UNIVERSITÀ DI PISA

LAUREA MAGISTRALE IN
INFORMATICA UMANISTICA

SEMINARIO DI CULTURA DIGITALE A.A. 2017/18

GDPR: impatto sul web e sul web marketing

Elisa Ammannati

Matricola: 518886

Sommario

Ecco cosa cambia con l'introduzione del GDPR, la nuova normativa europea sul trattamento dei dati personali. Confronto rispetto alla vecchia legge sulla privacy e analisi della criticità dell'impatto che il GDPR avrà sul web e sul digital advertising.

Introduzione

"Hai mai pensato di andare via e non tornare mai più? Scappare e far perdere ogni tua traccia, per andare in un posto lontano e ricominciare a vivere, vivere una vita nuova, solo tua, vivere davvero? Ci hai mai pensato?". Probabilmente, Luigi Pirandello nel 1904 scrivendo "Il Fu Mattia Pascal", mai avrebbe pensato che al giorno d'oggi, far perdere ogni traccia di sé, non sarebbe stato così facile.
Ormai, come ci muoviamo, all'interno della società o nella fitta rete del web, rilasciamo tracce delle nostre abitudini, delle preferenze, dello stile di vita, e, difficilmente ci soffermiamo a pensare che soggetti specifici raccolgono tutte le nostre informazioni, trattando ed analizzando i nostri dati personali. Attraverso la raccolta dei dati personali e la successiva creazione dei profili, si possono, ad esempio, intraprendere azioni di marketing mirate, come annunci pubblicitari personalizzati e campagne promozionali create ad hoc, al fine di fidelizzare sempre più la persona.
E' per questo motivo che sempre più aziende (Facebook e Google in primis) hanno adottato le tecnologie dei Big Data, raccogliendo ed analizzando enormi quantità di dati, principalmente in forma digitale per creare dei profili utente.
In Italia, per limitare e regolarizzare le operazioni eseguite sui dati personali è stata creata una norma emanata con il Decreto Legislativo del 30 giugno 2003, n.196, in vigore dal 1°gennaio 2004 che prende il nome di **Codice per la Protezione dei Dati Personali** che introduce delle garanzie per i cittadini in materia del trattamento della privacy e dei dati personali.
Tale norma, insieme alla direttiva 95/46/CE sulla protezione dei dati personali, è stata sostituita dal regolamento generale sulla protezione dei dati dell'UE (GDPR), progettato per **armonizzare le leggi sulla privacy di tutta Europa**, per proteggere e responsabilizzare tutti i cittadini europei sulla privacy e sul trattamento dei dati e per rimodellare il modo in cui le organizzazioni di tutta l'Unione Europea approcciano i dati personali.
Dopo quattro anni di preparazione e dibattito, il GDPR[1] è stato infine approvato dal Parlamento dell'UE il 14 aprile 2016. In data 25 maggio 2018, **il GDPR entra in vigore** e segna il momento in cui le organizzazioni, in caso di inadempienza, potranno essere soggette a pesanti ammende[2].
Adeguarsi alle norme del GDPR è la nuova sfida che i siti web si ritrovano a dover affrontare: poca chiarezza e molta rigidità lasciano ancora spazio ad interpretazioni personalizzate e spesso non in linea con la normativa europea. Queste problematiche, di conseguenza, impattano sul digital

[1] *General Data Protection Regulation*
[2] *https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_it*

advertising, dato che molte aziende ed organizzazioni si trovano rallentate da un insieme di problematiche che rendono difficile il corretto svolgimento della propria attività online.
Quindi, dopo una breve introduzione, sul significato dei dati personali, del loro trattamento e dopo aver dato una definizione del GDPR e averlo confrontato con la vecchia legge sulla privacy, si passa ad analizzare la privacy sui siti internet, differenziando tra il trattamento dei dati personali e i cookie, ponendo particolare attenzione su questi ultimi e chiedendosi se possano essere trattati come dati personali o no. Infine, si passerà a valutare l'impatto che la nuova normativa del GDPR ha e potrà avere sul settore del web marketing, andando ad analizzare le diverse tipologie di siti web, dagli e-commerce e siti aziendali, ai blog e siti di news, fino ad approdare ai social network.

1. Il trattamento dei dati personali e il GDPR

Quando si parla di **dato personale** di intendono tutte le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc[3].

Figura 1: breve infografica sui dati personali (fonte: Guida GDPR siti Wordpress)

In questa relazione si prendono in considerazione soltanto i dati che permettono l'identificazione diretta o indiretta, tralasciando i dati sensibili e tutti i siti web che trattano queste informazioni (siti di gestione delle buste paghe, siti di aziende sanitarie…). E' bene tenere presente che nel trattamento dei dati personali, ci sono sempre tre parti in gioco:

- **Interessato**: persona fisica alla quale si riferiscono i dati personali;
- **Titolare**: persona fisica, azienda, impresa o altro che decide gli scopi e le modalità del trattamento;

[3] *https://www.garanteprivacy.it*

- **Responsabile**: persona fisica o giuridica alla quale il titolare affida i compiti di gestione e controllo del trattamento dei dati per suo conto.

La raccolta, la gestione, la registrazione e qualsiasi altra operazione che viene effettuata sui dati rimanda alla nozione di "trattamento", concetto regolato fino al 24 maggio 2018 dal Codice della Privacy e della direttiva 95/46/CE. **E adesso, cos'è cambiato?**

1.1 Cos'è il GDPR?

Il regolamento generale sulla protezione dei dati è un regolamento dell'Unione Europea relativo alla **protezione delle persone fisiche** rispetto al trattamento e alla libera circolazione dei dati personali.
Il GDPR è una risposta necessaria ed urgente al dibattito aperto creato da un lato dai nuovi sviluppi tecnologici, che hanno portato ad un aumento dei rischi dovuti alla condivisione dei dati personali come la divulgazione non autorizzata, furto d'identità o abusi online, e dall'altro, di conseguenza, dalle esigenze di tutela da parte dei cittadini dell'UE.
In questo contesto, la nuova normativa ha come obiettivo principale proprio quello di restituire ai cittadini dell'UE il **controllo dei propri dati personali** e allo stesso tempo di cercare di semplificare ed armonizzare le norme riguardanti il trasferimento di dati personali dall'UE verso altre parti del mondo, rendendo in questo modo omogenea la normativa sulla privacy all'interno dell'Unione Europea[4].

1.2 GDPR: i punti fondamentali della normativa

In sintesi i punti fondamentali su cui si basa il GDPR sono i seguenti:

- Introduzione di regole più chiare su informativa e consenso;
- Definizione dei limiti sul trattamento automatizzato dei dati personali;
- Introduzione delle basi per la creazione di nuovi diritti per i cittadini;
- Stabiliti criteri rigorosi per il trasferimento dei dati al di fuori dell'UE;
- Fissate norme rigorose per i casi di violazione dei dati.

1.3 Cosa cambia rispetto alla vecchia legge sulla privacy

Con la nuova normativa si introducono nuovi diritti e nuovi doveri, rispettivamente per i cittadini e per le aziende titolari del trattamento dei dati. Prima dell'entrata in vigore del GDPR ogni stato dell'UE era libero di poter regolamentare il trattamento dei dati attraverso le proprie leggi: dopo il 24

[4] *https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati*

maggio 2018, ogni stato membro dovrà aderire alla nuova legge sulla privacy per rendere il trattamento un sistema più omogeneo.

Purtroppo, non c'è ancora molta chiarezza in materia: le disposizioni del GDPR hanno lasciato la possibilità, agli stati membri, di **legiferare in autonomia** per cercare di precisare, a seconda delle diverse esigenze, le norme contenute nel GDPR. In questo modo, però, il rischio è quello di tradire l'iniziale obiettivo dell'Unione Europea a causa dei contrasti che si possono venire a creare tra il regolamento stesso e le varie leggi nazionali adottate per allinearsi alle nuove indicazioni.

In generale gli aspetti più innovativi del GDPR rispetto alla precedente normativa sono tre, l'extraterritorialità, le sanzioni e il consenso:

- Per quanto riguarda l'**extraterritorialità**, le norme del GDPR si applicano a tutte le società che trattano o che gestiscono i dati degli utenti, a prescindere dal Paese in cui hanno sede legale o in cui i dati vengono elaborati.
- Il GDPR introduce **sanzioni economiche** a tutte quelle aziende che non rispettano il regolamento, ad esempio nel caso di un sito web che non ha policy adeguate per il consenso al trattamento dei dati personali.
- Le società che raccolgono o trattano dati personali devono spiegare in modo chiaro agli utenti tutte le **condizioni che regolano raccolta e trattamento dei dati**. E' responsabilità di chi raccoglie o gestisce i dati, redigere termini e condizioni in un linguaggio semplice, comprensibile a tutti i cittadini, senza possibilità di equivoco[5].

Proseguendo con le differenze rispetto alla vecchia legge sulla privacy, si nota che con il GDPR viene introdotto il concetto di **responsabilizzazione** (Accountability - responsabilità dei titolari del trattamento) dove saranno proprio le aziende ad analizzare le attività che comportano il trattamento dei dati personali e, sulla base di tale valutazione, identificare i possibili rischi per i diritti delle persone coinvolte, ponendo in sicurezza i dati e trattandoli in maniera lecita[6].

In più viene introdotto il **diritto alla portabilità dei dati** per trasferirli senza difficoltà da un titolare del trattamento ad un altro.

In sintesi ecco le novità (**doveri**) introdotte dal GDPR per le aziende che trattano i dati:

- Individuare il rischio e svolgere una valutazione d'impatto sui rischi e sulle tecniche per il trattamento dei dati;
- Rispettare i diritti delle persone;
- Redigere un registro dei trattamenti mantenendolo sempre aggiornato;

[5] *https://www.cwi.it/attualita/norme-e-regolamenti/gdpr*

[6] *https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati/*

- Garantire la sicurezza dei dati da parte del titolare e del responsabile del trattamento;
- Nominare un responsabile della protezione dei dati come punto di contatto tra cittadini, garante e il personale che tratta i dati.

Dal punto di vista dei cittadini, invece, ecco i **nuovi diritti** che dovrebbero garantire ulteriore chiarezza e sicurezza sul trattamento dei dati personali, sia online che offline:

- Ricevere informazioni chiare e comprensibili su chi sta trattando i dati;
- Richiedere l'accesso ai dati personali;
- Richiedere a un fornitore di servizi di trasmettere i dati personali ad un altro fornitore di servizi (es. quando si passa da un social network ed un altro);
- Diritto all'oblio, la possibilità di richiedere la cancellazione dei propri dati personali in modo che non vengano più visualizzati (es. da un motore di ricerca);
- Chiarezza nel caso della richiesta del consenso che deve scaturire da un'azione positiva della persona;
- Informazione nel caso di perdita o furto dei dati da parte di un'azienda;
- Nel caso di informativa rivolta ai minori, questa deve essere tradotta in un linguaggio più chiaro e comprensibile[7].

2. Privacy, GDPR e siti web

Dopo aver introdotto i punti chiave del GDPR è possibile passare all'analisi dell'impatto che la nuova normativa europea avrà sul web. La maggior parte delle aziende online si è trovata a doversi adeguare alle nuove norme sul trattamento dei dati personali muovendosi tra punti poco chiari e talvolta estremamente rigidi che riguardano in particolar modo i cookie, rivelatisi uno degli aspetti più controversi del GDPR.

Per questo motivo, in questa sezione analizzeremo l'impatto sui siti web distinguendo tra il trattamento dei dati personali rilasciati liberamente dall'utente e i cookie, rilasciati e raccolti indirettamente dall'utente. Ponendo l'attenzione sui cookie di profilazione, chiedendosi se essi debbano o possano essere trattati come dato personale o no, quindi in linea con la nuova normativa europea.

[7] *https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-citizens_it.pdf*

2.1 Trattamento dei dati inseriti dall'utente

I dati inseriti dall'utente sono tutti quei dati personali rilasciati ed inseriti liberamente dall'utente stesso su un sito.

Si inseriscono i dati personali ogni volta che si completa una registrazione ad un sito, ogni volta che si dà il consenso per ricevere newsletter, o ancora, ad esempio, se si vuole partecipare ad un forum e inserire commenti. La partecipazione a tutte queste attività è libera e facoltativa ed è per questo che **l'utente rilascia di sua spontanea volontà i propri dati personali** come il nome e il cognome, la residenza e il domicilio, il numero di telefono e l'indirizzo mail.

Questi dati vengono raccolti e trattati dall'azienda titolare del sito web e vengono utilizzati per erogare i vari servizi richiesti, per esigenze di tipo operativo, normativo, fiscale e gestionale, per finalità di ordine amministrativo e per eseguire eventuali obblighi di legge[8].

Secondo il codice italiano in vigore fino a maggio 2018, l'utente doveva essere informato circa il trattamento dei propri dati personali attraverso l'informativa a cui poteva dare il proprio consenso spuntando la casella apposita.

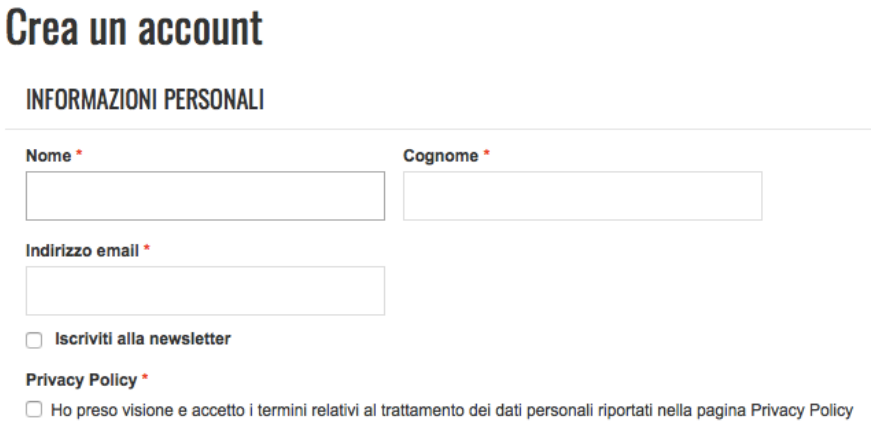

Figura 2: esempio di modulo per inserimento dei dati personali per registrazione ad un sito di e-commerce e successiva casella di spunta (Sito: Piccoleperle.it)

2.1.1 Dati personali: cosa cambia con il GDPR e l'impatto sui siti web

Secondo la nuova normativa GDPR, l'informativa e la casella di spunta non sono più considerati una condizione sufficiente per quanto riguarda il trattamento dei dati personali inseriti dall'utente. Il regolamento europeo, infatti, fissa parametri chiari per definire come deve essere ottenuto il consenso dall'utente al momento dell'inserimento dei suoi dati. In questo modo si indirizzano i siti web e altri servizi digitali a rivedere quelle procedure di consenso che risultano opache o, talvolta, completamente assenti.

[8] *https://it.wikipedia.org/wiki/Trattamento_dei_dati_personali*

Con il GDPR **il consenso deve essere libero, specifico, informato ed inequivocabile** e deve essere manifestato dall'utente attraverso una dichiarazione o un'azione positiva inequivocabile. Si eliminano, in questo modo, tutti i form che presentino caselle già spuntate.
Il consenso deve essere preceduto da **un'informativa** con dei requisiti minimi che deve essere resa nota attraverso un linguaggio chiaro, semplice e trasparente che sia comprensibile da una persona con un livello di cultura intermedia.
Tenendo conto di questi aspetti, viene alla luce il fatto che il consenso specifico e granulare richiesto dal GDPR risulta essere uno dei tanti aspetti controversi della normativa. Infatti, con il termine **granulare** si intende il fatto che l'utente ha la possibilità di dare o non dare il proprio consenso per ogni singola finalità che riguarda il trattamento dei dati personali in base alla nuova normativa: le singole finalità, infatti, non possono essere raccolte in un'unica casella di spunta, proprio perché verrebbe a mancare la libertà di scelta per ogni opzione da parte dell'utente. In pratica, attraverso la classica spunta che si vede in figura 2, l'utente sarebbe **obbligato ad accettare o a rifiutare in blocco tutte le finalità** per il trattamento dei dati personali senza altre possibilità di scelta.
Viene, quindi, da chiedersi, se il consenso granulare sia da considerare una novità positiva o negativa della nuova normativa. Certamente con il GDPR **viene tutelato maggiormente l'utente** grazie al fatto che viene informato punto per punto su come verranno trattati i propri dati personali, ma dall'altra parte è proprio l'utente stesso che, trovandosi di fronte ad un form con un elenco "infinito" di informative, scelte e spunte, rischia di accettare tutto, annullando il concetto chiave del GDPR, la chiarezza.

2.2 Cookie

Il consenso che riguarda i cookie è un altro degli aspetti controversi e caotici della nuova normativa. Ad una prima analisi sembra che il consenso all'uso dei cookie e il relativo utilizzo non siano in alcun modo regolati dal GDPR, ma dalla *Direttiva ePrivacy* che comunemente chiamiamo **Cookie Law**.
Attraverso il GDPR, infatti, si parla pochissimo dei cookie: viene specificato, soprattutto il fatto che le persone fisiche possono essere identificate tramite cookies. Quindi, il GDPR non abroga la Cookie Law, ma vi si affianca: GDPR e cookie diventano, in questo modo, complementari, andando ad aumentare il livello di protezione dei dati delle persone fisiche.
Sembra che, attualmente la Cookie Law, non richieda alcuna possibilità per l'utente finale di scegliere quali cookie accettare e quali no, nessuna selezione singola e neanche per categoria di cookie[9]: si accettano i cookie o si rifiutano, senza vie di mezzo.

[9] *https://www.garanteprivacy.it/cookie*

E' proprio basandosi su queste affermazioni e sui punti chiave del GDPR che è possibile notare l'aspetto controverso della questione: i **cookie di profilazione**, utilizzati per azioni di marketing, possono o devono essere considerati come dati personali dell'utente, visto che rimandano alle sue abitudini, ai suoi gusti e al suo stile di vita in generale? E in tal caso, dovranno sottostare alle imposizioni dettate dal GDPR? E con quali conseguenze sulla visibilità, sul marketing e sulla fruizione dei siti stessi?

2.2.1 Cookie: cosa sono, durata e tipologie

Utilizzando parole semplici, **i cookie sono piccole parti di codice** installate all'interno del browser dell'utente da parte di quasi tutti i siti web. I cookie non registrano alcuna informazione personale, bensì sequenze di dati salvati in file di testo collocati in apposite cartelle del browser dell'utente, file che possono essere interpretati solo dal sito che lo ha generato.
Per quanto riguarda la durata, i cookie possono essere **temporanei** (o di sessione) che si cancellano automaticamente una volta terminata la navigazione sul sito, o **persistenti** che rimangono in una apposita cartella del browser per un periodo predeterminato di tempo (in genere da 1 mese ad un anno).
Esistono tre tipologie di cookie:

- **Cookie tecnici**: necessari al funzionamento e all'ottimizzazione del sito web, gestiti direttamente dal titolare del sito;
- **Cookie di profilazione di prima parte**: utilizzati per azioni di marketing che hanno lo scopo di mostrare all'utente della pubblicità personalizzata basata sui siti precedentemente visitati o con lo scopo di creare statistiche disaggregate;
- **Cookie di profilazione di terze parti**: installati da altri siti rispetto al sito web visitato dall'utente e generati da script inseriti nel sito che richiamano funzionalità esterne. Un esempio sono i cookie raccolti da *Google Analytics* a fini statistici o da *Google AdSense* che crea annunci pubblicitari personalizzati. Nel caso di cookie di profilazione di terze parti, gli obblighi di informativa e consenso gravano sulle terze parti. Il titolare del sito è tenuto soltanto a specificare nella sua informativa quali sono i link delle aziende che trattano i cookie come terze parti[10].

[10] *https://www.capodanno-offerte.com/privacy/*

2.2.2 Cookie e GDPR: cosa cambia e l'impatto sui siti web

Con l'introduzione della nuova normativa, perché GDPR e Cookie Law siano in linea tra loro, occorre che si rispettino alcuni punti chiave che, si ribadisce, sono fondamentali per quanto riguarda i cookie di profilazione di prima parte e di terze parti e non per i cookie tecnici che non raccolgono dati personali:

- E' necessario il blocco preventivo dei cookie fino ad accettazione della cookie privacy;
- Il consenso deve essere informato, esplicito e preventivo da confermare con un'azione positiva;
- E' necessaria la registrazione del consenso in modo che sia provabile alle autorità competenti;
- La possibilità di revoca deve essere ben chiara e deve avere la stessa facilità dell'accettazione;
- L'informativa sull'utilizzo dei cookie e sugli installatori di terze parti deve essere descritta in modo semplice, chiaro e dettagliato;
- Ci deve essere un collegamento alla pagina della privacy;

Alcuni di questi punti venivano già rispettati con la Cookie Law. Attraverso il GDPR si rende soprattutto necessaria l'**introduzione della registrazione del consenso** e l'**accettazione positiva** dello stesso tramite spunta.

In sostanza, il GDPR imporrebbe un consenso esplicito più granulare che richiama alla mente la trasparenza e la chiarezza della nuova normativa a favore dell'utente, ma che allo stesso tempo rischia di far rallentare la navigazione sul sito web con conseguenze tangibili che riguardano il calo di visite e il calo di click pubblicitari[11].

Approfondendo la ricerca, si nota, in effetti, che la maggior parte dei siti che lavorano con la pubblicità, come quotidiani e blog, rispettano poco o nulla la nuova normativa del GDPR perché rischiano un netto calo del click advertising.

Questo, a mio avviso, a causa delle varie complicazioni e male interpretazioni della normativa che imporrebbe una mole di blocchi eccessiva, cautelativa per l'utente finale, ma eccessiva per i siti web.

Inoltre, un passo poco chiaro della normativa riguarda i **siti che utilizzano servizi terzi**, vale a dire i cookie di terze parti: un esempio sono tutti quei blog, siti e quei quotidiani che si affidano a concessionarie pubblicitarie come, ad esempio, *Google Adsense*. Queste a loro volta usano cookie traccianti, cioè di profilazione e, talvolta, aggregano dati e collaborano a loro volta con altre agenzie. In pratica, chiedere il consenso all'utente per cookie trattati da terze parti non è una procedura così scontata per il titolare del sito web visto che, a sua volta, non sa come vengono trattati i cookie di profilazione da parte di queste agenzie terze. Inoltre il loro modo di trattate i dati personali può

[11] *http://www.viralbeat.com/blog/gdpr-cookie-law/*

cambiare da un momento all'altro senza preavviso: in questo modo il titolare del sito si troverebbe a dare all'utente un'informativa, non tanto errata, quanto non in linea con il reale trattamento dei dati effettuato dalle terze parti.
La conseguenza peggiore, a mio avviso, potrebbe essere quella di un blocco di tutto il servizio terzo cioè del servizio pubblicitario, con conseguenze altrettanto pesanti per tutti i siti web che lavorano con il digital advertise.

2.2.3 Cookie e GDPR: l'evoluzione del banner

Fino all'introduzione della nuova normativa, per rispettare la Cookie Law, bastava inserire un **banner** ben visibile sul sito web che contenesse le finalità di installazione dei cookie e che descrivesse in modo chiaro le azioni intese come consenso (fig.3 e 4). In questo caso, l'utente poteva dare la propria accettazione in modo esplicito, sia cliccando su "accetta", sia attraverso il semplice scroll della pagina, che cliccando sulla "x" per chiudere l'informativa o, ancora, continuando la navigazione nel sito stesso.

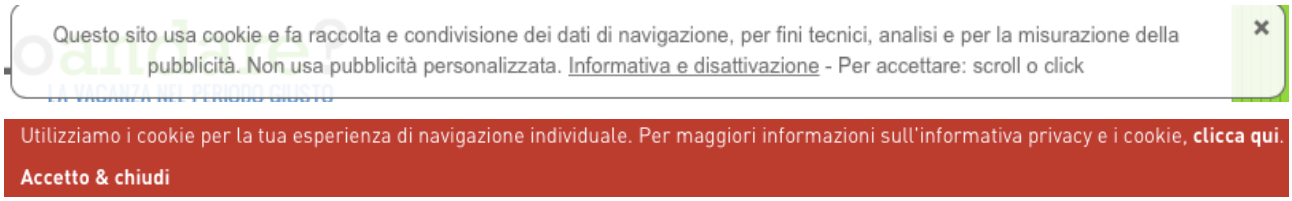

Figura 3 e 4: i banner di alcuni siti web che rispettano la Cookie Law.

Con il GDPR cambiano le finalità, il consenso e il funzionamento del cookie banner: infatti, il banner dovrà contenere una **descrizione dettagliata della finalità dei cookie di profilazione** e la richiesta di consenso dovrà essere non smarcata preventivamente, ma dovrà essere l'utente stesso a dare il proprio consenso esplicito e senza il quale, la navigazione continuerà senza cookie di profilazione. Per capire meglio come dovrebbero adeguarsi i siti web alla nuova normativa, si analizza un esempio in linea con il GDPR, presente in fig.5.

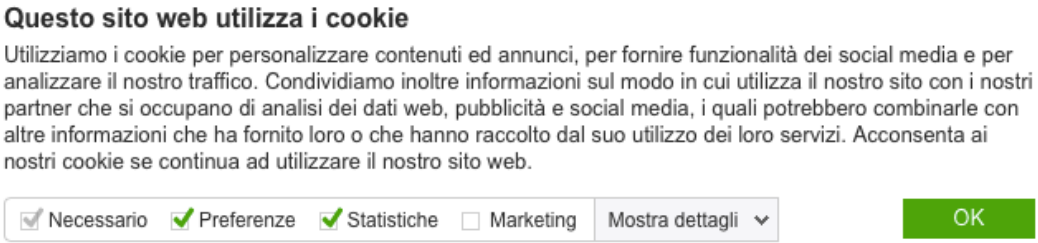

Figura 5: il cookie banner in linea con la normativa GDPR (Cookiebot.com)

Innanzitutto, l'utente si trova davanti ad un'informativa, sulle finalità dei cookie, più ampia e ben dettagliata. Si notano, poi, nella parte inferiore dell'informativa, 4 tipologie diverse di consenso:

1. **Necessario**: il consenso è già spuntato ed obbligatorio perché con l'accettazione vengono rilasciati i cookie tecnici e di sessione.
2. **Preferenze**: i cookie per le preferenze consentono ad un sito web di ricordare le informazioni che influenzano il modo in cui il sito si comporta o si presenta, come ad esempio la lingua preferita. Insieme a quelli utili ai fini della statistica, i cookie di preferenza non rientrano nella categoria dei cookie di profilazione: è per questo motivo che la casella è già spuntata in automatico e l'utente potrà decidere di non dare il consenso per questo tipo di cookie, deselezionando la casella.
3. **Statistiche**: i cookie statistici aiutano i proprietari dei siti web a capire come gli utenti interagiscono con il sito, raccogliendo e trasmettendo informazioni in forma anonima. Come i precedenti, si ricorda che non rientrano nella categoria dei cookie di profilazione.
4. **Marketing**: i cookie di marketing sono utilizzati per monitorare il comportamento e le abitudini degli utenti nel sito web. La finalità è quella di mostrare annunci pertinenti e coinvolgenti per il singolo utente e quindi quelli di maggior valore per gli editori e gli inserzionisti terzi. Come si nota, la casella che riguarda i cookie di marketing non è spuntata in automatico perché deve essere l'utente a selezionarla se vuole che vengano rilasciati i cookie di profilazione.

Come nel caso dei banner in fig.3 e fig.4, per rilasciare il proprio consenso (cliccando o no sulla spunta del marketing) l'utente può seguire tre strade: cliccare sul pulsante "ok", fare lo scroll della pagina o continuare la navigazione sul sito cliccando, ad esempio, su una delle voci del menù[12].

Le conseguenze immediate di questi moduli di consenso più granulari sono descritte nel prossimo capitolo che tratta l'impatto del GDPR sul web marketing e sulle varie tipologie di siti web, differenziando tra i siti che ospitano pubblicità, quelli che acquistano pubblicità e i social network.

3. GDPR e Web Marketing

3.1 Siti di quotidiani, news e blog (siti che ospitano pubblicità)

I siti di quotidiani, news e blog sono tutti siti che hanno in comune il fatto di offrire contenuti più o meno gratuiti agli utenti: in queste pagine web sono ospitati articoli, foto o video sia generici che riguardo ad un argomento in particolare.

[12] *https://www.cookiebot.com/it/*

Questa tipologia di siti web viene denominata **Publisher**, vale a dire siti di larga fruizione che hanno l'esigenza di sostenersi e di far monetizzare il proprio sito web grazie alla pubblicità ospitata nelle loro pagine: ad ogni click dell'utente sulla campagna pubblicitaria, il publisher effettua un guadagno. Analizzando la normativa del GDPR rispetto ai siti publisher è possibile notare **due tipi di impatto**, uno soft e meno invasivo e uno decisamente più critico.

Nel primo caso si prende in considerazione la parte relativa alla **privacy** utile per le interazioni di base con il sito, come l'utilizzo di pulsanti social, newsletter e commenti, notando il basso impatto creato dalla nuova normativa: in questo caso adeguarsi non è complesso, visto che basta utilizzare sia dei moduli a norma con la spunta che un'informativa ben fatta, entrambe soluzioni che possono essere create e controllate attraverso i diversi plugin presenti sulle piattaforme CMS, Content Management System, quest'ultime utilizzate molto spesso per la creazione di questi siti.

La parte più critica della nuova normativa riguarda la **pubblicità** e gli introiti dovuti ad essa. I siti si trovano costretti ad attuare un blocco preventivo che prevede la richiesta di consenso per il rilascio di cookie di profilazione, che a sua volta richiede un blocco preventivo delle funzionalità associate al cookie di profilazione stesso. Cioè? Quando un utente naviga in rete ed approda su questi siti, il rischio è quello che non potrà più vedere subito le pubblicità o almeno non tutte: infatti le pubblicità profilate potranno essere generate solo dopo esplicito consenso.

Questo comporta due problemi per i gestori dei siti: per prima cosa, una diminuzione di guadagni che, in alcuni casi, può risultare estremamente rilavante, e che dipende, in ogni caso, dalla percentuale della pubblicità rilasciata dalle agenzie terze come *Google Adsense*, e secondo, è che l'introduzione del cookie banner potrà risultare invasivo per l'utente e molto complesso da implementare per i gestori del sito.

Tenendo conto di ciò che è stato descritto nel paragrafo dedicato al cookie banner, è possibile fare un esempio pratico di funzionamento: quando l'utente arriva sul sito, il sito genera i propri contenuti e, di conseguenza, rilascia i cookie di sessione e tecnici che sono alla base del funzionamento del sito stesso. Allo stesso tempo, però, vengono bloccati preventivamente tutti i cookie di profilazione e, quindi, le pubblicità personalizzate, fino al momento in cui l'utente non dia esplicitamente il proprio consenso.

Ma, **l'utente darà il proprio consenso?** In pratica, ecco ciò che potrebbe accadere. Innanzitutto, a prima vista, il cookie banner può spaventare gli utenti che si trovano davanti ad un'informativa lunga ed articolata da leggere e capire: ciò può comportare un abbandono immediato del sito senza la conseguente fruizione dei contenuti e della pubblicità.

Nel secondo caso, una gran parte di utenti si troverà a fare click più rapidi per poter disattivare velocemente il banner e per poter navigare sul sito: secondo la normativa questo comporta una non

accettazione perché l'utente, cliccando sul pulsante "chiudi", facendo lo scroll della pagina o continuando la navigazione, in realtà non spunta, per poter accedere velocemente al sito, la casella relativa ai cookie di profilazione. Spesso anche perché disinteressato all'argomento.
Si deve porre l'attenzione sul fatto che l'utente non è disinteressato alla pubblicità profilata, che è un suo diritto rifiutare con il GDPR, ma è **disinteressato al processo di acquisizione del suo consenso**.
In pratica, i siti a contenuti si troveranno a dover mostrare poca pubblicità profilata e personalizzata, non perché sgradita all'utente, ma perché la richiesta di consenso è troppo complessa.
Si analizzano, adesso, alcuni dati riferiti al digital advertising: la percentuale di pubblicità personalizzata, su alcuni siti, arriva addirittura al 90% e più sono generalisti (come, ad esempio, i quotidiani) e più pubblicità personalizzata, hanno. Di conseguenza, la percentuale di abbandono (di rimbalzo) senza click di accettazione sul banner può essere misurata in un 20-30%, mentre, dato un cookie banner in linea con il GDPR, gli utenti che spunteranno e accetteranno i cookie di profilazione saranno circa il 15-20%. Gli altri utenti chiuderanno il cookie banner senza accettare la profilazione perché non vorranno essere scocciati da tutte le domande e dai consensi richiesti dal GDPR.
La conseguenza finale potrebbe essere la seguente: una probabile crisi dei siti che offrono contenuti gratuitamente con danni gravi sia a livello di libera informazione, dato che la fruizione di notizie gratuite è alla base della democrazia, sia al livello della miriade di aziende piccole, medie e grandi che offrono contenuti qualificati a fronte di introiti pubblicitari.
La normativa, inoltre, impone ai proprietari dei siti di non bloccare la fruizione dei contenuti del sito a chi decide di non accettare i cookie di profilazione: è possibile, quindi affermare, che questa norma sembra troppo sbilanciata a favore dell'utente, un po' come si imponesse ai ristoranti di offrire del cibo gratuito a chiunque sia di passaggio.

3.2 Siti di e-commerce e siti aziendali (siti che comprano pubblicità)

La situazione di questi siti è esattamente opposta rispetto a quella dei precedenti. Gli e-commerce e i siti aziendali non ospitano pubblicità di terze parti, ma al contrario acquistano pubblicità su circuiti e agenzie come *Google Ads* per rendersi visibili agli utenti.
Essere visibili agli utenti vuol dire ospitare sul proprio sito dei codici di remarketing: le agenzie pubblicitarie rilasciano cookie di tracciamento per i codici di remarketing e rendono visibile l'azienda e l'e-commerce attraverso i cookie di profilazione rilasciati dall'utente. Il funzionamento è lo stesso che regola i cookie dei siti dei publisher.
Come risultato si hanno quindi gli stessi problemi già elencati nel precedente paragrafo che, in questo caso, possono comportare un sostanziale abbandono del sito, una minore fruizione del sito aziendale,

una drastica diminuzione dell'accettazione alla profilazione e un indebolimento di un potente strumento di marketing in possesso di tutti coloro che acquistano pubblicità su internet.
Un altro punto da analizzare è il fatto che questi siti tendono molto più degli altri ad **acquisire dati personali in maniera diretta** come, ad esempio, nel caso degli e-commerce dove viene richiesta la registrazione di dati personali per evadere gli ordini. In questo caso, con l'introduzione del GDPR, sarebbe richiesto un adeguamento tecnologico con software che offrano un'informativa ben fatta e dei sistemi chiari di spunta per l'accettazione delle finalità del sito come l'evasione degli ordini, il consenso per la pubblicità da parte di terze parti e la cessione dei dati a terze parti.
Si sottolinea il fatto che in questo senso non si ravvedono molti cambiamenti rispetto alla vecchia legge della privacy perché in Italia, essa risultava già più stringente rispetto a quella di tanti altri Paesi dell'Unione Europea. Inoltre, chi sta acquistando un prodotto o un servizio, è più propenso a sottoporsi ad un rilascio dei consensi anche più approfonditi, rispetto all'utente che vuole accedere ai contenuti di un sito informativo.
Sicuramente il GDPR impone molti oneri in più per la **gestione del database dei dati degli utenti**: oneri per una buona conservazione, una maggiore attenzione alla sicurezza del sito, e un aspetto in particolare, quale l'adeguamento alla giusta durata della conservazione dei dati personali: in questo caso, il GDPR non pone limiti temporali definiti, ma introduce il concetto di conservazione per lo stretto tempo necessario rispetto alla funzione per la quale sono stati rilasciati i dati.
Quest'ultimo punto si può ricondurre al caso degli e-commerce: viene da chiedersi, cosa si deve fare del prezioso database dei clienti che acquistano un prodotto ogni anno, o saltuariamente, magari ogni due o tre anni?
Secondo la nuova normativa bisognerebbe provvedere ad una periodica cancellazione del database dei clienti, sostanzialmente perdendoli: questo appare un provvedimento che va contro l'interesse di tutte le parti, sia delle aziende che vedono depauperare il proprio patrimonio del pacchetto clienti creatasi nel tempo, sia del cliente stesso che ha piacere di rimanere censito per acquisti saltuari, evitando, quindi, di dover immettere ogni volta i propri dati personali.

3.3 Social Network

Tutti conosciamo *Facebook* e *Twitter*, ma in realtà i siti con funzioni social sono moltissimi, magari anche di nicchia e poco diffusi: in comune hanno il fatto di avere un grosso impatto sul volume del traffico web e sulle abitudini di navigazione degli utenti.
E' evidente che un social network, per la sua stessa natura, rappresenta una situazione di enorme criticità rispetto alla tutela dei dati personali e questo è tanto più vero quanto più di successo è il social network. Infatti esso acquisisce un'enorme quantità di informazioni e dati personali, analizzandoli e

mettendoli in relazione tra loro e, grazie alle enormi risorse che ha a disposizione, può arrivare a **generare profondi cambiamenti nella società** e nella cultura stessa. E' ovvio che allo stesso tempo, il social network deve anche trovare il modo di gestire i dati e di trattarli con gli strumenti adeguati, secondo la normativa vigente.

Questo appena descritto è il concetto di Big Data e senza addentrarsi ulteriormente in questo campo si ritiene comunque necessario sottolineare il fatto che la sfida che i social network si troveranno ad intraprendere nel futuro per garantire la loro stessa sopravvivenza, sarà proprio l'attenzione alla privacy degli utenti.

Infatti, la criticità, in questo caso, non è tanto una semplice esposizione di un banner o l'attivazione o meno della pubblicità (che comunque fanno), quanto la gestione veramente granulare delle informazioni personali che vengono inserite dall'utente: un esempio sono i pannelli di controllo come quelli di *Facebook* che hanno sezioni ampissime per la gestione della privacy dell'utente che, quest'ultimo si trova a settare e a scegliere. In effetti dando un'occhiata al pannello di controllo si notano molte sezioni e molte voci diverse che riguardano tutte la gestione della privacy e dei propri dati personali: viene da chiedersi quanti utenti risulteranno così consapevoli da leggere, controllare e gestire in modo approfondito le opzioni sulla propria privacy. Probabilmente la maggior parte di essi, attratti dal funzionamento del social network tralasceranno la maggior parte delle scelte, permettendo a *Facebook* di gestire e di diffondere i propri dati personali in modo quasi completamente inconsapevole.

Figura 5:il pannello di controllo di Facebook per la privacy

Conclusione

In ultima analisi, è possibile affermare che da un lato, i principi espressi dalla normativa sono condivisibili e dall'altro, invece, si rischia un'eccessiva burocratizzazione di molti processi del trattamento dei dati personali, in particolare nel trattamento dei dati non sensibili per i quali lo stesso utente potrebbe preferirebbe procedure più snelle.

Infatti, un'eccessiva complicatezza delle procedure, come nel caso del cookie banner o nel caso di informative cartacee lunghissime e prolisse, rischia di generare l'effetto opposto rispetto a quello voluto dalla legge, ovvero un'accettazione (o non accettazione) frettolosa e non consapevole dell'informativa che porta a vanificare tutti gli effetti voluti dalla nuova normativa GDPR.

A mio avviso sarebbe auspicabile un'attuazione di regole più snella per alcune procedure, come nel caso dell'accettazione dei cookie che potrebbe essere effettuata, ad esempio, a livello di browser e non di volta in volta, sito per sito: questo sarebbe utile per non sobbarcare gli utenti di continue richieste che, alla fine, sono sempre le stesse e per le stesse tipologie di cookie.

Bibliografia

Voigt, P. Bussche, A. *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 2017.

Sitografia

http://www.viralbeat.com/blog/gdpr-cookie-law/

https://www.cookiebot.com/it/

https://www.conflux.it/blog/gdpr-protezione-privacy-dati-marketing

https://www.capodanno-offerte.com/privacy/

https://www.garanteprivacy.it/cookie

https://www.facebook.com/privacy/

https://www.cwi.it/attualita/norme-e-regolamenti/gdpr

https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati/

https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati

https://it.wikipedia.org/wiki/Codice_in_materia_di_protezione_dei_dati_personali

https://it.wikipedia.org/wiki/Trattamento_dei_dati_personali

https://www.garanteprivacy.it/documents/10160/0/Guida+all+applicazione+del+Regolamento+UE+2016+679.pdf

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_it

https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-citizens_it.pdf