Cookie di Google Analytics: le nuove precisazioni, anche su GA4, del Garante danese

Il Garante danese risponde ai dubbi sull'utilizzo del GA4

Il garante privacy danese ha fornito utili indicazioni in forma di FAQ sull'uso di Google Analytics che fanno luce su coni d'ombra delle pronunce di altre autorità, compresa quella nostrana del Garante. Analizziamole nel dettaglio

Molte Ennesima puntata della diatriba europea (ormai un quasi-divieto) sull'uso dei cookie di Google Analytics: lo scorso 21 settembre è intervenuto il Datatilsynet, l'autorità di controllo privacy danese. Questa volta non si tratta di un provvedimento giudiziario o sanzionatorio, bensì di un'analisi e un supporto informativo autorevoli.

Indicazioni in forma di FAQ che, sebbene fornite da un'autorità estera, fanno luce su coni d'ombra delle pronunce di altre autorità, compresa quella nostrana del Garante.

I provvedimenti delle autorità in Italia, Austria e Francia

Possiamo solo accennare ai temi coinvolti, rimandando ad altre sedi per approfondimenti. Il "caso" è quello dell'utilizzo dei cookie di marca Google Analytics, per la precisione nella versione 3 (detta "Universal Analytics"). Strumenti fondamentali per l'analisi statistica e di mercato della "vita" di un sito web, potendo fornire dettagli altrimenti preclusi sull'andamento di utilizzo del sito web e così contribuire alle decisioni d'impresa.

Lo strumento in questione però, nella versione fornita da Google, comporta l'utilizzo di dati personali degli utenti, in varia misura. Se e come ciò possa comportare violazione dei diritti degli interessati, del GDPR, è il nodo affrontato dalle varie autorità coinvolte nell'analisi. Specie dopo che sono stati presentati reclami in tutta l'UE, soprattutto da parte della NOYB dell'attivista Max Schrems, incentrati sulla trasmissione illecita di dati personali a un fornitore come Google.

La quale, sentenza Schrems II alla mano, non pare poter garantire il rispetto dell'adeguatezza di trattamento dei dati imposta dal GDPR. In astratto sono possibili misure supplementari, tecniche-organizzative-contrattuali, per temperare i rischi di accesso USA ai dati ma l'approccio corrente delle autorità si è spostato su un'applicazione binaria, per principi, non già per valutazione di rischio.

Dai reclami si è giunti, finora, a tre pronunce di autorità di controllo sparse nell'UE, in casi concreti, dirette a titolari utilizzatori dello strumento cookie: anzitutto in Austria nel gennaio scorso, proprio ove ha sede NOYB, con la prima condanna per l'uso di Analytics da parte di una società locale.

Poi in Francia la seconda, a opera della CNIL in febbraio. Ha ribadito la violazione in un caso analogo, dando un tempo di grazie per adeguarsi al titolare, pena l'irrogazione di sanzioni. La CNIL ha pubblicato parimenti pagine informative che "smontano" soluzioni

tecniche come proxy server, visto che si ammettono solo alla luce di numerose restrizioni tecniche. Un titolare che riuscisse ad applicarle tutte, probabilmente, non avrebbe più dati utili come output d'analisi, svuotando di senso l'uso degli Analytics.

È stato il turno dell'Italia e del Garante nostrano, con il discusso provvedimento di giugno e che, seguendo il ragionamento e l'approccio francese, ha optato per un ammonimento e tre mesi concessi al titolare per mettersi in regola (termine scaduto il 9 settembre scorso).

Oltre a pubblici proclami per estendere tale monito a tutti i titolari, seppure in maniera ambigua. Tacciamo qui del correlato intervento "minatorio" e massivo di Federico Leva, pure questo oggetto di mille discussioni.

I dubbi sul se e come mettersi in regola, alla luce di un approccio paneuropeo auspicabilmente omogeneo (debitore dei principi di coerenza e armonia interna dell'Unione, imposti dal Regolamento nel proprio territorio), sono fioccati. Si erano moltiplicate le indicazioni da varie fonti, anche in veste di FAQ, su cosa vi fosse di certo e cosa di incerto nella situazione attuale. Per fornire una direzione strategica alle imprese che devono ripensare e riadattare le proprie analisi web a questa interdizione, magari in tempi brevi, sebbene di tali criticità si sapesse da tempo.

E a proposito di FAQ, in tale veste si innesta l'intervento puntuale dell'autorità danese. La quale non prende spunto da un proprio intervento sanzionatorio (almeno per quanto noto finora), bensì da un'evidente necessità di replicare a numerose istanze degli operatori locali e non.

A supporto, di fatto, di tutti gli operatori dell'UE, posti i principi sopra detti circa la necessaria armonia di approccio tra autorità di controllo.

È possibile così fruire dell'analisi dettagliata dell'autorità per dirimere, con un punto di vista autorevole, vari dubbi tuttora persistenti su vari frangenti. Quale avviso ai naviganti, che dovrebbero far tesoro di queste indicazioni, danesi (destinatari formali), italiani o europei in genere che siano.

Premesse e dichiarazioni ufficiali

Le FAQ nascono dall'analisi compiuta da Datatilsynet, confrontandosi con le predette pronunce europee, con la citata, dovuta omogeneità (e il suo portato nella certezza del diritto) nel territorio unionale.

Nel comunicato stampa, Makar Juhl Holst (consulente capo dell'autorità danese per la protezione dei dati) afferma che "le regole del GDPR sono progettate per proteggere la privacy dei cittadini europei.

Ciò significa, tra le altre cose, che devi essere in grado di visitare un sito web senza che le tue informazioni finiscano nelle mani sbagliate. Abbiamo esaminato attentamente le opzioni di Google

Analytics e siamo giunti alla conclusione che non è possibile utilizzare lo strumento nella sua forma attuale senza adottare misure aggiuntive".

Non solo: "sin dalle decisioni dei nostri colleghi europei, abbiamo esaminato più da vicino lo strumento e le impostazioni specifiche che puoi utilizzare se desideri utilizzare Google Analytics.

È stato particolarmente rilevante poiché, sulla scia della prima decisione dell'Austria, Google ha iniziato a rendere disponibili impostazioni aggiuntive in relazione a quali informazioni possono essere raccolte tramite lo strumento. Tuttavia, la conclusione è ancora che lo strumento non può essere utilizzato legalmente".

Sulla coerenza territoriale, il comunicato stampa aggiunge che "un atteggiamento paneuropeo tra le autorità di vigilanza significa, tra l'altro, anche che, in un caso concreto con circostanze simili, l'autorità di controllo per la protezione dei dati personali raggiungerà lo stesso risultato dei nostri colleghi europei". E che "Google ha indicato di aver implementato ulteriori misure contrattuali, organizzative e tecniche. Tuttavia, le autorità di controllo hanno ritenuto che tali misure non potessero garantire un livello efficace di protezione dei dati trasferiti in quanto le misure non erano idonee a impedire l'accesso ai dati personali trasferiti da parte delle autorità statunitensi".

Allo stesso tempo, si vuole precisare che l'approccio delle autorità è improntato ad essere "neutrali dal punto di vista tecnologico e pertanto non [hanno] alcun interesse [...] a vietare determinati prodotti".

La conclusione è la solita: se non è possibile adottare misure supplementari efficaci, è necessario interromperne l'utilizzo ed eventualmente trovare un altro strumento in grado di fornire statistiche web e che consenta di rispettare le norme sulla protezione dei dati.

Google Analytics: le FAQ dell'autorità danese

Si tratta ora di esaminare i punti fondamentali del Q&A specifico, le risposte che dovrebbero fugare molte "soluzioni di comodo" propinate ultimamente da varie fonti, senza che vi siano certezze sulla loro "tenuta" giuridica.

1. **Configurare Google per evitare il trasferimento dati negli USA**: qui Datatilsynet riprende la passata dichiarazione della stessa Google circa il fatto che i dati raccolti tramite Analytics vengono elaborati e archiviati negli Stati Uniti. L'autorità danese ammette di non essere a conoscenza di eventuali modifiche all'impostazione tecnica di Google, dopo le precedenti decisioni delle autorità europee, che permetta l'uso di Google Analytics senza alcun trasferimento di dati personali negli Stati Uniti. Per ulteriore chiarezza su questo argomento, l'autorità invita a contattare la stessa Google per approfondimenti. Ergo: non si esclude la possibilità di attuare misure idonee a evitare il

trasferimento dei dati, tuttavia non pare si riesca a comprendere come si possa fare, al momento.

2. **Configurare Google per evitare il trattamento di dati personali**: Analytics funziona assegnando un identificatore univoco al visitatore del sito web, inoltre vengono raccolti e abbinati (meta)dati aggiuntivi come data e ora di accesso, dati sul browser, ecc. Lo strumento ha due opzioni di condivisione dei dati, cioè "Data sharing" per la condivisione dei dati con Google e "Google Signals" che permette a Google di raccogliere dati aggiuntivi per fini di marketing. È vero che il titolare, oggi, può disattivare queste due opzioni di trattamento condiviso, almeno nell'ultima versione Analytics 4 (detto anche "GA4"). Tuttavia ciò non impedisce l'uso dell'identificatore e dei (meta)dati. Il fatto che il dato permetta non tanto un'identificazione precisa, con tanto di nome e cognome, ma sia sufficiente a effettuare un "singling-out" cioè a discernere un individuo presente in un gruppo [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf], è idoneo a configurarsi come un dato personale.

3. **Analytics, configurato senza l'uso di dati personali, è lecito**: in teoria è corretto, non vi è un divieto sull'uso di Google Analytics in sé, non rientra nei compiti dell'autorità vietare determinati prodotti o servizi. Si tratta "solo" di valutare la liceità nel loro utilizzo, del coinvolgimento dei dati personali nel flusso operativo. Nondimeno, come detto, sembra piuttosto arduo rendere non personali i dati utilizzati con questo strumento. Nel caso si ritenesse di riuscire a farlo, l'autorità raccomanda di documentare tutto con dovizia, in ossequio al principio di accountability del GDPR e di una valutazione del rischio quale onere continuativo del titolare.

4. **La pseudonimizzazione dei dati personali**: l'uso di tecniche di pseudonimizzazione, ricordiamolo, non rende i dati "non personali" di per sé, al contrario. I dati pseudonimizzati non possono essere attribuiti a una persona fisica senza l'uso di informazioni aggiuntive. Quindi l'analisi sulla pseudonimizzazione deve tener conto, in particolare, delle informazioni supplementari (ad es. gli indirizzi IP) che le autorità pubbliche del paese terzo interessato possono essere tenute a possedere e utilizzare per attribuire i dati pseudonimizzati, così, a una persona fisica. La c.d. "anonimizzazione" (in realtà, pseudonimizzazione) dell'IP dichiarata da Google sui dati utente, non è affatto chiara quanto agli step del processo se avvenga prima o dopo il trasferimento negli USA. Secondo l'analisi dell'autorità, è possibile che avvenga dopo il trasferimento, configurando la violazione. Circa GA4, l'autorità aggiunge che sebbene Google dichiari di usare l'IP solo per determinare la posizione approssimativa dell'utente e poi scartarlo, tecnicamente ciò comporta comunque una "chiamata" ai server USA per accertare tale posizione. Ciò comporta trattamento dei dati per vari motivi: è prevedibile che Google usi un firewall per

proteggere i propri server, il quale registrerà il traffico in entrata e i dati annessi, dal quale è possibile ricavare, tra l'altro, gli IP degli utenti. Inoltre, sul piano legale, è possibile che le autorità di Paesi terzi possano ottenere, con l'ausilio della polizia e dei provider di connettività, i dati aggiuntivi per identificare la persona connessa ai dati raccolti. Ergo: questa pseudonimizzazione non è efficace, in tal caso, per il rispetto del GDPR.

5. **Misure supplementari efficaci**: si richiamano le raccomandazioni dell'EDPB n. 1/2020 sulle misure da applicare per i trasferimenti extra-UE/SEE. Ovviamente si richiamano quelle tecniche, le uniche a poter reggere: anzitutto la predetta pseudonimizzazione (per cui si rimanda espressamente alle difficili prescrizioni tecniche di configurazione di Analytics già rese note dalla CNIL). Si menziona in seguito la cifratura, ricordando che nondimeno "le chiavi di crittografia devono essere detenute esclusivamente dall'esportatore di dati o da un terzo all'interno dell'UE/SEE o in un paese terzo sicuro". Nel caso di Google, è essa stessa a detenere e applicare le chiavi ai dati, con relativo accesso in chiaro, vanificandone l'efficacia lato GDPR.

6. **L'approccio basato sul rischio e sul possibile accesso da parte delle autorità governative USA**: come già affermato dalle altre autorità menzionate, si riafferma – seppure sia un esito molto criticato e discusso – che le operazioni di trasferimento/accesso di dati personali verso Paesi terzi non sono soggette a valutazioni di rischio, dunque di "probabilità" (in particolare, sul fatto che effettivamente le autorità USA possano effettivamente accedere ai dati e cosa possano desumerne). Si tratta, invece, di mera "possibilità": ciò è sufficiente per sancire la violazione dei principi del GDPR. E ciò sebbene molte delle altre prescrizioni del GDPR, al contrario, assumano un approccio improntato alla probabilità.

7. **L'uso del consenso dell'utente per sanare il trattamento**: il consenso ex art. 49.1.a GDPR, per i trasferimenti dei dati extra-UE/SEE, è ammissibile ma solo a fronte di adeguata informazione sui rischi connessi e – comunque sia – solo per trasferimenti occasionali. L'autorità si limita a riformulare il dettato normativo, è logico che non possa applicarsi a trattamenti generalizzati come quelli dei cookie in parola.

8. **Google dichiara di non aver mai ricevuto richieste dalle autorità statunitensi per l'accesso ai dati raccolti tramite Analytics**: dopo il provvedimento austriaco, Google ha precisato che nei 15 anni d'uso degli Analytics non ha mai ricevuto una richiesta di divulgazione dei connessi dati personali da parte delle autorità americane. L'autorità, richiamando le indicazioni dell'EDPB oltre alle proprie linee guida sull'uso dei cloud, pone dei limiti precisi in questo caso: ogni dichiarazione del fornitore ("importatore" dei dati) deve ricevere supporto, in regime di piena accountability, in informazioni obiettive, affidabili e accessibili.

Non pare sia il caso di Google per Analytics, basato solo sulle affermazioni della società USA.

9. **Un periodo di "grazia" per rendere lecito il trattamento**: l'autorità danese afferma che nel proprio Paese non saranno applicati ammonimenti, in genere, con un periodo per rimettersi in regola. Quindi presumibilmente provvederà a sanzionare subitamente ogni caso accertato, in generale. Sebbene affermi ugualmente di tenere in conto eventuali sforzi di compliance "in progress" da parte dei titolari. Ribadiamo che, al momento, l'unico provvedimento noto del Garante italiano in merito ha prescritto tre mesi al soggetto colpito nel caso concreto, per ricondursi alla liceità, e che si attende generalmente da tutti i titolari la dovuta di compliance, sempre a partire da settembre. Non è affatto detto che conceda altri ammonimenti con periodi per rimediare, invece di sanzionare da subito.
10. **Nuovo accordo USA-UE per trasferire i dati e garantire l'adeguatezza richiesta dal GDPR**: si è tutti in attesa dell'accordo politico formale che vada a sostituire il defunto Privacy Shield, già annunciato dal marzo scorso. L'autorità prevede un lungo iter ma non può prevedere date possibili per averne la versione approvata e vigente. Tuttora manca una bozza formale di accordo, nota al pubblico. Pertanto non è un orizzonte su cui fare affidamento, nel breve-medio termine.

Fonte: Cybersecurity360.it