



## WEB MARKETING E COOKIE: cosa sapere sui nuovi adempimenti

a cura del D&L Department dello [Studio Legale Lisi](#)

redatto da: Graziano Garrisi, Sarah Ungaro, Chiara Pascali,

Stefano Frontini, Enrica Maio

con la supervisione di Andrea Lisi e la collaborazione di **ANORC** che ha partecipato al tavolo di lavoro sui cookie dell'Autorità Garante per la protezione dei dati personali

## Sommario

1.	Ruoli e responsabilità privacy nelle attività di marketing, profilazione e cessione a terzi	3
2.	Direct marketing, soft spam e social marketing	4
3.	Il consenso e le finalità	6
4.	Cookie ed e-commerce	7
5.	Cookie tecnici e cookie di profilazione	7
6.	Cookie, informativa e consenso	9
7.	Banner e informativa breve sull'utilizzo dei cookie	10
8.	Consenso al trattamento dei cookie di profilazione (di prima o terza parte)	11
9.	L'informativa estesa	12
10.	La conservazione del cookie tecnico del consenso e il suo valore probatorio	13
11.	La notificazione del trattamento al Garante	16
12.	Sanzioni	16
13.	Gli ultimi chiarimenti del Garante circa l'attuazione della normativa sui cookie	17

## 1. Ruoli e responsabilità privacy nelle attività di marketing, profilazione e cessione a terzi

Il web ha avuto un notevole impatto sulle nostre vite: oggi, infatti, molte delle decisioni d'acquisto degli utenti sono influenzate dall'esperienza online, motivo per il quale anche le aziende hanno dovuto adeguare le loro **strategie di marketing e comunicazione** ai canali web. In questa prospettiva, le aziende si trovano davanti a nuove e importanti sfide. Internet ha diversificato i **target** creando "tribù", ossia nicchie di mercato a cui si può arrivare solo grazie a un'adeguata profilazione del proprio target di riferimento. Il pubblico del web ha un'attenzione limitata, gli utenti fruiscono solo dei contenuti per cui nutrono degli interessi specifici, sono abituati a interagire e condividere. Le attività di web marketing sono perciò concentrate sulla **user experience** dell'utente, ma spesso la necessità di **lead generation**<sup>1</sup> altamente profilata porta le aziende a trascurare le questioni legate alla privacy.

In effetti, l'attività di marketing promozionale spesso si scontra con la riservatezza degli individui (utenti e consumatori) e trovare un giusto equilibrio non è poi così semplice.

Per fornire un ausilio a tutti gli operatori commerciali, l'Autorità Garante per la protezione dei dati personali ha emanato il provvedimento "*Linee Guida in materia di attività promozionale e contrasto allo spam*" del 4 luglio 2013 (provvedimento del Garante n. 330/2013), con il quale ha fornito un primo schema di regole e indicazioni utili alle aziende che intendano avviare delle campagne promozionali o che già abbiano adottato specifiche politiche commerciali aziendali.

Il Garante ha voluto altresì regolamentare i ruoli e le relative responsabilità che, molto spesso, non vengono correttamente individuati tra i vari operatori coinvolti nel trattamento. A questo proposito, infatti, è da considerare il parere del Gruppo Art. 29 n. 1/2010, il quale ha chiarito che, ai fini dell'individuazione della titolarità concretamente esercitata, occorre esaminare anche "*elementi extracontrattuali, quali il controllo reale esercitato da una parte, l'immagine data agli interessati e il legittimo affidamento di questi ultimi sulla base di questa visibilità*".

Anche riguardo allo spam effettuato mediante agenti o terzi, il soggetto promotore, qualora abbia un ruolo preminente nel trattamento dei dati dei destinatari, assuma decisioni relative alla finalità e modalità del trattamento, fornisca istruzioni e direttive vincolanti e svolga verifiche e controlli sull'attività dell'agente, va considerato titolare ai sensi dell'art. 28 del Codice Privacy, **a prescindere dalla qualificazione contrattuale**. In più, egli dovrà nominare responsabile, ai sensi dell'art. 29 D.lgs. 196/2003, il soggetto agente o altro terzo di cui si avvale per attività promozionale, mentre i singoli operatori dovranno essere nominati incaricati ai sensi dell'art. 30.

---

<sup>1</sup> Azione di marketing che consente di generare una lista di possibili clienti interessati ai prodotti o servizi offerti da un'azienda.

Eventuali sub-agenti o terzi coinvolti nel trattamento, nell'ambito del rapporto titolare (promotore) e responsabile (agente), potranno essere nominati o direttamente dal promotore quali responsabili/incaricati o potranno assumere il ruolo di "titolari autonomi", ma solo se utilizzano proprie banche dati per le attività promozionali.

Perciò, il titolare sarà individuabile nell'impresa, nella società, nel soggetto che comunque si avvalga di tali piattaforme, oppure nel proprietario delle piattaforme se quest'ultimo le utilizza per svolgere attività promozionale per sé stesso.

Le società che hanno raccolto dati per finalità di marketing **possono cederli ad altri soggetti** che intendano utilizzarli per le stesse finalità solo dopo aver rilasciato al consumatore/utente un'adeguata informativa e aver acquisito il consenso specifico per la cessione e/o comunicazione a terzi dei dati personali per fini promozionali.

## 2. Direct marketing, soft spam e social marketing

Il **direct marketing** può essere definito come quell'insieme di attività di marketing finalizzate a porre in essere un'interazione con i clienti potenziali o reali di un'azienda. Possono individuarsi varie forme di direct marketing:

- **direct mail**: si realizza attraverso l'invio, a un preciso gruppo di soggetti, di materiale pubblicitario o promozionale specificatamente indirizzato e personalizzato, a mezzo posta, fax, email, SMS, etc.;

- **e-mail marketing**: si tratta di una forma di comunicazione tramite email o newsletter con obiettivi promozionali e informativi;

- **telemarketing**: trattasi di marketing realizzato mediante telefono. Si basa su un colloquio telefonico, svolto su liste di nominativi e finalizzato ad avere risposte precise in merito a una proposta di un'azienda, (outbound) e sulla raccolta sistematica di informazioni (inbound);

- **messaggi diretti multimediali (SMS, pay tv, etc.)**: una recente tipologia di marketing che sfrutta i nuovi media per comunicazioni di tipo promozionale e commerciale.

Il marketing diretto con fini promozionali, ovvero relativo all'invio di materiale pubblicitario, alla vendita diretta, al compimento di ricerche di mercato o alla comunicazione commerciale (con o senza l'uso di strumenti automatizzati di contatto quali email, SMS, telefax, MMS, etc.) e lo spam sono stati da sempre al centro dell'attenzione dell'Autorità Garante e, spesso, anche motivo di provvedimenti sanzionatori nei confronti dei numerosi titolari del trattamento che ponevano in essere campagne commerciali che oltrepassavano i limiti imposti dalla normativa.

L'Autorità Garante ha voluto ribadire che il **consenso** alla trasmissione dei propri dati del soggetto interessato deve essere sempre **specifico e distinto** a seconda del perseguimento di **finalità di marketing, profilazione o comunicazione a terzi**. C'è da sottolineare che il Codice Privacy prevede - all'art. 7 comma 4, lett. b, all'art.

130, comma 1 e all'art. 140 - più possibili finalità di marketing, ossia quelle di invio di materiale pubblicitario, di vendita diretta, di compimento di ricerche di mercato e di comunicazione commerciale e, a tal proposito, l'Autorità ha chiarito che non è necessario un consenso specifico per ciascuna di esse, in quanto ritiene che le suddette attività "siano funzionali a perseguire un'unica finalità *latu sensu* di marketing, con la conseguenza che il connesso trattamento appare giustificare l'acquisizione di un unico consenso".

Inoltre, il Garante, nel suo provvedimento n. 330 del 4 luglio 2013, ha citato per la prima volta il termine di "soft spam" per l'invio di posta elettronica promozionale, quale causa di esonero dall'acquisizione del consenso. Infatti, come stabilito dall'art. 130, comma 4 del Dlgs. 196/2003, *"se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni"*.

Tra gli altri temi affrontati, c'è quello del **social media marketing**, che può essere considerato come una branca del marketing che permette di dare visibilità a un'azienda o a un brand sui social media e, in generale, sulle diverse piattaforme del web 2.0.

Il **social media marketing**, infatti, consente di creare un rapporto paritetico tra aziende e clienti, i quali possono interagire tra loro, generando il cosiddetto *engagement*, avendo, così, la possibilità di ottenere feedback, consigli, opinioni e review.

Il mondo dei social network è ancora privo di una regolamentazione normativa e, per questo motivo, il Garante ha voluto indirizzare tutti gli interessati verso comportamenti che tutelino i dati personali degli utenti.

Posto, infatti, che l'agevole rintracciabilità di dati personali sul web e sui **social network** e altri servizi (come Facebook, Twitter, Skype, Whatsapp, Messenger, etc.) non autorizza nessuno a utilizzarli per inviare comunicazioni promozionali automatizzate senza il consenso dei destinatari, secondo il provvedimento del Garante n. 330/2013, il titolare del trattamento può tranquillamente inviare offerte commerciali ai propri "fan" o "follower" sui social media, quando dalla loro iscrizione alla pagina aziendale si evinca chiaramente l'interesse o il consenso a ricevere messaggi pubblicitari riguardanti il marchio, il prodotto o il servizio offerto, altrimenti sarà sempre necessario il consenso del destinatario per l'uso dei dati presenti su Internet e social network finalizzato all'invio di messaggi promozionali. Vi è un caso, tuttavia, per il quale si può prescindere dall'acquisire il consenso e riguarda l'invio di email o SMS con offerte promozionali ad "amici" a titolo meramente personale o attraverso il c.d. meccanismo del "passaparola".

### 3. Il consenso e le finalità

Il Garante Privacy, nel citato provvedimento n. 330/2013, ha sottolineato anche l'importanza di ottenere il consenso del contraente/utente come adempimento imprescindibile per effettuare attività di marketing.

Il consenso deve essere **libero, informato e documentato per iscritto**; l'Autorità ha spiegato che "documentato per iscritto" non vuol dire necessariamente in "forma scritta" e, infatti, gli operatori possono ritenersi liberi di scegliere il metodo organizzativo più opportuno per fornire la prova della sua acquisizione, tant'è che gli elementi minimi da attestare sono la data e gli estremi identificativi di chi lo ha concesso o un file di log che conservi traccia del rilascio di tale consenso.

Inoltre, circa la legittimità delle comunicazioni promozionali effettuate in assenza di preventivo consenso, esse non sono da considerarsi lecite né nel caso in cui con le medesime si avvisi il ricevente della possibilità di opporsi a ulteriori invii, né nel caso si chieda, con il primo messaggio promozionale, il consenso al trattamento dei dati per finalità promozionali<sup>2</sup>.

Il **consenso deve essere specifico** per ciascuna eventuale **finalità** perseguita, compresa la comunicazione a terzi dei dati dell'interessato per l'invio di messaggi promozionali. Il titolare dovrà acquisire un consenso specifico e distinto a seconda del perseguimento di finalità di marketing, profilazione o comunicazione/cessione a terzi.

In quest'ultimo caso, la comunicazione o cessione a terzi di dati personali per finalità di marketing non può fondarsi sull'acquisizione di un unico e generico consenso da parte degli interessati, tant'è che nell'informativa occorre indicare ciascuno dei terzi o, in alternativa, le categorie, economiche o merceologiche, di appartenenza degli stessi. In più, il consenso richiesto per eventuali comunicazioni o cessioni a terzi deve essere distinto da quello richiesto dal medesimo titolare per svolgere esso stesso attività promozionale.

Si ricorda che per il **direct marketing** vi è la possibilità di acquisire un solo consenso al trattamento, ai sensi dell'art. 130, comma 4 del Dlgs. 196/2003, adottando, ovviamente, tutte quelle misure atte a garantire il diritto alla protezione dei dati personali degli interessati.

L'Autorità Garante ha anche dichiarato che, ai fini dell'adempimento dell'obbligo del consenso, i soggetti appartenenti al medesimo gruppo societario debbano essere ritenuti quali "titolari autonomi" e distinti titolari dei rispettivi trattamenti.

---

<sup>2</sup> Questo punto deve essere ben interpretato dagli operatori del mercato per non rischiare di bloccare qualsiasi progetto o campagna promozionale e di marketing; una prima e-mail contenente una descrizione dell'azienda, senza l'indicazione di alcuna offerta commerciale o promozionale, infatti, si ritiene possa essere lecita e utilizzabile ai fini dell'acquisizione del consenso al trattamento.

#### 4. Cookie ed e-commerce

I **cookie** sono delle informazioni contenute in piccoli file di testo che vengono memorizzate dal dispositivo degli utenti (computer, tablet, smartphone, etc.) nel momento in cui visitano un sito web; una volta memorizzati, questi file vengono poi ritrasmessi agli stessi siti nelle visite successive. Queste porzioni di testo, che sono composte da lettere e numeri, sono oramai presenti nei browser di tutti gli internauti in massicce quantità e spesso hanno proprietà di notevole persistenza temporale.

I cookie possono avere **funzioni** molto differenti: dal monitoraggio di sessioni all'esecuzione di autenticazioni informatiche, alla memorizzazione delle preferenze o ad altre ancora, e l'impatto che essi hanno sulla privacy degli utenti dipende proprio da queste diverse finalità.

In base alle peculiarità del singolo cookie e al punto di vista da cui si prendono in considerazione, variano sensibilmente gli effetti e le criticità dell'utilizzo degli stessi. Si possono avere, infatti, cookie utili a migliorare la navigazione nel sito e solidali con il tipo di operazione che l'utente sta compiendo sul sito stesso (come ad esempio l'acquisto di prodotti online sui siti di e-commerce) e cookie che, invece, mirano a raccogliere informazioni sul tipo di navigazione effettuata dal soggetto per altre finalità, ad esempio di marketing. È, infatti, attraverso le informazioni raccolte da questi particolari cookie che gli internauti, dopo aver navigato sul web e fatto delle ricerche, magari riguardanti un hobby, una passione o un acquisto on line, vedono comparire sulla propria pagina social o nella casella di posta elettronica messaggi pubblicitari di oggetti simili o comunque inerenti alle ricerche effettuate sul web<sup>3</sup>.

Sebbene sul web siano individuabili innumerevoli e variegata tipologie di cookie, è possibile operare una classificazione funzionale degli stessi dalla quale derivano diversi rischi per la protezione dei dati personali e da cui conseguono, perciò, diversi adempimenti obbligatori per i soggetti che li utilizzano.

Per regolamentare questa delicata materia, l'Autorità Garante Privacy con un provvedimento generale pubblicato sulla Gazzetta ufficiale (*"Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie"* del 8 maggio 2014), adottato al termine di una consultazione pubblica, ha individuato modalità semplificate per rendere agli utenti l'informativa on line sull'uso dei cookie e ha fornito indicazioni per acquisire il consenso, quando richiesto dalla legge.

#### 5. Cookie tecnici e cookie di profilazione

In via generale, una prima distinzione riguarda i c.d. **"session cookie"**, che vengono cancellati non appena viene chiuso il browser dell'utente, e i c.d. **"cookie**

---

<sup>3</sup>Questo accade perché alcuni spazi web sono progettati per riconoscere il pc o un altro terminale che l'utente utilizza per collegarsi al web (smartphone, tablet) ed eventualmente indirizzargli messaggi promozionali c.d. "profilati" in base alle sue ricerche e al suo utilizzo di Internet.

**temporanei/permanenti**”, che vengono salvati sul dispositivo dell’utente per un lungo periodo o definitivamente.

Tuttavia, la più importante e utile diversificazione da tener presente ai fini del provvedimento dell’Autorità Garante è quella delle due grandi macro categorie dei **“cookie tecnici”** e dei **“cookie di profilazione”**.

I **cookie tecnici** sono quelli 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 dall’abbonato o dall’utente<sup>4</sup>. Questi cookie sono fondamentali per le normali funzionalità del sito e non sono utilizzati per scopi ulteriori. Essi possono, a loro volta, essere divisi in altre sottocategorie:

- **Cookie di navigazione**

Sono quelli che consentono al sito di funzionare correttamente, permettendo la navigazione e la fornitura dei servizi richiesti dall’utente. Essi sono temporanei e vengono cancellati al termine del periodo di durata. Senza il ricorso a tale tipo di cookie alcune operazioni sarebbero meno sicure o più complesse e, in alcuni casi, non potrebbero proprio essere compiute<sup>5</sup>.

- **Cookie funzionali**

Sono quelli che consentono al sito, in base alle indicazioni dell’utente, di memorizzare alcune delle informazioni della sua navigazione, al fine di riutilizzarle nelle navigazioni successive, migliorando così la qualità del servizio offerto.

- **Cookie analitici**

Sono quelli utilizzati per l’elaborazione di analisi statistiche delle modalità di navigazione del sito. Sono dati anonimi e sono, di solito, utilizzati per migliorare le funzionalità del sito tramite la raccolta dei dati dell’utenza che lo utilizza.

Altra macro categoria è, poi, quella dei **cookie di profilazione**.

Essi sono utilizzati per tracciare le abitudini di navigazione degli utenti con lo scopo di creare profili dei loro gusti, delle loro abitudini, delle scelte prese o di altre

---

<sup>4</sup>Così come indicato nel Provvedimento del Garante per la protezione dei dati personali dell’8 maggio 2014 – *Individuazione delle modalità semplificate per l’informativa e l’acquisizione del consenso per l’uso dei cookie*, [Doc-Web n. 3118884], viene fatto espresso riferimento al primo comma dell’articolo 122 del Decreto legislativo 30 giugno 2003, 196 (Codice in materia di protezione dei dati personali) dove è stabilito che l’archiviazione delle informazioni nell’apparecchio terminale di un contraente o di un utente o l’accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l’utente abbia espresso il proprio consenso dopo essere stato informato con le modalità semplificate di cui all’articolo 13, comma 3, ma che ciò non vieta l’eventuale archiviazione tecnica o l’accesso alle informazioni già archiviate se finalizzati unicamente a 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.

<sup>5</sup>Il Garante per la protezione dei dati personali (*Informativa e consenso per l’uso dei cookie – FAQ, Doc-Web:*

3585077) porta come esempio le attività di home banking (visualizzazione dell’estratto conto, bonifici, pagamento bollette, etc.) per le quali i cookie, che consentono di effettuare e mantenere l’identificazione dell’utente nell’ambito della sessione, risultano indispensabili.



informazioni. A seguito di questa attività vengono poi inviati all'utente profilato messaggi pubblicitari mirati, in linea con le preferenze manifestate dallo stesso durante la navigazione.

Ovviamente, come si può intuire, questi strumenti hanno un grado di invasività, nei confronti dei dati personali degli utenti, completamente diverso rispetto ai cookie tecnici e per questo sono necessari presidi differenti nell'utilizzo di questi sistemi di tracking.

Di notevole importanza è, poi, anche un'ulteriore differenziazione possibile: quella tra **cookie di prima e terza parte**. Tale declinazione deriva dall'individuazione del soggetto che invia i cookie ai dispositivi dei naviganti, a seconda che tale soggetto sia lo stesso editore del sito visitato (prima parte) o un altro soggetto proprietario di un sito differente, una "terza parte" appunto.

Le conseguenze che derivano dall'individuazione del soggetto che installa i cookie non sono affatto di poco conto. È sulla base di ciò, infatti, che vengono definiti ruoli e responsabilità relativamente al rilascio dell'informativa e all'acquisizione del consenso degli utenti del sito (qualora si utilizzino cookie di profilazione).

Sicuramente non è possibile imporre all'editore del sito principale l'obbligo di fornire l'informativa e di acquisire il consenso anche per i cookie installati dalle terze parti, perché non è detto che abbia la capacità economica e giuridica necessaria per farlo.

D'altronde, gli editori dei siti che permettono l'installazione di cookie di terze parti vengono considerati (ai sensi del provvedimento emanato dall'Autorità Garante) come una sorta di "intermediari tecnici" tra le terze parti e gli utenti, e non come contitolari delle stesse nel trattamento.

## **6. Cookie, informativa e consenso**

In considerazione dell'esponentiale diffusione dei cookie in rete e dell'importante e a volte imprescindibile funzione degli stessi, appare chiaro che le modalità di presentazione dell'informativa e di acquisizione del consenso abbiano un impatto di grande rilievo per gli utenti e per gli editori.

Nello specifico, il Garante con il provvedimento 8 maggio 2014 ha ritenuto che una soluzione efficace ai fini della semplificazione dell'**informativa** sia quella di impostare la stessa **su due livelli di approfondimento** successivi: un primo livello in cui viene presentata all'utente, al primo accesso, un'informativa breve, e un secondo livello in cui l'utente interessato possa accedere all'informativa estesa cliccando su un link.

Il Garante, inoltre, anche alla luce delle esigenze emerse in occasione della consultazione pubblica effettuata e degli incontri tenuti, ha maturato la convinzione che informativa e consenso vadano trattati congiuntamente al fine di scongiurare che il ricorso a modalità troppo complesse di espressione del consenso possa rendere vani gli sforzi di semplificazione dell'informativa.

Affinché le istanze di semplificazione siano soddisfatte, sostiene quindi il Garante, è necessario che la richiesta di consenso sull'uso dei cookie di profilazione sia presente proprio nel banner in cui è contenuta l'informativa breve.

## 7. Banner e informativa breve sull'utilizzo dei cookie

Ai fini del rispetto di quanto stabilito dall'art. 13 del Codice Privacy, nel momento in cui l'utente accede per la prima volta al sito web (sia essa la home page o un'altra pagina dalla quale l'utente possa accedere al sito) deve essergli fornita **l'informativa breve**, collocata in un **banner** a comparsa istantanea sulla pagina navigata, contenente anche un **link** attraverso il quale sia possibile accedere **all'informativa estesa**.

In particolare, il banner dovrà preferibilmente avere le seguenti caratteristiche:

- dimensioni tali da essere facilmente visibile, o – in alternativa – espandibile (ad esempio, strip autoespandibile o Pushbar);
- caratteri (font) più evidenti rispetto a quelli del sito;
- un colore del fondo contrastante rispetto allo sfondo del sito e al testo del banner stesso.

Tale banner - non "embedded" e dinamico - informerà l'utente circa l'utilizzo di cookie di profilazione da parte del sito, mentre se si utilizzano solo cookie tecnici, di prima o terza parte, nessun banner dovrà essere implementato (pur garantendo comunque all'utente una serie di informazioni che troverà nella privacy policy o nella cookie policy).

Nello specifico, il banner deve comparire non appena si accede al sito web e deve essere di dimensioni idonee, ossia, come stabilito dal Garante, tale da costituire una **percettibile discontinuità** nella fruizione dei contenuti della pagina web che si sta visitando e deve contenere le seguenti indicazioni:

- che il sito utilizza cookie di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete;
- che il sito consente anche l'invio di cookie terze parti (laddove ciò accada);
- il link dell'informativa estesa; ove vengano fornite indicazioni sull'uso di cookie tecnici e analytics, viene data all'utente la possibilità di scegliere quali specifici cookie autorizzare;
- l'indicazione della pagina dell'informativa estesa nella quale è possibile negare il consenso all'uso dei cookie;
- l'indicazione che la prosecuzione della navigazione mediante accesso ad altra area del sito o la selezione di un elemento dello stesso (ad esempio, di un'immagine o di un link) comporta automaticamente la prestazione del consenso all'uso dei cookie.

## **8. Consenso al trattamento dei cookie di profilazione (di prima o terza parte)**

Grazie alle semplificazioni introdotte dall’Autorità Garante, l’utente può, ad esempio, esprimere il proprio consenso nelle seguenti modalità (che devono essere riportate nel banner):

- compiendo un’azione di scorrimento (c.d. scroll down);
- facendo click su uno dei link interni della pagina;
- facendo click (preferibilmente) sul tasto "OK" del banner o sul tasto "X", che può essere posizionato in basso o in alto a destra.

Alla seconda visita dell’utente, ove quest'ultimo abbia espresso la propria preferenza (positiva o negativa) in relazione all'installazione dei cookie, lo script ovviamente non dovrà mostrare più il banner (informativa breve) all’utente. Ove invece l'utente non abbia espresso alcuna preferenza, lo script dovrà mostrare nuovamente il banner.

A titolo esemplificativo, si segnalano alcune tipologie di cookie per le quali è richiesto il consenso e altre per le quali non è richiesto:

### **Cookie esenti dal consenso**

1. “User-input” cookies
2. Authentication cookies
3. "User centric" security cookies
4. Multimedia player session cookies
5. Load balancing session cookies
6. UI customization cookies
7. Social plug-in content sharing cookies

### **Cookie non esenti dal consenso**

1. Social plug-in tracking cookies
2. Third party advertising
3. First party analytics
4. Retargeting/Remarketing
5. Cookie di statistica gestiti completamente dalle terze parti

### **Strumenti di analytics esenti dall’obbligo di consenso:**

- cookie di analytics installati direttamente sul server della prima parte o della propria server farm senza interazioni da parte di terzi (a titolo esemplificativo, strumenti come Piwik);

- cookie gestiti da terza parte, ma anonimizzati, ovvero in relazione ai quali la terza parte non possa accedere ai dati disaggregati di analytics a livello di IP.

L'editore del sito non può attivare cookie di profilazione prima che l'utente abbia volontariamente e in maniera informata prestato il proprio consenso al trattamento (anche secondo le modalità semplificate tracciate dall'Autorità Garante). Tenendo conto, dunque, che il consenso potrà ritenersi prestato se è manifesta la volontà dell'utente di proseguire nella navigazione al momento del primo accesso oppure mediante lo scroll, la digitazione di un tasto "OK" o "Accetto" o mediante la chiusura del banner (es. digitazione del tasto "X"), i cookie di profilazione non devono essere scritti sul dispositivo dell'utente senza il suo consenso ovvero potranno comunque essere scritti, ma solo se rimangono silenti prima della definitiva espressione delle preferenze da parte dell'utente (che dovrà avvenire nella cookie policy predisposta dall'editore del sito web).

Si ricorda, inoltre, che in tema di conservazione dei dati personali per finalità di profilazione, **i cookie di profilazione** (di prima o di terza parte) non possono rimanere archiviati sul dispositivo dell'utente per un periodo superiore a **12 mesi**.

## 9. L'informativa estesa

Come già scritto, l'informativa estesa deve poter essere raggiunta oltre che attraverso un **link** inserito nell'informativa breve, anche mediante un riferimento situato in calce a ogni pagina del sito.

Essa deve possedere tutti i requisiti previsti nell'**art. 13 del Codice Privacy**, deve dichiarare in modo strutturato e preciso le qualità e finalità dei cookie installati dal sito (magari anche la loro durata) e permettere all'utente di scegliere i singoli cookie di profilazione da mantenere (tutti i cookie tecnici, invece, possono essere immediatamente scritti sul browser utilizzato dall'utente). Infine, tale informativa può essere integrata nella privacy policy generale del sito web dell'editore oppure può essere autonoma e inserita in una specifica pagina web.

L'informativa estesa informerà così l'utente circa le diverse tipologie di cookie utilizzati dal sito visitato, anche mediante un'indicazione che li raggruppi per famiglie secondo le diverse finalità, senza quindi necessariamente indicare lo specifico nome del cookie utilizzato (ad esempio, l'indicazione di un cookie dal nome "xyz\_cookie" si ritiene un'informazione superflua e poco fruibile dall'utente). Il percorso che conduce dal banner (informativa breve) alla cookie policy (informativa estesa) deve comunque essere immune dall'attività dei cookie di profilazione.

Qualora, poi, siano installati anche cookie di terze parti, nell'informativa estesa deve essere presente un link aggiornato all'informativa e ai moduli di consenso di quei soggetti (terze parti, appunto) con cui l'editore principale ha stretto accordi per l'installazione di cookie tramite il proprio sito. Per questo fine si ritiene necessario che

tali link vengano acquisiti direttamente a livello contrattuale, per evitare così problemi in momenti successivi. Inoltre, nel caso in cui l'editore abbia contatti solamente indiretti con le terze parti, nell'informativa estesa dovranno essere presenti i link dei soggetti che fanno da intermediari tra lui e le terze parti.

In ultimo, all'interno dell'informativa estesa dovrà essere segnalata la possibilità per l'utente - anche ai sensi dell'art 122, comma 2 del Codice Privacy - di effettuare le proprie decisioni sulle opzioni di installazione dei cookie da parte del sito, anche mediante le impostazioni del browser (garantendo così il c.d. diritto di "opt-out"), segnalando almeno una procedura da seguire per consentire la configurazione. Qualora sia possibile, l'editore potrà anche creare un collegamento diretto con la sezione dei vari e più diffusi browser dedicata a tali impostazioni.

## **10. La conservazione del cookie tecnico del consenso e il suo valore probatorio**

In base a quanto stabilito nel citato provvedimento dell'Autorità Garante, è necessario tenere traccia dell'avvenuta prestazione del consenso da parte dell'utente, ad esempio per il tramite di un apposito cookie tecnico. Una volta acquisito, infatti, **il consenso va debitamente conservato**. Questa delicata operazione riserva alcune criticità da analizzare e risolvere, partendo dall'assunto che i cookie interagiscono principalmente con l'attività dell'utente e con il browser da questi utilizzato e - come canale per la restituzione dell'informazione raccolta - con il server dell'editore del sito navigato. Nel momento, quindi, in cui l'utente si presta a rendere il proprio **consenso**, partecipano al processo in maniera integrata cinque attori principali: **l'utente** stesso, **il sito** navigato, **il browser**, **il dispositivo utilizzato** e **il server dell'editore**. L'utente, primo attore, ha facoltà di scelta sui cookie del sito e sulle impostazioni relative ai cookie proposte dal browser ed è inoltre libero di cambiare dispositivo a suo piacimento. Il sito nella sua funzionalità dovrà tener conto sia delle scelte esplicite dell'utente che delle impostazioni dettate dal browser, rendendo all'utente la versione di navigazione più garantista tra quelle scelte e impostate, nel caso queste fossero contrastanti (gli opt-out prevalgono sugli opt-in, siano essi dettati dal sito o dal browser). Il browser, dal canto suo, imposta le scelte secondo le preferenze espresse dall'utente, libero di cambiarle a piacimento, e lo fa per tutto il traffico di navigazione, indifferentemente dal sito specifico che l'utente decide di navigare, interagendo di volta in volta con il sito visitato, in maniera tale da coordinare le preferenze ad hoc caso per caso. Detto ciò, bisogna tenere in considerazione che le **impostazioni dei cookie** espresse per un dato browser **si azzerano** nel momento in cui si decida di **cambiare browser o dispositivo** e che, pertanto, le stesse rimangono valide solo per lo specifico browser e sullo specifico dispositivo utilizzato, fino a un eventuale contrordine dell'utente.

Da ultimo, va considerato che il server dell'editore del sito registrerà la risultanza di tutte le interazioni precedenti, memorizzando solo le informazioni raccolte dai cookie che sono stati accettati e attivati. Il consenso sarà dunque composito, derivato da un'utenza che ha facoltà innanzitutto di decidere attivamente e in secondo luogo di

declinare le proprie scelte attraverso altri due canali: l'informativa estesa del sito e il browser (il primo di dominio e gestione dell'editore del sito, l'altro dell'utente). La prima criticità osservabile nel processo di conservazione di tale consenso è la parzialità della coerenza, soprattutto se si tiene conto della velocità della frequenza di cambiamento da parte dell'utente e delle sfaccettature che lo rendono, quindi, altamente variabile ed eterogeneo nelle percentuali: l'utente, infatti, può in qualsiasi momento cambiare le preferenze espresse sul sito, le impostazioni del browser, il dispositivo utilizzato. Un consenso con un così alto grado di variabilità risulta, pertanto, di difficile gestione, soprattutto in termini di coerenza e di rilevanza, ma anche in termini di qualità e quantità delle informazioni raccolte, nel momento in cui ci si appresta a registrarlo per la conservazione ai fini di un eventuale onere di prova. In termini logici, il consenso da conservare dovrebbe essere la risultanza di un continuo confronto di tutte le indicazioni utili fornite da ognuno degli attori implicati; ma c'è a questo punto una seconda criticità che giunge a complicare ulteriormente il salvataggio di un consenso univoco e coincidente ai fini della conservazione richiesta: **l'interazione tra l'interessato e il proprio browser**. Se da una parte questa interazione sostiene e dà supporto alla gestione dei cookie durante la navigazione, garantendo all'utente una gestione trasversale (aldilà del sito navigato), dall'altra parte non rende nessun riscontro, nessuna evidenza che l'editore del sito possa registrare e calcolare nel bilancio del consenso da conservare sul proprio server.

Ancora oggi, pertanto, non esiste un sistema tecnico "perfetto" in relazione alla modalità di registrazione del consenso da parte di un browser e il Garante Privacy non ha indicato una specifica soluzione tecnologica. La problematica deve essere indubbiamente approfondita, cercando le soluzioni che prevedano la possibilità per le aziende di potersi difendere - in sede amministrativa e civilistica - dimostrando di aver posto in essere tutti i presidi necessari al fine di evitare che i cookie operino senza il previo consenso dell'utente.

Una soluzione percorribile potrebbe essere quella di salvare il consenso in maniera relativa, per ogni singola sessione. Al momento del consenso, un cookie tecnico informerà l'editore del sito delle preferenze dell'utente e questa informazione, seppur relativa a un'unica sessione, verrà registrata e conservata. Alla chiusura della sessione il browser utilizzato avrà registrato le scelte fatte dall'utente conservandone memoria (cosa che sarà gradita dall'utente che possiede il dispositivo che utilizza, e meno gradita dall'utente che utilizza un dispositivo non suo).

Altre soluzioni al momento idonee ai fini della prova dell'acquisizione del consenso prevedono l'adozione di:

- un sistema di acquisizione della prova per il mezzo di un apposito cookie tecnico, così come previsto dalle FAQ del Garante;
- un sistema automatico o personalizzato di risposta al consumatore, il quale in caso di lamentela deve ricevere una risposta entro 15 giorni su come cancellare i cookie dal proprio dispositivo;
- un sistema di certificazione che permetta di assicurare la compliance ai requisiti di legge (autocertificazione o verifica da parte della stessa Autorità).

Occorre, quindi, predisporre l'opportuna registrazione delle azioni con le quali l'utente manifesta il proprio consenso all'utilizzo dei cookie e, unitamente a queste, è opportuno memorizzare, o comunque rendere disponibile in fase di controllo, anche l'informativa a seguito della quale l'utente ha prestato tale consenso: tutto ciò deve essere correttamente memorizzato in un documento informatico che sia successivamente possibile esibire in fase d'ispezione o in giudizio.

Sul punto, le **nuove regole tecniche sulla formazione del documento informatico** (DPCM 13 novembre 2014), all'art. 3, prevedono che un documento informatico possa essere formato anche mediante: c) *"registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente"*; d) *"generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica"*.

In definitiva, dunque, ora è chiaro a tutti che il documento informatico non è solo un .pdf o l'immagine digitale di un documento cartaceo acquisita con lo scanner, ma - in un'ottica dinamica, strutturata e multicanale - sono da considerare documenti informatici anche i flussi informativi giuridicamente rilevanti, opportunamente resi statici e immutabili. Quella delineata dalle nuove norme, quindi, è una nuova dimensione documentale nella quale grande attenzione viene riservata al completamento automatico di processi digitali giuridicamente rilevanti perché garantiti (e certificati) da sistemi di conservazione, i quali di fatto aprono le porte a nuove forme di documenti dinamici a formazione progressiva.

Inoltre, lo stesso art. 3, comma 6, del DPCM 13 novembre 2014 stabilisce che l'integrità e l'immutabilità dei documenti informatici formati mediante tecniche di cui alle lett. c) e d) devono essere garantite con la registrazione dell'esito dell'operazione e con l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

A prescindere, poi, da come verrà raccolto il consenso (mediante compilazione di un apposito modulo on-line, mediante la registrazione delle scelte di navigazione compiute dall'utente o ancora mediante audit trail), in ogni caso il documento informatico attestante il rilascio del consenso dovrà essere **reso integro e immutabile**: a ciò si potrà provvedere predisponendo **idonee misure di sicurezza** in grado di tracciare gli accessi al database contenente le registrazioni relative alle scelte dell'utente, oppure mediante **conservazione a norma di un'estrazione statica di tali registrazioni**.

Risulta, quindi, di fondamentale importanza provvedere alla **corretta conservazione** - a norma degli artt. 43 e ss. del CAD e delle relative Regole tecniche sulla conservazione (DPCM 3 dicembre 2013) - dei dati informatici relativi al consenso all'utilizzo dei cookie tecnici: ciò ovviamente al fine di tenere traccia dello specifico evento informatico che si genera durante una delle possibili azioni che l'utente ha a disposizione (chiudere il banner, cliccare su ok, fare lo scroll ed entrare nel sito, cliccare sulla X, etc.). Con tali attività, infatti, l'utente presta inequivocabilmente il

proprio consenso al trattamento (ed esempio, quello relativo all'acquisizione dei cookie finalizzati alla profilazione) e il fornitore del servizio può tenerne traccia, memorizzarle e conservarle a norma, per mantenere una prova idonea della prestazione del consenso da parte dell'utente interessato.

## **11. La notificazione del trattamento al Garante**

Va rilevato in tema di notificazione che, ai sensi dell'art. 37, comma 1, lett. d) del Codice Privacy, l'utilizzo di cookie è sottoposto all'obbligo di notificazione preventiva al Garante privacy solo nel momento in cui esso sia finalizzato "a definire il profilo e la personalità dell'interessato, o ad analizzare le abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti".

Al contrario, **l'uso dei cookie è invece sottratto all'obbligo di notificazione**, in base a quanto stabilito dal provvedimento del Garante del 31 Marzo 2004, allorché esso sia finalizzato alla sola trasmissione di identificativi di sessione solo con lo scopo di agevolare l'accesso ai contenuti di un sito internet.

Concretamente, quindi, sarà necessario adempiere all'**obbligo preventivo di notificazione solo nel caso in cui si stiano utilizzando cookie di profilazione di prima parte**, mentre per quanti utilizzano solamente cookie tecnici (che siano di prima o di terza parte), tale obbligo non vige.

## **12. Sanzioni**

Così come previsto dallo stesso Garante Privacy nel provvedimento dell'8 maggio 2014, tutti i soggetti che **entro il 2 giugno 2015** non abbiano provveduto all'adeguamento alle prescrizioni in esso contenute (relativamente a notificazione, informativa e consenso), saranno passibili di **sanzioni amministrative** di diversa entità.

Disattendere la disciplina in materia di cookie, infatti, potrà comportare sanzioni derivanti da "omessa o inidonea informativa" (da € 6.000 a 36.000 – Art. 161 Codice Privacy), "utilizzo dei cookie di profilazione in assenza di consenso" (da € 10.000 a 120.000 – Art. 162, comma 2-bis Codice Privacy) e "omessa o incompleta notificazione" al Garante Privacy del loro utilizzo (da € 20.000 a 120.000 – Art. 163 Codice Privacy)<sup>6</sup>.

In caso di accertata violazione delle norme del Codice Privacy, inoltre, fatta salva l'eventuale adozione di provvedimenti inibitori (blocco e inutilizzabilità dei dati) o prescrittivi, si corre il rischio anche dell'applicazione dell'articolo 164 bis, comma 2, 3 e 4 del Codice Privacy, relativo alle ipotesi aggravate (con possibilità che le sanzioni

---

<sup>6</sup>L'omessa notificazione (articolo 163 del Codice Privacy) comporta anche sanzioni penali a carico del Titolare del trattamento.



amministrative precedentemente indicate possano essere raddoppiate o quadruplicate).

Ovviamente, si ricorda che qualora dovessero emergere i presupposti di un possibile trattamento illecito di dati personali avente una specifica rilevanza di natura penale, l'Autorità Garante è tenuta anche a denunciare i fatti configurabili come reati perseguibili d'ufficio all'autorità giudiziaria, per l'eventuale applicazione della sanzione penale prevista dall'art. 167 del Codice (reato a dolo specifico che comporta la reclusione sino a 2 anni).

Dal punto di vista delle sanzioni civilistiche, non è da escludere nemmeno una possibile richiesta da parte dell'interessato/utente di un risarcimento del danno ai sensi dell'art. 15 del Codice Privacy (artt. 2043 e 2050 del Codice Civile).

### **13. Gli ultimi chiarimenti del Garante circa l'attuazione della normativa sui cookie**

Nonostante tutto il tempo concesso per adeguarsi alla disciplina sui cookie, dopo solo pochi giorni dall'entrata in vigore del provvedimento, il Garante Privacy è dovuto nuovamente intervenire con un comunicato stampa e con un nuovo provvedimento esemplificativo di quello precedente ("Chiarimenti in merito all'attuazione della normativa in materia di cookie") per placare gli animi e rassicurare blogger e piccoli editori web che per ora non ci saranno sanzioni.

Come spiegato dalla stessa Autorità garante, infatti, sono pervenute numerosissime richieste di chiarimento da piccoli gestori - e non solo - in merito ad alcuni punti del provvedimento dell'8 maggio 2014, e proprio alla luce della delicatezza e dell'importanza della tematica si è ritenuto opportuno fornire ulteriori istruzioni.

Tra i vari dubbi chiariti dall'Autorità Garante, c'è quello che attiene all'utilizzo dei "cookie analitici di terze parti": è stato infatti specificato che i siti non sono soggetti agli obblighi e agli adempimenti previsti dalla normativa (notificazione al Garante in primis) qualora adottino strumenti idonei a ridurre il potere identificativo dei cookie analitici che utilizzano (ad esempio, mediante il mascheramento di porzioni significative dell'indirizzo IP) o purché i dati degli utenti raccolti siano conservati separatamente e non "arricchiti" o "incrociati" con altre informazioni già in possesso delle terze parti (es. Google), oppure ancora se la terza parte si impegna comunque a non incrociare le informazioni contenute nei cookie con altre di cui già dispone<sup>7</sup>.

Di seguito i principali interventi chiarificatori:

- i siti che non utilizzano cookie non sono soggetti ad alcun obbligo;

---

<sup>7</sup> Questo impegno ovviamente è ricavabile anche dalla lettura delle policy della terza parte (e non c'è naturalmente bisogno di un accordo formalizzato in tal senso, in quanto implicitamente la terza parte si assume tutte le responsabilità derivanti da un uso non conforme rispetto al trattamento dichiarato).

- per l'utilizzo di cookie tecnici è richiesta la sola informativa (ad esempio nella privacy policy del sito). Non è necessario realizzare specifici banner;
- i cookie analitici sono assimilati a quelli tecnici solo quando realizzati e utilizzati direttamente dal sito prima parte per migliorarne la fruibilità;
- in caso di cookie analitici messi a disposizione da terze parti, i titolari non sono soggetti ad obblighi (notificazione al Garante in primis) qualora:
  - a) siano adottati strumenti che riducano il potere identificativo dei cookie (ad esempio tramite il mascheramento di porzioni significative dell'IP);
  - b) la terza parte si impegni a non incrociare le informazioni contenute nei cookie con altre di cui già dispone;
- se sul sito ci sono link a siti terze parti (es. banner pubblicitari; collegamenti a social network) che non richiedono l'installazione di cookie di profilazione non c'è bisogno di informativa e consenso;
- nell'informativa estesa il consenso all'uso di cookie di profilazione potrà essere richiesto per categorie (es. viaggi, sport);
- è possibile effettuare una sola notificazione per tutti i diversi siti web che vengono gestiti nell'ambito dello stesso dominio;
- gli obblighi si applicano a tutti i siti che installano cookie sui terminali degli utenti, a prescindere dalla presenza di una sede in Italia.

Per rendere ancora più esemplificativi i punti salienti del provvedimento l'Autorità Garante ha pubblicato sul proprio sito un grafico di sintesi:



## Il tuo sito/blog installa cookie? Cosa devi fare

**IMPORTANTE:** per una corretta interpretazione degli adempimenti previsti, si raccomanda la consultazione del **Provvedimento del Garante dell'8 maggio 2014** e dei «**Chiarimenti in merito all'attuazione della normativa in materia di cookie**». I documenti sono disponibili su [www.garanteprivacy.it/cookie](http://www.garanteprivacy.it/cookie)

Segnalarli  
nell'informativa

Art. 2, par. 5, Direttiva 2009/136/CE  
e art. 122, comma 1, Codice privacy

Inserire il banner e  
richiedere il consenso  
ai visitatori

Art. 2, par. 5, Direttiva 2009/136/CE  
e art. 122, comma 1, Codice privacy

Notificare  
al Garante

Art. 37, comma 1, lett. d),  
Codice privacy

CHE TIPO DI COOKIE INSTALLI?

LEGENDA: ✓ adempimento previsto ✗ adempimento non previsto



Nessun cookie



Tecnici o analitici  
prima parte



Analitici terze parti  
(se sono adottati strumenti che riducono il potere identificativo dei cookie e la terza parte non incrocia le informazioni raccolte con altre di cui già dispone) - vedi punto 2 dei «Chiarimenti in merito all'attuazione della normativa in materia di cookie»



Analitici terze parti  
(se **NON** sono adottati strumenti che riducono il potere identificativo dei cookie e la terza parte non incrocia le informazioni raccolte con altre di cui già dispone) - vedi punto 2 dei «Chiarimenti in merito all'attuazione della normativa in materia di cookie»



Di profilazione prima parte



Di profilazione terze parti



1

La notificazione è a carico del soggetto terza parte che svolge l'attività di profilazione

Va infine rilevato come tale ultimo provvedimento emanato dal Garante si collochi nel solco di una prassi che vede fare spesso largo e variegato uso di provvedimenti e circolari. Se da un lato si può dire che negli ultimi anni il ricorso a provvedimenti del genere sia stato, in qualche maniera, sollecitato al Garante dalla normativa europea, dall'altra parte occorre ammettere che sono troppo spesso i giuristi a chiedere al Garante di spiegare, rispiegare, dettagliare, in un'ostinata paura di sbagliare. Appare utile riflettere, a questo punto, se sia corretto investire l'Autorità Garante di poteri interpretativi così invasivi su questa materia e se non sia, invece, auspicabile che siano proprio i giuristi a trovare la corretta interpretazione, partendo dalle radici del diritto della protezione dei dati personali.