ne discende permanga in linea con il raggruppamento per categorie omogenee come già effettuato.

Anche in questo caso, il rispetto degli obblighi di *privacy by default* impone che le possibili scelte granulari siano inizialmente tutte preimpostate sul diniego all'installazione dei *cookie*, e che pertanto l'utente possa, esclusivamente, accettarne, anche appunto in modo granulare, il posizionamento.

Nell'eventualità in cui sia prevista la sola presenza di *cookie* tecnici o altri strumenti analoghi, di essi potrà essere data informazione nella *homepage* o nell'informativa generale senza l'esigenza di apporre specifici *banner* da rimuovere a cura dell'utente.

Queste premesse consentono anche di chiarire possibili fraintendimenti nel significato da attribuire all'azione dell'utente in relazione alla specifica configurazione dei pulsanti e dei colori utilizzati dai publisher, sinora di non univoca interpretazione. Basti, al riguardo, ribadire che, a prescindere dalla configurazione adottata, dai colori utilizzati per i pulsanti e in definitiva dalle modalità attuative prescelte, l'azione positiva nella disponibilità dell'utente al momento del primo accesso al sito dovrà comunque essere esclusivamente volta alla manifestazione del consenso (*cd. opt-in*) e non potrà mai riferirsi invece all'espressione di un diniego (*cd. opt-out*).

A tale riguardo, il Garante torna a sottolineare tuttavia l'importanza di avviare nelle sedi più opportune e tra tutti i soggetti interessati (accademia, industria, associazioni di categoria, decisori, *stakeholder* etc.) una riflessione circa la necessità dell'adozione di una codifica standardizzata relativa alla tipologia dei comandi, dei colori e delle funzioni da implementare all'interno dei siti *web* per conseguire la più ampia uniformità, a tutto vantaggio della trasparenza, della chiarezza e dunque anche della migliore conformità alle regole; tale esigenza, che sulla base dei contributi pervenuti nell'ambito della consultazione pubblica risulta essere unanimemente avvertita e condivisa, non ha tuttavia sin qui trovato delle proposte concrete idonee al conseguimento dello scopo.

Gli utenti, naturalmente, dovranno essere posti in condizione di modificare le scelte compiute – sia in termini negativi che in termini positivi e dunque prestando un consenso negato o revocando un consenso prestato - in ogni momento e ciò in maniera semplice, immediata e intuitiva attraverso un'apposita area da rendere accessibile attraverso un *link* da posizionarsi nel *footer* del sito e che

ne renda esplicita la funzionalità attraverso l'indicazione di «rivedi le tue scelte sui *cookie*» o analoga.

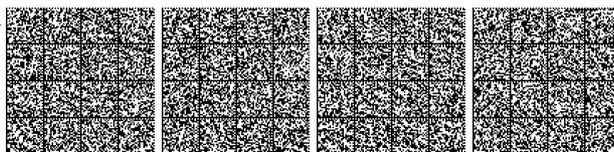
Resta, peraltro, inteso che in ogni ipotesi di riproposizione del *banner* contenente l'informativa breve e le opzioni di scelta dell'utente, così come laddove l'utente modifichi le scelte originariamente compiute in conformità al periodo precedente, le scelte negoziali compiute in occasione degli accessi successivi dovranno sovrascrivere e superare le precedenti ed essere, dunque, considerate come modifica delle precedenti opzioni anche in questo caso, indifferentemente, in termini di prestazione di un consenso originariamente negato o di revoca di un consenso precedentemente prestato.

Per assicurare che gli utenti non siano influenzati ovvero penalizzati da scelte di design che inducano a preferire una opzione anziché l'altra, si sottolinea inoltre l'esigenza dell'utilizzo di comandi e di caratteri di uguali dimensioni, enfasi e colori, che siano ugualmente facili da visionare e utilizzare.

Al fine di rendere concretamente azionabile tale possibilità di mutare avviso e dunque effettiva la disponibilità per l'utente della espressione libera della propria volontà, il Garante suggerisce allora l'adozione di una buona prassi, individuata attraverso l'esame dei contributi pervenuti nel corso della consultazione pubblica. Ci si riferisce al posizionamento in ciascuna pagina del dominio, eventualmente pure accanto al *link* all'area dedicata alle scelte, di un segno grafico, una icona o altro accorgimento tecnico che indichi, anche in modo essenziale, lo stato dei consensi in precedenza resi dall'utente consentendone, dunque, in ogni momento l'eventuale modifica o aggiornamento.

Per realizzare la memorizzazione delle azioni e delle scelte, anche di dettaglio, rimesse all'interessato (mantenimento delle impostazioni di *default*, espressione, anche granulare, del consenso ovvero revoca del consenso precedentemente espresso mediante ripristino delle impostazioni di *default*), il gestore del sito *web* potrebbe avvalersi o di appositi *cookie* tecnici (in tal senso, si veda anche il considerando 25 della direttiva 2002/58/CE) o anche di ulteriori modalità che la tecnologia dovesse rendere disponibili, la cui individuazione rientra nell'autonomia imprenditoriale e nell'*accountability* del titolare, adattando opportunamente la propria condotta in modo da tenere comunque costantemente aggiornata la documentazione delle scelte compiute dall'interessato.

Resta in ogni caso impregiudicata la possibilità per i titolari di adottare eventualmente anche diverse modalità di raccolta del consenso, ad esempio con riferimento a quegli utenti che accedano ai relativi servizi mediante uso di credenziali di autenticazione o di accesso e per i quali dunque, fin dal momento della creazione dell'*account*, si porrebbe un naturale momento di discontinuità nella navigazione idoneo, per il titolare, all'assolvimento degli obblighi che interessano l'impiego di *cookie* e degli altri strumenti di tracciamento; con l'avvertenza che a questi specifici utenti, *cd. autenticati*, dovrà inoltre essere consentito di scegliere consapevolmente - menzionando



dunque tale possibilità pure nell'informativa resa - se accettare la possibilità che il tracciamento che li riguarda venga effettuato anche attraverso l'analisi incrociata dei comportamenti tenuti tramite l'utilizzo di diversi *device*.

7.2 I *cookie analytics* di prima parte e delle cd. terze parti

I *cookie* possono anche essere utilizzati, tra l'altro, per valutare l'efficacia di un servizio della società dell'informazione fornito da un *publisher*, per la progettazione di un sito *web* o per contribuire a misurarne il «traffico», cioè il numero di visitatori anche eventualmente ripartiti per area geografica, fascia oraria della connessione o altre caratteristiche.

L'autorità ha affermato, nel provvedimento del maggio 2014, che tali identificativi, definiti *cookie analytics*, possono essere ricompresi nella categoria di quelli tecnici, e come tali essere utilizzati in assenza della previa acquisizione del consenso dell'interessato, al verificarsi di determinate condizioni. Anche in questo caso, l'entrata in vigore del regolamento impone un ripensamento critico delle condizioni identificate allora, nonché una più specifica definizione delle misure oggi idonee all'applicazione della richiamata esenzione.

Si impone, in primo luogo, la necessità di individuare soluzioni di maggior tutela dell'interessato attraverso l'impiego di misure in linea con le disposizioni dell'art. 25, paragrafo 1, del regolamento in materia di *privacy by design*, tali da «attuare in modo efficace i principi di protezione dei dati».

In questa prospettiva, il Garante reputa che, nel caso di specie, tale obiettivo debba essere conseguito attraverso il ricorso a misure di minimizzazione del dato che riducano significativamente il potere identificativo dei *cookie analytics*, qualora il loro utilizzo avvenga ad opera di «terze parti».

Affinché i *cookie analytics* siano equiparati ai tecnici è, in altri termini, indispensabile precludere la possibilità che si pervenga, mediante il loro utilizzo, alla diretta individuazione dell'interessato (cd. *single out*), il che equivale impedire l'impiego di *cookie analytics* che, per le loro caratteristiche, possano risultare identificatori diretti ed univoci.

La struttura del *cookie analytics* dovrà allora prevedere la possibilità che lo stesso *cookie* sia riferibile non soltanto ad uno, bensì a più dispositivi, in modo da creare una ragionevole incertezza sull'identità informatica del soggetto che lo riceve. Di regola questo effetto si ottiene mascherando opportune porzioni dell'indirizzo IP all'interno del *cookie*.

Tenuto conto della rappresentazione degli indirizzi IP versione 4 (IPv4) a 32 bit, che sono usualmente rappresentati e utilizzati come sequenza di quattro numeri decimali compresi tra 0 e 255 separati da un punto, una delle misure implementabili al fine di beneficiare dell'esenzione consiste nel mascheramento almeno della quarta componente dell'indirizzo, opzione che introduce una incertezza nell'attribuzione del *cookie* ad uno specifico interessato pari a 1/256 (circa 0,4%).

Analoghe procedure dovrebbero essere adottate in riferimento agli indirizzi IP versione 6 (IPv6), che hanno una

differente struttura e uno spazio di indirizzamento enormemente superiore (essendo costituiti da numeri binari rappresentati con 128 *bit*).

Il Garante sottolinea, inoltre, la necessità che l'uso dei *cookie analytics* sia limitato unicamente alla produzione di statistiche aggregate e che essi vengano utilizzati in relazione ad un singolo sito o una sola applicazione mobile, in modo da non consentire il tracciamento della navigazione della persona che utilizza applicazioni diverse o naviga in siti *web* diversi.

Resta inteso pertanto che i soggetti terzi, che forniscono al *publisher* il servizio di *web measurement*, non dovranno comunque combinare i dati, anche così minimizzati, con altre elaborazioni (file dei clienti o statistiche di visite ad altri siti, ad esempio) nè trasmetterli a loro volta ad ulteriori terzi, pena l'inaccettabile incremento dei rischi di identificazione dell'utente; tranne il caso in cui la produzione di statistiche da loro effettuata con i dati minimizzati interessi più domini, siti *web* o app riconducibili al medesimo *publisher* o gruppo imprenditoriale.

È tuttavia possibile reputare lecito, anche in assenza dell'adozione delle prescritte misure di minimizzazione, il ricorso ad analisi statistiche relative a più domini, siti *web* o app riconducibili al medesimo titolare purché questi proceda in proprio all'elaborazione statistica, senza in ogni caso che tali analisi si risolvano in una attività che, travalicando i confini di un mero conteggio statistico, assuma in realtà le caratteristiche di una elaborazione volta all'assunzione di decisioni di natura commerciale.

8. Le novità in materia di informativa

8.1 Le informazioni da rendere in conformità al regolamento

Da ultimo, il Garante intende illustrare alcuni miglioramenti che i titolari potranno adottare al fine di rendere agli utenti una informativa conforme ai rinnovati requisiti di trasparenza imposti dagli articoli 12 e 13 del regolamento, compresa l'indicazione circa gli eventuali altri soggetti destinatari dei dati personali ed i tempi di conservazione delle informazioni acquisite.

È inoltre necessario fornire informazioni su come le persone fisiche possono esercitare tutti i diritti previsti dal regolamento, incluso quello di avanzare una richiesta di accesso e di proporre un reclamo a un'autorità di controllo.

In aggiunta a quanto stabilito nel provvedimento sui *cookie* del maggio 2014, e nel confermare la logica di semplificazione cui le sue indicazioni sono improntate, si ritiene inoltre che l'informativa, oltre che *multilayer*, e cioè dislocata su più livelli, possa ad oggi essere resa, eventualmente in relazione a specifiche necessità, anche per il tramite di più canali e modalità (cd. *multichannel*), in modo da sfruttare al massimo più dinamici e meno tradizionali ulteriori punti di contatto tra il titolare e gli interessati.

Si pensi, ad esempio, al sempre più diffuso ricorso a canali video, a *pop-up* informativi, a interazioni vocali, ad assistenti virtuali, all'impiego del telefono, al ricorso a *chatbot*, etc.

Sarà allora onere del titolare, cui è rimessa la scelta in ordine alla modalità ovvero all'impiego combinato delle



modalità ritenute più idonee, verificare la corrispondenza del sistema implementato, specie in termini di completezza, chiarezza espositiva, efficacia e fruibilità, con i requisiti imposti dal regolamento.

Allo stesso modo, sarà onere del titolare adottare ogni più opportuno accorgimento affinché le informazioni contenute nel *banner* siano fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari, in linea con quanto previsto dalla legge 9 gennaio 2004, n. 4 (come modificata, da ultimo, dal d.l. 16 luglio 2020, n. 76, convertito in legge, con modificazioni, dalla legge 11 settembre 2020, n. 120).

8.2 La necessità di una integrazione delle informazioni da comunicare agli utenti

La pratica operativa degli ultimi anni ha evidenziato come il sistema difetti di un elemento di cruciale rilievo, specie a fini di *enforcement*.

Ci si riferisce al fatto che non esiste ancora, ad oggi, un sistema universalmente accettato di codifica semantica dei *cookie* e degli altri strumenti di tracciamento che consenta di distinguere oggettivamente, ad esempio, quelli tecnici dagli *analytics* o da quelli di profilazione, se non basandosi sulle indicazioni rese dal titolare stesso nella *privacy policy*.

È stato riscontrato, inoltre, che le interrogazioni e le verifiche circa il posizionamento di *cookie* da parte di uno specifico sito *web* possono avere esiti diversi a seconda del *browser* considerato.

In tale situazione, e con l'auspicio che si addivenga in tempi rapidi ad una codifica di carattere generale, tanto più importante specie nell'attuale mondo connesso *on-line*, nel quale le distanze geografiche perdono rilevanza a fronte delle sempre più accentuate potenzialità della rete, il Garante intende richiamare i titolari che facciano impiego di tali strumenti alla necessità di rendere manifesti, mediante apposita, opportuna integrazione dell'informativa, almeno i criteri di codifica degli identificatori adottati da ciascuno. In alternativa, i titolari potranno valutare di posizionare tale codifica anche all'interno della *privacy policy*.

Tali criteri potranno, inoltre, a richiesta, costituire oggetto di comunicazione all'autorità, quale strumento di ausilio alle attività di carattere istruttorio che saranno intraprese con riguardo al fenomeno in considerazione.

Tutto ciò premesso, il Garante:

ai sensi dell'art. 154-*bis*, comma 1, lett. *a*), del Codice, delibera di adottare le presenti linee guida affinché tutti i fornitori dei servizi della società dell'informazione di cui all'art. 1, paragrafo 1, punto (b) della direttiva (EU) 2015/1535, nonché tutti i soggetti che comunque offrono ai propri utenti servizi online accessibili al pubblico attraverso reti di comunicazione elettronica o cui si riferiscano siti *web* che facciano impiego di *cookie* e/o altri strumenti di tracciamento, con specifico riguardo ai trattamenti di dati personali relativi all'utilizzo delle funzionalità offer-

te, tengano conto delle indicazioni e delle semplificazioni illustrate; segnatamente, per quanto concerne:

il consenso preventivo degli utenti in relazione al trattamento, per finalità di tracciamento *on-line*, delle informazioni che li riguardano, anche derivanti dall'uso di *cookie* ed altri strumenti di tracciamento, ai sensi degli artt. 122 del codice e 4, punto 11) e 7 del regolamento (secondo i criteri e le modalità indicate ai paragrafi 6 e 7);

il rispetto del diritto di revoca del consenso nei termini di cui all'art. 7.3 del regolamento (secondo quanto indicato al paragrafo 7.1);

il rispetto degli obblighi di *privacy by design e by default* di cui all'art. 25 del regolamento anche per mezzo dell'adozione di misure di minimizzazione dei dati preliminarmente alla comunicazione ed al loro impiego ad opera delle cd. terze parti (secondo quanto indicato al paragrafo 7.2);

l'informativa da rendere agli interessati ai sensi degli artt. 12 e 13 del regolamento, con particolare riguardo all'indicazione dei criteri di codifica utilizzati da ciascun titolare per la classificazione dei *cookie* e degli altri strumenti di tracciamento che consenta di distinguere quelli tecnici dagli *analytics* o da quelli di profilazione (secondo quanto indicato al paragrafo 8 delle presenti linee guida).

In considerazione della potenziale complessità di eventuali adeguamenti dei sistemi e dei trattamenti già in atto ai principi espressi dalle presenti linee guida, l'autorità reputa congruo individuare un termine pari a sei mesi dal momento della loro pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana entro il quale i soggetti tenuti dovranno conformarsi; con l'avvertenza che i consensi già raccolti, purché conformi alle caratteristiche richieste dal regolamento, potranno essere ritenuti validi a condizione che, al momento della loro acquisizione, siano stati registrati e siano dunque debitamente documentabili, anche mediante evidenze informatiche.

Si allega alle presenti linee guida una scheda di sintesi (allegato 1) che ne costituisce parte integrante e sostanziale.

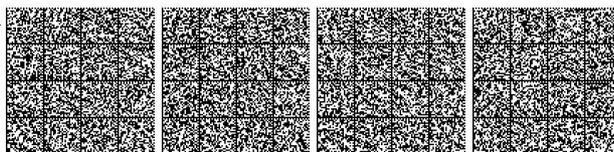
Si dispone la trasmissione di copia delle presenti linee guida al Ministero della Giustizia-ufficio pubblicazione leggi e decreti, per la loro pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 10 giugno 2021

Il presidente
STANZIONE

Il relatore
SCORZA

Il segretario generale
MATTEI



Allegato 1

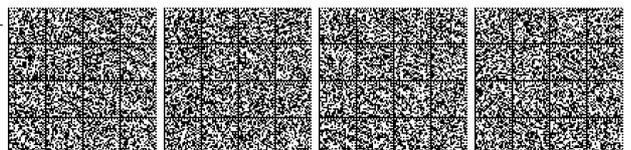
LINEE GUIDA COOKIE E ALTRI STRUMENTI DI TRACCIAMENTO

SCHEDA DI SINTESI

Oggetto	Cookie e altri strumenti di tracciamento.
Normativa	Artt. 122 del <i>Codice</i> e 4, punto 11), 7, 12, 13 e 25 del <i>Regolamento</i> .
Cookie ed altri strumenti di tracciamento	I <i>cookie</i> sono di regola stringhe di testo che i siti <i>web</i> (cd. <i>publisher</i> o “prima parte”) visitati dall’utente ovvero siti o <i>web server</i> diversi (cd. “terze parti”) posizionano e archiviano all’interno di un dispositivo terminale nella disponibilità dell’utente (cd. identificatori “attivi”). Analoghe funzioni possono essere svolte da altri strumenti che, pur utilizzando una tecnologia diversa (c.d. identificatori “passivi”), consentono di effettuare trattamenti analoghi a quelli svolti per il tramite dei <i>cookie</i> .
Cookie ed altri identificatori tecnici	Sono utilizzati al solo fine di “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” (cfr. art. 122, comma 1 del <i>Codice</i>). Non richiedono l’acquisizione del consenso, ma vanno indicati nell’informativa.
Cookie analytics prime e terze parti	Sono equiparabili ai <i>cookie</i> e agli altri identificatori tecnici solo se: - vengono utilizzati unicamente per produrre statistiche aggregate e in relazione ad un singolo sito o una sola applicazione mobile; - viene mascherata, per quelli di <i>terze parti</i> , almeno la quarta componente dell’indirizzo IP; - le <i>terze parti</i> si astengono dal combinare i <i>cookie analytics</i> , così minimizzati, con altre elaborazioni (<i>file</i> dei clienti o statistiche di visite ad altri siti, ad esempio) o dal trasmetterli ad ulteriori terzi. È tuttavia consentita alle <i>terze parti</i> la produzione di statistiche con dati relativi a più domini, siti <i>web</i> o <i>app</i> che siano riconducibili al medesimo <i>publisher</i> o gruppo imprenditoriale. Il titolare che effettui in proprio la mera elaborazione statistica dei dati relativi a più domini, siti <i>web</i> o <i>app</i> ad esso riconducibili può utilizzare anche i dati in chiaro, nel rispetto del vincolo di finalità.
Cookie e altri identificatori di tracciamento con funzione non tecnica	Utilizzati per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell’uso delle funzionalità offerte (<i>pattern</i>) al fine del raggruppamento dei diversi profili all’interno di <i>cluster</i> omogenei di diversa ampiezza, in modo che sia possibile anche modulare la fornitura del servizio in modo sempre più personalizzato, nonché inviare messaggi pubblicitari mirati, cioè in linea con le preferenze manifestate dall’utente nell’ambito della navigazione in rete.
Principali novità introdotte dal GDPR	- <i>accountability</i> ;



aventi effetti sull'uso dei cookie e altri strumenti di tracciamento	<ul style="list-style-type: none"> - integrazione dell'informativa (specificare anche i tempi di conservazione dei dati); - rafforzamento del consenso (deve essere "inequivocabile"); - rispetto dei principi di <i>privacy by design e by default</i>.
Informativa e consenso	<p>Come rendere l'informativa:</p> <ul style="list-style-type: none"> - linguaggio semplice ed accessibile; - fruibile, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari; - anche in modalità <i>multilayer e multichannel</i>; - se si utilizzano solo <i>cookie</i> tecnici, la relativa informazione può essere collocata nella <i>home page</i> del sito o nell'informativa generale; - se si trattano anche altri <i>cookie</i> e altri identificatori "non tecnici", si può utilizzare un <i>banner</i> a comparsa immediata e di adeguate dimensioni che contenga: <ul style="list-style-type: none"> a) l'indicazione che il sito utilizza <i>cookie</i> tecnici e, previo consenso dell'utente, <i>cookie</i> di profilazione o altri strumenti di tracciamento indicando le relative finalità (informativa breve); b) il <i>link</i> alla <i>privacy policy</i> contenente l'informativa completa, inclusi gli eventuali altri soggetti destinatari dei dati personali, i tempi di conservazione dei dati e l'esercizio dei diritti di cui al <i>Regolamento</i>; c) l'avvertenza che la chiusura del <i>banner</i> (ad es. mediante selezione dell'apposito comando contraddistinto dalla X posta al suo interno, in alto a destra) comporta il permanere delle impostazioni di <i>default</i> e dunque la continuazione della navigazione in assenza di <i>cookie</i> o altri strumenti di tracciamento diversi da quelli tecnici. <p>Ai fini dell'acquisizione del consenso, il <i>banner</i> dovrà pertanto contenere:</p> <ul style="list-style-type: none"> d) il menzionato comando (es. una X in alto a destra) per chiudere il <i>banner</i> senza prestare il consenso all'uso dei <i>cookie</i> o delle altre tecniche di profilazione mantenendo le impostazioni di <i>default</i>; e) un comando per accettare tutti i <i>cookie</i> o altre tecniche di tracciamento; f) il <i>link</i> ad un'altra area nella quale poter scegliere in modo analitico le funzionalità, le <i>terze parti</i> e i <i>cookie</i> che si vogliono installare e poter prestare il consenso all'impiego di tutti i <i>cookie</i> se non dato in precedenza o revocarlo, anche in unica soluzione, se già espresso. Al riguardo, è buona prassi l'impiego di un segno grafico, una icona o altro accorgimento tecnico che indichi, anche in modo essenziale, ad es. nel <i>footer</i> di ogni pagina del dominio, lo stato dei consensi in precedenza resi dall'utente consentendone l'eventuale modifica o aggiornamento.



	<p>Tale area dedicata alle scelte di dettaglio dovrà essere raggiungibile anche tramite un ulteriore <i>link</i> posizionato nel <i>footer</i> di qualsiasi pagina del dominio;</p> <p>No alla reiterazione della richiesta del consenso in presenza di una precedente mancata prestazione dello stesso, tranne: se mutano significativamente le condizioni del trattamento; se è impossibile, per il sito, sapere se un <i>cookie</i> sia stato già memorizzato nel dispositivo; se sono trascorsi almeno 6 mesi dalla precedente presentazione del <i>banner</i>.</p> <p>Nel caso di utenti provvisti di <i>account</i> (cd. utenti autenticati), divieto di incrocio dei dati relativi alla navigazione effettuata tramite uso di più dispositivi se non previo consenso.</p>
Informazioni ulteriori da rendere agli utenti	I criteri di codifica dei <i>cookie</i> e degli altri strumenti di tracciamento adottati, da comunicare, su richiesta, all'Autorità; la possibilità, per gli utenti autenticati, di acconsentire al tracciamento effettuato anche attraverso l'analisi incrociata dei comportamenti tenuti tramite l'utilizzo di diversi <i>device</i> .
Analisi di alcune modalità di raccolta del consenso	<p>Scrolling: di per sé inadatto alla raccolta di un idoneo consenso, salva la sola ipotesi in cui venga inserito in un processo più articolato nel quale l'utente sia in grado di generare un evento, registrabile e documentabile presso il <i>server</i> del sito, che possa essere qualificato come azione positiva idonea a manifestare in maniera inequivoca la volontà di prestare un consenso al trattamento.</p> <p>Cookie wall: illecito, salva l'ipotesi -da verificare caso per caso- nella quale il sito offra all'interessato la possibilità di accedere, senza prestare il proprio consenso all'installazione e all'uso di <i>cookie</i>, ad un contenuto o a un servizio equivalenti, da valutarsi alla luce dei principi del <i>Regolamento</i>.</p>
Validità dei consensi già raccolti	Se conformi alle caratteristiche richieste dal Regolamento, i consensi raccolti in precedenza mantengono la loro validità a condizione che, al momento della loro acquisizione, siano stati registrati e siano dunque documentabili
Tempo per l'adeguamento dei sistemi e dei trattamenti già in atto ai principi espressi dalle Linee Guida	6 mesi dalla pubblicazione delle Linee Guida nella Gazzetta Ufficiale

