Richiesta di valutazione del trattamento dei dati personali svolto da 1116 pubbliche amministrazioni

Indice

I. Introduzione e scopo della presente segnalazione

1. Sono uno sviluppatore che contribuisce al progetto Monitora PA, cui lavorano hacker, 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 automatico[1] 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 AgID[2], affinché possano essere segnalati e risolti nel più breve tempo possibile.

3. In data 28 febbraio 2023 il nostro osservatorio automatico ha rilevato la presenza di trasferimenti illeciti di dati personali verso Microsoft Corporation, avviati sistematicamente a causa dell'utilizzo, per la posta elettronica ordinaria (PEO), dei servizi forniti dalla stessa Microsoft Corporation.

4. Abbiamo quindi inviato a detti Enti una PEC che conteneva l'invito ad interrompere tali trasferimenti.

5. In data 30 maggio 2023, 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, come evidenziato dalla presenza dei server SMTP di Microsoft nei record MX associati al dominio istituzionale di ciascun Ente nel DNS autoritativo.

6. Si 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 continuino a utilizzare i servizi sopra indicati, 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_2023-05-14.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 … sviluppatore del progetto Monitora PA[3]…

III. I Soggetti segnalati

9. La Segnalazione viene presentata nei confronti di 1116 enti elencati nel file allegato Enti-Segnalati.csv (di seguito congiuntamente "**Enti Segnalati**") nonché nei confronti di:

   - **Microsoft Corporation**, One Microsoft Way, Redmond, Washington, USA
   - **Microsoft Central and Eastern Europe**, Konrad-Zuse-Str.1, 85716 Unterschleißheim, Germany
   - **Microsoft S.R.L.**, Viale Pasubio 21, Milano (MI)

   (di seguito congiuntamente "**Fornitori 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 "**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 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 violino le disposizioni rilevanti del Capo V del GDPR, ma 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

[3] https://monitora-pa.it

(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, puntualizzando tra l'altro che "l'accesso remoto da parte di un'entità di un paese terzo a dati situati nel SEE è considerato un trasferimento" (nota 22, p. 9).

14. Il Garante Austriaco (Datenschutzbehörde) con la decisione D155.027 GA del Dicembre 2021[4] ha dichiarato l'illegittimità dell'uso di Google Analytics; anche il Garante Francese (CNIL) si è pronunciato nello stesso senso nel febbraio 2022[5] 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 Uniti[6].

15. Nel documento "2022 Azione esecutiva coordinata - Utilizzo di servizi basati su cloud da parte del settore pubblico" adottato come raccomandazione il 17 gennaio 2023 l'EDPB ribadisce che: "*..l'utilizzo da parte di un ente pubblico del software fornito dal fornitore di servizi cloud può comportare trasferimenti verso molte destinazioni che non garantiscono un livello di protezione sostanzialmente equivalente a quello dell'UE, compresi gli Stati Uniti d'America (USA). In questi casi, l'ente pubblico - che agisce in qualità di titolare del trattamento - deve valutare attentamente i trasferimenti che possono essere effettuati per suo conto dal fornitore di servizi cloud, ad esempio identificando le categorie di dati personali trasferiti, le finalità, i soggetti a cui i dati possono essere trasferiti e il paese terzo coinvolto. La valutazione dei trasferimenti internazionali di dati personali in atto*
dovrebbe essere effettuata prima di impegnarsi con il fornitore di servizi cloud. Gli enti pubblici devono fornire istruzioni all'incaricato del trattamento per individuare e utilizzare uno strumento di trasferimento

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

[5] https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply

[6] https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/questions-reponses-sur-les-mises-en-demeure-de-la-cnil-concernant-lutilisation-de-google-analytics

adeguato e, se necessario, per individuare e attuare misure supplementari appropriate che garantiscano che le garanzie contenute nello strumento di trasferimento prescelto possano essere rispettate dall'importatore, in modo da assicurare che il livello di protezione offerto dal GDPR non sia compromesso quando i dati sono trasferiti a un paese terzo. […]
Emerge dall'analisi effettuata dalle Autorità che il solo uso di un Cloud Service Provider che sia parte di un gruppo multinazionale soggetto alla normativa di paesi terzi, può determinare l'applicazione di tale normativa anche a dati salvati nel EEA. Eventuali richieste verrebbero inviate direttamente al CSP presente nel EEA e riguarderebbero dati presenti nel EEA e non dati già oggetto di trasferimenti." [7]

16. Human Rights Watch quest'anno ha pubblicato un rapporto sulle violazioni della privacy di studenti, genitori ed insegnanti da parte delle piattaforme educative adottate durante la pandemia [8].

17. 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*".

18. Dopo quasi tre anni dalla sentenza Schrems II non è ammissibile, in uno Stato di diritto[9], continuare a violare la normativa vigente e i diritti fondamentali di milioni di cittadini italiani nell'attesa che il processo di adozione di una nuova decisione di adeguatezza per la sicurezza dei flussi di dati con gli USA, attivato dalla Commissione UE il 13.12.2022[10], si concluda positivamente: infatti come chiarito dall'EDPB con parere n. 5/2023[11] e dal Parlamento UE con risoluzione dell'11 maggio 2023[12], affinché i dati personali dei cittadini europei possano godere di una protezione equivalente a quella garantita in Europa, saranno necessarie ulteriori e profonde modifiche alla normativa statunitense che, se mai verranno adottate, richiederanno comunque tempi ancora molto lunghi.

[7] https://edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf
[8] https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments
[9] https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/upholding-rule-law_it
[10] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631
[11] https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en
[12] https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html

19. Anche i servizi di posta elettronica analizzati e i servizi ad esso associati (v. punto 3 della presente) 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 Analitycs.

    Si tratta specificamente dei servizi:

    - Outlook.com
    - OneDrive
    - Microsoft Office Online
    - Microsoft Teams

    L'uso di tali servizi - in assenza di efficaci misure tecniche supplementari (che non risultano presenti secondo la nostra analisi) - è pertanto anch'esso illegittimo, ciò in linea con quanto emerge chiaramente dai precedenti sopra citati (v. parte IV della presente).

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

20. In assenza di efficaci misure tecniche supplementari, puntualmente descritte dal Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz [13] (estremamente costose in pratica), che non risultano presenti alla nostra analisi, i dati personali di migliaia di cittadini italiani vengono condivisi sistematicamente con Microsoft.

21. La natura dei dati resi accessibili, spesso riconducibili alle speciali categorie elencate all'articolo 9 comma 1 del GDPR (si pensi ad esempio ai dati trattati da ASL, Università e Scuole), compromette la riservatezza delle comunicazioni fra gli Enti segnalati e i cittadini (spesso minori).

22. Microsoft dichiara espressamente nel Microsoft Products and Services Data Protection Addendum (DPA) [14] che "comunicherà né consentirà l'accesso ai Dati Trattati, tranne nel caso in cui ciò sia [...] previsto dalla legge. [...] Microsoft tenterà di reindirizzare tali autorità alla Società stessa per la comunicazione diretta di tali dati. Nel caso in cui sia costretta a divulgare i Dati Trattati o a consentirne l'accesso alle autorità giudiziarie o di polizia, Microsoft ne darà immediata comunicazione alla Società e le fornirà una copia della richiesta, **salvo disposizioni di legge contrarie**.". In altri termini, Microsoft riconosce di dover adempiere alle

[13] https://www.datenschutz.rlp.de/de/themenfelder-themen/microsoft-office-365/

[14] https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=17 pagina 6

normative statunitensi anche in violazione dei diritti fondamentali degli interessati.

23. Inoltre Microsoft, nello stesso documento[15], richiede ai Titolare del Trattamento la piena accettazione dei trasferimenti di dati personali verso gli Stati Uniti: "la Società autorizza Microsoft a trasferire i Dati della Società, i Dati dei Servizi Professionali e i Dati Personali negli Stati Uniti o in qualunque altro paese in cui Microsoft o gli Altri suoi Responsabili del Trattamento sono presenti e di archiviare e trattare i Dati della Società e i Dati Personali per fornire i Prodotti, fatto salvo quanto descritto in altri Articoli delle Condizioni dell'Addendum."

24. 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 Microsoft esercita sul software eseguito da tutte le sue filiali.

25. Pertanto, stante il fatto che l'uso di software eseguiti da server di Microsoft comporta 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 da ritenersi illegittimo**.

26. 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 Segnalati* nonché tra i Titolari (Enti Segnalati) e le filiali europee dei Fornitori 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;

[15] https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=17 pagina 10

3. all'esito dell'istruttoria, valuti la condotta degli Enti Segnalati sopra elencati 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 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 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 rispettivi *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 Segnalati come previsto dall'articolo 83(5)(c) del GDPR, tenendo in considerazione:
     a) che molti cittadini italiani (ed in particolare moltissimi minori) 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 efficaci misure tecniche supplementari a protezione dei dati personali trasferiti, limitandosi, nella migliore delle ipotesi, a scaricare l'onere della protezione dei dati personali sugli interessati stessi, suggerendo agli stessi pratiche del tutto inefficaci nel caso in specie, come l'uso della modalità di navigazione in incognito del browser;[16]
     c) che sono trascorsi quasi tre anni dalla sentenza della CGUE all'esito della causa n. C-311/18, nonché quasi un anno 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,

[16] https://www.howtogeek.com/117776/htg-explains-how-private-browsing-works-and-why-it-doesnt-offer-complete-privacy/

nonostante le diverse soluzioni alternative fornite sul marketplace ACN da aziende italiane ed europee.[17]

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.

03 giugno 2023

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/

[17] Per una rapida panoramica si veda l'ottimo seminario organizzato dall'Intendenza Scolastica della Provincia Autonoma di Bolzano per 70 scuole dell'Emilia Romagna: https://fuss.bz.it/post/2023-03-28_incontro-dirigenti-emilia-romagna/