

Richiesta di valutazione del trattamento dei dati
personali svolto da 2679 pubbliche
amministrazioni

Indice

I. Introduzione e scopo della presente segnalazione	2
II. Il Richiedente	3
III. I Soggetti segnalati	3
IV. Contesto Giurisprudenziale	3
V. Perché il Garante per la protezione dei dati personali dovrebbe prendere in considerazione questa segnalazione	5
VII. Istanze	5
Firma	7

I. Introduzione e scopo della presente segnalazione

1. Sono uno sviluppatore che contribuisce ad una delle tante comunità hacker italiane, composta da attiviste e attivisti, cittadine e cittadini attenti alla riservatezza delle proprie vite e alla libertà dei nostri concittadini.
2. Al fine di proteggere i nostri concittadini e aiutare la Pubblica Amministrazione a realizzare una transizione cibernetica democratica, abbiamo creato un osservatorio automatico¹ che estende la nostra capacità individuale di identificare problemi di conformità al GDPR nelle Pubbliche Amministrazioni e nei gestori di pubblici servizi (IPA) elencati da AgID², affinché possano essere segnalati e risolti nel più breve tempo possibile.
3. In data 4 novembre 2022 il nostro osservatorio automatico ha rilevato la presenza di trasferimenti illeciti di dati personali verso le società statunitensi sotto segnalate, avviati sistematicamente dai siti web degli Enti indicati nell'elenco allegato, attraverso l'incorporamento di diverse risorse scaricate dai servizi
 - Google Hosted Libraries (di Google LLC)
 - Google Maps (di Google LLC)
 - reCAPTCHA (di Google LLC)
 - Font Awesome (di Fonticons, Inc. distribuito da Cloudflare, Inc.)(si veda l'introduzione a riguardo nell'Allegato Tecnico, punti da 1 a 9).
4. Abbiamo quindi inviato a detti Enti una PEC che conteneva l'invito ad interrompere tali trasferimenti.
5. In data 27 novembre 2022, un'ulteriore esecuzione dell'osservatorio automatizzato ha rilevato che gli Enti segnalati di seguito effettuano ancora i trasferimenti sistematici di cui era stata richiesta l'interruzione.
6. S'invia la presente Segnalazione ai sensi e per gli effetti dell'art. 144 del Codice in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003, n. 196 e successive modifiche e integrazioni) affinché il Garante valuti la condotta delle Amministrazioni che continuano a utilizzare le risorse incorporate da aziende USA nei propri siti istituzionali, anche ai fini dell'emanazione dei provvedimenti di cui all'art. 58 del GDPR.
7. L'allegato tecnico (`Allegato-Tecnico.pdf`), l'elenco degli Enti oggetto di questa segnalazione (`Enti-Segnalati.csv`), nonché l'archivio compresso `MonitoraPA_2022-11-26.zip`, sono da intendersi parte integrante della presente segnalazione.

¹<https://github.com/MonitoraPA>

²<https://indicepa.gov.it/ipa-dati/dataset/enti>

II. Il Richiedente

8. La presente Segnalazione viene presentata da **Giacomo Tesio** nato a XXXXXXXX il XX/XX/XXXX (codice fiscale: XXXXXXXXXXXXXXXX), in proprio e per conto della comunità di hacker che ha realizzato Monitora PA³, eleggendo ai fini del presente atto domicilio fisico in XXX XXXX XXX, XXXXX (XXXX) e domicilio digitale presso la casella PEC comunicazioni@pec.monitora-pa.it.

III. I Soggetti segnalati

9. La Segnalazione viene presentata nei confronti di 2679 enti elencati nel file allegato Enti-Segnalati.csv (di seguito congiuntamente “**Enti Segnalati**”) nonché nei confronti di:
 - **Fonticons, Inc.**, 307 S Main St Ste 202 Bentonville, AR 72712-9214, USA,
 - **Cloudflare Inc**, 101 Townsend St. San Francisco, CA 94107, USA,
 - **Google LLC**, 1600 Amphitheatre Parkway Mountain View, CA 94043, USA,
 - **Google Ireland Limited**, Gordon House, Barrow Street, Dublin 4, Irlanda (di seguito congiuntamente “**Fornitori USA Segnalati**”).

IV. Contesto Giurisprudenziale

10. La Corte di Giustizia dell’Unione Europea ha riconosciuto la nullità della decisione d’adeguatezza della Commissione UE n. 2016/1250 (basata sull’accordo c.d. “*EU-US Privacy Shield*”) con sentenza del 16 luglio 2020 resa nella causa C-311/18 (cd. “Schrems II”, di seguito “la Decisione”). Di conseguenza, i Titolari non possono più utilizzare tale decisione di adeguatezza per trasferire i dati a soggetti con sede negli Stati Uniti d’America così come previsto dall’Articolo 45 GDPR.
11. In particolare, la Corte ha accertato che il diritto degli Stati Uniti d’America non offre adeguate garanzie di tutela dei diritti degli interessati: il fornitore statunitense è soggetto a norme (FISA 702 e E.O. 12333, in combinato disposto con PPD-28) che permettono attività di sorveglianza di massa in modo non rispettoso dei diritti fondamentali riconosciuti nell’UE e i Fornitori USA Segnalati rientrano nella definizione di “*electronic communication service provider*” fornita dal paragrafo 50 U.S. Code § 1881(b)(4) e, in quanto tali, sono soggetti ai programmi di sorveglianza statunitense di cui al paragrafo 50 U.S. Code § 1881a (“FISA 702”). La Corte ha anche chiarito che eventuali trasferimenti in favore di società soggette alla disciplina di cui al paragrafo 50 U.S. Code § 1881a non solo violano le disposizioni rilevanti del Capo V del GDPR, ma

³<https://monitora-pa.it>

anche gli Articoli 7 e 8 (della Carta dei Diritti Fondamentali dell'Unione Europea, da ora CDF), nonché il nucleo essenziale dell'Articolo 47 CDF (cfr. C-362/14 ("Schrems I"), par. 95). Ogni trasferimento di dati, dunque, comporta la contemporanea violazione di diversi diritti fondamentali (privacy, protezione dei dati personali, diritto a un rimedio effettivo e al giusto processo).

12. I Titolari non possono utilizzare, ai fini del trasferimento, le "clausole tipo di protezione dei dati" di cui all'Articolo 46(2)(c) e (d) GDPR se, come avviene nel caso in esame, il paese terzo non assicura un livello di protezione adeguato ai sensi del diritto UE (cfr. par. 134, 135 della Decisione), a meno di adottare efficaci misure tecniche supplementari.
13. Anche l'EDPB, con le Raccomandazioni 01/2020, ha precisato che si possono trasferire dati personali negli USA utilizzando altre basi legali (come le clausole contrattuali tipo di protezione dei dati) ma solo adottando efficaci misure tecniche supplementari (per esempio la cifratura dei dati personali con chiavi indisponibili ai riceventi) di modo che non sia possibile utilizzare i dati personali in violazione dei diritti degli utenti al di fuori dell'UE.
14. Il Garante Austriaco (Datenschutzbehörde) con la decisione D155.027 GA del 22 Dicembre 2021⁴ ha dichiarato l'illegittimità dell'uso di Google Analytics; anche il Garante Francese (CNIL) si è pronunciato nello stesso senso nel febbraio 2022⁵ e, il 7 giugno 2022 ha pubblicato delle domande/risposte che forniscono dettagliate informazioni sull'illegittimità dell'uso di Google Analytics e del trasferimento dei dati negli Stati Uniti⁶.
15. L'Autorità Garante per la Protezione dei dati Personali destinataria della presente segnalazione, con Provvedimento del 9 giugno 2022 [docweb n. 9782890] pubblicato il 23 giugno 2022 ha richiamato "all'attenzione di tutti i gestori italiani di siti web, pubblici e privati, l'illiceità dei trasferimenti effettuati verso gli Stati Uniti attraverso GA" e invitato "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".
16. Anche gli altri servizi analizzati rientrano senz'altro nella definizione di strumento di tracciamento e risultano essere - per la loro modalità di funzionamento - strumenti la cui inclusione produce effetti analoghi a Google Analytics (v. allegato tecnico, punti da 10 a 15). L'uso di tali servizi, in assenza di efficaci misure tecniche supplementari (che non risultano

⁴<https://www.dsb.gv.at/dam/jcr:c1eb937b-7527-450c-8771-74523b01223c/D155.027%20GA.pdf>

⁵https://www.cnil.fr/sites/default/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf

⁶<https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply>

presenti secondo la nostra analisi) è pertanto anch'esso illegittimo. Infatti anche l'incorporamento delle risorse specifiche di ciascun servizio produce sistematicamente il trasferimento transfrontaliero di dati personali che in assenza di una condizione legittimante ai sensi degli artt. 44 e ss. GDPR, espone a rischi ingiustificati tutti i visitatori dei siti.

V. Perché il Garante per la protezione dei dati personali dovrebbe prendere in considerazione questa segnalazione

18. In tutte le configurazioni note, l'inclusione di chiamate verso i server dei Fornitori USA Segnalati nelle pagine di un sito web determina la possibilità da parte di tali aziende di trattare dati personali (si veda l'Allegato Tecnico, punti da 10 a 15).
19. La natura dei dati resi accessibili almeno una volta al giorno a causa dell'inclusione di tali risorse sul sito web istituzionale, compromette la riservatezza delle comunicazioni fra gli Enti segnalati e i cittadini (si veda l'Allegato Tecnico, punti da 10 a 15).
20. La collocazione geografica dei server che ricevono e trattano i dati raccolti da suddetti servizi è irrilevante sia per le disposizioni previste dalla succitata legge statunitense sulla sorveglianza ("FISA 702"), sia per il controllo centralizzato che le aziende fornitrici esercitano sul software eseguito da tutte le sue consociate (si veda l'Allegato Tecnico, punti da 16 a 18).
21. Pertanto, stante il fatto che l'incorporamento delle risorse elencate da server di aziende USA permette un trasferimento di dati personali verso gli Stati Uniti d'America senza il consenso dell'interessato né altra idonea condizione di liceità, **l'uso di tali servizi è illegittimo.**
22. Concludendo, quando utilizzano i server di aziende USA i Titolari non possono garantire un livello adeguato di protezione dei dati trasferiti in favore di tali aziende e devono dunque astenersi dal trasferire i dati personali dei cittadini italiani ed europei verso di esse.

VII. Istanze

Per tutti questi motivi, Giacomo Tesio, con il sostegno delle associazioni elencate in calce, chiede che l'Autorità garante per la protezione dei dati personali, nell'esercizio delle proprie funzioni:

1. imponga immediatamente l'interruzione o sospensione di qualunque flusso di dati tra i Titolari (Enti Segnalati) e i Fornitori USA Segnalati nonché tra

i Titolari (Enti Segnalati) e le filiali europee dei Fornitori USA Segnalati ai sensi dell'Articolo 58(2)(f) del GDPR;

2. ai sensi e per gli effetti dell'art. 58 del GDPR e dell'art. 144 del Codice in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003, n. 196 e successive modifiche ed integrazioni), apra un'istruttoria in proposito;
3. all'esito dell'istruttoria, valuti la condotta degli Enti Segnalati sopra elencati (v. punto 9) anche ai fini dell'emanazione dei provvedimenti di cui all'art. 58 del GDPR, e in particolare:
 - stabilisca quali dati personali degli utenti siano stati trasferiti dai Titolari (Enti Segnalati) ai succitati Fornitori USA Segnalati negli Stati Uniti d'America o in qualunque altro paese terzo o organizzazione internazionale;
 - chiarisca quale sia stata, in questi anni, la base legale utilizzata dai Titolari per effettuare il suddetto trasferimento di dati personali, come richiesto dagli Articoli 44 e seguenti del GDPR;
 - ordini il ritrasferimento di tali dati presso datacenter fuori dal controllo di tali Fornitori USA Segnalati e all'interno del territorio EU/EEA, o presso un altro paese che garantisca una protezione efficace e adeguata ai sensi degli Articoli 58(2)(d) e (j) del GDPR;
 - chiarisca se le disposizioni dei *Google Maps Terms of Service*, *Google reCAPTCHA Terms of Service*, *Google Hosted Libraries Terms of Service* e *Font Awesome Terms of Service* rispettino il disposto di cui all'Articolo 28 del GDPR con riferimento al trasferimento di dati personali verso paesi terzi;
 - imponga - laddove sussistano le condizioni - una sanzione pecuniaria effettiva, proporzionata e dissuasiva nei confronti dei Titolari (Enti Segnalati) e dei Fornitori USA Segnalati come previsto dall'articolo 83(5)(c) del GDPR, tenendo in considerazione:
 - a) che molti cittadini italiani sono danneggiati dalle sopra evidenziate condotte illecite (Articolo 83(2)(a) del GDPR);
 - b) che i Titolari (Enti Segnalati) hanno ricevuto da Monitora PA comunicazione delle circostanze riferite nella presente segnalazione, e nulla hanno fatto per porre in essere quanto meno delle efficaci misure tecniche supplementari a protezione dei dati personali degli utenti dei propri siti web;
 - c) che sono trascorsi oltre due anni dalla sentenza della CGUE all'esito della causa n. C-311/18, nonché più di tre mesi dal sopra citato Provvedimento del Garante per la Protezione dei Dati Personali, al quale è seguito un lungo dibattito sulla stampa anche non specializzata, senza che i Titolari (Enti Segnalati) abbiano posto in essere alcuna azione concreta per conformare il

proprio trattamento di dati personali alle disposizioni del GDPR, nonostante la semplicità con cui avrebbero potuto avviare.

4. in conformità con le disposizioni di cooperazione e assistenza reciproca del Capo VII del GDPR, il Richiedente invita l'Autorità a collaborare con le altre autorità europee per la protezione dei dati personali che abbiano ricevuto segnalazioni o reclami aventi come oggetto le stesse problematiche in questa sede evidenziate.

Alba, 30 novembre 2022

Firma

Giacomo Tesio
Co-fondatore del progetto Monitora PA
<https://monitora-pa.it>

Con il sostegno di:

- **Hermes Center**, Associazione con sede in Via Aterusa n. 34, 20129 Milano, in persona del suo legale rapp.te p.t Fabio Pietrosanti
C.F. 97621810155 <https://www.hermescenter.org/>
- **LinuxTrent**, Associazione con sede in Via Marconi n. 105, 38057 Pergine Valsugana, in persona del suo legale rapp.te p.t Roberto Resoli
C.F. 96100790227 <https://www.linuxtrent.it/>
- **Open Genova**, Associazione con sede in Piazza Matteotti n. 5 c/o Mentelocale.it, 16123 Genova, in persona del suo legale rapp.te p.t Pietro Biase C.F. 95165570102 <https://associazione.opengenova.org/>
- **AsCII**, Associazione con sede in Via del Mare n.108, 80016 Marano di Napoli, in persona del suo legale rapp.te p.t Avvocato Marco Andreoli
C.F. 94200750639 <https://www.ascii.it>
- **AsSoLi**, Associazione con sede in Via San Quintino n. 32, 10121 Torino, in persona del legale rappresentante p.t Angelo Raffaele Meo C.F. 94082140487 <https://www.softwarelibero.it/>