GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Allegato 1 all'Avviso relativo alla consultazione sulle "Linee guida sull'utilizzo di cookie e di altri strumenti di tracciamento" del 26 novembre 2020
(vedi anche allegato 2)

LINEE GUIDA SULL'UTILIZZO DI *COOKIE* E DI ALTRI STRUMENTI DI TRACCIAMENTO

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 *online* 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 (cd. direttiva *ePrivacy*) e successive modifiche, come recepita nell'ordinamento nazionale all'art. 122 del d.lgs. 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 (provvedimento n. 229, dell'8 maggio 2014), teso a "*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, par. 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 attuato 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 regolamentari frattanto intervenute e al monitoraggio che, anche per il tramite delle numerose segnalazioni e richieste di pareri pervenute, l'Autorità ha effettuato sulla concreta 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 di non ancora codificate potenziali pervasività.

Infine, deve essere tenuta in considerazione l'evoluzione comportamentale degli stessi utenti della rete, sempre più orientati alla proliferazione delle proprie identità digitali come risultanti dall'accesso a molteplici 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 (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.

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 "prima parte") 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 personal 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* ed 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*.

[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*).

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 funzioni tra le più disparate, compresi l'esecuzione di autenticazioni informatiche, il monitoraggio di sessioni, la memorizzazione di informazioni su specifiche configurazioni riguardanti gli utenti che accedono al *server*, l'agevolazione nella fruizione dei contenuti *online* 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. I *cookie* cd. "di autenticazione" sono di particolare importanza ogni qualvolta sia necessaria una verifica in ordine al soggetto che accede a determinati servizi, come ad esempio quelli bancari.

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.

3. Altri strumenti di tracciamento

Il medesimo risultato può essere conseguito anche mediante l'utilizzo di altri strumenti (c.d. "identificativi attivi" e "passivi", questi ultimi presupponendo la mera osservazione), che consentono di effettuare trattamenti analoghi a quelli sopra indicati.

Tra gli strumenti "passivi", risulta sempre più utilizzato il *fingerprinting*, ossia quella tecnica che consente di identificare il dispositivo utilizzato dall'utente tramite la raccolta 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*. 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*, 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 accesso che non presuppone l'archiviazione di informazioni all'interno del dispositivo dell'utente, bensì la mera lettura 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.

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 inviare messaggi pubblicitari sempre più mirati, cioè in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete.

Analogamente, gli altri strumenti di tracciamento possono essere catalogati secondo una serie di criteri diversi, dei quali il principale resta, tuttavia, la finalità con la quale vengono utilizzati: tecnica o di natura commerciale.

5. Normativa applicabile

Per l'impiego di *cookie* tecnici, in virtù della funzione assolta e nei limiti ed alle condizioni richiamate, il titolare del trattamento sarà assoggettato al solo obbligo di fornire l'informativa, anche eventualmente inserita all'interno dell'informativa di carattere generale, rientrando il loro impiego in una ipotesi codificata di esenzione dall'obbligo di acquisizione del consenso dell'interessato; i *cookie* di profilazione e gli altri strumenti di tracciamento 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*, già menzionato, 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* n. 2002/58/Ce, precedente rispetto alla data della piena operatività degli effetti del *Regolamento* e anch'essa, al pari delle norme di diritto interno che la recepiscono, 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*").

Ad esclusione delle fattispecie disciplinate in via esclusiva ed esaustiva dalla direttiva *ePrivacy*, molte attività di trattamento devono dunque essere ricondotte all'ambito di applicazione tanto della direttiva quanto del *Regolamento*[2], con la specificazione 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 regole del *Regolamento*, essa, in quanto *lex specialis,* dovrà essere applicata e prevarrà sulle (più generali) disposizioni del *Regolamento*. Queste ultime restano 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 identificativi; ma è nel *Regolamento* che andranno ricercate le specifiche caratteristiche di quel consenso ai fini della sua validità e conformità alla disciplina generale.

6. Le modalità per l'acquisizione del consenso *online* alla luce di alcuni opportuni chiarimenti e nuove raccomandazioni

6.1 Il c.d. "*scrolling*" e il divieto di *cookie wall*

Il Garante ritiene che l'impianto teso alla individuazione della modalità tecnica per l'acquisizione del consenso *online* per il tracciamento a mezzo *cookie* illustrato nel menzionato provvedimento del maggio 2014 sia da ritenersi tuttora valido, anche nel mutato assetto normativo che privilegia ed impone ai titolari di agire in ossequio al nuovo regime di *accountability* (art. 5, par. 2 del *Regolamento*).

[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).

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

Si ritiene, 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* di profilazione nonché all'utilizzo del c.d. *cookie wall*.

Al riguardo appare, innanzitutto, opportuno ricordare 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. 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*".

Con specifico riferimento alla materia oggetto delle presenti linee guida, l'EDPB ha, inoltre, di recente (parere n. 5/2020, del 4 maggio 2020) chiarito che il semplice *scrolling* non sarebbe mai idoneo, 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 equivarrebbe consenso "in nessuna circostanza"[4].

Tale affermazione ha creato talune incertezze interpretative in relazione alla prassi diffusa, anche in Italia, di procedere alla raccolta del consenso all'installazione e utilizzo dei *cookie* attraverso il semplice ricorso al c.d. "*scroll down*", l'azione consistente nel lasciare scorrere la pagina così da mostrarne sullo schermo la parte sottostante al banner contenente la c.d. informativa breve.

Il Garante condivide naturalmente l'opinione dell'EDPB che si pone, peraltro, in una coerente linea di continuità rispetto alla posizione già rappresentata con il provvedimento del 2014 e i "*Chiarimenti in merito all'attuazione della normativa in materia di cookie*" del 5 giugno 2015: 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.

Lo *scrolling*, tuttavia, può essere una componente 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 nel senso di prestare il proprio consenso all'uso dei *cookie*.

In questo senso, già nelle FAQ in materia di informativa e consenso per l'uso dei *cookie* del 3 dicembre 2014 si è affermato che qualora le soluzioni adottate "*siano in grado di generare un evento, registrabile e documentabile presso il server del gestore del sito (prima parte), che possa essere qualificato come azione positiva dell'utente*", idonea a manifestare in maniera inequivoca la volontà di prestare un consenso al trattamento, esse saranno da ritenersi "*in linea con i requisiti di legge*".

---

[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).

I *publisher* potrebbero, in ipotesi, fare ricorso a modalità più evolute basate sul paradigma del c.d. "*web dinamico*", che consentono una fluida comunicazione degli eventi generati dall'utente al sito sul quale lo stesso sta navigando. Si fa riferimento, ad esempio, alla trasmissione dal *browser* di eventi quali movimenti del *mouse* all'interno del sito (c.d. "*pattern*"), in grado di segnalare più facilmente, rispetto ai tradizionali bottoni virtuali, azioni positive e inequivocabili dell'utente.

A tali azioni potrebbero corrispondere, infatti, cambiamenti di stato di specifiche aree del sito (quali cambiamenti di colore, formato, posizione, etc.) e/o delle informazioni in esse presenti, cambiamenti che, in funzione del tipo di evento che li ha generati, potrebbero essere codificati dal sito ed interpretati anche come una forma di registrazione del consenso espresso dall'utente per l'installazione dei *cookie*.

Alla ulteriore rigorosa condizione, tuttavia, che tali modalità alternative di espressione del consenso *online*, affinché lo stesso risulti acquisito legittimamente, siano realizzate, appunto, in modo tale da rendere inequivoco anche per l'utente l'effetto finale prodotto dalla propria azione. Ciò, allo scopo di limitare l'incidenza dei c.d. "falsi positivi", ossia di erronee 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 e dotato delle menzionate caratteristiche anche sotto il profilo della riconoscibilità 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, appunto, un meccanismo di "*take it or leave it*", nel quale l'utente venga cioè obbligato ad esprimere il proprio consenso alla ricezione di *cookie* di profilazione, 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, 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*.

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 nella richiesta di consenso

Ancora con riferimento alle modalità di acquisizione del consenso, l'osservazione del comportamento dei siti *web* e il 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. 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'articolo 7 del *Regolamento* richiede che l'acquisizione del consenso sia dimostrabile, il che significa che i titolari che utilizzano *cookie* e altri sistemi di tracciamento devono implementare

meccanismi che permettano loro di provare, in qualsiasi momento, di aver ottenuto validamente il consenso dell'utente.

Il consenso, una volta correttamente acquisito, non dovrà essere nuovamente richiesto se non all'eventuale mutare di una o più delle condizioni alle quali è stato raccolto ovvero 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 nell'ipotesi in cui l'utente scelga di cancellare i *cookie* legittimamente installati nel proprio dispositivo e il titolare non abbia adottato altro sistema per tenere traccia del consenso espresso.

A tale ultimo riguardo giova sottolineare come una simile azione dell'utente, non coinvolgendo il titolare, non sia in alcun modo equiparabile all'esercizio del diritto di revoca del consenso ai sensi del *Regolamento*, che in base alla disposizione del suo art. 7, punto 3, deve essere tanto agevole per l'interessato quanto concederlo.

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 – lo si è anticipato - che il meccanismo di acquisizione del consenso *online* tramite presentazione di un *banner*, come lo si è analiticamente descritto nel provvedimento del maggio 2014, mantenga, ad oggi, una sua intrinseca, sostanziale validità. È tuttavia necessario, anche in questo caso, valutarne 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 consentirne 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* diverso da quelli tecnici venga posizionato all'interno del suo dispositivo, né che venga utilizzata alcuna altra tecnica attiva o passiva di profilazione.

Tuttavia, poiché occorre assicurare anche la libertà di scelta di chi invece intenda accettare di essere profilato, il Garante suggerisce che i gestori dei siti *web* implementino un meccanismo in base al quale l'utente, accedendo alla *home page* (o ad altra pagina) del sito *web*, visualizzi immediatamente un'area di dimensioni sufficienti da costituire una percettibile discontinuità

nella fruizione dei contenuti della pagina *web* che sta visitando, che sia 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 profilazione, dovrebbe dunque limitarsi a chiudere tale finestra o area mediante selezione dell'apposito comando usualmente utilizzato a tale scopo, cioè quello contraddistinto da una X di regola posizionata in alto a destra del *banner* medesimo, senza essere costretto ad accedere ad altre aree o pagine a ciò appositamente dedicate. Si garantirebbe, in tal modo, che appunto *by default*, l'interessato che non intenda esprimere il proprio consenso non sia in alcun modo tracciato o profilato.

In altri termini, il consenso potrà intendersi come validamente prestato soltanto se sarà conseguenza di un intervento attivo e consapevole dell'utente (ad esempio la selezione di un esplicito comando ovvero di un elemento contenuto nella pagina sottostante l'area stessa), 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 area dovrà allora contenere almeno le seguenti indicazioni ed opzioni:

i) l'indicazione di una informativa minima relativa al fatto che il sito utilizza *cookie* tecnici e potrà, esclusivamente previa acquisizione del consenso dell'utente, utilizzare anche *cookie* di profilazione o altri strumenti di tracciamento 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 e/o allo scopo di effettuare analisi e monitoraggio dei comportamenti dei visitatori di siti *web*;

ii) il *link* alla *privacy policy*, ovvero ad una informativa estesa posizionata in un *second layer* 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* tecnici (cfr., al riguardo, il successivo paragrafo 8);

iii) l'indicazione che la prosecuzione della navigazione 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…*" che produca un evento informatico registrabile comporta la prestazione del consenso alla profilazione;

iv) un comando attraverso il quale sia possibile esprimere il proprio consenso alla profilazione accettando il posizionamento di tutti i *cookie* o l'impiego di altre tecniche 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 - ed i *cookie*, anche eventualmente raggruppati per categorie omogenee, al cui utilizzo l'utente scelga di acconsentire.

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.

Evidentemente, laddove sia prevista la sola presenza di *cookie* tecnici, di essi potrà essere data informazione nella *home page* o nell'informativa generale senza l'esigenza di appore 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 *provider*, 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 sottolinea 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.

Sempre all'interno di questa stessa area dovrebbero trovare collocazione anche due ulteriori comandi idonei a garantire il cd. "*diritto di ripensamento*" e di revoca del consenso agli utenti che, avendo già effettuato una specifica scelta al momento del primo accesso al sito *web*, intendano successivamente optare per una scelta diversa. A tali utenti, proprio in ragione della scelta già compiuta e debitamente registrata, ad ogni accesso successivo al primo non verrà infatti riproposto il meccanismo del *banner*, ma la pagina iniziale del sito dovrà comunque rendere sempre disponibile il *link* alla *privacy policy* nonché all'area dedicata alle scelte di maggiore dettaglio.

Appunto in questa area, che qui si descrive, è opportuno vengano collocati, oltre ai comandi relativi alle scelte granulari, due ulteriori comandi che consentano di modificare anche in blocco una scelta precedente; uno per acconsentire all'impiego di tutti i *cookie* o di altri strumenti di tracciamento per chi non vi avesse acconsentito in precedenza, l'altro per revocare, anche in unica soluzione, il consenso eventualmente già espresso. Anche tale scelta dell'utente dovrà naturalmente essere adeguatamente documentata dal titolare.

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

Per realizzare la memorizzazione delle azioni e delle scelte, anche di dettaglio, rimesse all'interessato (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), oppure di altri strumenti di tracciamento diversi dai *cookie* o anche di ulteriori modalità la cui individuazione rientra nell'autonomia imprenditoriale del titolare, adattando opportunamente la propria condotta in modo da tenere comunque costantemente aggiornata la documentazione delle scelte compiute dall'interessato.

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 integrando la struttura dell'indirizzo IP all'interno del *cookie* e mascherando opportune porzioni di quell'indirizzo.

Tenuto conto della rappresentazione degli indirizzi IP versione 4 (IPv4) che, costituiti da numeri interi rappresentati con 32 bit, 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).

Resta inteso che i dati, anche così minimizzati, non dovranno comunque essere combinati con altre elaborazioni (*file* dei clienti o statistiche di visite ad altri siti, ad esempio) o trasmessi a terzi, pena l'inaccettabile incremento delle potenzialità e dunque dei rischi di identificazione dell'utente.

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.

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.

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 *online*, 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. 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.