

Come alcuni ricorderanno, a maggio 2022, Monitora PA varò il proprio osservatorio richiedendo a 7833 pubbliche amministrazioni di interrompere i trasferimenti illeciti verso un'azienda statunitense dovuti all'utilizzo di Google Analytics.

Poco più di un mese dopo l'Autorità Garante per la Protezione dei Dati Personali pubblicò [un comunicato stampa](#) in cui, [a valle del provvedimento Caffèina](#), richiamava "all'attenzione di tutti i gestori italiani di siti web, pubblici e privati, l'illiceità dei trasferimenti effettuati verso gli Stati Uniti attraverso GA, **anche in considerazione delle numerose segnalazioni e quesiti che stanno pervenendo all'Ufficio.** E invita tutti i titolari del trattamento a verificare **la conformità delle modalità di utilizzo** di cookie e altri strumenti di tracciamento utilizzati sui propri siti web, **con particolare attenzione a Google Analytics e ad altri servizi analoghi**, con la normativa in materia di protezione dei dati personali."

Web Analytics Italia...

Alcuni ricorderanno che nella primissima PEC di Monitora PA, oltre a richiedere l'interruzione dei trasferimenti illeciti verso Google, suggerimmo l'adozione di [Web Analytics Italia](#) un servizio di statistiche web basato sul software open source [Matomo](#), fornito direttamente da AgID - Agenzia per l'Italia Digitale.

Purtroppo il successo straordinario della nostra campagna colse AgID impreparata: moltissime pubbliche amministrazioni richiesero di accedere al servizio ed evidentemente l'hardware dedicato al servizio non era stato dimensionato sulla base delle reali esigenze della PA italiana.

AgID disabilitò temporaneamente la possibilità di registrarsi al servizio, spiegando il problema e promettendo, entro il gennaio del 2023, la riabilitazione delle registrazioni, in modo che tutte le altre PA potessero finalmente usufruirne.

...su Amazon Web Service

Purtroppo, come ci è stato segnalato da diverse persone che dentro e fuori dalla pubblica amministrazione apprezzano il lavoro di Monitora PA, per risolvere il problema di carico, AgID ha adottato i servizi forniti da Amazon Web Service, Inc. società statunitense controllata da Amazon che ripropone tutti

i problemi di trasferimento transfrontaliero dei dati personali, già posti da Google Analytics.

In questo caso, naturalmente, la responsabilità morale dei trasferimenti in corso verso AWS è anzitutto di AgID: il trasferimento dei servizi è infatti stato probabilmente del tutto trasparente per le PA, con un semplice reindirizzamento del dominio ingestion.webanalytics.italia.it verso i server di Amazon su cui era già stato predisposto Matomo.

Tuttavia la responsabilità **legale** di tali trasferimenti rimane, ai sensi del GDPR, in capo al Titolare del Trattamento (ovvero, nel caso di ogni Pubblica Amministrazione, del suo legale rappresentante).

Il Titolare del Trattamento deve infatti assicurarsi (ed essere in grado di dimostrare, anche attraverso accurati audit tecnici) che tutti i Responsabili e Subresponsabili del Trattamento cui affida i dati personali di cittadini europei rispettino pienamente la normativa e i diritti fondamentali di **tutti** gli interessati.

D'altronde il GDPR stabilisce che ogni Responsabile del Trattamento (in questo caso AgID) deve trattare i dati personali del trattamento esclusivamente entro i termini prescritti dal Titolare.

Abbiamo dunque invitato 2340 Pubbliche Amministrazioni ad intimare ad AgID l'interruzione dei trasferimenti verso Amazon Web Service, Inc entro 15 giorni da oggi.

Basta infatti leggere l'[AWS Data Processing Addendum](#) che integra l'[AWS Customer Agreement](#) per scoprire che Amazon dichiara esplicitamente di rispettare le normative statunitensi cui Amazon Web Services, Inc (parte dell'accordo, come indicato in premessa) è sottoposta:

- al punto 1.4, chiarendo che ogni sottoscrittore rispetterà *"tutte le leggi, le regole e i regolamenti ad esso applicabili e per esso vincolanti"*
- al punto 3, chiarendo che *"AWS non accederà, utilizzerà o rivelerà a terze parti i dati del cliente eccetto che per rispettarle la legge o un ordine valido e vincolante di un'agenzia governativa."* Inoltre AWS dichiara che *"se costretta a rivelare dati del cliente ad una agenzia governativa, AWS darà al cliente una ragionevole notifica della richiesta [...] a **meno che ciò non sia vietato dalla normativa in questione.**"*

La "normativa in questione" è costituita dal combinato disposto fra [FISA 702](#), l'[Executive Order 12333](#) e il [CLOUD Act](#), ovvero le leggi statunitensi che hanno costretto la Corte di Giustizia Europea a riconoscere l'invalidità del Privacy Shield a causa della palese violazione dei diritti umani dei cittadini europei.

Tali normative infatti costringono le aziende statunitensi a fornire, a qualsiasi agenzia governativa che ne faccia richiesta, accesso ai dati dei cittadini europei, **ovunque si trovino**, segretamente e **senza nemmeno l'autorizzazione di un Magistrato** (ovvero senza alcuna garanzia per le vittime di tale accesso illecito).

Amazon dunque, esattamente [come Google](#) e [come Microsoft](#), **dichiara espressamente** di rispettare la normativa statunitense che ne rende incompatibili i servizi con la protezione dei dati personali dei cittadini europei.

Non potrebbe fare altrimenti: la Legge prevale su qualsiasi clausola contrattuale.

E' dunque responsabilità di chi ne adotta i servizi in Europa, **utilizzarli esclusivamente per dati non personali**, ovvero dati non riferiti o riferibili a persone fisiche.

Infatti, come chiarito dallo European Data Protection Board nelle [Raccomandazioni del 17 gennaio 2023](#) sull'uso del cloud da parte della Pubblica Amministrazione, *"il solo uso di un Cloud Service Provider che sia parte di un gruppo multinazionale soggetto alla normativa di paesi terzi, può risultare nell'applicazione di tale normativa anche a dati salvati nel EEA"*. Ed è ovvio: il controllo sul software che elabora i dati dei cittadini europei implica la possibilità di accedere ai dati stessi. Amazon Web Service, Inc potrebbe essere costretta, nei termini delle già citate normative USA, a inviare presso uno o più dei suoi data center europei aggiornamenti in grado di prelevare i dati di interesse di una agenzia governativa e rimuovere ogni evidenza di tale "data breach" prima del riavvio dei servizi.

Come sempre, se allo scadere dei 15 giorni AgID non avrà spostato i server di Web Analytics Italia presso una società europea che non possa tecnicamente trasferire dati personali a governi extra-UE privi di una decisione di adeguatezza, saremo costretti a segnalare le PA che ancora utilizzano tale servizio (e AgID stessa, come responsabile del trattamento) all'Autorità Garante per la Protezione dei Dati Personali.

Naturalmente rimane diritto delle Pubbliche Amministrazioni eventualmente danneggiate dalla condotta di AgID [sporgere reclamo](#) all'Autorità Garante per la Protezione dei Dati Personali nei confronti della stessa, soprattutto nel caso in cui questa non dovesse prontamente adempiere alla richiesta di interrompere i trasferimenti transfrontalieri in atto.

Siamo però fiduciosi che AgID, comprendendo appieno la gravità del problema, si attiverà prontamente per spostare i server di Web Analytics Italia presso un fornitore italiano o almeno europeo, al fine di garantire il rispetto dei diritti fondamentali dei cittadini italiani ed una vera sovranità cibernetica del nostro Paese.