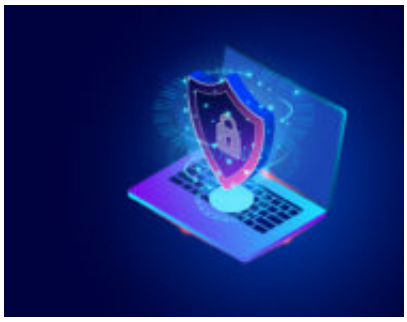
Globalizzazione e privacy: una difficile convivenza all'interno dei siti internet, soprattutto nella gestione dei cookie

Author : Alessandra Delli Ponti

Date : 13 Gennaio 2020



I principali provvedimenti UE del 2019 in tema di cookie e siti internet

Nel corso di quest'anno sono state molte le questioni e gli aspetti oggetto di chiarificazione sul Regolamento UE 2016/679 (**GDPR**) da parte delle autorità comunitarie, dei Garanti nazionali e della Corte di Giustizia.

Come garantire il corretto trattamento dati e il rispetto del GDPR nei siti internet soprattutto se collegati a pagine social e piattaforme? La corretta **gestione dei cookie** è uno dei principali problemi della gestione del dato nei siti web. L'origine del problema è che la tematica è disciplinata dalla direttiva e-privacy (direttiva comunitaria 2009/136/CE, che ha modificato la direttiva 2002/58/CE) che va però oggi armonizzata da quanto previsto nel GDPR, in attesa di un conseguente aggiornamento del testo legislativo[1].

Molte le pronunce sul tema siti web e cookie, sia sanzionatorie sia interpretative di una difficile materia.

Ecco, quindi, di seguito sintetizzate i **principali provvedimenti** emanati nel corso dell'anno, da cui risulta che il problema di validità del consenso e quello di stabilire la titolarità del trattamento sono i punti più delicati su cui occorre prestare molta attenzione.

Provvedimento del Garante Olandese 7 marzo 2019, Guida sull'utilizzo dei cookie nei siti web [2]

Il Garante Olandese si esprime nella guida in maniera netta rispetto ai "**cookie wall",** cioè di quei banner che informano l'utente dell'utilizzo dei cookie che consentono di accedere al contenuto del sito solo a seguito dell'accettazione in toto degli stessi.

Per il Garante, sono illegittimi: l'unico modo che hanno i fruitori del sito stesso per accedere ai contenuti della pagina web è quello di accettare i cookie in questione.

L'Autorità olandese ha motivato la propria posizione ritenendo che il cookie wall non permette di ottenere validamente il consenso degli utenti. Infatti, ai sensi dell'articolo 4, n. 11) del Regolamento (UE) 2016/679, il consenso dell'interessato si definisce come "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

Secondo l'Autorità il problema è il requisito della **"libertà del consenso"**, che sarebbe pregiudicato nel caso in cui all'interessato non fosse data la possibilità di rifiutare l'installazione dei cookie, in particolare quelli di profilazione, quantomeno senza incorrere in conseguenze negative, quali l'impossibilità di utilizzare il sito.

In altri termini: il gestore del sito, nel proporre il banner, deve effettuare una distinzione tra i cookie tecnici e quelli di profilazione, dando la possibilità di accedere ai contenuti anche a coloro che dovessero rifiutare i secondi.

La posizione del Garante Olandese, peraltro è in linea con l'approccio già adottato dall'Autorità per la protezione dei dati personali austriaca (decisione del 30 novembre 2018) dove è stato sanzionata la modalità di acquisizione del consenso al "cookie di marketing" che non era realmente volontario in conformità con i principi del GDPR[3]. Lo stesso approccio si ritrova nella sentenza del Consiglio di Stato francese il 6 giugno 2018[4], il quale ha ulteriormente precisato che i cookie che hanno finalità pubblicitaria non possono essere ritenuti "strettamente necessari", e quindi sono soggetti a consenso preventivo.

Sentenza della CGUE del 29 luglio 2019 (causa C-40/17) - Caso *Fashion ID* [5]

Il caso

L'associazione tedesca a tutela degli interessi dei consumatori, ha intentato causa contro Fashion ID, per avere quest'ultimo incorporato nel proprio sito web il plug-in "Mi piace" del social network Facebook, con conseguente trasmissione al server di Facebook di alcuni dati personali dei visitatori, a prescindere dalla loro interazione con tale plug-in. Per l'associazione ciò comportava una violazione della normativa sulla protezione dei dati.

In particolare, l'associazione dei consumatori ha contestato al gestore dell'e-commerce di agire quale titolare del trattamento nella raccolta e trasmissione di tali dati personali alla piattaforma social, senza fornire al visitatore preventiva idonea **informativa** e senza raccoglierne il **consenso**.

Dopo il primo grado è seguito il ricorso della Fashion ID durante il quale il Giudice Tedesco ha chiesto alla Corte di giustizia d'interpretare varie disposizioni della precedente direttiva del

1995 sulla protezione dei dati, applicabile alla causa nonostante l'entrata in vigore del GDPR.

Il Giudizio della Corte UE

Secondo la Corte **il proprietario di un sito web che incorpori un plug-in social, mantiene la titolarità del trattamento** rispetto ad alcune delle operazioni effettuate tramite plug-in: la raccolta e la trasmissione dei dati personali dei visitatori al social network, ciò anche in mancanza di un effettivo accesso ai dati trasmessi.

Infatti, unicamente in relazione a tali trattamenti (e non rispetto alle operazioni successive effettuate dal social network) si individuano in capo alla società autonome finalità di trattamento, in particolare, ad esempio, la scelta di utilizzare il plug-in, ottimizzare la pubblicità dei suoi prodotti rendendoli più visibili sul social e beneficiare del vantaggio commerciale che consiste nell'aumentare la pubblicità dei suoi beni.

Interessanti sono le considerazioni della Corte in relazione alla base giuridica.

Per quanto riguarda il caso in cui la persona interessata abbia manifestato il proprio consenso, la Corte decide che il gestore di un sito Internet come la Fashion ID è tenuto a ottenere tale consenso preventivamente (soltanto) per le operazioni di cui è (cor)responsabile, vale a dire la raccolta e la trasmissione.

Per quanto riguarda i casi in cui il trattamento dei dati sia necessario alla realizzazione di un interesse legittimo (art. 6 GDPR), la Corte decide che ciascuno dei cor(responsabili) del trattamento, vale a dire il gestore del sito Internet e il fornitore del plug-in social, deve perseguire, con la raccolta e la trasmissione dei dati personali, un interesse legittimo affinché tali operazioni siano giustificate per quanto lo riguarda, il tutto conforme a quanto

Sentenza della CGUE del 1 ottobre 2019 (causa C?673/17) - Caso Planet49 [6]

Il caso

La società Planet49 ha organizzato un gioco a premi sul sito Internet www.dein-macbook.de. Gli utenti di Internet che desideravano partecipare a detto gioco dovevano fornire il loro codice postale, il che li rinviava ad una pagina web in cui dovevano inserire il loro nome e il loro indirizzo. Al di sotto dei campi da riempire per l'indirizzo si trovavano due didascalie accompagnate da caselle di spunta. La prima didascalia, la cui rispettiva casella (in prosieguo: la «prima casella di spunta») non era preselezionata, recitava come segue:

«*Acconsento a ricevere informazioni per posta, per telefono, per posta elettronica o via SMS da sponsor e partner sulle offerte del loro rispettivo settore commerciale. È mia facoltà stabilire qui autonomamente i soggetti legittimati ad inviarmi dette offerte, in caso contrario la scelta spetta all'organizzatore. Posso revocare il consenso in qualsiasi momento. Ulteriori informazioni al riguardo si trovano qui*».

La seconda didascalia, la cui rispettiva casella (in prosieguo: «la seconda casella di spunta») era preselezionata, recitava come segue:

«*Acconsento a sottopormi al servizio di analisi web Remintrex. Di conseguenza, l'organizzatore del gioco a premi, [la Planet49], a seguito dell'approvazione della mia registrazione al gioco, installa cookie al fine di analizzare tramite Remintrex le mie navigazioni sul web e le mie visite ai siti Internet dei partner commerciali e di inviarmi pubblicità centrata sui miei interessi. Posso cancellare i cookie in ogni momento. Per ulteriori dettagli si legga qui*».

Era possibile partecipare al gioco a premi solo dopo aver selezionato quanto meno la prima casella di spunta.

Il caso viene esaminato dalla Corte federale di giustizia tedesca (Bundesgerichtshof) che sottopone alla Corte di giustizia europea di chiarire se, alla luce del diritto UE, il consenso all'istallazione di cookie possa essere validamente ottenuto nei modi sopra descritti, e quali informazioni debbano essere fornite all'utente riguardo all'uso dei cookie affinché si possa ritenere che il consenso espresso sia "informato".

Il giudizio della Corte UE

La definizione di "consenso" attualmente fornita dall'articolo 4(11) del GDPR specifica che, oltre a dover essere libero, specifico ed informato, il consenso debba tradursi in una manifestazione di volontà "inequivocabile" dell'interessato, con la quale lo stesso manifesta il proprio assenso a che i dati personali che lo riguardano siano oggetto di trattamento.

Tali definizioni di consenso si applicano anche ai fini della Direttiva ePrivacy.

Secondo la Corte Ue, in particolare il consenso dev'essere **manifestato in maniera attiva**.

A tal proposito, non è da considerarsi valido un consenso espresso mediante una dichiarazione preformulata che richieda all'utente di opporsi attivamente qualora non acconsentisse al trattamento dei dati.

Inoltre, la Corte ritiene che, al momento in cui gli viene richiesto di prestare il proprio consenso all'uso di cookie, l'utente debba essere informato, tra le altre cose, sulla durata dei cookie, nonché sul fatto che taluni terzi abbiano accesso o meno ai cookie stessi.

Le ultime recenti pronunce sui cookie dell'Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos (di seguito, "AEPD") ha emesso due provvedimenti sanzionatori in materia di Cookie.

1. Il Caso Vueling[7] con una multa pari a 30.000 euro (riducibile a 18.000 euro in caso di pagamento immediato in un'unica soluzione) per non aver dato agli utenti del proprio

sito web la possibilità di gestire le proprie preferenze sulle tipologie di cookie installati, ovvero di opporsi al relativo utilizzo. In particolare, il banner cookie sanzionato specifica che l'utente può accettare l'utilizzo dei cookie tecnici e di profilazione acconsentendovi espressamente, ovvero continuando nella navigazione. Sul lato destro del banner un unico button con il quale viene fornita all'utente la sola opzione di accettare i cookie, mentre non vi è alcuna menzione circa la possibilità di opporsi.
Tale banner, uguale a quello della maggior parte dei siti italiani, non va bene.
Il Garante privacy spagnolo, in particolare, ha rilevato che la compagnia aerea dovrebbe dotarsi di un sistema di gestione o un pannello di configurazione dei cookie che permetta all'utente non solo di accettarne/rifiutarne l'utilizzo, bensì anche di scegliere la tipologia di cookie che desidera vengano installati sul proprio dispositivo, manifestando in tal modo un consenso "granulare", finalizzato alla gestione delle proprie preferenze.

2. Recentemente, infine, l'Agenzia Spagnola ha imposto una sanzione di 10.000 euro a Ikea Spagna per violazioni sui cookie. Infatti, in seguito a un reclamo, l'Autorità ha scoperto che ogni volta che un utente accedeva al sito, venivano scaricati in automatico 23 cookie, per i quali non veniva richiesto il consenso dell'utente[8].

Note

[1] Sul tema interessante è quanto previsto da *"Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities"* dell'European Data Protection Board https://edpb.europa.eu/our-work-tools/our-documents/stanovisko-vyboru-cl-64/opinion-52019-interplay-between-eprivacy_it. L'Opinione – stimolata da una richiesta dell'Autorità belga – cerca di stabilire quando un trattamento di dati ricada sia sotto l'ambito applicativo del GDPR sia sotto quello della Direttiva ePrivacy.
L'EDPB ritiene che le autorità sono competenti per far rispettare il GDPR. Il semplice fatto che un sottoinsieme del trattamento rientri nell'ambito della direttiva ePrivacy, non limita la competenza delle autorità di protezione dei dati ai sensi del GDPR.
Una violazione del GDPR può allo stesso tempo costituire una violazione delle regole nazionali di ePrivacy e le autorità nazionali possono tenerne conto nell'applicare il GDPR (ad esempio, quando valutano la conformità ai principi di legalità o correttezza).

[2] https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies

[3] https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00.html

[4] http://www.conseil-etat.fr/fr/arianeweb/CE/decision/2018-06-06/412589

[5] http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=7768314

[6] http://curia.europa.eu/juris/document/document.jsf?text&docid=218462&pageIndex=0&doclang=IT&mode=req&dir&occ=first&part=1&cid=1996312

[7] https://www.aepd.es/resoluciones/PS-00300-2019_ORI.pdf?utm_source=POLITICO.EU&utm_campaign=fc1f5e664f-EMAIL_CAMPAIGN_2019_10_17_04_52&utm_medium=email&utm_term=0_10959edeb5-fc1f5e664f-190359285

[8] https://www.aepd.es/resoluciones/PS-00127-2019_ORI.pdf?fbclid=IwAR2mblxGgPuevoeVPD598tpwjSgR9Gc9CPocpeoaj4w-bRGWm0ROs9EpwyM

Articolo a cura di **Alessandra Delli Ponti**