GARANTE PRIVACY
LINEE GUIDA SULL'UTILIZZO DI COOKIE E DI ALTRI STRUMENTI DI TRACCIAMENTO

1. Introduzione

Le **Linee Guida** sull'utilizzo dei cookie e degli altri strumenti di tracciamento delle attività degli utenti online contengono novità di rilievo. Benché in pubblica consultazione per 30 giorni a partire dal 9 dicembre, saranno certamente oggetto di ampi e approfonditi dibattiti.
Il tanto atteso regolamento che dovrebbe sostituire la direttiva ePrivacy (2002/58/CE) in materia di rispetto della vita privata e protezione dei dati personali nelle comunicazioni elettroniche tarda nel trovare una definitiva comunanza di accordi e le ragioni sono ben note.
I grandi player (i cc.dd. OTT) hanno fatto e fanno del tracciamento capillare degli utenti, unitamente alla sempre più attenta analisi e previsione dei comportamenti e dei desideri dei consumatori un mercato florido, fiorente, massivo e instancabilmente pervasivo, da cui derivano guadagni astronomici. Il behavioural advertising, il fingerprinting, il real time bidding sono fenomeni forse poco conosciuti dal grande pubblico ma estremamente utilizzati dalle big tech.
Il tutto in un settore sostanzialmente governato da imprese private che condizionano il comportamento e le scelte di milioni di utenti.
Le regioni che in Europa vorrebbero riportare il controllo delle attività sulla rete dalla parte degli individui si scontrano con interessi economici enormi: questa, in parole estremamente semplificate, la ragione per cui il Regolamento che avrebbe dovuto "accompagnare" il GDPR (che si applica esclusivamente al trattamento dei dati personali degli interessati persone fisiche, mentre la direttiva ePrivacy si applica anche alle attività poste in essere da "utenti" e "contraenti" e, pertanto, anche dalle imprese: v. per riferimenti l'art. 121 Cod. Privacy), stenta nel trovare il definitivo via libera.

2. Fonti normative

Le fonti normative in materia:

- Direttiva 2002/58/Ce (cd. **direttiva ePrivacy**) e successive modifiche,
- **Art. 122** del d.lgs. 30 giugno 2003, n. 196, Codice Privacy,
- **G.D.P.R.** (Reg. EU 679/2016, in particolare artt. 4 e 7),
- **Guidelines 05/2020 on consent under Regulation 2016/679** (4 maggio 2020),
- Provv. Garante Italiano **8 maggio 2014**.

3. Cookie tecnici e cookie di profilazione. Opt-In.

Riassumendo in modo estremamente sintetico quanto si desume dal complesso delle disposizioni normative e dalle indicazioni dei Garanti in tema, la principale suddivisione che deve essere tenuta

a mente in relazione ai cookie e agli altri strumenti di tracciamento delle attività degli utenti deve essere riguardata sotto la lente della **finalità dello strumento**.

Un cookie è una stringa di testo che i siti web (cd. publisher o "prima parte") visitati dall'utente, o siti e web server diversi (cd. "terze parti") posiziona e archivia (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 (si tratti di un tablet, di un pc, di uno smartphone o di altro dispositivo comunque connesso alla rete, come avviene nel campo dell'IoT).

Il sito visitato trasmette il cookie al device dell'utente che, in occasione di una visita successiva, viene riconosciuto, mantenendo così memoria della sua visita precedente nonché delle attività poste in essere. I cookie possono dunque avere finalità assai utili, come ricordare gli articoli del carrello già selezionati, autenticazioni vere e proprie (le credenziali di accesso a particolari pagine), scelte e preferenze come quelle della lingua dell'utente e molte altre specificità.

Certamente favoriscono la c.d. *user experience* e rendono la navigazione più celere. Altrettanto, "registrando" tutte le attività del navigante, consentono di tracciarne un profilo sia di comportamento attuale sia eventualmente futuro, notevolmente accurato.

Laddove utilizzati, come avviene oggigiorno, in combinazione con altri tracciamenti derivanti dalle tante altre, molteplici attività che ogni utente giornalmente compie, con più dispositivi, su tanti siti, ecco che possiamo ben dire che la combinazione, il collegamento e l'interconnessione di più fonti di informazione derivanti dai cookie consentono non solo di individuare con assoluta precisione gli utenti, ma anche di prevederne, se non addirittura di condizionarne, i comportamenti (Cambridge Analytica è un esempio ormai noto).

A queste indicazioni devono ulteriormente sommarsi quelle, forse più rilevanti, che vedono soprattutto nel campo dei **cookie di terza parte un settore estremamente attivo e pervasivo**: il cookie proveniente da una terza parte consente a quest'ultima e a tutte quelle a questa collegate di creare profili, interconnessi e mutualmente disponibili, che scandagliano le azioni degli utenti e vengono, di fatto, utilizzate per scambi monetari rilevanti.

Gli strumenti di tracciamento oggi disponibili, inoltre, **non sono solo di tipo "attivo"**, ossia che dipendono dalle attività poste in essere dal "navigante", **ma anche "passivi"**: il c.d. **fingerprinting**, per esempio, è una 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.

La tecnica è, se si vuole, ancora più "invasiva" o potenzialmente pericolosa per gli utenti, perché non consente loro di averne conoscenza e l'eventuale "disattivazione" di un tale "controllo" non

dipende dall'utente stesso, ma da colui che tale tecnica utilizza: come indica il Garante, essa consente una "mera lettura delle configurazioni che contraddistinguono (il dispositivo, *ndr*) 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".

Quel che importa sottolineare è che, al di là della "durata" dell'installazione del cookie (o di altro strumento: solo per la "sessione" o per una "durata" maggiore, da qualche ora a diversi mesi o anni), è un'altra la caratteristica, già evidenziata, più rilevante, ovvero che lo strumento, il tracciante, può essere installato direttamente dal titolare del sito (publisher, o **prima parte**) o, da questi, per conto di terzi (di **terza parte**).

Sono questi i cookie che, in gran parte, vengono installati sui nostri dispositivi: una semplice occhiata ai banner oggi disponibili rende pacificamente l'idea di un **mercato ad tech** estremamente vasto e ingordo di nostre navigazioni, preferenze, abitudini e comportamenti.

Il tutto, ovviamente, solo in parte per offrire una "migliore navigazione", giacché la finalità è, in realtà, prettamente commerciale: offrire ai produttori di beni dati per vendere i beni.

Ai fini delle Linee Guida è però opportuno segnalare quanto segue: è la finalità del cookie che ne determina il regime giuridico. In particolare:

- **i cookie tecnici non richiedono il consenso** mentre
- per quanto riguarda **i cookie di profilazione** il regime è quello, esclusivo, dell'**opt in: l'utente deve prestare il proprio consenso**.

Viene pertanto confermata l'impostazione per la quale la direttiva ePrivacy, in quanto norma speciale, si applica in relazione agli obblighi relativi all'installazione dei traccianti e prevede, anche in Italia, trasfusa nel Codice Privacy post DL.gs. 101/2018, il necessario consenso per il posizionamento (salvi, ex art. 122, i cookie tecnici).

Per quanto riguarda, invece, le "caratteristiche" del consenso, valgono i principi dettati dal Regolamento Europeo n. 679/2016, sia in relazione alla manifestazione dello stesso, libera, specifica, inequivocabile, informata e revocabile, sia in relazione agli obblighi, ricadenti sul titolare, di poter giustificare e documentare, nel solco dell'*accountability*, la concreta attuazione dei principi di protezione dei dati personali (v. al riguardo art. 5 GDPR).

4. Come strutturare la home page di default

L'art. 25 del GDPR impone, per qualsiasi trattamento di dati, che il titolare garantisca 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.

a. Opt out di default

Ciò significa, né più né meno che nessun cookie (né altro strumento, attivo o passivo), al di fuori di quelli tecnici effettivamente necessari, possa essere installato di default dal titolare del sito.

Dovrà essere prevista una apposita "area" del sito, nella homepage o in altra pagina (e, di conseguenza, anche nelle pagine interne se direttamente disponibili alla navigazione) che, con una **apprezzabile discontinuità nella fruizione dell'esperienza dell'utente**, dia facoltà, a chi non intenda acconsentire all'utilizzo degli strumenti di tracciamento (tutti, si ribadisce: attivi e passivi), **semplicemente di chiudere il banner e proseguire la navigazione senza essere tracciato** e senza essere costretto, per ottenere il medesimo risultato, ad accedere ad altre pagine o aree ove effettuare una scelta.

Chi, al contrario, desiderasse optare per il tracciamento, potrà e dovrà farlo consapevolmente, per ciascuna, separata, finalità proposta dal titolare del sito. Va da sé che si dovrà prevedere un adeguato meccanismo per documentare tale scelta, libera, attiva e consapevole, tenendo presente anche la possibilità di modifica della stessa da parte dell'utente.

b. La configurazione del sito

Il Garante propone dunque che i siti siano configurati come segue:

1. Predisposizione di una **informativa "minima"** con indicazione dell'utilizzo di cookie tecnici che chiarisca che, esclusivamente dietro consenso dell'utente, sarà possibile utilizzare anche strumenti di profilazione o tracciamento, con specificazione delle relative finalità;

2. Predisposizione del **link alla privacy policy** o informativa estesa in un secondo layer, un secondo "strato" informativo completa ai sensi dell'art. 12 e dell'art. 13 del GDPR, anche con riferimento ai cookie tecnici;

3. L'**indicazione** che il consenso alla profilazione deve consistere in 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…" e che ciò produce un evento informatico registrabile;

4. La predisposizione dell'**apposito comando** (casella per il flag o altro) per esprimere chiaramente tale consenso o l'utilizzo di altre modalità chiaramente individuabili che esprimano senza margini di dubbio il comportamento attivo dell'utente che intenda manifestare il consenso;

5. Predisposizione di un **apposito link** dove sia possibile una analitica selezione

a. delle funzionalità,
b. delle terze parti e
c. dei cookie (anche raggruppati per categorie omogenee) cui l'utente scelga di aderire.
d. All'interno di questa area deve essere prevista una sezione dedicata al "**ripensamento**" e alla "revoca" dei precedenti consensi.

c. Gli accessi successivi

Ne deriva che il titolare deve predisporre un sistema per il quale agli utenti che, avendo già effettuato una specifica scelta al momento del primo accesso al sito web agli accessi successivi 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.

d. Diniego di default

Fermo restando che se presenti solo cookie tecnici di questi si potrà dare informazione anche solo nella Informativa "generale", per quanto riguarda le restanti tipologie di cookie il Garante precisa che "le possibili scelte granulari" dovranno essere **"inizialmente tutte preimpostate sul diniego all'installazione dei cookie"**.

In sostanza l'utente deve poter **esclusivamente accettare l'installazione in modo granulare**.

5. I cookie wall e il mero scrolling

Il Garante rivede anche, in chiave di adeguamento delle proprie prescrizioni al mutato contesto tecnologico e all'entrata in vigore del Regolamento, le indicazioni di cui al provvedimento del maggio 2014.

Lo ***scroll down***, pertanto, ossia il mero "scivolamento" sulla pagina, del cursore o del mouse non può più, oggi, ritenersi qualificabile quale consenso all'installazione dei cookie di profilazione e ciò, come indicato anche dall'EDPB nelle già citate Linee Guida 5/2020, "in nessuna circostanza".

Inadatto, da solo, alla raccolta dei cookie, lo scrolling, tuttavia, ove "componente di un più articolato processo, che consenta comunque all'utente di segnalare al titolare, con la generazione di un vero e proprio *pattern*, una scelta inequivoca", nel senso della prestazione del proprio consenso, potrà invece ritenersi metodologia confacente.

Come si vedrà oltre, ove il titolare, anche mediante particolari configurazioni grafiche e tecnologiche, precostituisca un "processo" atto a informare compiutamente l'utente delle scelte operabili e delle relative conseguenze, e lo faccia anche mediante l'utilizzo di schemi comportamentali inequivoci: già con le precedenti indicazioni del WP 29 (dell'aprile 2018) e ulteriormente con le citate Linee Guida del 2020, il Comitato dei Garanti Europei ha ribadito che la manifestazione del consenso deve consistere in una non equivoca e non ambigua manifestazione di volontà, concretantesi in un atto positivo e affermativo, attraverso un movimento o una dichiarazione attive, di modo che sia "ovvio che l'interessato abbia prestato il proprio consenso per quel particolare trattamento" (Linee Guida citt., punto n. 3.4., 75). Va da sé che un consenso di tal genere potrà essere prestato solo in presenza di idonee informazioni, nel senso già visto, e adeguatamente documentabile (si richiama al riguardo il Considerando n. 32 del Regolamento).

Anche il c.d. ***cookie wall***, ossia il "banner" o, comunque, il meccanismo che impone all'utente di accettare integralmente l'installazione dei traccianti deve essere ritenuto non conforme, soprattutto laddove esso, ove non "acconsentito", impedisca l'ulteriore navigazione: salva l'ipotesi in cui il titolare offra all'interessato la possibilità di accedere comunque ad un servizio equivalente senza prestare alcun consenso, tale modalità, del tipo "take it or leave" è da considerarsi illecita.

6. Informazioni stratificate, multilayer, multichannel

Da tempo le Autorità, nazionale ed europee come anche lo stesso GDPR sottolineano l'importanza di improntare le informazioni rese agli interessati ai principi di completezza, chiarezza espositiva, efficacia e fruibilità: basti pensare alle informative "minime" o abbreviate già un uso nel settore dei dispositivi di videosorveglianza.

Il Garante sottolinea, oltre quanto già suggerito nel precedente provvedimento del 2014, come le impostazioni debbano essere improntate ad una logica di semplificazione, che può concretizzarsi con informative ***multilayer***, dislocate su più livelli, oppure per il tramite di più canali e modalità (***multichannel***), in modo da sfruttare al massimo più dinamici e meno tradizionali ulteriori punti di

contatto tra il titolare e gli interessati. Gli esempi fanno riferimento “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.”.

7. Gli analytics

Questi cookie servono per valutare l’efficacia di un servizio, per la progettazione di un sito, per misurare il traffico, per verificare le aree di appartenenza degli utenti, gli orari di connessione, ecc..

Sebbene in precedenza indicati come meramente “tecnici”, l’entrata in vigore del GDPR e lo sviluppo tecnologico impongono una diversa valutazione.

Il Garante ritiene imprescindibile che a tali strumenti venga applicato il principio di minimizzazione, di modo che sia significativamente ridotto il loro potere identificativo, soprattutto laddove il loro utilizzo avvenga ad opera di “terze parti”.

Perché si possano inquadrare tra i “meramente” tecnici, è pertanto “indispensabile **precludere la possibilità che si pervenga, mediante il loro utilizzo, alla diretta individuazione dell’interessato** (cd. single out), il che equivale a impedire l’impiego di cookie analytics che, per le loro caratteristiche, possano risultare identificatori diretti ed univoci.”

Sulla base della struttura di tali cookie, l’Autorità suggerisce pertanto di provvedere al mascheramento almeno di una parte della componente dell’indirizzo Ip (sia per le versioni IPv4 sia per le versioni IPv6), di modo che ne derivi la non identificabilità dell’utente.

Il problema, peraltro, da affrontare da parte dei Titolari e dei tecnici, sarà quello di **evitare combinazioni con altre elaborazioni**, o di **impedirne la trasmissione a terzi**, mantenendone l’uso esclusivamente per la produzione di statistiche aggregate e in relazione a un singolo sito o applicazione mobile, affinché non ne derivi il tracciamento dell’utente.

Va da sé che la parte più ardua da affrontare del provvedimento in esame pare proprio quella dei cookie in questione, diffusi e utilizzati in grandissima parte sino a oggi dai siti e che, in base a quanto per ora previsto e salve eventuali modifiche post consultazione, renderebbero la stragrande maggioranza dei siti attualmente online non conformi.

**

Sarà interessante leggere le reazioni e i suggerimenti degli stakeholder: l'attuale panorama dei siti web, che ha visto, anche mercé l'utilizzo di applicativi di grandi operatori, un fiorire di banner e pop up dei più diversi tipi, è in fermento.

Di certo, leggendo le Linee Guida, non si trova alcun accenno al tanto utilizzato, ultimamente, dai *publisher*, "legittimo interesse", base giuridica "alternativa", per così dire... che in molti hanno già evidenziato non essere affatto legittima, sebbene dichiarata in molti banner informativi proposti dai titolari per finalità di profilazione degli utenti.

Staremo a vedere.