Sulla risposta inviata a Federico Leva

Domande allo Studio Lisi

Indice

Introduzione e scopo della missiva

Alla cortese attenzione di

- Redazione del sito https://studiolegalelisi.it
- Titolare del Trattamento per il sito https://studiolegalelisi.it

e p.c. al Data Protection Officier dello stesso per quanto concerne l'esercizio delle sue funzioni e responsabilità.

Sono Giacomo Tesio, hacker e co-fondatore di Monitora PA.
In calce a questa mail troverete i miei dati personali identificativi che vi chiedo espressamente di non diffondere.

Come anticipato all'Avvocato Andrea Lisi che ci ha recentemente fatto l'onore di partecipare alle nostre conversazioni in rete, ho fatto visita al vostro sito per leggere con maggiore calma la vostra risposta a Federico Leva, hacker indipendente nonché attivista che partecipa, come l'avvocato Lisi stesso, alle riflessioni della nostra comunità.

Metodo hacker: un dialogo pubblico costruttivo e sicuro

Vi scrivo anzitutto perché un'attenta lettura del vostro articolo [1] ha fatto sorgere molte domande che vi vorrei sottoporre per migliorare col vostro aiuto l'efficacia della nostra lotta cibernetica non violenta.

Sono domande di un hacker: richiedono risposte puntuali ed esaustive, domanda per domanda, per non rischiare che interessantissime digressioni storiche o politiche ci distraggano dal caso in specie.

Tuttavia, laddove per ragioni di sicurezza informatica riteneste di non poter rispondere, sentitevi liberi di spiegare la natura del rischio cibernetico cui la specifica risposta vi esporrebbe: avrò cura di ideare domande alternative che proteggano la vostra sicurezza pur facilitando la nostra comprensione della vostra prospettiva.

In spirito di collaborazione ed assoluta trasparenza e come anticipato all'Avvocato Lisi, vi autorizzo a pubblicare la risposta a questa mia missiva (privata dei dati personali non strettamente necessari) sul vostro sito web. In alternativa, la pubblicheremo noi sul nostro sito [2] al fine di arricchire con il vostro prezioso contributo quel dibattito civile, costruttivo e di merito sulla protezione dei dati personali e delle nostre democrazie cui tutti teniamo.

[1] https://studiolegalelisi.it/novita/google-analytics-pubblichiamo-la-risposta-inviata-a-federico-leva/
[2] https://monitora-pa.it

Breve sintesi dei fatti: l'iniziativa di Federico Leva

Una doverosa premessa sui fatti di cui dibattiamo: all'indomani del recente pronunciamento del Garante della Privacy su Google Analytics, Federico Leva ha generosamente realizzato un software con cui ha visitato migliaia di siti web per segnalare, a chi a due anni dalla sentenza Schrems II stesse ancora utilizzando tale strumento di sorveglianza di massa, il comunicato dell'Autorità ed il rischio, dopo 90 giorni, di sanzioni per i Titolari dei siti stessi.

Il suo atto, in assoluta buona fede, era evidentemente e dichiaratamente finalizzato ad aiutare i Titolari dei siti in questione ad **evitare una severa sanzione**. Sanzione che, a due anni dal pronunciamento cristallino della Corte di Giustizia Europea, sarebbe **assolutamente meritata**.

Nel contesto di tale segnalazione, fatta nell'interesse dei Titolari stessi (molti dei quali hanno intelligentemente ringraziato il nostro amico), Federico ha altresì richiesto la cancellazione dei suoi dati personali, registrati durante tale navigazione.

La presente missiva non vuole e non può essere una difesa personale di Federico Leva che, pur agendo pienamente nel solco della cittadinanza cibernetica che cerchiamo di diffondere, non ha concordato o coordinato con noi la propria iniziativa.

Vogliamo però difendere la legittimità della sua azione perché auspichiamo che molti altri utilizzino il nostro osservatorio automatico distribuito in modo analogo, seppur con maggiore accortezza nella stesura delle comunicazioni ai Titolari.

Dall'hack di Federico abbiamo infatti imparato moltissimo.
Come hacker, non posso che ringraziarlo.

E per meritare il dono di conoscenza che ci ha fatto, speriamo di poter condividere quanto abbiamo imparato con migliaia di cittadini, affinché intraprendano iniziative analoghe ma più incisive ed inattaccabili sotto il profilo giuridico.

Domande sulla risposta a Federico che avete pubblicato

Fatta questa doverosa premessa, ecco le mie domande.

Sulla "azione di spamming"

Anzitutto la richiesta di Federico Leva viene qualificata, sin dall'introduzione del vostro articolo, come "un'azione di spamming".

L'articolo 130 del Codice della Privacy definisce lo spam sulla base di due caratteristiche che devono essere compresenti nella comunicazione:

- l'uso di sistemi automatizzati per l'invio
- le finalità commerciali, ovvero consistenti nell'invio
  - di materiale pubblicitario o di vendita diretta
  - per il compimento di ricerche di mercato o di comunicazione commerciale

A quale di queste categorie ritiene che la segnalazione di Federico appartenga? Ha forse cercato di venderle un proprio prodotto? Ha forse richiesto di partecipare ad una ricerca di mercato?

Fra noi informatici, gli spammer hanno una pessima accoglienza e chi di noi non dovesse conoscere Federico Leva potrebbe essere seriamente influenzato da parole così autorevoli che lo qualificano come tale.

Personalmente, mi sentirei gravemente oltraggiato ed offeso se il mio nome fosse stato indebitamente accostato a tale odioso illecito.

Federico Leva potrebbe subire gravi ripercussioni lavorative in futuro se il suo nome dovesse restare associato ad "un'azione di spamming". Le vostre parole, proprio perché autorevoli, rischiano di produrre un danno gravissimo alla sua carriera futura.

Non credete che sia opportuno e urgente rettificare pubblicamente tale qualificazione (che peraltro ho sentito ripetere in altri contesti) chiarendo che, come specificato anche dall'Avvocato Guido Scorza, componente del Consiglio dell'Autorità Garante per la Protezione dei Dati Personali in una recente intervista[3], l'azione di Federico Leva è stata un legittimo esercizio di diritti in

[3] «La richiesta che viene effettuata, al di là del provvedimento del Garante che l'ha preceduta, va nella direzione di esercitare un suo diritto e i dati vanno assolutamente cancellati, anche se le modalità con cui è stata rivolta ai soggetti interessati può essere in qualche modo interpretata come un gesto politico [...] Non vedo grande spazio per il grigio: la richiesta va adempiuta. Forse per evitare di incorrere in richieste simili e portarsi avanti con il lavoro, si potrebbero accorciare i tempi di retention di determinati dati, così da evitare di ritrovarsi sommersi da queste richieste o perlomeno di poter rispondere efficacemente a queste richieste, dimostrando che in questo preciso momento non si stanno trattando i dati dei richiedenti» https://www.giornalettismo.com/mail-di-federico-leva-analisi-guido-scorza-garante-privacy/

nessun modo riconducibile ad un odioso illecito come lo SPAM?

Sull'IP-Anonymization

Leggendo oltre nel testo della mail vera e propria, apprendo che parte dell'indirizzo IP dei visitatori del vostro sito viene nascosta al Titolare da Google attraverso l'opzione di IP-Anonymization.

Su questo punto è importante ricordare che tutti i Garanti europei hanno chiarito come tale opzione non sia sufficiente a proteggere i dati dei cittadini europei dalle normative USA nate per legittimare i trattamenti illegali rivelati da Snowden nel 2013.

Questo semplicemente perché se è un software di Google a scartare un qualsiasi dato, Google può essere costretta a rendere tale dato accessibile alle agenzie governative statunitensi prima di scartarlo.

Per essere supplementari, le misure tecniche che il Titolare del Trattamento deve assumere per continuare ad effettuare trasferimenti verso aziende USA devono essere sotto il pieno controllo fisico ed amministrativo del Titolare stesso: se le adotta Google, smettono di essere sia supplementari che efficaci, perché come le adotta le può aggirare senza che il Titolare possa impedirlo o anche solo saperlo.

Detto questo, se dai vostri audit avete verificato che Google effettivamente scarta tale dato prima di registrarlo nei database che vi rende disponibili attraverso l'interfaccia di Google Analytics, è chiaro che i primi 16 bit dell'IP di Federico Leva non saranno sufficienti ad identificarne le richieste da cancellare.

Potete condividere i risultati di tali audit prontamente effettuati all'indomani della sentenza Schrems II? Se no, perché?

Qualora invece le vostre ispezioni non avessero evidenziato una irreversibile ed incontrovertibile rimozione di tali dati, perché continuate ad utilizzare tale opzione, che **non protegge i dati personali degli utenti** ma **impedisce loro un più semplice esercizio dei propri diritti**?

Sulla richiesta del Client Id

Chiedete al Leva il Client Id utilizzato.

In quanto hacker, sono certo che Federico non avrà alcun problema a fornirvelo.

Ma avete verificato, prima di richiederlo, che tale dato non venga già registrato nei log HTTP del vostro web server? I cookie `_ga` e `_gid` di Google Analytics vengono infatti impostati via JavaScript per *apparire* come cookie "di prima parte" e aggirare in questo modo le protezioni predefinite fornite dai browser. Il vostro web server riceve dunque quell'informazione ad ogni navigazione dell'utente sul vostro sito: è possibile (se non probabile) che venga registrata nei log del vostro web server per ragioni di sicurezza.

Concorderete con me che in tal caso, la richiesta di un Client Id già nella disponibilità del Titolare apparirebbe come evidentemente strumentale, finalizzata ad impedire l'esercizio del diritto dell'interessato.

Qualora però effettivamente non salviate (né voi né il vostro fornitore di hosting web) tale informazione, avete indicato al richiedente i passi necessari per ottenerla dal proprio browser? Potete condividere con noi di Monitora PA queste indicazioni?

Sarebbe una guida utilissima per gli utenti meno esperti che utilizzano innumerevoli versioni di browser diversi su sistemi operativi mobili e non. Credo concorderete con me che in assenza di tale guida, facile ed esaustiva, pretendere tale informazione corrisponderebbe di fatto all'impedire l'esercizio di un diritto a milioni di cittadini. Soprattutto perché, appunto, il vostro web server riceve tale dato ad ogni navigazione sul vostro sito.

Dunque se fornire il Client Id è l'unico modo per ottenere la cancellazione dei propri dati illecitamente trasmessi a Google, sarete certamente disponibili spiegare gratuitamente a qualsiasi richiedente come ottenerlo.

Dove possiamo leggere tale guida gratuita?
Vi assicuro che faremo quanto in nostro potere per diffonderla.

Sulle competenze dei Titolari del Trattamento

Sono altresì rimasto sorpreso da due frasi della vostra risposta:

> Riteniamo opportuno anticiparLe sin d'ora, ad ogni buon conto, che le Sue richieste sono connotate da un grado di tecnicismo che eccede le competenze medie di un Titolare del trattamento che non abbia specifica formazione in campo informatico.

Intendete dire che oltre il 50% dei Titolari non sono in grado di esaudire una richiesta di cancellazione? Assumendo una distribuzione normale, se le "competenze medie" non bastano, allora più della metà della popolazione dei Titolari deve avere competenze inadeguate a svolgere il ruolo che il GDPR gli affida.

D'altro canto, Federico ha scritto a voi: le vostre specifiche competenze sono sufficienti ad esaudire la sua richiesta o no?

Sia chiaro: non ho ragione di dubitare della vostra valutazione.
In fondo **sono passati oltre due anni dalla sentenza Schrems II** e molti titolari e DPO cadono incredibilmente dal pero.

Sull'impegno eccessivo necessario ad effettuare la cancellazione

Scrivete inoltre a Federico:

> il riscontro alle stesse richieste implica un impegno eccessivo rispetto ai compiti ordinariamente attribuiti ai nostri collaboratori.

in che senso “un impegno eccessivo”?

Eccessivo rispetto a cosa? Quale sarebbe un impegno non eccessivo?

Sulla presunta “strumentalità” delle richieste

Sorvolo sulla “dichiarata strumentalità delle richieste”: Federico vi ha scritto per aiutarvi e vi ha chiesto in cambio solo di eliminare i dati che Google aveva raccolto nel processo. Cosa possiate vedere di strumentale nell’esercizio di questo diritto, davvero mi sfugge.

Vi faccio però notare che il GDPR protegge **i dati personali** di Federico.
Se voi avete ricevuto tali dati personali, quali che siano le ragioni o gli strumenti tecnici di tale trasmissione, voi ne restate responsabili. Esattamente come se quei dati fossero stati inviati presso di voi da una persona terza: i diritti dell’interessato su di essi non verrebbero meno.

Sarebbe assurdo se l’uso di un automatismo facesse decadere un diritto.
Il browser è un automatismo. Il server web è un automatismo.

E questo vale a maggior ragione per un automatismo scritto dall’utente che lo avvia: la scrittura del software in uso non cancella i diritti dell’utilizzatore in quanto tale software è una semplice espressione di quell’utente e della sua volontà.

Se l’uso di un automatismo per trasmettere dati personali facesse decadere la protezione degli stessi, il GDPR sarebbe carta straccia.
E a cosa servirebbero i DPO a quel punto?

A garantire una protezione formale ma fittizia dei dati personali?
A fare la foglia di fico sulla manipolazione di massa dei GAFAM?

Sul contributo spese e i costi amministrativi

Chiedete poi al Leva “un contributo spese commisurato ai costi amministrativi che dovremo sostenere per intraprendere le azioni da Lei richieste”: potete dettagliare pubblicamente questi costi amministrativi che “dovrete sostenere”?

Come informatico, fatico ad immaginarli.

Forse intendete addebitare a Federico il tempo impiegato “dagli esperti del nostro Studio” nello scrivere la risposta pubblicata sul vostro sito?
Non ne avete invece tratto un ritorno positivo in termini di visibilità?
Quante visite ha ricevuto il vostro sito in media a Luglio negli anni scorsi?
Quante visite ha ricevuto la risposta per Federico Leva?

E siete sicuri che tale addebito sia conforme alle “Guidelines 01/2022 on data subject rights - Right of access” del EDPB?

Siete sicuri che pubblicare la vostra risposta su un sito web determini un canale di comunicazione amichevole per l'utente?

A ben guardare, se anche Google non avesse potuto identificare Federico Leva come autore di quella specifica visita al vostro sito, la vostra lettera avrebbe rivelato al vostro fornitore l'identità del soggetto cui fanno riferimento i dati registrati durante la stessa.

E questo vale, ovviamente, non solo per voi, ma per tutti coloro che, invece di esaudire semplicemente la richiesta di Federico, hanno iniziato a scriverne e dibatterne sul web, facendo nome e cognome dell'interessato che pure non aveva richiesto tale pubblicità.

Vi ha scritto per farvi un favore.

Non aveva ragione di aspettarsi una **gogna mediatica su scala nazionale**.

Un dono più prezioso del contributo che vi serve

Voglio però che sappiate che vostra richiesta di un contributo economico a Federico Leva è stata fonte di grande ispirazione.

Se Federico vorrà condividere con me l'elenco dei siti web i cui Titolari gli invieranno la vostra risposta, avrò cura di visitarli personalmente per segnalare loro eventuali trattamenti illeciti che dovessero apparire evidenti alle mie competenze informatiche.

A tutti ovviamente segnalerò i trasferimenti illeciti riscontrati, chiedendo di porvi rimedio prima di presentare eventualmente reclamo presso l'autorità Garante in caso non dovessero ottemperare nei termini prescritti.

E naturalmente, qualora i miei dati dovessero subire trasferimenti illeciti, sarò costretto io stesso a chiederne la cancellazione.

Tuttavia, nonostante le notevoli competenze informatiche che metterò a disposizione dei vostri clienti, tengo a sottolineare che **non richiederò alcun compenso per il servizio**, né a voi né a loro.

Monitora PA non è infatti una azienda, non persegue finalità economiche ma sociali: tutto ciò che vogliamo è il rispetto dei diritti e delle libertà dei nostri concittadini, nel solco della nostra Costituzione.

Sul consenso raccolto dal vostro banner

In chiusura la vostra risposta suggerisce a Federico Leva di non prestare il consenso, in futuro, al trasferimento di dati presso Google.

Questo passaggio mi ha francamente sorpreso.

Io stesso ho letto con attenzione il vostro banner prima di accettarlo e non vi ho letto alcuna richiesta di autorizzare un trasferimento verso una azienda sottoposta ad una legislazione incompatibile con i miei diritti fondamentali.

Ho dovuto riaprire il sito in modalità incognito, per rileggere il banner ed accertarmi di non essere stato colpevolmente superficiale nel prestare il mio consenso all'installazione dei cookie.

Ne riporto il testo come apparso alla mia lettura:

> Questo Sito utilizza cookies al fine di offrirti un'esperienza di navigazione migliore. Facendo clic su "Accetta" acconsentirai all' uso di tutti i cookie. Facendo clic su "Rifiuta" rifiuterai l'uso di tutti i cookie ad eccezione di quelli necessari oppure cliccando su "Gestisci Preferenze" potrai selezionare i cookie da abilitare.

Io ho accettato serenamente l'uso di tutti i cookie perché consapevole della storia del vostro Studio Legale e fiducioso nella sua aderenza alla normativa vigente.

Ho però poi dovuto constatare con sorpresa ed enorme disagio che

- **prima ancora che io esprimessi qualsiasi consenso**, diversi miei dati personali erano già stati inviati a Google attraverso gli header HTTP delle richieste effettuate per il caricamento dei Google Fonts, fra cui:
  - il mio indirizzo IP
  - il mio User Agent
  - il mio sistema operativo
  - la mia visita presso il vostro sito
  - la data e la fascia oraria di tale visita
  - gli interessi culturali che da tale visita è possibile dedurre
- a valle del mio consenso, fra i cookie installati sul mio browser vi erano quelli di Google Analytics che aveva già iniziato a tracciare in modo ancora più dettagliato la mia navigazione sul vostro sito attraverso diverse comunicazioni inviate ai server del vostro fornitore.

Non posso biasimare Federico Leva per aver subito la stessa sorte.

Il vostro cookie banner chiede di accettare cookie "al fine di offrire un'esperienza di navigazione migliore".

Come avrei potuto leggere in questa finalità l'autorizzazione ad un trasferimento dei miei dati personali verso terze parti? Come avrei potuto sospettare che tali terze parti includessero aziende soggette a normative incompatibili con i miei diritti fondamentali?

Secondo quale criterio definite "consenso informato" tale accettazione?

Quanti di tali "consensi informati" avete raccolto dalla sentenza Schrems II?

Google Analytics: trasferimenti sistematici a Google

Google Analytics, in tutte le sue versioni, trasferisce sistematicamente i dati personali che raccoglie a Google. **By design and by default**.[4]

[4] Si veda, per approfondire, l'Allegato Tecnico alla segnalazione inviata al Garante italiano da Monitora PA https://monitora-pa.it/2022/06/22/Allegato-Tecnico.pdf

Tali trasferimenti sistematici sono strumentali alle attività di profilazione e manipolazione cognitivo-comportamentale individuale su larga scala che Google notoriamente conduce attraverso la sua tecnologia AdTech.

Chi sostiene che Google Analytics non sia sostituibile con le decine di alternative open source disponibili lo fa proprio sulla base della strettissima integrazione fra tale strumento sorveglianza e la piattaforma di AdTech controllata da Google stessa.

Dunque sostenere che Google Analytics non sia sostituibile sulla base dei ritorni economici garantiti da tale manipolazione di massa è in diretta contraddizione logica con l'affermazione che il trasferimento di dati verso Google non sia sistematico by design.

Ora sappiamo tutti bene che il consenso dell'utente non può essere utilizzato come base giuridica per trasferimenti sistematici verso aziende statunitensi. E tale consenso non è comunque stato richiesto per i trasferimenti avviati prima della stessa accettazione, con lo scaricamento dei Google Fonts, che sono altrettanto sistematici in quanto avvengono sempre ed automaticamente alla visita delle vostre pagine Web.

La compromissione della confidenzialità e il conseguente data breach

Da un punto di vista informatico siamo di fronte ad un vero e proprio **data breach**: ai visitatori del vostro sito sembra essere impedito un effettivo controllo sui propri dati personali che vengono sistematicamente esposti all'accesso terze parti non autorizzate, come le agenzie governative statunitensi, senza consapevolezza degli interessati e senza una base giuridica.

Ne risulta una **grave compromissione della riservatezza delle comunicazioni** con il vostro Studio Legale.

Non era mia intenzione informare Google della mia visita presso il vostro Studio: volevo solo leggere la risposta che suggerite ai vostri clienti di inviare a Federico. Dopo il comunicato del Garante italiano generosamente portato alla vostra attenzione da Federico Leva, mai mi sarei potuto aspettare di incappare ancora in trasferimenti verso Google sul vostro sito web.

Sull'articolo 28 del GDPR e le responsabilità dei Titolari

Giova ricordare a questo punto il primo comma dell'articolo 28 del GDPR:

> Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato

Da due anni sappiamo tutti che i trasferimenti verso Google e tutte le altre aziende statunitensi sono gravati da una normativa incompatibile con i diritti degli interessati.

Google dunque non rientra nell'insieme dei fornitori cui un Titolare può affidare i dati degli interssati.

Come si conciliano la scelta di usare (e continuare ad usare, per due anni) Google come data processor e questo articolo del GDPR?

Le alternative non mancano: installare i font sul vostro server e farli scaricare da esso avrebbe evitato che Google venisse informato di ogni visita effettuata presso di voi, arricchendo i profili cognitivo-comportamentali tramite cui manipola i nostri concittadini.

E le alternative open source a Google Analytics sono così numerose che non saprei dove iniziare per elencarle. Matomo? AWStat? Plausible? Sono moltissime, ciascuna installabile gratuitamente sui vostri server.

Richiesta di esercizio dei diritti garantiti dal GDPR

Come Federico vi devo chiedere di esercitare alcuni miei diritti.

Ho visitato il vostro sito per circa 10 minuti intorno alle 16:50 del 30 Luglio 2022. Il mio IP era nella classe 93.41.0.0/16. Lo User Agent del mio browser era

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/123.00
(KHTML, like Gecko) Chrome/1984.6.6.6 Safari/123.00
```

Queste informazioni dovrebbero fornire bit di entropia sufficienti ad identificare la mia navigazione con precisione, anche in presenza di migliaia di visitatori simultanei nella stessa fascia oraria.

Vi chiedo dunque, ai sensi degli artt. 12, 13, 14, 15 e 17 del Regolamento (UE) 2016/679:

- se trasferite direttamente (a dei responsabili del trattamento) o indirettamente (a dei responsabili del trattamento che trasferiscono a dei subresponsabili del trattamento) dati personali al di fuori dell'Unione Europea ai sensi dell'art. 45 del GDPR e, se sì, verso quali paesi terzi e/o organizzazioni internazionali
- su quali
  (i) decisioni di adeguatezza ai sensi dell'articolo 45, paragrafo 3,
  (ii) garanzie adeguate ai sensi dell'articolo 46, o
  (iii) altre condizioni ai sensi dell'art. 49 del GDPR è basato ciascuno dei trasferimenti di dati personali che realizzate al di fuori dell'Unione Europea,

- se, oltre Google, utilizzate altri responsabili e/o subresponsabili del trattamento statunitensi, se questi ultimi siano o meno soggetti agli obblighi previsti dal FISA Section 702, dall'Executive Order 12.333 o da altre norme che possono indebolire la protezione dei dati personali prevista dal GDPR
- di ricevere attraverso una semplice mail cifrata (allego la mia chiave PGP corrente), copia di tutti i dati che mi riguardano trattati sotto la vostra responsabilità, inclusi log registrati dal web server HTTP del vostro sito, in un formato standard a vostra scelta.
- di cancellare, ai sensi dell'articolo 17 comma 1 punto (d), da tutti server del vostro fornitore Google:
  - i dati personali che mi riguardano ricevuti da Google per effetto dell'inclusione di risorse fornite da Google Fonts sulla vostra home page e sulle pagine che ho visitato
  - i dati personali che mi riguardano trasmessi a causa dell'inclusione degli script di Google Analitics sul vostro sito, eseguiti sul mio computer senza il mio esplicito e consapevole consenso.
- di interrompere subito qualsiasi trasferimento presso aziende sottoposte a normative incompatibili con i diritti dei cittadini europei o, in alternativa, di adottare efficaci misure **tecniche** supplementari che rendano inaccessibili i dati personali dei visitatori a tali aziende, ad esempio rendendo il vostro sito accessibile esclusivamente dalla rete Tor e rimuovendo qualsiasi form ivi presente che richieda dati personali (come moduli di contatto o per la sottoscrizione di newsletter).

Inoltre, laddove l'analisi tecnica effettuata dai vostri consulenti informatici a valle della mia segnalazione confermasse il trasferimento non autorizzato di dati personali dei vostri visitatori verso Google o l'esecuzione non autorizzata di software potenzialmente personalizzato dalla stessa azienda sul browser di detti utenti, vi esorto

- a notificare il data breach occorso all'Autorita Garante per la Protezione dei Dati Personali nei termini previsti dal articolo 33 del GDPR
- a comunicare ai visitatori del vostro sito suddetto data breach, caratterizzato dalla perdita di controllo sui propri dati personali che la presenza di Google Font e Google Analytics sullo stesso ha loro causato, nei termini dell'articolo 34 del GDPR.

  Vi prego di non sottovalutare il rischio di compromissione della libertà e dei diritti dei vostri visitatori, elevatissimo e per diverse ragioni:

  - **ogni nuovo bit** raccolto da Google **duplica (almeno) l'efficacia della manipolazione cognitivo-comportamentale** che Google può effettuare su di essi (individualmente e collettivamente) e sulle persone che presentano le stesse caratteristiche negli aspetti rilevanti

per ogni singola previsione comportamentale (behavioural future); questa crescita esponenziale comporta di per sé una forte riduzione dell'autonomia e della libertà effettiva degli utenti stessi ed un danno enorme per la nostra Democrazia

- la Legge statunitense impedisce a Google di comunicare ai Titolari tutti gli accessi ai dati personali dei vostri utenti che permette routinariamente per le agenzie governative USA e dunque qualsiasi vostra valutazione in merito è condannata a sottostimare gravemente tale rischio
- cittadini dodati di coscienza civica e cibernetica (definiti genericamente "attivisti"), come Federico e me, sono particolarmente esposti ad intromissioni illecite nella propria vita privata da parte di agenzie di intelligence e società private come evidenziato da diverse ricerche e rivelazioni recenti [5]
- tali rischi però esistono per moltissime categorie di cittadini che visitano il vostro sito, inclusi politici, avvocati, sindacalisti, DPO, imprenditori ed intellettuali che considerano come punto di riferimento il vostro autorevole Studio Legale [6]

Qualora la vostra valutazione dei rischi per gli interessati vi facesse decidere di non informarli del data-breach, vi chiedo di condividere pubblicamente tale valutazione, così che tutti possiamo imparare da essa i criteri che uno Studio Legale della vostra levatura adotta nella protezione dei diritti cibernetici dei propri concittadini.

Qualora invece l'analisi tecnica dei vostri consulenti informatici non evidenziasse i trasferimenti che ho registrato durante la mia visita, vi chiedo di condividerne il rapporto completo, in modo da potermi liberare, dopo averne verificato la correttezza, da ogni preoccupazione sull'uso che Google o il Governo degli Stati Uniti potrebbero fare dei miei dati personali.

Per quanto sia improbabile che ciò si renda necessario, ritengo opportuno anticiparvi sin d'ora, ad ogni buon conto, che nonostante l'enorme stima e il rispetto che nutro per il vostro Studio e per la vostra storia, in difetto di ottemperanza nei termini di Legge o qualora mi fosse nuovamente impedito di esercitare un pieno controllo sui miei dati personali come già avvenuto durante la prima visita al vostro sito, sarò costretto a presentare un reclamo presso l'Autorità Garante per la Protezione dei Dati Personali.

[5] Subversion Inc: The Age of Private Espionage https://www.journalofdemocracy.org/articles/subversion-inc-the-age-of-private-espionage/

[6] EU found evidence employee phones compromised with spyware https://www.reuters.com/technology/exclusive-eu-found-evidence-employee-phones-compromised-with-spyware-letter-2022-07-27/

Conclusione

Spero che vorrete rispondere puntualmente a ciascuna di queste domande che vi pongo sia come cittadino cibernetico (hacker), sia come soggetto interessato ai trattamenti ed ai trasferimenti effettuati dal vostro sito.

Confido nella vostra pazienza e comprensione laddove le mie affermazioni giuridiche non fossero rigorose quanto quelle informatiche: sono un hacker, non un giurista, per cui sentitevi liberi di correggermi pubblicamente.
Sarà per me un'occasione per imparare cose nuove ponendo nuove domande.

Come detto, contrariamente a Federico Leva, vi autorizzo e vi invito a pubblicare la vostra risposta anche sul vostro sito (senza riportare i dati personali in calce) giacché pubblicherò io stesso questa missiva sul sito di Monitora PA.

In Fede

Giacomo Tesio
Co-fondatore di Monitora PA
https://monitora-pa.it