GDPR e Profilazione Inconsapevole

ovvero: profiliamo gli utenti a nostra insaputa (e il GDPR non è affatto contento ...)

Autore: Andrea Rui
LinkedIn: andrearui
2 Settembre 2018

Abstract

La recente definitiva entrata in vigore del GDPR 2018 – il nuovo regolamento europeo per la protezione dei dati personali - e soprattutto l'inizio della decorrenza per la sanzionabilità per i comportamenti non conformi ad esso (25 Maggio 2018), hanno dato un forte impulso agli interventi di adeguamento dei trattamenti di dati effettuati da ogni azienda ed organizzazione, anche governativa.

Tale sforzo viene tuttavia spesso vanificato da prassi talmente consolidate da risultare invisibili all'occhio dei legali e dei professionisti chiamati a supportarci nel mettere a norma tutti i processi aziendali.

In questo articolo descrivo una di tali consuetudini, in forma discorsiva e poco tecnicistica, proprio per per poter raggiungere tutti coloro che non hanno un adeguato background tecnico per comprendere il problema.

Concludo con una panoramica sugli approcci più frequentemente adottati (nel bene e nel male) da vari enti ed organizzazioni, in modo da potersi fare un'idea di quali siano i modi migliori per gestire la compliance con il GDPR.

In questo articolo si farà principalmente riferimento a titolo esemplificativo ai servizi di web analytics di Google, ma gli stessi concetti devono considerarsi generali ed applicabili a qualunque servizio analogo (Yahoo, ShiniStat, etc.).

Situazione

Con la definitiva entrata in vigore del GDPR tutte le aziende ed organizzazioni di ogni tipo che utilizzano un sito web per presentarsi al pubblico si sono trovate a dover affrontare in profondità le implicazioni derivanti dall'utilizzo dei '*cookie*' e di

dover quindi pubblicare una politica per la privacy attentamente ragionata in cui descrivere a quale scopo li si utilizza, distinguendo tra l'altro tra cookie 'tecnici' e 'di profilazione', attivando meccanismi per ottenere il consenso all'utilizzo dei secondi.

Ad eccezione di poche aziende con una reale attenzione al valore dei dati e con le necessarie competenze e risorse per poter affrontare e gestire il problema, la quasi totalità di esse affronta il problema servendosi di consulenti esterni, molto più preparati dal punto di vista normativo che tecnico, oppure arrangiandosi copiando e adattando modelli e politiche reperite in Rete.

Il Problema

Purtroppo un'operazione banale ed apparentemente innocua mette a rischio tutti gli sforzi profusi in azienda per aderire alle prescrizioni del Regolamento.

Da anni il sito web istituzionale di ogni organizzazione è la sua imprescindibile vetrina esposta al mondo: chi non ha o comunque non sente l'esigenza di sapere e misurare quanto e come vengano fruiti il proprio sito ed i suoi contenuti?

Ma come fare? Cercare, installare, configurare e mantenere aggiornato un software di web analytics richiede competenza e tempo.

Per fortuna ci viene incontro Internet: possiamo disporre di tutto ciò che ci occorre per misurare l'utilizzo del nostro sito semplicemente aggiungendo un piccolo pezzettino di codice facilmente scaricabile da Google (o similari di altre terze parti che offrono servizi di web analytics), che ha una forma simile a `<script type="text/javascript">...</script>`.

Pochi click ed in un minuto possiamo già iniziare a consultare, misurare ed analizzare il traffico verso il nostro sito.

Solo per curiosità, provate a leggere il codice sorgente di qualsiasi pagina web che visitate: in generale è sufficiente premere il tasto destro del mouse in qualunque punto della pagina, e dal menu che compare selezionare l'opzione '*visualizza sorgente pagina*', o analoga.

Non vi si richiede di comprendere ciò che vedrete, ma provate a cercare, generalmente in fondo al testo, quel pezzettino di codice di cui vi ho appena accennato: lo troverete praticamente in tutte le pagine che visitate (a volte in altre forme, e spesso ne troverete anche altri di altri provider).

A titolo di esempio, ad oggi utilizzano Google Analytics:

- il sito del Ministero dell'Interno (http://www.interno.gov.it);
- il sito del Ministero dell'Istruzione (http://www.miur.gov.it);
- l'ISPRA (http://www.isprambiente.gov.it)
- il sito europeo per la parità di genere (http://eige.europa.eu)

- il Joint Research Centre europeo (https://green-driving.jrc.ec.europa.eu)
- Il Corriere (https://www.corriere.it/)
- Il Sole 24 ore (http://www.ilsole24ore.com/)
- La Borsa Italiana (https://www.borsaitaliana.it)
- Il Meteo.it (https://www.ilmeteo.it/)
- …

In http://eige.europa.eu/cookies-policy viene esplicitamente dichiarato che i cookie non possono essere utilizzati per identificare l'individuo, cosa che in realtà non corrisponde a verità: infatti se una qualsiasi pagina web consultata dall'utente include contenuti provenienti da due siti diversi controllati dal medesimo fornitore di servizi (ad esempio, google-analytics e youtube.com) consentono a Google di associare i cookie di google-analytics a quelli già associati all'identità del visitatore.

Tanto per fare un esempio, la home page del sito del MIUR contiene il seguente pezzo di codice:

```
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-111193015-1"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', 'UA-111193015-1');
</script>
```

Se andiamo ad analizzare questo pezzettino di codice, osserveremo che l'unica personalizzazione che dobbiamo fare è di inserire un codice identificativo della nostra organizzazione, così come ottenuta mediante registrazione su Google: si tratta di una stringa di pochi caratteri.

D'altra parte, chi non ha un account su Google oggi ...?

Si tratta di un codice breve, che non contiene informazioni personali: è assolutamente innocuo … o almeno così sembra.

Fin da piccolo mi sono sentito ripetere che nessuno regala niente: a voler ben ragionare, quanto può costare un sistema che offre servizi di web analytics su scala planetaria?

… beh, occorrerà certamente qualche migliaio di server, come minimo (e chissà quanta corrente consumeranno ...).

… in quanto tempo risponde alle mie consultazioni il sito di analytics? Forse meglio del mio sito stesso … ma che connettività avranno? Costerà un sacco di soldi …

Ed il personale che installa, manutiene e aggiorna il software? … beh, gli stipendi so quanto costano, e questi lavorano 365H24 … occorreranno più persone per più turni al giorno …

Milioni di dollari in infrastrutture, e milioni di dollari di costi ogni anno, per offrirmi un bellissimo servizio gratuito … e non si aspettano neppure un ringraziamento!

Tutto in cambio di quel piccolo codice identificativo che rappresenta la mia organizzazione …

E cosa c'entra il GDPR?

Il GDPR prescrive di non profilare gli utenti, a meno di ottenerne l'esplicito, consapevole ed informato consenso.

Ma noi, con quel pezzettino di codice, non abbiamo raccontato nulla di nessuno: inoltre, quel codice rappresenta una persona giuridica, non ricompresa nel Regolamento.

Di conseguenza, non devo neppure includere il sito di analytics tra i miei trattamenti, nella mia analisi dei rischi e nella DPIA.

Eppure tutta questa benignità nei nostri confronti avrebbe dovuto metterci la pulce nell'orecchio …

Proviamo a leggere meglio quel piccolo script pre-confezionato che abbiamo inserito in fondo alle nostre pagine HTML … no, non ci troviamo nulla di sospetto: semplicemente una chiamata ad un URL del sito di web analytics, a cui viene passato il codice identificativo della nostra organizzazione …

Strano … proviamo a rileggere meglio ... niente: non troviamo nulla di sospetto; quello script passa soltanto il nostro codice identificativo (ed anonimo): continuiamo a non vedere invii di dati personali.

Ed anzi, forse nella nostra informativa sulla privacy abbiamo inserito anche un riferimento alla politica per la privacy dell'azienda che ci fornisce il servizio di web analytics, ma a ben guardare, noi di cookie di quest'azienda non ne abbiamo proprio gestiti; forse quell'inclusione nella nostra politica è superflua, ma male non fa, e poi la inseriscono tutti: non possiamo essere da meno.

Ma veniamo ai cookie: li abbiamo citati nella nostra politica per la privacy, ma … sappiamo cosa sono realmente?

Sono delle sequenze di caratteri identificate da un nome ed associate al dominio di provenienza che i server che visitiamo inviano al nostro browser, insieme al contenuto contenuto richiesto, confidando che il browser le memorizzi e le restituisca al server la successiva volta che viene consultata una pagina o richiesto un contenuto dello stesso dominio.

Anche qui, nessuna violazione della privacy: il nostro browser non invia alcun nostro dato al server, ma semplicemente restituisce al server dei dati che questo ci aveva precedentemente inviato, e di cui pertanto è già a conoscenza.

Addirittura i browser, come misura di sicurezza, prevengono il fatto che i cookie associati ad un dominio possano essere inviati ad un dominio diverso: nessun sito potrà mai sapere quali altri cookie siano stati memorizzati nel nostro browser.

Quindi se visito il sito del mio giornale o del mio social network preferito, i cookie relativi ad essi non verranno mai comunicati al sito di web analytics che abbiamo deciso di utilizzare.

Per generalità occorre naturalmente tenere presente che possiamo utilizzare contemporaneamente più siti di web analytics diversi, semplicemente includendo nelle nostre pagine gli script relativi a ciascuno di essi.

Quindi siamo in una botte di ferro: il GDPR non ci tocca in nessun modo.

Volendo riepilogare:

1. l'identificativo che utilizziamo è anonimo: non contiene informazioni personali;
2. inoltre, tale identificativo è di norma associato ad una persona giuridica (un'azienda, organizzazione, associazione, …): non fa quindi riferimento ad una persona fisica, e quindi non è ricompreso nell'ambito di applicazione del GDPR;
3. abbiamo verificato che il nostro browser non invia assolutamente dati personali prelevati dal nostro computer;
4. inoltre gli unici dati che vengono scambiati sono i cookie, che provengono dal server: quando li restituiamo al server non gli raccontiamo nulla di più di quanto già non sapesse (ce li ha inviati lui);
5. inoltre abbiamo anche l'assicurazione offerta dal browser che il server del sito che consultiamo non potrà mai ricevere i cookie che il browser ha ricevuto da altri siti.

Rileggiamo più volte l'elenco precedente, fino ad essere praticamente certi che di rischi per la privacy proprio non ce ne siano.

… eppure la pulce nell'orecchio non se ne è andata ...

Ma allora, questi cookie? Dove sta il problema?

Per comprendere dove sta l'inghippo, occorre comprendere un aspetto fondamentale dei cookie e del protocollo HTTP, che tra le righe abbiamo già parzialmente descritto, ma che sfugge facilmente anche ad un occhio attento.

Il protocollo HTTP (o HTTPS, se viene utilizzata una connessione sicura) è il protocollo che il nostro browser utilizza per interrogare i siti web e per ricevere le pagine che desideriamo consultare.

Per consentire al server di servirci i contenuti nella forma più fruibile per noi, tale protocollo consente al browser di inviare al server alcune informazioni 'tecniche'. L'effetto di tali 'informazioni' lo notiamo quotidianamente quando consultiamo il medesimo sito da un PC e da uno smartphone: non possiamo non notare che l'impaginazione è diversa ed ottimizzata, e se siamo attenti notiamo anche che verso gli smartphone vengono trasferiti, di norma, meno byte per il medesimo contenuto, per fornirci dei buoni tempi di risposta anche se la connettività è più lenta rispetto alla fibra ottica a cui siamo ormai abituati a casa ed in ufficio.

Vi sono molte informazioni che il browser può inviare al server quando richiede la consultazione di una pagine; tra queste vi sono:

- sistema operativo utilizzato e sua versione (che può consentire di identificare il tipo di hardware),
- browser utilizzato e sua versione,
- URL della pagina di provenienza (l'eventuale pagina su cui avete cliccato il collegamento che vi ha rimandato alla pagina che volete consultare),
- URL della pagina visitata,
- eventuali chiavi dell'interrogazione o di ricerca (potrebbero contenere informazioni su acquisti, prenotazioni, nonché disabilità, ricerche di tipo medico o penale, etc.),
- profilo di sicurezza del browser,
- e, come già detto prima, **i cookie ricevuti dal sito che stiamo visitando**,
- … ed altro ancora ...

Inoltre, per poterci restituire i contenuti desiderati, il server riceve ovviamente l'indirizzo IP del nostro dispositivo, che consente di geo-localizzare, con diversi gradi di approssimazione, la nostra posizione, oltre che il nome della nostra azienda o del nostro provider di connettività.

Il provider di web analytics può inferire anche altre informazioni, tra cui:

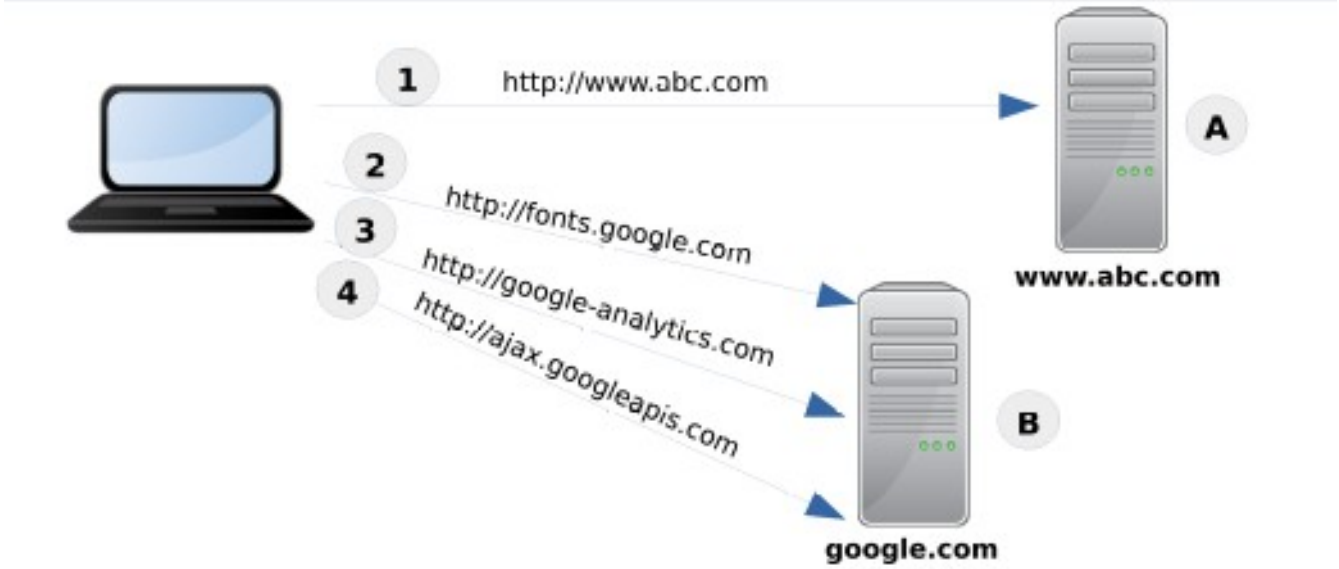
- data e ora della visita,
- tempo di permanenza sulla pagina,
- dominio / azienda di provenienza del visitatore,
- profilo di accesso alle pagine ad parte del visitatore (orari abituali, localizzazione abituale, etc.),
- e molto altro ancora

Ma veniamo alla chiave di volta del problema: come abbiamo già detto prima, quando il browser richiede lo scaricamento di una pagina da un sito web, inserisce nella richiesta anche tutti i cookie di tale sito memorizzati localmente.

Ma se consulto una pagina dal sito **A**, devo ricordarmi che essa contiene quel piccolo script, che richiama un servizio dal sito **B** (cioè quello di web analytics).

Ciò significa che il sito di analytics (**B**) riceve, oltre ai propri cookie, tutte le informazioni sopra descritte, ed anche l'informazione sulla pagina di provenienza (quella che state consultando dal sito A, e che include lo script di web analytics).

Il problema è che i cookie del sito di web analytics (B) vengono inviati dal nostro browser al server di analytics ogni volta che consultiamo una qualsiasi pagina di qualsiasi dominio che contenga quel piccolo script che anche noi abbiamo incluso nelle nostre pagine.



Ciò significa che ogni volta che un visitatore passa per il nostro sito, il sito di web analytics riceve una copia dei propri cookie, e la stessa cosa accade quando il medesimo utente visita altri siti che includono il medesimo script di web analytics.

Di conseguenza, il provider del servizio di analytics riceverà da questo utente, insieme ai propri cookie, anche tutte le informazioni sopra elencate, per ogni sito ed ogni pagina che contiene il solito script, e potrà profilare il comportamento in Rete dell'utente, tracciando i siti, i momenti e la sequenza delle pagine visitate, oltre che i dispositivi utilizzati e da dove vengono effettuate le consultazioni.

Se poi tale utente dispone anche un account sul sito del provider (ad esempio, GMail, o GoogleDrive), il provider di analytics potrà associare tutte le informazioni di navigazione sopra descritte all'identità reale del visitatore.

Ma non è finita qui!

Prendendo ad esempio i servizi di Google, per il fatto che includiamo nelle nostre pagine lo script che fa riferimento a google-analytics.com, potremmo essere indotti a pensare che i cookie utilizzati per la profilazione della navigazione dei nostri visitatori restino circoscritti a tale dominio, e che non possano essere correlati con quelli, ad esempio, provenienti da google.com, o youtube.com, etc.

… peccato che tutti questi siti appartengano ad un'unica azienda, e che l'identità dell'utente che accede a google.com, o google.it, o youtube.com, sia la medesima, e Google può correlare tutte le informazioni di navigazione che includono anche uno solo di tali cookie alla medesima persona.

Altro aspetto subdolo è che molti nomi di dominio che appaiono distinti in realtà ridirigono al medesimo dominio:

- ajax.googleapis.com → developers.**google.com**
- google-analytics.com → analytics.**google.com**
- googletagmanager.com → marketingplatform.**google.com**
- e così via ...

E quanto sopra descritto avviene anche se per comodità includiamo nella nostra pagina dei font scaricabili da Internet (*fonts.google.com* vi dice niente …?) o librerie di funzioni come *ajax.googleapis.com*, e molto altro ancora.

Ogni volta che includiamo nella nostra pagina un font o una libreria di funzioni o delle immagini provenienti dal sito del provider o di un'azienda ad esso collegata, passiamo a tale sito tutte le informazioni sopra elencate.

Per essere precisi …

In effetti, supponendo che in una pagina siano contenuti riferimenti, ad esempio, a google-analytics e a fonts.google.com, il sistema che riceve le richieste non può essere assolutamente certo che provengano dallo stesso utente.

Tuttavia può considerarsi assolutamente improbabile che arrivino al server, nell'arco di pochi millisecondi, due richieste praticamente identiche, provenienti da due sistemi identici, con il medesimo indirizzo IP, e riferite alla medesima pagina e con i medesimi parametri della richiesta.

Ciò consente al provider di correlare i cookie relativi alle due richieste (e non dimentichiamoci che tali cookie li ha generati il server stesso!).

In conclusione

Per quanto la nostra organizzazione si sforzi di proteggere i dati delle persone, ed elimini dai propri sistemi qualsiasi dato e qualsiasi programma che possa consentire la profilazione degli utenti, in realtà consente di fare tutto ciò a terze parti.

Pur non fornendo alcun dato in nostro possesso, fungiamo da mediatori in un trattamento di profilazione di terze parti (tra l'altro estremamente pervasiva e profonda), senza l'autorizzazione degli inconsapevoli visitatori del nostro sito.

Il semplice utilizzo di servizi e strumenti gratuitamente disponibili ci portano di fatto a servire su un piatto d'argento a terze parti le informazioni a loro necessarie per la profilazione del comportamento in rete dei nostri visitatori, senza che con esse vi sia il minimo contratto di fornitura, né condizioni contrattuali che regolamentino il trattamento dei dati, né lettere di nomina a responsabile o incaricato.

Inoltre il non utilizzare esplicitamente servizi esterni di web analytics non ci mette al riparo dall'essere stati mediatori invisibili della profilazione dei nostri visitatori da parte di terze parti.

E le informazioni che traiamo dal servizio di web analytics sono minime rispetto a quelle acquisite dalla terza parte.

Inoltre, in tutta la documentazione che avremo prodotto per conformarci alle richieste del GDPR avremo escluso categoricamente ogni forma di profilazione degli utenti (di fatto dichiarando il falso, perché comunque beneficiamo dei servizi di profilazione legati alla web analytics, derivati dalla profilazione), ed in ogni caso manifestando la mancanza di una reale conoscenza di quali dati dei nostri visitatori vengono coinvolti nei trattamenti effettuati dalla nostra azienda.

Non avremo infatti incluso tali trattamenti nel nostro registro, e di conseguenza non ne avremo tenuto conto nell'analisi dei rischi e nella DPIA.

E quindi, come posso continuare a fare analytics del mio sito?

L'unico modo che il Titolare ha per essere certo che non venga effettuata profilazione sui dati dei visitatori del proprio sito è implementare in house i servizi di web analytics, avendo cura non non salvare dati non pertinenti o eccedenti i trattamenti necessari, di anonimizzarli se necessario, e di eliminarli il prima possibile per ridurre i rischi relativi alla conservazione.

Una variante più rispettosa della privacy dei nostri visitatori è quella di implementare in house un bridge software che sostituisca il codice di profilazione delle terze parti con un alias predisposto internamente, pseudoanonimizzando così i dati della richiesta al servizio di web analytics; tali approccio può essere tuttavia invalidato qualora all'interno della medesima pagina vi siano richiami ad altri servizi offerti dal provider, che potrebbe quindi associare l'alias da noi fornito con il proprio profilo del visitatore.

In alternativa si può appaltare il servizio ad un fornitore esterno qualificato, previe le necessarie verifiche (che possono anche limitarsi alla verifica del possesso di adeguate certificazioni), ed alla stipula di un accordo che espliciti quali siano le responsabilità delle parti e le modalità di trattamento dei dati (fermo restando naturalmente il necessario consenso del visitatore).

Di tali trattamenti il Titolare è formalmente responsabile nei confronti di tutti i visitatori del proprio sito, e deve darne adeguata informativa e richiedere il necessario, consapevole ed informato consenso.

L'Europa affronta brevemente l'argomento nel proprio ThinkTank qui, e segnala alcuni strumenti di web analytics qui (sebbene una ricerca in Rete offrirà certamente anche altre alternative).

Bello fare analytics, ma … e se il visitatore non vuole?

Supponendo di essere riusciti ad organizzarci per fare web analytics in conformità al GDPR, resta ancora un ostacolo: ottenere il consenso del visitatore.

Il GDPR pone almeno tre requisiti vincolanti: occorre richiedere ed ottenere il consenso dell'interessato, e che tale consenso sia libero ed informato; inoltre, vi è il concetto di '*privacy by default*' che in pratica significa che non è consentito profilare l'utente a meno che lui attivamente autorizzi l'invio dei cookie di profilazione.

Ciò significa in pratica che:

1. non posso inviargli i cookie di profilazione (quelli tecnici si, in generale di sessione);
2. devo presentargli un'informativa adeguatamente chiara per spiegargli perché potrebbe o dovrebbe essere interessato ad attivare la profilazione
3. ottenerne il consenso,
4. ed a questo punto iniziare ad inviargli i cookie.

Resta comunque il fatto che almeno un cookie dovrà essere inviato al visitatore, ed è quello che ha lo scopo di 'memorizzare nel browser' la volontà di non ricevere cookie di profilazione; in caso contrario saremmo costretti a richiedergli un nuovo consenso ad ogni pagina che visita; l'importante è che tale cookie non venga associato in nessun modo al visitatore nel sistema di web analytics aziendale.

La questione non è di lana caprina, perché si è già verificato in passato che aziende profilassero gli utenti utilizzando proprio il cookie inviato per memorizzare la preferenza di non essere profilati.

Cosa fanno gli altri ...

Andando a spasso per la Rete se ne vedono di tutti i colori: mi cimento nel raccontare alcuni approcci che ho incontrato, con qualche considerazione sulla loro conformità alle indicazioni del GDPR.

Sarei tentato di fare dei nomi, ma, come suolsi dire, si dice il peccato e non il peccatore …

Per i pochi che eccellono invece rischierei di fare pubblicità, e quindi mi asterrò anche da questo.

Per quanto riguarda l'informativa ai visitatori, ho visto (pochi) siti presentarla in modo estremamente sintetico e chiaro, senza *legalese* e prolissità inutili; in

generale le politiche esposte classificano i cookie in tecnici e di profilazione (a volte anche necessari, funzionali e di pubblicitari o di marketing, ma ho visto classificazioni anche più articolate).

L'approccio più frequente è invece quello di sommergere il visitatori con montagne di informazioni dettagliatissime, con rimandi ad altre pagine e sotto-pagine, senza arrivare facilmente (o a volte mai) ad una pagina ove si possano esprimere le proprie preferenze, il tutto con il chiaro scopo di costringere l'utente ad accettare per disperazione tutti i cookie e proseguire con la navigazione.

È vero che il visitatore potrebbe anche rinunciare alla visita e spostarsi altrove, ma spesso se è arrivato sul un particolare sito, è perché ne ha la necessità o un specifico interesse, e può non voler rinunciare alla consultazione dei contenuti desiderati.

Ho visto anche di peggio: vi sono siti che, a parte l'incomprensibile legalese, rimandano il visitatore alla consultazione delle politiche per la privacy di tutte le aziende di cui vengono propinati i cookie o a cui vengono comunicati i dati di profilazione, ed eventualmente a gestire le impostazioni per la privacy direttamente su tali siti (Google, Facebook, siti di *adware* e marketing, etc.).

… solo per curiosità: vi siete mai cimentati nella verifica e modifica delle impostazioni per la privacy di tali siti?

Altri siti richiedono al visitatore di scaricare ed installare dei plug-in per il browser per effettuare l'opt-out presso il sito di web analytics (https://tools.google.com/dlpage/gaoptout, e similari): riuscite ad immaginare un anziano o un comune utente che comprenda almeno vagamente il problema che provi ad eseguire l'operazione?

Su un sito di un'importante organizzazione ho addirittura trovato tali collegamenti dissimulati come testo sottolineato, per impedire al visitatore di andare realmente a consultare le politiche e le impostazioni per la privacy dei siti referenziati.

Alcuni siti rimandano a politiche per la gestione dei cookie di terze parti in lingua straniera e senza versione in italiano (come Google-Analytics e HotJar).

Il sito di un'importante produttore di computer addirittura non presenta neppure un banner informativo sulla privacy né consente di effettuare l'opt-out per la ventina di cookie utilizzati (è vero che potrebbero essere tutti cookie tecnici, ma sarebbe carino darne informazione all'utente).

Per quanto riguarda l'effettiva espressione del proprio consenso, molti siti nascondono dietro ad altre pagine quelle ove prestarlo, ed a volte tali pagine neppure vi sono, in quanto i cookie di profilazione vengono spacciati per cookie tecnici necessari per la conduzione del sito.

Tra i siti ben fatti, ne ho visitati alcuni in cui il consenso poteva essere manifestato mediante delle check-box, una per ogni terza parte di cui vengono offerti i cookie.

D’altra parte la lista di check-box da spuntare era talmente lunga da farmi chiedere se ne valesse la pena per visitare le poche pagine che mi interessavano.

Dulcis in fundo, il miglior sito che ho avuto modo di visitare ha implementato con semplicità encomiabile esprimere le proprie preferenze: un semplice slider, che consente di posizionare il proprio ‘appetito’ per i cookie da solo tecnici, a cookie di profilazione, a cookie di marketing.

L’unica pecca che vi ho trovato è che lo slider era impostato di default sulla massima profilazione.

Cosa possiamo fare ...

… come aziende …

- imparare a seguire i dati, e comprendere cosa rappresentino e quanto siano critici;
- verificare con i nostri web designer se sia possibile copiare sul proprio server i contenuti esterni, in modo da non consentire la profilazione da parte di terze parti (fonts, codice, ...);
- attrezzarci per fare web analytics in house;
- nel caso si intenda esternalizzare i servizi di web analytics, imparare a stipulare contratti GDPR-compliant per il trattamento dei dati;
- informare gli utenti sulle implicazioni legate al possesso di account direttamente o indirettamente associati ai servizi di web analytics utilizzati;
- implementare la privacy by default;
- trovare valide ragioni per motivare i visitatori ad acconsentire alla profilazione dei propri dati;
- imparare ad identificare quali dati siano realmente importanti per la profilazione (… ci interessa davvero sapere con quale sistema operativo stiano consultando il nostro sito …?);
- fare lo sforzo di provare a leggere le politiche per la privacy dei siti di cui si utilizzano i servizi;
- quando possibile, utilizzare servizi alternativi e più rispettosi della privacy;
- fornire direttamente all’utente tutte le informazioni utili, ed in ogni caso limitare rimandi a pagine di terze parti in lingue straniere;
- imparare a semplificare la vita agli utenti: apprezzeranno il nostro sforzo e ci verranno incontro se riusciremo a trasmettere fiducia ed onestà di intenti.

… come utenti ...

- comprendere quale sia il nostro ‘appetito’ per la profilazione, ovverosia capire a quante delle funzionalità offerte dai siti siamo disposti a rinunciare

in cambio della nostra privacy, e comprendere quali siano i siti che trattano i dati in modo più rispettoso della nostra privacy;

- configurare i nostri browser perché inviino di default ai siti l'opzione DNT (Do Not Track), richiedendo esplicitamente ai siti di non effettuare tracciamento dei propri accessi;
- installare nel proprio browser un plugin di autodelete dei cookie alla chiusura della pagina consultata;
- installare nel proprio browser un plugin per prevenire l'esecuzione di script provenienti da siti non affidabili o non graditi, come google-analytics.com; si noti tuttavia che bloccare domini quali fonts.google.com o ajax.googleapis.com potrebbe compromettere il corretto funzionamento della pagina consultata;
- per tutti i siti su cui disponiamo di un account, o almeno per quelli più critici (Google, Facebook, Twitter, ...), accedere alle impostazioni relative alla privacy del proprio profilo, e effettuare l'opt-in o l'opt-out per ciascuna opzione di privacy (l'operazione può essere particolarmente lunga in relazione alla quantità di opzioni di tracciamento / anti-tracciamento disponibili);
- fare lo sforzo di provare a leggere le politiche per la privacy dei siti visitati;
- consultare le pagine su ciò che i siti sanno di noi (Google ad esempio offre questo servizio, e vi stupirete di quante informazioni sono state memorizzate sull'utilizzo del vostro account da quando l'avete creato!).

