queste istituzioni

L'utilizzo di *Google Analytics* viola il GDPR? La decisione del Garante austriaco e il trasferimento dei dati personali verso gli USA

Maria Lilia La Porta
Arianna Micci
Luca Tufarelli

Numero 2/2022
30 giugno 2022

L'utilizzo di *Google Analytics* viola il GDPR? La decisione del Garante austriaco e il trasferimento dei dati personali verso gli USA

Maria Lilia La Porta[*], Arianna Micci[•], Luca Tufarelli[#]

Sommario

Sintesi

L'Autorità garante per la protezione dei dati personali austriaca ha stabilito che l'utilizzo di Google Analytics da parte di provider di siti web non è conforme alla disciplina europea in materia di protezione dei dati personali. Secondo il Garante austriaco, i siti web che utilizzano Google Analytics trasferirebbero "illegittimamente" i dati così raccolti (quali gli indirizzi IP e gli identificatori univoci memorizzati nei cookie) negli Stati Uniti, violando il Regolamento (UE) n. 2016/679 ("GDPR") alla luce della sentenza "*Schrems* II". Il Garante austriaco è stata la prima Autorità a pronunciarsi in merito ai 101 reclami presentati dalla ONG a tutela dei diritti digitali Noyb a varie *Data Protection Authorities* ("DPA") europee per contestare il trasferimento di dati personali.

Abstract

The Austrian Authority for the protection of personal data has established that the use of Google Analytics by website providers does not comply with the European regulations about the protection of personal data. According to the Austrian Authority, the websites that use Google Analytics would "illegitimately" transfer the data collected (such as IP addresses and unique identifiers stored in cookies) to the United States, violating Regulation (EU) no. 2016/679 ("GDPR") according to "Schrems II". The Austrian Authority is the first Authority to rule on the 101 complaints presented by the NGO for the protection of digital rights Noyb to various European Data Protection Authorities ("DPA") to contest the transfer of personal data.

[*] Avvocato, Foro di Roma.
[•] Dottoressa in Giurisprudenza.
[#] Avvocato, Foro di Roma.

Parole chiave
Privacy; Garante protezione dati personali; Autorità indipendenti; Data Protection Authority.

1. Premessa.

L'Autorità garante per la protezione dei dati personali austriaca ("*Datenschutzbehörde*" o anche "DSB"), con decisione D155.027 GA del 22 dicembre 2021[1], ha stabilito che l'utilizzo di Google Analytics da parte di provider di siti web non è conforme alla disciplina europea in materia di protezione dei dati personali.

Google Analytics è un servizio di analisi web fornito dalla società americana Google LLC ("Google") utilizzato da aziende, istituzioni pubbliche e ONG per analizzare il comportamento dei visitatori delle loro pagine web o applicazioni. Ciò avviene attraverso la creazione di vari tipi di statistiche sulla base delle informazioni raccolte dai *cookie analytics* (quali, ad esempio,la localizzazione approssimativa degli utenti, la durata della sessione, il numero di pagine visitate e le caratteristiche del *device*) nell'ambito della navigazione online[2].

Secondo il Garante austriaco, i siti web che utilizzano Google Analytics trasferirebbero "illegittimamente" i dati così raccolti (quali gli indirizzi IP e gli identificatori univoci memorizzati nei cookie) negli Stati Uniti, violando il Regolamento (UE) n. 2016/679 ("GDPR") alla luce della sentenza "*Schrems* II"[3].

Il Garante austriaco è stata la prima Autorità a pronunciarsi in merito ai 101 reclami ("*101 US Transfer complaints*") presentati dalla ONG a tutela dei diritti digitali Noyb[4] a varie *Data Protection Authorities* ("DPA") europee per contestare il trasferimento di dati personali dall'Europa a società con sede negli Stati Uniti (quali, principalmente, Facebook e Google). I reclami sono stati presentati a seguito della invalidazione da parte della Corte di giustizia dell'Unione europea ("GGUE"), con la nota sentenza "*Schrems* II", dell'accordo che regolava i trasferimenti di dati verso gli U.S.A.(il c.d. "*Privacy Shield*") a causa dell'incompatibilità della legislazione statunitense con il diritto alla protezione dei dati personali così come delineato nell'ambito dell'Unione europea.

Tale decisione, cui hanno fatto seguito pronunce di altre autorità garanti europee, potrebbe avere conseguenze significative nei confronti dei gestori di siti web che operano

[1] https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2021-0.586.257_(D155.027).

[2] L'Autorità Garante per la protezione dei dati ha definito i *cookie analytics* quali «strumenti che possono anche essere utilizzati, tra l'altro, per valutare l'efficacia di un servizio della società dell'informazione fornito da un publisher, per la progettazione di un sito web o per contribuire a misurarne il "traffico", cioè il numero di visitatori anche eventualmente ripartiti per area geografica, fascia oraria della connessione o altre caratteristiche». Cfr. Linee guida cookie e altri strumenti di tracciamento – 10 giugno 2021 [doc. web n. 9677876].

[3] Sentenza della Corte di Giustizia europea del 16 luglio 2020, *https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:62018CJ0311.*

[4] https://noyb.eu/it/esercitate-i-vostri-diritti.

nell'Unione europea. L'orientamento prevalente, infatti, sembra tendere verso una forte limitazione (se non addirittura un divieto generale) dell'utilizzo, oltre che di Google Analytics, di tutti i servizi forniti dalle *big tech* statunitensi, ove comportino un trattamento di dati personali e implicitamente un trasferimento dei dati extra UE.

Ci si deve allora chiedere se e in che misura sia possibile per i soggetti operanti nell'Unione europea continuare a ricorrere ai principali strumenti e servizi digitali statunitensi che, se da un lato assicurano prestazioni migliori e servizi leader a livello mondiale, dall'altro potrebbero non garantire la tutela dei dati personali prevista dal GDPR.

2. Contesto normativo e giurisprudenziale di riferimento.

Il GDPR disciplina al Capo V il trasferimento di dati personali verso un paese terzo (ossia in Paesi extra SEE - Spazio Economico Europeo) o una organizzazione internazionale, prevedendo una serie di misure volte ad assicurare un livello di protezione delle persone fisiche sostanzialmente equivalente a quello garantito dal diritto dell'Unione europea. Il trasferimento all'estero può, alla luce di tali previsioni, considerarsi legittimo solo ove: i) sia supportato da una decisione di adeguatezza (art. 45 GDPR) o, in mancanza, ii) sia soggetto a garanzie adeguate (art. 46 GDPR), quali, ad esempio, le clausole tipo di protezione dei dati adottate dalla Commissione europea ("Standard ContractualClauses– SCC")[5].

Con specifico riferimento ai trasferimenti di dati personali verso gli U.S.A., decisiva è stata la sentenza "*Schrems* II", che ha invalidato la pronuncia di adeguatezza adottata dalla Commissione europea nel 2016 in ragione dell'incompatibilità della legislazione statunitense con il diritto fondamentale alla protezione dei dati personali europeo. Infatti, in base alla legge federale "*Clarifying Lawful Overseas Use of Data Act*" o "*CloudAct*", i fornitori di servizi di comunicazione elettronica statunitensi hanno l'obbligo di esibire (*disclosure*) alle forze dell'ordine e di *intelligence* i dati personali di cui abbiano il possesso, il controllo o la custodia, a prescindere da dove siano localizzati tali dati.

La Corte ha ritenuto che neppure le clausole contrattuali tipo ("SCC") fossero in grado di garantire la sicurezza del trasferimento dei dati personali verso gli Stati Uniti, non essendo opponibili alle Autorità statunitensi. La Commissione ha perciò proposto alcuni emendamenti integrativi delle SCC, quali l'adozione di misure tecniche e organizzative supplementari e la garanzia da parte del fornitore statunitense di non mettere a disposizione delle Autorità governative locali i dati trattati.

[5] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=it&uri=CELEX:32021D0914.

La pronuncia del Garante Austriaco ha posto invece in discussione la portata risolutiva di questo intervento, ritenendo tali emendamenti inidonei a garantire l'effettiva protezione dei dati personali trasferiti verso gli U.S.A.

Pertanto, alla luce del contesto descritto, sembrerebbe che nessuno degli strumenti di garanzia offerti dal GDPR possa attualmente legittimare il trasferimento dei dati verso gli Stati Uniti.

3. La decisione del Garante Austriaco.

Il reclamo al DSB aveva ad oggetto l'illegittimo trasferimento di dati personali negli Stati Uniti da parte del fornitore di un sito web austriaco, che utilizzava il servizio Google Analytics.

In particolare, il reclamante sosteneva di aver visitato il sito web mentre era "*loggato*" al suo account Google, collegato all'indirizzo e-mail personale. Nel corso della visita il fornitore del sito web, attraverso lo strumento Google Analytics, avrebbe elaborato e trasmesso negli Stati Uniti taluni dati personali, quali almeno l'indirizzo IP e i dati dei cookie.

Secondo il reclamante, il trasferimento dei dati si sarebbe dovuto considerare illegittimo in quanto le SCC, stipulate tra il provider del sito web (in qualità di Titolare del trattamento) e Google (in qualità di Responsabile), non offrirebbero un adeguato livello di protezione dei dati personali, così come richiesto dal GDPR, in ragione del fatto che:

a) Qualificandosi Google come "fornitore di servizi di comunicazione elettronica" ai sensi del 50 US Code §1881(b)(4), esso è soggetto a sorveglianza da parte dei servizi di *intelligence* statunitensi e può essere obbligato a esibire loro i dati dei cittadini europei;

b) le misure supplementari adottate e gli emendamenti alle SCC non riducono le possibilità di monitoraggio e accesso da parte dei servizi di *intelligence* statunitensi.

Nell'esaminare il reclamo, il Garante austriaco ha in primo luogo risolto positivamente la questione relativa alla qualificabilità dei dati raccolti tramite il servizio di Google Analytics come dati personali ai sensi dell'art. 4, par. 1 del GDPR (ossia "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*"). Google, nell'ambito della propria difesa, sosteneva infatti che l'anonimizzazione dei dati raccolti mediante mascheramento dell'indirizzo IP non rendesse possibile l'identificazione degli utenti e, dunque, non vi fosse trasferimento di dati personali.

Il Garante ha disatteso la tesi difensiva sulla base di un duplice ordine di considerazioni. Anzitutto, ha rilevato che l'anonimizzazione non era stata correttamente implementata a causa di un errore tecnico. In secondo luogo, ha osservato che l'anonimizzazione, quand'anche correttamente posta in essere, avrebbe comunque consentito di identificare l'utente attraverso i cookie installati sul suo dispositivo nell'ambito della navigazione sul sito web. Infatti, a parere del Garante austriaco, i numeri identificativi contenuti nei cookie sono in ogni caso da

considerarsi dati personali, in ragione del fatto che, ove abbinati con altri dati (quali l'indirizzo IP, informazioni sul browser e sul sistema operativo, risoluzione dello schermo, ecc.) permettono la ricostruzione di un "*digital footprint*" associabile all'utente che visita un sito web che utilizza Google Analytics.

Il problema dell'identificabilità dell'utente si è posto non solo nei confronti di Google, ma anche e soprattutto con riferimento alle autorità di *intelligence* statunitensi che, grazie al ricorso a determinati identificatori online (quali, ad esempio, indirizzo IP o numeri di identificazione univoci), combinati con altre informazioni potenzialmente già raccolte, potrebbero essere in grado di identificare l'interessato.

Il Garante austriaco ha poi proseguito nella propria indagine ribadendo, sulla base delle considerazioni già espresse dalla CGUE, che il trasferimento dei dati non può basarsi esclusivamente sulle SCC, ma richiede l'adozione di misure integrative che forniscano un livello di protezione adeguato ai sensi degli artt. 44 e ss. GDPR.

Tuttavia, le misure integrative implementate da Google nel caso concreto – quali la crittografia e la pseudonimizzazione – sono state valutate insufficienti dal Garante austriaco. Con particolare riferimento alle tecniche di crittografia, il DSB ha rilevato che esse non possono in ogni caso impedire ai servizi di *intelligence* statunitensi di accedere ai dati personali dell'utente, in quanto l'obbligo di *disclosure* previsto dal *Cloud Act* si estende alle chiavi crittografiche, che ne consentono la lettura.

Di conseguenza, a parere del DSB, Google non ha assicurato un adeguato livello di protezione per il trasferimento dei dati negli Stati Uniti, in violazione dell'art. 44 GDPR.

Di rilievo è che la violazione sia stata imputata esclusivamente al gestore del sito web e non anche a Google, in quanto mero "destinatario" dei dati. Tuttavia, anche nei riguardi del *provider* del sito, l'Autorità non ha irrogato alcuna sanzione, limitandosi a ordinare l'interruzione del trasferimento dei dati verso gli Stati Uniti tramite l'utilizzo di Google Analytics.

Quanto a Google, il Garante austriaco si è riservato di approfondire in un procedimento separato il corretto adempimento dei suoi obblighi di Responsabile del trattamento e in particolare, quello di trattare i dati personali su istruzioni documentate del Titolare del trattamento anche in relazione ai trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, come stabilito dall'articolo 28, paragrafo 3, lettera a) e dall'articolo 29 del GDPR.

Infine, in una pronuncia successiva a quella in esame, il DSB ha posto la sua attenzione sul concetto di "approccio basato sul rischio" – sostenuto in via difensiva da Google – quale principio in virtù del quale poter considerare lecito il trasferimento di dati negli Stati Uniti in

assenza di una decisione di adeguatezza,qualora sia possibile dimostrare che la probabilità per il governo di accedere ai dati personali trasferiti sulla base di garanzie aggiuntive sia minima.

Il Garante austriaco, non concordando con la tesi difensiva di Google, ha affermato che il capo V del GDPR non prevede un approccio basato sul rischio[6] e che la violazione dell'art. 44 GDPR si verifica ogni qualvolta i dati personali sono trasferiti in un paese terzo senza un livello di protezione adeguato (come gli Stati Uniti), a prescindere dall'esistenza o meno del rischio che i servizi di *intelligence* statunitensi possano effettivamente avere accesso a tali dati.

4. La posizione delle altre *Data Protection Authorities.*

La pronuncia del Garante austriaco ha sollevato non pochi interrogativi circa le sorti dell'utilizzo di *Google Analytics* e in generale dei servizi offerti dalle *big tech* statunitensi nell'ambito dell'Unione europea. Sicuramente molto dipenderà dalla strada che intraprenderanno le altre DPA nel decidere dei 101 reclami presentati da Noyb. Viene allora da domandarsi: la pronuncia del Garante austriaco può considerarsi un *leading case*?

Molte sono le circostanze che portano a ritenere che le varie autorità europee collaboreranno fra di loro. Prima fra tutte, la costituzione di una *task force* da parte dell'*European Data Protection Board* (EDPB) al fine non solo di far fronte al numero cospicuo di reclami presentati da Noyb, ma anche di fornire ai Titolari e i Responsabili del trattamento raccomandazioni sul corretto adempimento dell'obbligo di adozione di misure integrative che assicurino un livello di protezione adeguato nei trasferimenti di dati extra-UE.

In linea con il DSB si è espresso il Garante francese[7] ("*Commission nationale de l'informatique et des libertés*" e di seguito anche "CNIL") che, al fine di superare le criticità già riscontrate dall'autorità austriaca, ha esortato ad utilizzare servizi di misurazione e analisi dei visitatori dei siti *web* al solo fine di produrre dati statistici anonimi, così da rendere esente il Titolare del trattamento dal richiedere il consenso necessario. A tal fine, l'Autorità ha avviato un programma di valutazione per determinare quali soluzioni siano esenti da consenso.

Anche il Garante italiano, con un provvedimento di recente adozione[8], ha dichiarato l'illegittimità dell'utilizzo di Google Analytics da parte di siti *web* europei sulla base di considerazioni analoghe a quelle poste a fondamento della decisione del DSB. L'Autorità italiana, infatti, ha dapprima valutato la sussistenza del trasferimento, tramite Google Analytics,dei dati personali degli utenti del sito verso gli Stati Uniti e ne ha dichiarato poi l'illiceità alla luce della sentenza "*Schrems* II".

---

[6] Che invece è espressamente previsto dal legislatore in altri articoli del Regolamento, quali, in particolare, gli artt. 24 c. 1 e 2; art. 25 c. 1; art. 30 c. 5, art. 32 cc. 1 e 2, art. 34 c. 1, art. 35 cc. 1 e 3 e art. 37 par. 1 lett. b) e c).

[7] Provvedimento della CNIL del 10 febbraio 2022, https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply.

[8] Provvedimento n. 224 del 9 giugno 2022 [doc. web n. 9782890].

La pronuncia del Garante italiano, differentemente da quella del DSB, non si è limitata a valutare l'inidoneità della cifratura quale misura tecnica supplementare, ma ha altresì approfondito il tema delle misure contrattuali e organizzative adottate da Google. In particolare, tali misure (quali, ad esempio, l'impegno assunto da Google a non accogliere le richieste di accesso ai dati delle Autorità statunitensi che appaiano sproporzionate in base ai presupposti stabiliti dalla normativa di riferimento) quand'anche astrattamente idonee a circoscrivere il perimetro degli obblighi di *disclosure*, risultano nel concreto insufficienti ove non accompagnate, come nel caso esaminato, da misure tecniche efficaci.

Rileva, inoltre, l'adesione del Garante italiano all'orientamento del DSB secondo cui l'idoneità delle misure supplementari poste in essere dall'importatore dei dati non può basarsi su un "approccio basato sul rischio", ossia sulla probabilità di accesso da parte dell'*intelligence* ai dati personali. Piuttosto, essa deve basarsi su fattori oggettivi, quali la legislazione e la prassi del paese terzo verso il quale avviene il trasferimento.

Ad ogni modo, anche nel caso italiano il provider del sito web non ha ricevuto una sanzione ma soltanto una ammonizione. La fattispecie è stata infatti qualificata come violazione minore e al gestore è stato ordinato di adottare, entro novanta giorni, misure supplementari adeguate a garantire la sicurezza dei trasferimenti ai sensi del Capo V del GDPR, pena la sospensione dei flussi verso gli Stati Uniti dei dati raccolti tramite Google Analytics. La mancata irrogazione di una sanzione è stata motivata in ragione della asimmetria di potere contrattuale tra il provider e la posizione primaria di Google nel mercato dei servizi digitali, del carattere meramente colposo della violazione nonché dell'adozione da parte del gestore di ulteriori misure di sicurezza nel corso del procedimento[9].

La pronuncia del Garante nazionale non sarà certo l'ultima: in occasione dell'adozione del provvedimento in questione e alla luce delle varie segnalazioni pervenute, l'Autorità ha invitato tutti i gestori italiani di siti web di verificare la conformità dei cookie e degli altri strumenti di tracciamento da loro utilizzati con la normativa in materia di protezione dei dati personali.

Infine, anche il Garante europeo per la protezione dei dati (EDPS) ha adottato – sempre a seguito di un reclamo presentato da Noyb – una decisione avverso il Parlamento europeo[10], per aver riscontrato la presenza in un portale web relativo ai test anti-Covid di cookie appartenenti a Google Analytics e Stripe (altra società avente sede negli U.S.A.)[11].

---

[9] Quali, ad esempio, l'adesione all'opzione di "IP-Anonymization" messa a disposizione da Google; il miglioramento infrastrutturale in termini di sicurezza e l'analisi della fattibilità dell'implementazione di uno strumento alternativo di web analytics.

[10] https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf.

[11] L'EDPS si riferisce esplicitamente, nella nota 27 della decisione, al procedimento di fronte al Garante austriaco "*in merito all'uso di Google Analytics nell'ambito dei 101 reclami presentati da noyb sul trasferimento di dati negli Stati Uniti durante l'utilizzo di Google Analytics*".

Ad oggi, le uniche *Authorities* ad essersi pronunciate in senso contrario all'illegittimità dell'utilizzo di servizi digitali offerti da società aventi sede negli Stati Uniti sono il Garante spagnolo ("*Agencia Española de Protección de Datos*" o anche "AEPD") e quello lussemburghese ("*Commission nationale pour la protection des données*" o "CNPD"). L'AEPD ha respinto il reclamo proposto, in quanto il provider del sito web ha proceduto alla rimozione di Google Analytics dal sito web. Per la stessa motivazione, il CNPD ha respinto tre reclami riguardanti il trasferimento di dati ai server di Facebook negli Stati Uniti.

Non resta che attendere le decisioni delle altre *Data Protection Authorities* per comprendere il destino del mercato del *digital advertising*, il quale attualmente si fonda quasi completamente su servizi offerti da fornitori statunitensi. Tuttavia, a prescindere dalle posizioni dei vari Garanti europei, l'adozione di un accordo internazionale tra Unione Europea e Stati Uniti che sostituisca il vecchio *Privacy Shield* potrebbe definitivamente risolvere la questione.

5. Il *Trans-Atlantic Data Privacy Framework*.

Del resto, è proprio in questa direzione che sembrano muoversi gli attori istituzionali coinvolti. La Commissione europea e gli Stati Uniti stanno lavorando congiuntamente per il raggiungimento di un nuovo accordo per il trasferimento transatlantico dei dati: il *Trans-Atlantic Data Privacy Framework*.

Tale accordo, garantendo il livello di protezione previsto dalla legislazione europea, consentirà il flusso di dati che è alla base di oltre 1 trilione di dollari annui nel commercio transfrontaliero e permetterà alle aziende di tutte le dimensioni di competere nei rispettivi mercati.

Da quanto si legge nel comunicato stampa rilasciato dalla Commissione europea, per rendere legittimo il trasferimento di dati,gli Stati Uniti saranno tenuti a:

i) porre in essere misure per limitare l'accesso ai dati trasferiti negli U.S.A.da parte delle autorità di *intelligence* alle sole ipotesi in cui ciò sia necessario e proporzionato al perseguimento degli obiettivi di sicurezza nazionale;

ii) prevedere un meccanismo di ricorso a due livelli per rispondere ai reclami dei cittadini europei circa l'accesso ai dati da parte delle autorità di *intelligence* statunitensi, anche attraverso l'istituzione di una "*Data Protection Review Court*";

iii) imporre obblighi stringenti per le società che elaborano i dati trasferiti dall'Unione europea, che dovranno presentare una autocertificazione relativa alla propria adesione ai principi al *Department of Commerce*;

iv) adottare procedure per garantire un controllo efficace dei nuovi standard sulla *privacy*.

L'accordo sarà ora tradotto in atti giuridici. Gli impegni degli Stati Uniti saranno inclusi in un *Executive Order,* che costituirà la base della decisione di adeguatezza della Commissione, per mettere in atto il nuovo *Trans-Atlantic Data Privacy Framework*.

6. Conclusioni.

In attesa del *Trans-Atlantic Data Privacy Framework* rimane da comprendere come comportarsi e che misure adottare con riferimento ai servizi forniti da società americane e normalmente utilizzati da società private e enti pubblici di tutta Europa.

Lo stesso Presidente dell'EDPB ha dichiarato che «*le implicazioni della sentenza [Schrems II] sono di ampia portata e i contesti dei trasferimenti di dati verso paesi terzi molto diversi. Pertanto, non può esserci una soluzione valida per tutti e rapida. Ogni organizzazione dovrà valutare le proprie operazioni di trattamento dei dati e trasferimenti e adottare le misure appropriate*»[12].

Nonostante i principali fornitori di servizi con sede in U.S.A.-quali, ad esempio, Google e Facebook- abbiano costituito una sede o si siano dotati di *server* nello Spazio Economico Europeo, anche al fine di sottrarsi agli effetti della sentenza *Schrems* II, ciò non sembrerebbe configurarsi quale soluzione applicabile e definitiva. Infatti, gli obblighi di *disclosure* previsti dal *CloudAct* trovano applicazione i) a prescindere dalla localizzazione dei *server* e ii) nei confronti di soggetti sottoposti alla giurisdizione U.S.A., e dunque, anche nei confronti delle controllate europee di società aventi sede negli Stati Uniti.

Attualmente, in attesa del *Trans-Atlantic Data Privacy Framework*, una possibile soluzione idonea a garantire la sicurezza e la protezione del trasferimento dei dati all'estero è stata individuata da Amazon Web Services S.a.r.l. (avente sede in Europa, ma controllata dalla statunitense Amazon). Nell'ambito di un procedimento che la vedeva protagonista[13], la società è stata ritenuta dal Consiglio di Stato francese conforme alla normativa europea sulla protezione dei dati personali, in quanto i dati da lei ospitati sono stati protetti attraverso una procedura di crittografia basata su una terza parte di fiducia situata in Francia. Ciò impedirebbe, infatti, la lettura dei dati da parte di terzi, rendendo il trattamento conforme alla normativa europea.

Inoltre, a seguito delle decisioni che lo hanno visto coinvolto, il 16 marzo 2022 Google ha annunciato il lancio di "Google Analytics 4", definita quale soluzione di misurazione di nuova generazione che andrà a sostituire Universal Analytics. A detta di Google, il nuovo servizio sarà

---

[12] https://edpb.europa.eu/news/news/2020/european-data-protection-board-thirty-seventh-plenary-session-guidelines-controller_en?mkt_tok=eyJpIjoiTVRrMVlqRmpOMlF3TnpCbCIsInQiOiJFekdLKzFydWlOSHpaU1RDUTNUaHVWR2JxTVN4MnRDUm9jYTRkOGRxWG1LSDBWY1lBQkhaM2dsTkdoSEdYNlQrN2lFbm84d1Y3STRWMFlXZk5lM0dzeGFMd2p2NGFjVmltS1wvNnlCSmhrK3Nra1dGcGNjd2lEQWN6UW9EQVdtNmsifQ%3D%3D.

[13] https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-03-12/450163.

"una proprietà incentrata sul rispetto della privacy" e infatti, come impostazione di default, non permetterà più la memorizzazione degli indirizzi IP degli utenti.

In conclusione, si può ritenere che il trasferimento dei dati negli Stati Uniti presenta svariate problematiche, che allo stato possono essere superate mediante accorgimenti tecnici, strumenti di *accountability* e introduzione di ulteriori e valide misure di sicurezza adeguate al rischio connesso al trattamento. L'adozione del *Trans-Atlantic Data Privacy Framework* fugherebbe comunque ogni dubbio interpretativo ed applicativo e consentirebbe alle società europee che usufruiscono di servizi forniti da società statunitensi di effettuare un legittimo trasferimento verso gli Stati Uniti, in conformità al capo V del GDPR.