Commenti alle nuove Linee Guida del Garante Privacy sui cookie

Il Garante per la Protezione dei Dati Personali ha recentemente pubblicato delle "Linee **Guida sull'utilizzo dei cookie ed altri strumenti di tracciamento**" in consultazione pubblica. Quindi, in base ai commenti ricevuti da diverse fonti, emanerà successivamente le Linee Guida definitive.

In questo articolo, pertanto, fornisco alcune considerazioni personali sulle Linee Guida stesse ed in generale sull'argomento "cookie ad altre tecnologie traccianti", che normalmente sono presenti sui siti web – ma anche su *app* per dispositivi portatili -, ad integrazione ed aggiornamento di quanto riportato in un mio precedente articolo. Si consideri anche che, nel frattempo, alcune Autorità di Controllo Europee (ICO, CNIL,…) hanno pubblicato proprie linee guida e l'EDPB ha più recentemente pubblicato le **Linee Guida sul Consenso**, che riportano anche alcuni esempi sulla gestione dei cookie.

Nel panorama generale dei siti web gestiti dalle imprese italiane si possono identificare due grandi categorie:

1. Siti basici, di tipo istituzionale e/o divulgativo, che rappresentano una sorta di pubblicità via web, brochure digitale online, priva di funzionalità dinamiche attive (ad eccezione, in alcuni casi, di un blog con articoli divulgativi su argomenti inerenti all'attività dell'impresa o dello studio professionale). In siti di questo genere non ci sono aree riservate a cui accedere previa registrazione, è solo presente un *form* di contatto per porre domande e richieste di informazioni al proprietario del sito. In alcuni casi è possibile iscriversi alla *newsletter* fornendo il proprio indirizzo e-mail, al fine di rimanere informati sulle novità, nuove proposte e nuovi articoli del blog. Li chiameremo **siti del primo tipo**.
2. Siti che prevedono attività di *direct-marketing* anche molto invasive; dunque, non solo cookie traccianti, ma anche raccolta di informazioni aggiuntive degli

utenti, profilazione degli stessi con attività di re-marketing e marketing targettizzato in funzione delle preferenze degli utenti, registrazione al sito – anche con *account social* – ed eventuali attività di e-commerce. Li chiameremo siti del **secondo tipo**.

Fra queste due macro-categorie ci possono essere, ovviamente, situazioni intermedie, che si avvicinano più al primo o secondo tipo.

Al momento le interpretazioni prevalenti – soprattutto a livello europeo – dell'applicazione del GDPR e delle Linee Guida EDPB sul consenso – ed in parte anche queste Linee Guida del Garante Privacy italiano – rendono l'applicazione della normativa sui cookie piuttosto difficoltosa per le PMI, gli Studi Professionali e i singoli liberi professionisti che possiedono un sito web del primo tipo. Una gestione dei cookie granulare, fornendo la possibilità all'utente di decidere quali (tipi di) cookie accettare e quali no, costringerebbe queste organizzazioni a aderire ad uno dei servizi di gestione dei cookie e delle relative cookie policy e/o rivolgersi all'assistenza specialistica di un *webmaster* o società specializzate nello sviluppo e la gestione di siti web. Paradossalmente la creazione e manutenzione di un sito web per una piccola organizzazione – al netto del tempo necessario per creare ed aggiornare i contenuti – potrebbe costare meno di 100 euro l'anno (costi di registrazione del dominio, *web hosting*, database per ospitare CMS come WordPress, caselle di posta incluse), mentre la gestione dei cookie sarebbe più onerosa, anche semplicemente volendo gestire cookie tecnici e cookie analitici di prima parte e di terza parte (es. Google Analytics).

Dal punto di vista dell'utente medio, gli elementi più fastidiosi nella navigazione sul web sono possono invece essere classificati nei seguenti:

1. Subire banner pubblicitari molto invasivi, anche di argomenti non pertinenti con il sito internet che si sta consultando, con il rischio abbastanza frequente di cliccare involontariamente sul banner pubblicitario e, quindi, vedersi proiettati in siti non pertinenti e talvolta inappropriati, se non si sono impostati determinati filtri a livello di browser o di anti-malware.
2. Subire *spamming* e campagne pubblicitarie particolarmente invasive (a volte anche tramite telefonate commerciali indesiderate, se è stato in qualche modo carpito il numero di telefono) per il solo fatto di aver consultato un determinato sito o aver ricercato o visionato un determinato prodotto in un sito di e-commerce.
3. Dover continuamente accettare, rifiutare i cookie (o scegliere quali accettare e quali no) per ogni accesso ad una nuova pagina web, considerando anche la reiterazione dell'operazione ad ogni nuovo accesso allo stesso dominio effettuato in tempi diversi o tramite dispositivi diversi.

Il nuovo approccio alla gestione dei cookie ed altre tecnologie traccianti introducono sistematicamente il terzo elemento nell'elenco sovrastante, ma non eliminano a priori i disagi ed i disturbi dei primi due casi.

D’altro canto occorre considerare la seguente domanda: quanti utenti conoscono l’esatto significato delle diverse tipologie di cookie? Le informative che si vedono nella maggior parte dei siti, anche quelle gestite in modo automatico dai servizi specialistici di *cookie management*, non aiutano certamente l’utente a capire cosa egli potrebbe escludere e cosa accettare.

In altre parole, credo che anche l’approccio più rigoroso e garantista per la protezione dei dati personali dell’utente nella gestione dei cookie non cauteli adeguatamente l’utente stesso, soprattutto se minore, dalle situazioni di cui ai punti a) e b) sopra citati. L’applicazione delle regole sancite dalle linee guida a livello europeo ha finora portato ad aumentare la difficoltà dell’utente che volesse non accettare tutti i cookie di un sito o un servizio che utilizza a scopo di lucro i dati personali degli utenti (es. Google, Microsoft, Facebook, Amazon ed altri). Inevitabilmente i rischi per l’interessato nella gestione dei cookie di siti del primo tipo di piccole organizzazioni, ad eccezione di quelle che trattano dati sanitari, sono infinitamente inferiore ai rischi che corrono navigando su siti del secondo tipo. Purtroppo, il Regolamento e le Linee Guida pubblicate recentemente **non recepiscono questa differenziazione** e le relative cookie policy/privacy policy non sembrano evidenziare le enormi differenze per l’utente in queste due situazioni tipiche. Perché le scelte sulla gestione dei cookie non possono discendere da una valutazione dei rischi per i relativi trattamenti di dati personali? Tale valutazione potrebbe prendere in considerazione la gravità del rischio, ovvero delle conseguenze per l’interessato del trattamento dei cookie effettuato dal sito e dalle terze parti, e della probabilità che tale evento si verifichi (si consideri che cookie e indirizzi IP, ad esempio, non sono sempre dati personali, in molti casi non è possibile risalire da essi a persone fisiche individuabili).

In attesa che la normativa a livello europeo non sancisca le regole sui cookie e tecnologie similari in modo definitivo, attraverso il **nuovo Regolamento e-Privacy**, occorre prudenza nel definire regole prescrittive troppo severe a partire da interpretazioni del GDPR del concetto di consenso, quando la gestione di un consenso *off-line* (ad es. su un modulo cartaceo) è ben diversa da un consenso *on-line* (su un sito internet). E soprattutto la gestione dei diritti dell’interessato, come li prevede il RGPD, è alquanto complicata.

Relativamente all’inadeguatezza dello *scrolling* ad attestare il consenso dell’interessato, da un lato sono d’accordo, ma dall’altro viene da chiedersi perché certi banner pubblicitari possono essere talmente ingannevoli che l’utente facilmente finisce per essere veicolato su un sito indesiderato, senza che nessuno gli abbia chiesto se veramente avesse voluto navigare su tale sito. Dunque, occorrerebbe più coerenza nello stabilire regole omogenee in diversi contesto e, soprattutto, nel farle rispettare.

Riguardo all’uso, ritenuto illecito, dei c.d. *cookie wall*, mi permetto di dissentire in via generale, almeno per i siti del primo tipo. In particolare, mi riferisco a siti web che forniscono informazioni utili su diversi argomenti, tramite articoli

del blog o sezioni specifiche (community, documenti da scaricare, ecc.): per i gestori di tali siti mi sembra legittimo richiedere l'accettazione di cookie analitici per il monitoraggio degli accessi al sito al solo fine di elaborare statistiche, necessariamente elaborate da terze parti, quali Google, per fornire informazioni a titolo gratuito. Il bilanciamento fra il servizio fornito a titolo gratuito e il minimo trattamento dei cookie mi sembra adeguato.

Diverso potrebbe essere il caso in cui si subordina l'accesso al sito ad attività di profilazione più invasive, sebbene ci si potrebbe chiedere che differenza c'è rispetto alla sottoscrizione di fidelity card nei negozi fisici, che prevedono l'attivazione di raccolte punti con sconti e premi subordinate ad attività di profilazione a fini di marketing. Ancora una volta il cittadino e l'impresa richiedono coerenza a 360° nei diversi ambiti.

Un aspetto non completamente chiarito dalle linee guida è quello costituito dai plugin social presenti in molti siti web per la condivisione di contenuti su Facebook, Linkedin, Twitter, ecc.. In tal caso se l'utente intende condividere un articolo o una pagina di un sito web su un social network è bene comprendere che tale attività viene svolta attraverso l'account dell'utente nel *social network*, dunque la condivisione dei dati (utente X che condivide un articolo del sito Y sul social network Z tramite il proprio account social) avviene nella piena consapevolezza dell'utente, dunque non dovrebbe essere richiesto alcun consenso per mantenere questi *plugin social* nel proprio sito, a condizione che svolgano solo questo compito.

Analogamente un utente che naviga su un sito tramite Chrome dopo essersi autenticato con il proprio account Google, e magari aver effettuato una ricerca per arrivare proprio a quel sito, dovrebbe essere pienamente consapevole che la sua attività nel sito – e nelle pagine consultate prima e dopo – è stata completamente tracciata da Google, in maniera del tutto indipendente.

In generale credo possa essere accettabile, sempre per siti del primo tipo, richiamare alcune istruzioni generali per disabilitare i cookie direttamente nel browser, in base alle funzioni messe a disposizione da Firefox, Chrome, Edge, Safari, Opera ed altri browser, sebbene comunque alcuni siti richiederanno l'abilitazione dei cookie, anche quelli più invasivi per la privacy, per funzionare. Alleviando così l'onere in capo al proprietario del sito di implementare complicate gestioni dei consensi per tipologie di cookie.

L'obbligo di mantenere evidenza documentata del consenso obbligherebbe ancora una volta i proprietari dei siti di primo tipo a rivolgersi ai rispettivi gestori con attività onerose dal punto di vista economico. Ancora una volta dal punto di vista dell'utente che ha implementato nel browser funzionalità di cancellazione automatica dei cookie al termine della sessione si troverebbe a dover nuovamente acconsentire ai cookie ad ogni nuovo accesso al medesimo sito, benché il consenso sia già stato dato, magari il giorno precedente.

Meno oneroso sarebbe in ogni caso dimostrare un comportamento corretto da parte del proprietario del sito, ovvero l'applicazione di una procedura di accettazione o rifiuto dei cookie ad ogni accesso al sito, nella consapevolezza che la registrazione del precedente consenso sarebbe inutile laddove l'utente abbia cancellato automaticamente i cookie. Anche in questo caso occorre differenziare il consenso prestato *on-line* da quello *off-line* essenzialmente su modulistica cartacea, a vantaggio di una gestione semplificata e più snella per le piccole e medie organizzazioni, senza inutili sprechi di risorse economiche a fronte di modesti vantaggi e limitatissimi rischi per l'utente in termini di privacy.

Più in generale il contesto nel quale si trova l'utente comprende siti nei quali è impossibile disabilitare tutti i cookie e app su smartphone che richiedono genericamente l'accesso a risorse del dispositivo senza chiarire in quali casi vengono utilizzati i dati personali dell'utente (nome, numero di telefono, e-mail, le immmagini e i video memorizzati, ecc.) e dei suoi contatti.

Pur apprezzando il lavoro dell'Autorità Garante per la Protezione dei Dati personali che sta prendendo in considerazione anche le esigenze delle piccole e medie imprese del nostro tessuto economico, credo che molti aspetti di questo complicato argomento debbano ancora essere chiariti e resi applicabili in modo più snello.

Aggiornamento relativamente al Regolamento e-Privacy del 04/03/2021

Il Regolamento e-Privacy ha ottenuto dal Consiglio UE parere favorevole sulla versione finale del testo, con un mandato negoziale per la revisione definita delle regole in materia di tutela della riservatezza nell'uso di servizi di comunicazione elettronica. Ora ci si attende l'emanazione del nuovo Regolamento – che abrogherà la vecchia Direttiva e tutta la legislazione precedente in materia di cookie – entro qualche mese, al massimo entro l'anno 2021.Al momento della pubblicazione sulla G.U. Europea il Regolamento diverrà operativo (dunque sarà applicabile), ma sarà concesso un periodo transitorio di due anni per adeguarsi.

Si precisa che il Regolamento e-Privacy si applicherà a tutte le comunicazioni elettroniche, non solo ai dati personali, e pertanto riguarderà non solo le persone fisiche, ma anche le persone giuridiche.

Riguardo ai cookie la proposta pervenuta durante la presidenza portoghese dell'Unione ha portato alcune soluzioni di compromesso, tra cui la possibilità di utilizzare cookie analitici di terze parti per la raccolta di statistiche di navigazione senza esplicito consenso da parte dell'utente. Anche relativamente al

c.d. “*cookie wall*” viene ammessa la possibilità di permettere l’accesso al sito solo concedendo l’installazione e l’utilizzo di cookie, ma sotto determinate condizioni: l’utente deve poter accedere a servizi equivalenti senza dover necessariamente concedere il consenso ai cookie, eventualmente pagando un compenso. Ma tale postilla è frutto di interpretazioni varie, per cui occorre attendere l’approvazione del Regolamento per saperne di più.

Il GPDP al momento non ha ancora concluso l’iter di consultazione ed approvazione delle nuove Linee Guida.