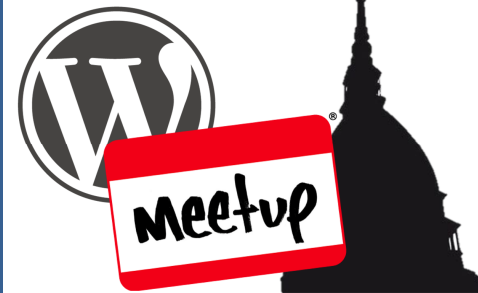


# Cookie Law Italiana e Europea



Ovvero: come far risolvere un (1) problema  
a decine di milioni di persone

Marco Lago - [@marcolago](https://twitter.com/marcolago)  
Interaction Designer e Frontend Developer – HUB09

# Disclaimer – 1/2

In questa presentazione NON ci sono le seguenti cose:

- Certezze assolute:  
perché ci si sono messi in tanti a buttare entropia sull'argomento.
- Una soluzione unica per tutti i casi:  
perché vedremo (forse) che non ce ne sono due uguali.
- Foto di biscotti:  
perché hanno rotto (e perché ce ne sono di più tipi, non solo frollini con scaglie di cioccolato).

## Disclaimer – 2/2

Ci sono però, in abbondanza, le seguenti cose:

- Riferimenti a risorse ufficiali.
- Riassunti dei riferimenti ufficiali.
- Un parere personale formato sul campo.
- Spunti di riflessione e fonti per domande à gogo (anche, e soprattutto, durante la presentazione).

## Cosa sono i cookies (sì, ancora una volta)

Cookies: stringhe di testo di piccole dimensioni che i siti visitati dall'utente inviano al suo terminale (solitamente al browser) dove vengono memorizzati per poi essere ritrasmessi agli stessi siti alla successiva visita del medesimo utente.

Definizione da:

[bit.ly/cookie-law-it-modalita-semplificate](http://bit.ly/cookie-law-it-modalita-semplificate)

(ma quindi, se sono **stringhe** di testo, non dovrebbe essere "le cookies"?)

# Per cosa sono usati?

Per qualunque cosa necessiti di “persistenza” di un dato durante la navigazione di un sito (session) o tra una navigazione un'altra successiva in un secondo momento.

Ad esempio:

- Login.
- Preferenze utente.
- Tracciamento dei dati.
- Profilazione delle abitudini di navigazione.
- Memorizzazione delle opzioni relative ai cookies (!?!).

# La Cookie Law in Europa (e in Italia)

Nasce con lo scopo di regolamentare la gestione dei dati degli utenti memorizzati e trasmessi, attraverso cookies, tra siti “di prima parte” e siti “di terze parti”.

In pratica definisce come informare i visitatori di siti web e acquisire il consenso all’uso dei cookies per il trattamento dei dati.

- 25 novembre 2009: direttiva 2009/136/CE del Parlamento Europeo e del Consiglio
- 8 maggio 2014: provvedimento italiano in materia di cookie.
- 2 giugno 2015: termine ultimo per la regolarizzazione.
- 5 giugno 2015: Chiarimenti in merito all’attuazione della normativa in materia di cookie (!!!)

# Obblighi

Chiunque, privato o azienda, abbia un sito la cui giurisdizione ricade all'interno del territorio dello Stato, a prescindere dalla presenza di una sede fisica nel territorio dello Stato stesso, deve notificare il visitatore che il sito installa dei cookies sul suo computer e deve spiegare quali sono, che cosa fanno e come è possibile bloccarli o impedirne l'installazione.

Inoltre, per alcuni tipi di cookies, è necessario bloccare preventivamente l'installazione finché il visitatore non abbia prestato esplicito consenso.

## Esclusioni – a.k.a. Cookies tecnici

Sono esclusi dall'obbligo i cookie che ricadono in uno dei seguenti criteri:

**Criterio A:** cookie usati per **IL SOLO SCOPO** di effettuare una trasmissione di una comunicazione attraverso una rete di comunicazione elettronica.

**Criterio B:** cookie **STRETTAMENTE NECESSARI** per il funzionamento di un servizio erogato dalla società ed espressamente richiesto dall'utente o dal sottoscrittore.

Evidenziamenti mie.

Tenetele a mente, ci serviranno tra poco.



## Cosa si deve fare?

- Se si utilizzano solamente **cookies tecnici**, è sufficiente **informare l'utente** all'interno dell'**informativa estesa** (vale anche per gli analytics di prima parte).
- Se si utilizzano cookies di terze parti, o analytics di terza parte, si deve informare su quali cookies il sito installa e si **può considerare un consenso implicito**.  
**Si deve usare il banner!**
- Se si utilizzano cookies di profilazione, sia di prima che di terza parte, **si deve ottenere un consenso esplicito** per poter installare i cookies.  
E ovviamente si deve informare.

# Cosa si deve fare? Un'immagine vale...



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

## 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)

**Segnarli  
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: <span style="color: green;">✔</span> adempimento previsto <span style="color: red;">✘</span> adempimento non previsto		
 Nessun cookie	<span style="color: red; font-size: 2em;">✘</span>	<span style="color: red; font-size: 2em;">✘</span>	<span style="color: red; font-size: 2em;">✘</span>
 Tecnici o analitici prima parte	<span style="color: green; font-size: 2em;">✔</span>	<span style="color: red; font-size: 2em;">✘</span>	<span style="color: red; font-size: 2em;">✘</span>
 Analitici terze parti <small>(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»</small>	<span style="color: green; font-size: 2em;">✔</span>	<span style="color: red; font-size: 2em;">✘</span>	<span style="color: red; font-size: 2em;">✘</span>
 Analitici terze parti <small>(se <b>NON</b> 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»</small>	<span style="color: green; font-size: 2em;">✔</span>	<span style="color: green; font-size: 2em;">✔</span>	<span style="color: green; font-size: 2em;">✔</span>
 Di profilazione prima parte	<span style="color: green; font-size: 2em;">✔</span>	<span style="color: green; font-size: 2em;">✔</span>	<span style="color: green; font-size: 2em;">✔</span>
 Di profilazione terze parti	<span style="color: green; font-size: 2em;">✔</span>	<span style="color: green; font-size: 2em;">✔</span>	<span style="color: red; font-size: 2em;">✘</span>

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

# Cookies tecnici

Ricordate cosa letto poco fa?

— **Criterio A:** cookie usati per IL SOLO SCOPO di effettuare una trasmissione di una comunicazione attraverso una rete di comunicazione elettronica.

— **Criterio B:** cookie STRETTAMENTE NECESSARI per il funzionamento di un servizio erogato dalla società ed espressamente richiesto dall'utente o dal sottoscrittore.

Un cookie tecnico è, quindi, un cookie **NECESSARIO** al funzionamento del sito **senza il quale** l'intero sito, o una sua specifica funzionalità, espressamente richiesta dal visitatore, **non funziona**.

**Almeno uno** dei requisiti A o B deve essere soddisfatto.

In questo caso è **sufficiente avere una privacy policy con paragrafo sui cookie usati** (e perché).

# Ricapitolando – Non serve il consenso 1/2

**Cookies solitamente esenti dall'obbligo del consenso, secondo i criteri visti.**

- **Input dell'utente**  
permettono la memorizzazione delle scelte del visitatore sul sito, ad esempio la precompilazione dei campi o le aggiunte ad un carrello ecommerce.
- **Autenticazione**  
identificano l'utente una volta che ha effettuato l'accesso all'interno della sessione corrente; un cookie persistente per riconoscere l'utente tra una sessione e l'altra NON ricade all'interno del criterio B già visto (a meno che non sia richiesto dal visitatore con il classico checkbox "ricordati di me").
- **Sicurezza**  
cookie utilizzati per aumentare la sicurezza, ad esempio tenendo traccia del numero di tentativi di login falliti.
- **Sessione player multimediali**  
cookie utilizzati dai player multimediali, solitamente video, per scopi tecnici relativi alla riproduzione.

Continua...

# Ricapitolando – Non serve il consenso 2/2

**Cookies solitamente esenti dall'obbligo del consenso, secondo i criteri visti.**

- **Load balancing**  
necessari per mantenere il balancing durante la sessione attiva (criterio A).
- **Personalizzazione della UI**  
mantengono l'informazione relativa alla personalizzazione dell'interfaccia utente durante la sessione in corso, ad esempio la lingua o il numero di risultati di ricerca.
- **Social plugin di condivisione sui social network**  
cookies usati dai social plugins per la condivisione quando il visitatore è loggato sul social network di riferimento (hai voglia a capire quali non profilino).

# Cookies di terze parti

Un cookie di terze parti è un cookie settato da un “**data controller**” che non amministra il sito che l’utente sta visualizzando.

Non è quindi una questione (solo) di dominio.

I cookie di terze parti sono solitamente quelli legati a **social plugin** (Like, Tweet, Follow...) ma anche quelli legati ad **analytics di terze parti** (Google su tutti).

Per questi cookie è necessario informare preventivamente il visitatore grazie al **Mirabolante Deus Ex Machina Banner (MDEMB™)**.

E **acquisire il consenso implicito**.

## Cookies Analytics di terze parti (e prime)

Gli **analytics di terze parti**, rispetto a quelli di prima parte, non garantiscono la **completa anonimizzazione** dei dati ma, soprattutto, non garantiscono che non sarà fatto **remarketing**. Per questo motivo devono essere elencati nell'**informativa estesa** e, per sicurezza, anche nell'**informativa breve** (Banner).

Gli analytics di prima parte sono **più probabilmente adatti a passare come tecnici**, ma questo solo grazie ad **un'eccezione specifica**:

*“I cookie analitici sono assimilati a quelli tecnici solo quando realizzati e utilizzati direttamente dal sito prima parte per migliorarne la fruibilità”.*

<http://bit.ly/cookie-law-it-chiarimenti>

# Cookies di profilazione

Questo è facile.

Dovete:

1. **Notificare.**
2. **Informare.**
3. **Raccogliere il consenso esplicito.**

Quindi:

1. **Mostrate il banner** con la richiesta di accettazione.
2. **Linkate la normativa** estesa dove sarà tutto quanto spiegato a dovere.
3. **NON installate il cookie** fino a quando non avrete avuto il consenso. Il che vuol dire che...



# Ricapitolando – Serve il consenso

**Cookies NON esenti dall'obbligo del consenso.**

- **Social plugin per il tracciamento**  
cookie installati dalle terze parti per il tracciamento del comportamento dell'utente (che poi è quello che succede con il like button di Facebook).
- **Tracciamento di terze parti (advertising e analytics)**  
che siano di analisi del comportamento o semplice tracciamento aggregato anonimo.
- **Tracciamento di prima parte (analytics)**  
sebbene più sicuri di quelli di terze parti non sono comunque considerabili strettamente necessari.

Evidenziate le differenze principali tra la normativa europea e quella italiana.

Quanto evidenziato è relativo alla normativa europea (paragrafi 4.2 e 4.3) :

<http://bit.ly/cookie-law-eu-opinion-recommendation>

**In Italia si lascia più correre sugli analytics, insomma.**

# Non installerai cookies senza consenso

Secondo gli esempi portati dal sito [europa.eu](http://europa.eu) tutte le funzionalità legate all'autorizzazione all'uso dei cookies dovranno essere **disabilitate** e notificate al visitatore in attesa del **consenso esplicito**.

In pratica, se avete banner (pubblicitari) o social plugin che profilano gli utenti (e qui si cade su Facebook) dovete raccogliere il consenso **PRIMA di installare il cookie**.

Se **NON raccogliete il consenso** vi si rompe il sito (o avete gestito il caso).

# Come ottenere il consenso 1/2

È possibile ottenere il consenso generale all'uso dei cookies (per tutti i cookies che lo richiedono ma che non siano di profilazione) in **modo implicito**, ovvero tramite la **prosecuzione dell'azione sul sito**.

Ecco quindi, di nuovo, il banner nella sua forma più diffusa, ovvero che recita più o meno letteralmente:

*“Questo sito utilizza cookies tecnici e per il tracciamento anonimo e aggregato della navigazione al fine di migliorare l'esperienza del visitatore.  
Continuando la navigazione, cliccando su elementi sottostanti a questo banner o scrollando la pagina, si accettano implicitamente questi cookies.  
Per maggiori informazioni, e per scoprire come bloccare i cookies, consultare [l'informativa privacy e cookies](#)”.*

Qualunque azione compia l'utente sul sito viene considerata come consenso informato—a parte l'andarsene, ovviamente.

## Come ottenere il consenso 2/2

Nel caso di cookie di profilazione invece è necessario che il consenso venga fornito **esplicitamente** con un click su uno specifico **pulsante di accettazione**. \*

**Solo in questo** caso i cookies **possono essere installati**.

Da qui la confusione su:

**quando installo i cookie nel caso di un consenso implicito?**

Bella domanda... parliamone.

\* Ci sarebbe un'eccezione a questa regola, secondo il Garante italiano.

# Come ottenere il consenso 2/2 (IT)

The diagram illustrates a web browser window. At the top, there is a address bar containing the text "http://www.....it". To the right of the address bar are three navigation icons: a left-pointing arrow, a right-pointing arrow, and a home icon. Below the address bar is a header area labeled "SITO WEB". The main content area of the browser displays a large, semi-transparent "INFORMATIVA" (Information) banner. The banner has a title "INFORMATIVA" and contains the following text: "Questo sito utilizza *cookie* di profilazione [propri e di altri siti] per inviarti pubblicità in linea con le tue preferenze..", "Se vuoi saperne di più o negare il consenso a tutti o ad alcuni *cookie*, [clicca qui](#)", and "Se accedi a un qualunque elemento sottostante questo banner acconsenti all'uso dei *cookie*". To the left of the banner is a circular icon containing a person silhouette, and below it is a square icon containing a play button symbol. A mouse cursor is shown pointing at the banner. A large, red, diagonal watermark reading "esempio" is overlaid across the entire browser window.

# Come ottenere il consenso 2/2 (EU)



1. The cookie header banner displayed on all pages of a site using cookies that require informed consent.
2. A link to the specific cookie notice page is also available.
3. This element of the page will only display its content once the user chooses to accept the site's cookies.

<http://bit.ly/cookie-law-eu-europa-example>

# Installare i cookies

Nel caso di cookies di **profilazione** è facile.  
Vanno installati solo **DOPO aver ricevuto l'autorizzazione (opt-in)**.  
Nessun dubbio su questo.

Nel caso di cookies **NON di profilazione** è opinabile.  
Fermo restando che deve essere sempre disponibile una modalità  
per disabilitarli, d'uso comune è averli **attivi fin da subito\*** e  
permettere di **cancellarli successivamente (opt-out)**.

Disabilitarli, è tutto un altro paio di maniche.

*\* "For implied consent to work there has to be some action taken by the consenting individual from which their consent can be inferred.*

*This might for example be visiting a website, moving from one page to another or clicking on a particular button."* (evidenziazione mia)

<http://bit.ly/cookie-law-eu-ico-ebook>

# Rimuovere i cookies "

La normativa prevede che nell'apposita informativa estesa venga data l'opzione per **disabilitare tutti i cookies non tecnici**.

Questo è possibile **facendosi carico** della cancellazione di ogni cookie e relativo blocco della nuova installazione.

Oppure indicando le pagine dei **titolari dei cookies di terze parti** (e mantenerle sempre aggiornate). A trovarle tutte.

Ad esempio, **Facebook**:

- Informativa sull'uso dei dati personali di Facebook  
<https://www.facebook.com/help/206635839404055>
- Modifica del consenso all'uso dei cookie (cercare Facebook nell'elenco)  
<http://www.youronlinechoices.com/it/le-tue-scelte>

Oppure **Google**:

- Informativa sull'uso dei dati personali di Facebook  
<https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage>
- Modifica del consenso all'uso dei cookie per Google Analytics  
<https://tools.google.com/dlpage/gaoptout>



# Il Garante ha detto 1 – 8 maggio 2014

1. ai sensi degli artt. 122, comma 1 e 154, comma 1, lett. h), del Codice -ai fini dell'individuazione delle modalità semplificate per l'informativa che i gestori di siti web, come meglio specificati in premessa, sono tenuti a fornire agli utenti in relazione ai cookie e agli altri dispositivi installati da o per il tramite del proprio sito stabilisce che nel momento in cui si accede alla home page (o ad altra pagina) di un sito web, deve immediatamente comparire in primo piano un banner di idonee dimensioni contenente le seguenti indicazioni:

- a) 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;
- b) che il sito consente anche l'invio di cookie "terze parti" (laddove ciò ovviamente accada);
- c) il link all'informativa estesa, che deve contenere le seguenti ulteriori indicazioni relative a:
  - uso dei cookie tecnici e analytics;
  - possibilità di scegliere quali specifici cookie autorizzare;
  - possibilità per l'utente di manifestare le proprie opzioni in merito all'uso dei cookie da parte del sito anche attraverso le impostazioni del browser, indicando almeno la procedura da eseguire per configurare tali impostazioni;
- d) l'indicazione che alla pagina dell'informativa estesa è possibile negare il consenso all'installazione di qualunque cookie;
- e) l'indicazione che la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso (ad esempio, di un'immagine o di un link) comporta la prestazione del consenso all'uso dei cookie;

2. ai sensi dell'art. 154, comma 1, lett. c), del Codice ai fini di mantenere distinta la responsabilità dei gestori di siti web, come meglio specificati in motivazione, da quella delle terze parti prescrive ai medesimi gestori di acquisire già in fase contrattuale i collegamenti (link) alle pagine web contenenti le informative e i moduli per l'acquisizione del consenso relativo ai cookie delle terze parti (con ciò intendendosi anche i concessionari).

# Il Garante ha detto 2 – 5 giugno 2015

- I siti che non utilizzano cookie non sono soggetti ad alcun obbligo
- 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.
- Se i cookie analitici sono messi a disposizione da terze parti i titolari non sono soggetti ad obblighi (notificazione al Garante in primis) qualora:
  - A) siano adottati strumenti che riducono il potere identificativo dei cookie (ad esempio tramite il mascheramento di porzioni significative dell'IP);
  - B) la terza parte si impegna a non incrociare le informazioni contenute nei cookies 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.

## Ci sarebbe la questione dei 150 euro

Solo nel caso di cookies di profilazione di prima parte, ovvero quando si è quelli che maneggia i dati raccolti, si **deve comunicare al Garante** per la Privacy come verranno trattati questi dati.

Il gesto di comunicare la cosa al garante fa **150 euro** così, sull'unghia.

Dicono però che se l'azienda che raccoglie i dati ha nominato un responsabile del trattamento la notifica non è obbligatoria.

Dicono.

Ma io sapevo che la nomina di un responsabile del trattamento è obbligatoria a sua volta e quindi... non mi fiderei!

# E ci sarebbe poi la questione delle multe

La normativa italiana cita:

## **Sanzioni**

*Si ricorda che per il caso di omessa informativa o di informativa inidonea, ossia che non presenti gli elementi indicati, oltre che nelle previsioni di cui all'art. 13 del Codice, nel presente provvedimento, è prevista la sanzione amministrativa del pagamento di una somma da seimila a trentaseimila (6.000–36.000) euro (art. 161 del Codice).*

*L'installazione di cookie sui terminali degli utenti in assenza del preventivo consenso degli stessi comporta, invece, la sanzione del pagamento di una somma da diecimila a centoventimila (10.000–120.000) euro (art. 162, comma 2-bis, del Codice).*

*L'omessa o incompleta notificazione al Garante, infine, ai sensi di quanto previsto dall'art. 37, comma 1, lett. d), del Codice, è sanzionata con il pagamento di una somma da ventimila a centoventimila (20.000–120.000) euro (art. 163 del Codice).*

(In Inghilterra si arriva a 500.000 Sterline)

# Risorse Online

## Garante della Privacy italiano

- <http://bit.ly/cookie-law-it-modalita-semplificate>
- <http://bit.ly/cookie-law-it-chiarimenti>
- <http://bit.ly/cookie-law-it-faq>

## Opinion 04/2012 on Cookie Consent Exemption

- <http://bit.ly/cookie-law-eu-opinion-recommendation>

## Esempi su europa.eu (e kit per implementare la propria versione)

- <http://bit.ly/cookie-law-eu-europa-example>

## Aiutare i publisher a ottenere il consenso all'uso dei cookie

- <https://www.cookiechoices.org/>

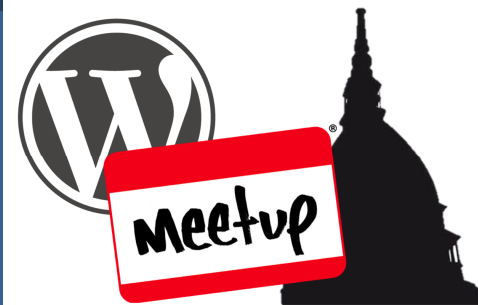
## Disabilitare i cookie di Google Analytics

- <http://bit.ly/google-analytics-disable-cookies>

## Ebooks

- ICO: <http://bit.ly/cookie-law-eu-ico-ebook>
- Silktide: <http://bit.ly/cookie-law-eu-silktide-ebook>

# Cookie Law Italiana e Europea



Ovvero: come aumentare l'entropia  
cercando di fare chiarezza

# GRAZIE

Marco Lago - [@marcolago](#)  
Interaction Designer e Frontend Developer – HUB09