Spett.le
Garante per la protezione dei dati personali
Piazza Venezia 11
00187 – Roma

A mezzo PEC: protocollo@pec.gpdp.it

e, p.c.,
Spett.le
Autorità Nazionale Anticorruzione
c/o Palazzo Sciarra,
Via Minghetti, 10
00187 Roma

A mezzo PEC: protocollo@pec.anticorruzione.it

Lecce, 22 settembre 2022

Oggetto: segnalazione ai sensi dell'art. 144 del d. lgs. n. 196/2003

Segnalazione ai sensi dell'art. 144 del D.Lgs. n. 196/2003

Sommario

I. SCOPO E OGGETTO DEL PRESENTE DOCUMENTO 4

II. CONTESTO ECONOMICO E OPERATIVO DI RIFERIMENTO 5

1. La posizione dominante delle aziende statunitensi nel mercato italiano (ed europeo) 6

2. Lo strapotere contrattuale di GAFAM 8

III. TRASFERIMENTO DI DATI PERSONALI VERSO GLI STATI UNITI A SEGUITO DELLA SENTENZA SCHREMS II: NECESSARIA CHIAREZZA PER GLI UTILIZZATORI DEI SERVIZI FORNITI DAGLI OTT 9

1. Premessa 9

2. Brevi riflessioni sulle responsabilità delle organizzazioni che usufruiscono dei servizi erogati da GAFAM 10

IV. PROFILI DI CRITICITÀ INERENTI ALLE RECENTI AZIONI DEGLI ATTIVISTI 13

1. Sintesi delle recenti azioni degli autodefiniti "attivisti" 13

2. Caratteristiche in comune 16

2.1 Assenza di interazione umana sia nelle visite ai siti web che nei controlli sugli effettivi trasferimenti dei dati 16

2.2 Richiesta perentoria di rimozione dei servizi Google – formulata dagli "attivisti" ai Titolari/gestori dei siti web come sola e unica condizione possibile per evitare ulteriori azioni, tra cui la segnalazione all'Autorità 17

2.3 Istanze copia-incolla - non specifiche per casi/Titolari 17

2.4 Nelle comunicazioni massivamente inviate non sono state fornite ai Titolari informazioni in merito all'adeguatezza dei trattamenti effettuati dai c.d. attivisti 18

3. I rischi insiti in tali azioni 19

3.1 Profili di dubbia liceità e pericoli per gli stessi attivisti 19

3.1.1 Trattamento dei dati in relazione alle istanze 20

3.1.2 Controlli non coerenti - falsi positivi 21

3.2 Pericoli per le organizzazioni, gli enti e le aziende bersaglio di tali azioni 21

3.3 Pericoli per la percezione diffusa delle norme e dei diritti contenuti nel RGPD 22

3.4 Pericoli per la crescita della micro-imprenditoria 22

3.5 Pericoli per il mercato 23

3.6 Pericoli per l'Autorità Garante 25

4. Ulteriori elementi di riflessione 25

4.1 Chi tratta i dati? Per quali finalità? 25

4.2 Abuso dell'esercizio di un diritto 26

V. L'AUSPICATO INTERVENTO DEL GARANTE 29

I. SCOPO E OGGETTO DEL PRESENTE DOCUMENTO

Con il presente documento si intende sottoporre all'attenzione di Codesta Autorità Garante per la protezione dei dati personali alcune questioni sottese a due diverse tematiche che, seppur tra loro giuridicamente indipendenti, si ritiene utile – a beneficio della stessa Autorità e degli altri soggetti a vario titolo interessati – esporre contestualmente in quanto afferenti a fatti e circostanze tra loro concatenati.

La **prima tematica** – sviluppata nel par. 1 – è da ricondursi sostanzialmente nell'alveo della normativa in materia di **trasferimento di dati personali verso paesi terzi**. In mancanza di una nuova decisione di adeguatezza che renda leciti i trasferimenti di dati personali dall'Unione europea verso gli Stati Uniti, e a cui si auspicava potesse addivenirsi a seguito della **sentenza C-311/18 (c.d. Sentenza Schrems II) emanata dalla Corte di giustizia dell'Unione europea**, professionisti, imprese, enti e organizzazioni italiane pubbliche e private, che intrattengono rapporti con fornitori statunitensi, si trovano oggi in una situazione di incertezza, dovuta anche al **rischio che di tale sentenza venga data una interpretazione arbitrariamente estensiva, dagli esiti impropri e distorsivi**.

In tal senso, si ritiene che tale situazione meriti un intervento chiarificatore e generalizzato da parte di Codesta Autorità Garante, che potrebbe ad esempio consistere nella formulazione di indicazioni e linee guida di carattere generale, a supporto di organizzazioni, enti, società, operatori economici e tutti i soggetti giuridici che trattino dati personali, in qualità di Titolari o di responsabili del trattamento, e soprattutto che tengano in debita considerazione anche la reale ed effettiva situazione del mercato dei servizi IT in cui tali soggetti operano.

La **seconda tematica** – che si affronta nel par. 2 del presente documento – riguarda, invece, **alcune azioni di attivisti che, singolarmente o organizzati in gruppo, hanno di recente coinvolto in maniera automatizzata, indiscriminata e, ad avviso di chi scrive, illegittima sotto diversi aspetti**, un numero elevatissimo di soggetti, proprio

facendo leva su quanto stabilito dalla Sentenza Schrems II, proponendone un'interpretazione arbitrariamente estensiva e dagli effetti giuridicamente distorsivi, di fatto non ragionevolmente sostenibile. Con il presente documento intendiamo, peraltro, segnalare all'Autorità tale fenomeno, evidenziandone alcuni **profili di potenziale illiceità**, o quantomeno di criticità, e chiedendo a Codesta Spettabile Autorità di volerli valutare e di voler intraprendere le opportune iniziative, affinché azioni di "attivismo digitale" siano condotte nel rispetto dei diritti e delle libertà delle persone fisiche, nonché secondo i **principi fondamentali generali di buona fede e correttezza che permeano il nostro ordinamento**, dunque senza trascendere illegittimamente nell'**abuso dell'esercizio dei diritti** attribuiti dall'ordinamento stesso.

In tal senso, infatti, giova ricordare che tutte le norme – comprese quelle di derivazione europea sulla protezione dei dati – devono essere interpretate e attuate alla luce del complesso dei principi fondamentali inderogabili dell'ordinamento.

Oltre a tali profili, come meglio si specificherà nei paragrafi successivi, occorre, altresì, considerare che **le particolari modalità automatizzate con cui sono state attuate alcune azioni dimostrative di "attivismo digitale"** (di cui si dirà di seguito) **risultano avere il paradossale effetto di presentare profili di violazione proprio delle norme del Regolamento (UE) 679/2016 (di seguito "RGPD" o "Regolamento"), in particolare, dell'art. 22**.

II. CONTESTO ECONOMICO E OPERATIVO DI RIFERIMENTO

Una proficua trattazione dei temi sopra introdotti richiede un preliminare inquadramento del contesto socioeconomico in cui generalmente operano le aziende italiane ed europee (Titolari o responsabili del trattamento, nella misura in cui trattino dati personali nell'ambito delle loro attività).

Proprio dal contesto di riferimento, infatti, non dovrebbe potersi prescindere in fase di interpretazione e applicazione del diritto alla protezione dei dati personali e, per quanto qui di maggiore interesse, in fase di interpretazione e applicazione della Sentenza Schrems II, tanto più in una situazione, quale quella attuale, potenzialmente in grado di esplicare impatti devastanti sul piano economico e sociale.

Nel presente paragrafo, quindi, si intende provare a illustrare brevemente, in chiave riflessiva, alcuni degli aspetti caratterizzanti il quadro socioeconomico di riferimento, ponendo particolare attenzione sui seguenti, di importanza cruciale ai nostri fini:

- la tipologia del rapporto tipicamente intercorrente tra i professionisti, le imprese, gli enti e le organizzazioni italiane ed europee da una parte, e i grandi player che offrono piattaforme, applicazioni e altri servizi informatici e che sono soggetti alla normativa statunitense, dall'altra;

- la difficoltà, per la generalità dei soggetti operanti in Italia e in Europa, di reperire sul mercato valide e concrete soluzioni alternative ai servizi sviluppati dai fornitori di cui sopra e in grado di offrire così analoghi servizi idonei a garantire livelli altrettanto soddisfacenti di efficienza, economicità, capacità di integrazione con altri servizi IT.

1. La posizione dominante delle aziende statunitensi nel mercato italiano (ed europeo)

L'erogazione dei servizi IT in Italia, e più in generale in Europa, si concentra nelle mani di poche grosse aziende, tutte facenti parte di gruppi societari le cui società controllanti hanno sede legale negli Stati Uniti. Il riferimento è, in particolare, a Google, Apple, Facebook (oggi Meta), Amazon, Microsoft, da cui l'acronimo "**GAFAM**". Tali aziende offrono servizi in ambito IT, destinati alla vita privata e professionale, e dei quali

usufruiscono pressoché la totalità dei cittadini, oltre che tutte le categorie di aziende e di professionisti, in qualunque settore dell'economia.

La scelta di detti servizi è spesso, di fatto, obbligata, per professionisti, imprese, enti e organizzazioni pubbliche e private. Ciò per almeno due ordini di ragioni:

i) l'esigenza di raggiungere agevolmente una vasta platea di utenti e comunicare agevolmente con i fruitori dei servizi. Ciò vale, ad esempio, per l'utilizzo delle piattaforme social: lo stesso Garante per la protezione dei dai personali, d'altronde, è attivamente presente su tutti i principali social network per comunicare con una vasta platea di soggetti, anche minori;

ii) per via della posizione dominante che hanno acquisito sul mercato di riferimento, e dell'elevato grado di *expertise* nel settore IT – rafforzatisi nel tempo in maniera esponenziale e sempre più irreversibile –, professionisti, imprese, enti e organizzazioni non hanno spesso altre opzioni ragionevolmente considerabili, sotto il profilo dell'efficienza dei servizi. O meglio, non dispongono di soluzioni alternative valide e concrete, che diano loro almeno pari garanzie in termini di sicurezza, economicità, facilità d'uso, efficienza, integrazione con altri servizi IT, anche in considerazione dell'effetto di rete che interessa molte delle soluzioni offerte da GAFAM, diffuse capillarmente su tutto il territorio nazionale. E quelli di economicità ed efficienza, peraltro, sono criteri che devono ispirare l'operato delle pubbliche amministrazioni, e la cui osservanza risulta preziosa anche per qualsiasi operatore economico. A tal proposito, non si deve inoltre trascurare che l'adozione di strumenti e servizi alternativi a quelli offerti da GAFAM richiede talvolta importanti (e non sempre giustificabili) investimenti da parte dei soggetti che ne usufruiscono, sia in termini di risorse e di competenza, sia in termini più prettamente finanziari. E in molti casi sforzi simili non sono verosimilmente ponderabili, a maggior ragione nel contesto di crisi economica attuale. Giova evidenziare come il tessuto economico italiano è costituito per la maggior parte da

microimprese aventi da 1 a 9 addetti (Rapporto ISTAT sulle imprese 2021 – Struttura, comportamenti e performance dal censimento permanente[1]).

2. Lo strapotere contrattuale di GAFAM

A quanto sopra indicato si aggiunga – ma in parte ne è una conseguenza – che il rapporto contrattuale intercorrente tra le grandi aziende operanti nel mondo IT e chi di esse si avvale per ragioni professionali, economiche o istituzionali è contraddistinto da un fortissimo squilibrio contrattuale che pende vistosamente a favore delle prime.

Aziende, enti, organizzazioni e professionisti che utilizzano i servizi erogati da GAFAM (ma ciò può valere in generale per i servizi offerti da tanti altri operatori nel settore IT) non possono che limitarsi a scegliere se aderire o meno alle condizioni contrattuali offerte dall'altra parte. E ciò vale anche con riferimento alle condizioni contrattuali che impattano, più o meno direttamente, sul trattamento di dati personali. Il cliente – ipotizziamo agisca esso in qualità di Titolare del trattamento – pacificamente non è nelle condizioni di poter imporre a soggetti quali Google, Microsoft, etc. alcuna condizione contrattuale, o clausola personalizzata (per esempio finalizzata a rafforzare le misure di sicurezza offerte), così come non è in grado di imporre alcuna istruzione su come trattare i dati personali, potendo anche qui limitarsi a scegliere tra le opzioni eventualmente offerte dal provider. Può, invece, questo sì, selezionare il provider in base alle garanzie offerte, anche in termini di protezione dei dati personali.

[1] Il documento integrale è reperibile al seguente link: https://www.istat.it/storage/rapporti-tematici/imprese2021/Rapportoimprese2021.pdf. In particolare, il citato Rapporto ISTAT rileva come nel 2019 "in Italia erano attive quasi 4,4 milioni di imprese non agricole, con 17,4 milioni di addetti. Oltre il 60% delle imprese aveva al più un solo addetto (in genere ditte individuali con il Titolare lavoratore indipendente), e un ulteriore terzo della popolazione erano microimprese tra i 2 e i 9 addetti; questi due segmenti insieme occupavano circa 7,5 milioni di addetti. Le piccole imprese, tra i 10 e i 49 addetti erano quasi 200 mila e quelle medie e grandi 28mila, cioè meno dello 0,7% […]".

Muovendo da tale contesto di operatività, si procede con una sintetica trattazione delle due tematiche inizialmente introdotte.

III. TRASFERIMENTO DI DATI PERSONALI VERSO GLI STATI UNITI A SEGUITO DELLA SENTENZA SCHREMS II: NECESSARIA CHIAREZZA PER GLI UTILIZZATORI DEI SERVIZI FORNITI DAGLI OTT

1. Premessa

Come noto, la Corte di giustizia dell'Unione europea, con la sentenza C-311/18 (c.d. Sentenza Schrems II), ha invalidato la decisione di adeguatezza relativa allo "scudo per la privacy", sulla quale sostanzialmente si fondava la liceità dei trasferimenti di dati personali dai Paesi membri dell'UE verso gli Stati Uniti. Ad avviso della Corte, la normativa interna degli Stati Uniti non presenta un livello adeguato di protezione dei dati personali, nella misura in cui rende possibile l'accesso da parte delle autorità pubbliche statunitensi, per finalità di sicurezza nazionale, ai dati personali trasferiti dall'Unione europea agli Stati Uniti. Il quadro diviene più complesso ove si consideri che, in base al combinato disposto di specifiche norme, potrebbero risultare oggetto di potenziale accesso da parte delle autorità pubbliche statunitensi anche i dati detenuti da soggetti controllati da società con sede negli Stati Uniti, seppur archiviati su server localizzati su territorio UE.

Tuttavia, occorre necessariamente considerare che i risvolti di un'applicazione di detto provvedimento che non sia frutto di una corretta interpretazione delle norme che richiama potrebbe comportare il rischio di porre milioni di professionisti, imprese, enti e organizzazioni - Titolari del trattamento, operanti sul territorio nazionale ed europeo

- di fronte a problematiche di fatto non risolvibili, se non mediante azioni drastiche e intransigenti, consistenti a ben vedere nella rinuncia all'utilizzo di servizi IT – oggi difficilmente sostituibili – forniti da società con sede legale negli Stati Uniti o anche semplicemente controllate da società statunitensi, con **conseguenti pregiudizi che simili azioni comporterebbero in termini di libera circolazione dei dati e delle informazioni, quindi dello sviluppo del mercato in termini di competitività su scala globale**.

2. Brevi riflessioni sulle responsabilità delle organizzazioni che usufruiscono dei servizi erogati da GAFAM

Alla luce del contesto economico e operativo di riferimento sopra brevemente delineato, in un rapporto che tipicamente intercorre tra i menzionati provider operanti su scala globale e i soggetti che vi ricorrono, sfugge del tutto al controllo di questi ultimi l'utilizzo che tali provider decide di fare con riguardo ai dati personali trattati al fine di erogare il servizio richiesto.

A maggior ragione, pertanto, **nella misura in cui un provider** (eventualmente anche per ottemperare al rispetto della normativa statunitense) **decida di trattare dati personali per finalità non riconducibili a quelle perseguite dal soggetto che si avvale dei suoi servizi** (ad esempio, decida di comunicare i dati personali alle autorità pubbliche statunitensi per ottemperare a una loro richiesta) – così violando di conseguenza il Regolamento (UE) 2016/679 – **tale provider dovrebbe risponderne in qualità di Titolare autonomo del trattamento, ai sensi dell'art. 28, par. 10 dello stesso, oltre che – eventualmente – a livello di responsabilità contrattuale, qualora abbia anche garantito contrattualmente al cliente di trattare esclusivamente tramite server allocati in territorio UE i dati oggetto del servizio IT erogato in favore di quest'ultimo**.

In un rapporto siffatto, tra gli obblighi del Titolare del trattamento che decide di avvalersi di un provider IT, dovrebbe darsi prevalenza **all'obbligo di effettuare tale scelta in base alle garanzie contrattuali da questo offerte** (poiché solo qualora le garanzie contrattuali fornite fossero inidonee o insufficienti si potrebbe valutare la sussistenza di una responsabilità del Titolare del trattamento per non aver attentamente ponderato le misure di sicurezza offerte dal provider IT, in ossequio al principio della **c.d. "culpa in eligendo"**).

Tale obbligo, tuttavia, non può avere come corollario l'obbligo per il Titolare di dover opporre un automatico rifiuto di un determinato provider IT, o di un determinato servizio da questi fornito, per il solo fatto che il provider in questione potrebbe dover soddisfare una richiesta di accesso ai dati trattati (anche su server europei) di interessati al trattamento residenti in UE proveniente da autorità statunitensi per il perseguimento di rilevanti finalità di sicurezza nazionale.

Sul tema, risulta necessario evidenziare che **non appare trascurabile la distinzione – giuridica e fattuale – tra potenziale "accesso" e "trasferimento" dei dati, nonché risulta parimenti per nulla irrilevante l'eventuale circostanza per cui il servizio IT, che preveda il trattamento dei dati personali, sia contrattualizzato dal Titolare del trattamento con società provider di diritto europeo** (come risulta dal fenomeno che di recente si registra sul mercato europeo dei servizi IT), anche qualora questa sia controllata o appartenente allo stesso gruppo di imprese di una società di diritto statunitense. **In tal caso, infatti, non potrebbero ignorarsi le norme del diritto internazionale, per cui un'autorità pubblica estera non potrebbe obbligare un soggetto giuridico di un altro Stato a consentire l'accesso o a trasferire dati o documenti a tale autorità, senza esperire preventivamente una rogatoria internazionale**[2].

[2] Sul punto, si segnala il report reperibile al seguente link: https://d1.awsstatic.com/certifications/Information_Request_Report_H1_2022.pdf, dal quale emergerebbe che nessun documento collocato al di fuori degli Stati Uniti sia stato consegnato al governo statunitense nel periodo intercorrente tra gennaio 2022 e giugno 2022. Tale circostanza, in ottica di accountability, sembra

È necessario, peraltro, che le predette circostanze, tra cui, in primis, le misure di sicurezza o le diverse garanzie contrattualmente assicurate dal provider, siano prese in considerazione dal Titolare del trattamento anche **nell'analisi del rischio svolta in fase di selezione del provider IT**, e che – in tal senso – sia dato doveroso rilievo al **principio di accountability**, che altrimenti rischierebbe di diventare lettera morta.

Per contro, un'automatica attribuzione di responsabilità sul singolo titolare del trattamento, a cui di fatto sono pressoché imposte le condizioni contrattuali da parte dei grandi provider IT e che non ha realmente la possibilità di verificare o effettuare audit sull'operato di tali soggetti, **dovrebbe portare a considerare non ascrivibile al cliente, Titolare del trattamento, anche la responsabilità derivante da c.d. "culpa in vigilando", poiché risulta di fatto impossibile effettuare nei confronti di tali grandi provider IT (c.d. GAFAM) ad es. attività di audit o di controllo.** Diversamente, in riferimento alle garanzie offerte contrattualmente, un'automatica attribuzione di responsabilità sul singolo Titolare del trattamento non sembra essere risolutiva del problema, che **invece sarebbe forse opportuno e corretto affrontare direttamente con le aziende GAFAM, incentivandole ad agire conformemente alla normativa in materia di protezione dei dati personali** e più nello specifico, se del caso, **imponendo a queste ultime di implementare misure di sicurezza appropriate e ulteriori**, in quanto **unici, effettivi e autonomi Titolari del trattamento, per quanto concerne le comunicazioni di dati extra UE non contrattualizzate (o non autorizzate)**.

deporre a favore dell'efficacia della misura organizzativa - prevista nelle clausole della documentazione contrattuale del servizio IT scelto dal Titolare del trattamento - che vincola il provider a trattare i dati personali, per conto del Titolare, solo in Paesi UE..

IV. PROFILI DI CRITICITÀ INERENTI ALLE RECENTI AZIONI DEGLI ATTIVISTI

1. Sintesi delle recenti azioni degli autodefiniti "attivisti"

Come accennato in premessa, di recente si sono registrate alcune azioni di gruppi o singoli soggetti – talvolta autodefinitisi "attivisti digitali" – che hanno coinvolto in maniera automatizzata, indiscriminata e anche potenzialmente illegittima, un numero elevatissimo di professionisti, imprese, enti e organizzazioni italiane, proprio facendo leva su quanto stabilito dalla Sentenza Schrems II, **provando ad imporne un'interpretazione arbitrariamente estensiva e dagli effetti giuridicamente distorsivi, in alcuni casi mediante espressa minaccia** – formulata contro i soggetti che non avessero accontentato le loro richieste – **di porre in essere ulteriori azioni, tra cui la segnalazione alle Autorità competenti**.

Il riferimento è, in particolare, alle iniziative che di seguito sono riportate in ordine cronologico, a partire dalla meno recente.

i) Monitora-PA e le migliaia di richieste a mezzo PEC inviate alla pubblica amministrazione, aventi ad oggetto la richiesta di rimozione di Google Analytics

La prima iniziativa, e per certi aspetti forse la più rilevante, è quella promossa da Monitora-PA, sul cui sito internet (https://monitora-pa.it/) è possibile reperire ogni dettaglio. In sintesi, essa si può descrivere come una scansione massiva e sistematica di tutti i siti riconducibili alla pubblica amministrazione i cui gestori, nel caso in cui il sito integri Google Analytics, sono stati raggiunti da comunicazioni massive automatizzate contenenti richieste di rimozione e annuncio di segnalazione all'autorità Garante per asserito trattamento illecito. Questa iniziativa ha generato 7.833 PEC alle PA.

ii) L'e-mail di Federico Leva, sempre su Google Analytics

Tale iniziativa è stata seguita da quella portata avanti da un singolo attivista, il signor Federico Leva, e che ha interessato sia soggetti pubblici sia soggetti privati.

In questo caso, l'iniziativa consiste in scansioni automatizzate basate sul sistema "webbkoll" (sessioni di durata 0, istantanee e costituite da una mera richiesta da parte di un server, senza interazione umana) di cui sono stati destinatari 500.000 siti tra il 1° giugno e il 4 luglio 2022.

Si specifica che tali scansioni effettuate automaticamente su iniziativa di Leva hanno colpito indiscriminatamente siti sia di enti pubblici sia di soggetti privati, comprese medie/piccole/microimprese e soggetti operanti sul web per finalità non professionali.

Sulla base di queste scansioni effettuate tramite sistemi automatizzati, sono state inviate massivamente – e trattando tali indirizzi e-mail sempre mediante sistemi automatizzati – altrettante segnalazioni ai gestori dei siti internet, contenenti tra l'altro l'avviso della necessità di eliminare Google Analytics e la richiesta di provvedere a un riscontro all'interessato consistente nella rimozione dei dati personali del segnalante da Google Analytics.

Questi fatti sono documentati sul sistema Zenodo Version 2 con file CSV con elenco siti e timestamp degli accessi.

iii) Monitora-PA e le richieste relative a Google Fonts

A distanza di pochi giorni dal messaggio di Federico Leva, la comunità di attivisti che fa capo a Monitora-PA, rappresentata da uno dei suoi esponenti, ha intrapreso una nuova battaglia, inviando a migliaia di enti pubblici un messaggio PEC inteso a segnalare la pretesa illegittimità di Google Fonts, con l'invito a provvedere alla rimozione dello strumento "*e di qualsiasi altra risorsa incorporata nel suddetto sito web che produca effetti analoghi*". A differenza delle comunicazioni inviate da Federico Leva, peraltro, questo secondo invio automatizzato e massivo di messaggi PEC ha avuto come unico obiettivo quello di indurre gli enti destinatari a "*ottemperare*" alla

richiesta di rimozione di Google Fonts, con l'avvertimento che, in mancanza, si "*sarebbero visti costretti*" a segnalare la ritenuta violazione a codesta Spett.le Autorità. In questo caso, dunque, non è stata formulata alcuna richiesta di esercizio dei diritti riconosciuti dal RGPD, restando, invece, i toni perentori e intimidatori e le velleità epurative.

iv) Lo "Speciale Elezioni 2022"

Di recente, Monitora PA ha messo in atto una campagna di denuncia nei confronti di oltre 60 partiti politici italiani che incorporano, sui propri siti web, Google Analytics e/o Google Fonts. L'obiettivo, anche in questo caso, è stato quello di intimare l'interruzione di ogni trasferimento di dati personali verso Google LLC "*o altra società sottoposta a normative incompatibili con i diritti fondamentali dei cittadini italiani ed europei*". Nelle comunicazioni inviate ai partiti politici, inoltre, i trasferimenti di dati personali dovuti all'utilizzo di Google Fonts e di Google Analytics sono addirittura qualificati come data breach, scaturendone la richiesta di procedere alla notifica e alla comunicazione della asserita violazione ai sensi degli artt. 33 e 34 del RGPD. Come nei casi precedenti, è stato inserito l'avvertimento che, a fronte della mancata rimozione degli strumenti di Google entro 10 giorni dalla ricezione della comunicazione, sarebbe seguita una segnalazione a codesta Spett.le Autorità.

v) Le 8.254 domande alle Scuole Italiane

Da ultimo, Monitora PA ha avviato un'azione di "accesso civico generalizzato" sempre in modo automatizzato, richiedendo via PEC a più di 8.000 istituti scolastici italiani l'esibizione di diversa documentazione in grado di attestare la legittimità nell'utilizzo di strumenti di comunicazione elettronica e di videoconferenza, con lo spirito – si legge nel loro comunicato – di aiutarli "a comprendere sia i gravi danni che l'uso di piattaforme di sorveglianza per la didattica causa a studenti, insegnanti e genitori

(nonché a tutta la società), sia i notevoli rischi legali che la loro adozione comporta per i Dirigenti scolastici"[3].

2. Caratteristiche in comune

Per tali iniziative, seppur a fronte delle differenze di tenore/tipologia nelle istanze, si riscontrano i seguenti fattori comuni e costanti:

2.1 Assenza di interazione umana sia nelle visite ai siti web che nei controlli sugli effettivi trasferimenti dei dati

Le operazioni sono state dichiaratamente effettuate esclusivamente in modo automatizzato da script/bot all'uopo utilizzati, senza alcuna interazione umana.

Non risultano esserci stati, dunque, operazioni effettuate direttamente e personalmente dagli utenti/persone fisiche durante le visite ai siti web (lettura informative/consensi e gestione delle scelte), né tantomeno verifiche puntuali effettuate da utenti/persone fisiche atte a porre in essere salvaguardie addizionali in favore dei Titolari e gestori dei siti web (es. esclusione falsi positivi) sui dati acquisiti a seguito delle operazioni automatizzate effettuate.

Inoltre, non viene fornita alcuna prova documentata del trasferimento di dati personali in atto, che viene semplicemente dato per scontato.

[3] Ognuna di queste azioni è puntualmente descritta sul sito di Monitora PA: http://monitora-pa.it/

2.2 Richiesta perentoria di rimozione dei servizi Google – formulata dagli "attivisti" ai Titolari/gestori dei siti web come sola e unica condizione possibile per evitare ulteriori azioni, tra cui la segnalazione all'Autorità

Gli "attivisti" – anche per questioni più ideologiche che tecniche – non prendono in considerazione la possibilità di salvaguardie addizionali da parte dei Titolari, mediante l'implementazione di misure tecniche adeguate al controllo o all'anonimizzazione dei dati (es. proxyficazione delle richieste inoltrate a server/endpoint Google), o – comunque – di garanzie informative che con trasparenza abbiano dato atto nelle policy del sito web dell'eventuale e possibile trasferimento di dati extra UE agli utenti.

Peraltro, non vi è da parte di tali "attivisti" un legittimo invito ai Titolari affinché effettuino – semmai – le valutazioni/verifiche di adeguatezza (es. DPIA/DTIA e salvaguardie addizionali) per quanto riguarda il trasferimento dei dati – secondo le linee guida ed indicazioni rilasciate da EPDB e da codesta Spettabile Autorità.

2.3 Istanze copia-incolla - non specifiche per casi/Titolari

In virtù sia del ricorso ai soli script/bot che hanno acquisito dati in modo automatizzato, che della finalità primaria (intimazione alla pronta rimozione dei servizi il cui utilizzo viene definito arbitrariamente *ex se* "illegittimo") delle comunicazioni massivamente inviate – sempre in maniera automatizzata – ai Titolari/gestori dei siti web, le stesse comunicazioni e-mail e le relative richieste non possono qualificarsi come specifiche o mirate.

Le informazioni fornite dagli "attivisti" nelle comunicazioni risultano, quindi, necessariamente generiche e indistinte per i diversi destinatari, al punto da risultare persino insufficienti ai Titolari del trattamento nel caso delle richieste di accesso ai dati personali formulate ai sensi dell'art. 15 RGPD, comportando – ex articolo 11 paragrafo 2 del RGPD – la necessità di richiedere ulteriori informazioni, onde identificare

adeguatamente l'interessato e poter procedere correttamente al soddisfacimento delle formulate richieste di esercizio dei diritti. **Sempre che la navigazione di un sito web lanciata tramite un bot o altro sistema automatizzato** e, dunque, **evidentemente non eseguita direttamente da un utente/persona fisica che possa esprimere – o meno – validamente un consenso libero, specifico, informato a un determinato trattamento dei suoi dati** tramite quel sito web e per le finalità e nelle modalità descritte nella specifica informativa di quel sito web, **possa davvero integrare un trattamento di dati personali, nel senso letterale, logico e giuridico** della relativa definizione.

2.4 Nelle comunicazioni massivamente inviate non sono state fornite ai Titolari informazioni in merito all'adeguatezza dei trattamenti effettuati dai c.d. attivisti

Le comunicazioni inviate ai Titolari/gestori dei siti non includono alcuna informazione sui trattamenti dei dati personali effettuati: in effetti, occorre considerare che i dati trattati in tali operazioni di analisi e comunicazioni automatizzate e massive, url e dominio di siti web e indirizzi PEC/e-mail, in primis, possono essere pacificamente considerati – in molti casi, anche qualora si tratti di riferimenti istituzionali, aziendali o afferenti all'organizzazione di riferimento - **dati direttamente o indirettamente riferibili a un interessato persona fisica**.

Inoltre, non viene fornita un'informativa in relazione alle terze parti coinvolte (eventualmente in qualità di responsabili del trattamento, ai sensi dell'art. 28 del RGPD) per le attività di scansione automatizzata (provider delle istanze/VPS su cui vengono eseguiti script/bot) e per invio/ricezione e archiviazione delle comunicazioni con i Titolari (provider servizi PEC/email e nel caso delle richieste di accesso ai dati personali formulate ai sensi dell'art. 15 RGPD anche LimeSurvey, in virtù del caricamento dati in Survey Participant Table per l'invio delle e-mail e la raccolta dei moduli di risposta).

In tali comunicazioni non risultano rinvenibili nemmeno gli altri elementi obbligatori di un'informativa ai sensi degli artt. 13 e 14 RGPD (tra i quali, l'espressa indicazione di dati di contatto di DPO e/o altri contatti deputati a fornire chiarimenti in merito ai trattamenti dei dati), qualora in tali analisi e comunicazioni automatizzate e massive siano anche trattati dati personali.

Peraltro, nessuno di tali soggetti "attivisti", nonostante abbiano condotto tali azioni e tali trattamenti automatizzati e massivi su un numero vastissimo di siti web e indirizzi e-mail e PEC, talvolta direttamente o indirettamente riferibili a interessati persone fisiche, risulta aver effettuato una preventiva e documentata analisi del rischio o una valutazione d'impatto, che quanto meno sarebbe stata opportuna, ai sensi dell'art. 35 RGPD, considerati i trattamenti automatizzati su larga scala.

3. I rischi insiti in tali azioni

Desideriamo evidenziare come le suddette azioni, riconducibili all'interno dell'allarmante fenomeno c.d. di "*weaponization* di *DSAR*"[4] (Data Subject Access Request, richieste di accesso ai dati personali formulate ai sensi dell'art. 15 RGPD) sono pericolose sotto diversi profili.

3.1 Profili di dubbia liceità e pericoli per gli stessi attivisti

I soggetti "attivisti", promotori delle iniziative innanzi descritte, in mancanza di una completa e accurata valutazione delle implicazioni di tali azioni, hanno purtroppo ignorato – o mancato di valutare adeguatamente – due elementi rilevanti:

[4] Ci si riferisce al fenomeno per cui le richieste di accesso ai dati ai sensi dell'art. 15 RGPD, nonché l'esercizio degli altri diritti sanciti dallo stesso Regolamento europeo, sono strumentalmente utilizzati per esercitare pressione sul Titolare del trattamento, ad es. in una controversia.

3.1.1 Trattamento dei dati in relazione alle istanze

Le attività condotte dagli "attivisti" si traducono in trattamenti sistematici di dati personali su larga scala. Si ritiene, infatti, che **tali trattamenti non siano effettuati nell'ambito di attività a carattere esclusivamente personale o domestico[5] e, quindi, non possano essere sottratti all'applicazione del RGPD**. Gli autori delle comunicazioni, peraltro, si qualificano espressamente come "hacker" e "attivisti", che agiscono in modo coordinato nell'ambito di una comunità impegnata nell'esecuzione di verifiche e segnalazioni, condotte metodicamente e con mezzi automatizzati.

Gli attivisti, pertanto, non avendo messo in atto gli adempimenti richiesti ai Titolari del trattamento, rischiano essi stessi di divenire autori di violazioni di norme del RGPD (si pensi, ad es., alla mancata informativa), nonché destinatari di richieste di esercizio dei diritti di cui agli artt. 15 - 22 sanciti dal RGPD da parte dei soggetti contattati, o ancora di reclami presentati presso l'Autorità Garante per la protezione dei dati personali. Oltre a questo, gli "attivisti" si troverebbero in difetto rispetto a adempimenti quali la tenuta del registro dei trattamenti, l'effettuazione di una analisi del rischio o una valutazione di impatto (quanto meno, opportuna, visti i trattamenti su larga scala) e tutti gli altri adempimenti previsti dal RGPD a carico del Titolare del trattamento.

Qualora, poi, siano stati utilizzati **sistemi automatizzati**, le implicazioni e i rischi sono addirittura superiori per via dell'applicazione dell'art 22 del RGPD e della conseguente inadempienza rispetto ai puntuali obblighi informativi imposti dal Regolamento europeo.

Gli "attivisti", pertanto, hanno finito col porre in essere delle azioni in evidente violazione del RGPD e, a causa dei contenuti perentori delle comunicazioni, dei diritti e le libertà delle persone fisiche.

[5] Sul punto, si rinvia a quanto rilevato al paragrafo 2.3 della presente segnalazione.

Tuttavia, ad essere compromesse, a ben vedere, risultano essere anche le iniziative dell'intera comunità degli attivisti, che potrebbero subire pregiudizi in termini di immagine e di reputazione da tali operazioni non adeguatamente valutate nei dettagli.

3.1.2 Controlli non coerenti - falsi positivi

L'invio delle comunicazioni sulla base di analisi esclusivamente automatizzate tramite custom script/bot comporta comunque un rischio base di falsi positivi.

Rischio che viene incrementato dall'utilizzo di custom script/bot amatoriali, che – a differenza di strumenti utilizzati per le verifiche condotte dalle autorità Garanti (come, per es., EDPS Website Evidence Collector)[6], – possono innescare le misure di controllo/redirezione di protezioni WAF / anti-Bot implementate sui siti.

3.2 Pericoli per le organizzazioni, gli enti e le aziende bersaglio di tali azioni

Le organizzazioni, gli enti e le aziende raggiunte dalle suddette azioni, o da azioni analoghe a quelle in oggetto, rischiano di confondere le operazioni condotte da collettivi o gruppi di "attivisti" con iniziative ufficiali promosse da parte delle istituzioni e delle autorità competenti.

I soggetti destinatari, infatti, potrebbero non interpretare correttamente queste iniziative poste in essere da gruppi privati, e le stesse iniziative, pertanto, potrebbero essere percepite come decettive o addirittura estorsive, e dunque risultare dannose o controproducenti.

Inoltre, la gestione delle richieste pervenute potrebbe risultare ingiustificatamente onerosa sia in termini organizzativi che economici.

[6] https://edps.europa.eu/edps-inspection-software_en

3.3 Pericoli per la percezione diffusa delle norme e dei diritti contenuti nel RGPD

Spicca, nelle iniziative oggetto della presente segnalazione, una strumentalizzazione dei diritti che il Regolamento (UE) 2016/679 prevede in capo agli interessati, con tutte le conseguenze che ciò comporta, tra cui la possibilità di banalizzazione e ridicolizzazione di tali – preziosi – strumenti a seguito di una percezione errata da parte dei destinatari delle iniziative.

L'utilizzo dei diritti come arma di disturbo di massa, come atto ritorsivo verso chi utilizza un determinato servizio o si appoggia ad un determinato provider, indebolisce l'autorevolezza e l'importanza del diritto della protezione dei dati personali.

Assistiamo quotidianamente a fenomeni di delegittimazione, tanto delle autorità Garanti, quanto delle norme stesse che garantiscono le libertà fondamentali e la protezione dei dati personali. Sempre più spesso si sentono termini come "talebani della privacy" o si fa riferimento al Garante come ad un ente "inerme".

Queste iniziative, avvolte da grande clamore mediatico, danneggiano l'alto profilo e il rigore della norma nonché, più in generale, il diritto della protezione dei dati personali, riducendone la percezione a fastidioso balzello, odioso adempimento, strumento di disturbo.

3.4 Pericoli per la crescita della micro-imprenditoria

In tale quadro, è utile considerare che uno dei più grandi ostacoli per le imprese è quello del reperimento delle risorse economiche che risultano spesso insufficienti quando non del tutto assenti (finanziamenti bancari, venture capital, ecc.): si stima che tra esse vi sia l'83% delle imprese che hanno investito nel digitale.

Orbene, in tale quadro delicato, fondamentale per la crescita, l'integrazione e il miglioramento del tessuto sociale, azioni arbitrarie e poco mediate che vadano a forzare una risposta delle Autorità volta a colpire i "piccoli" Titolari del trattamento,

potrebbero portare a frustrare gli sforzi di soggetti fragili e ad erigere nuove barriere d'accesso per forme d'imprenditoria che utilizzino mezzi digitali facilmente reperibili per la promozione o per il loro esercizio.

È chiaro che con ciò non si vuole affermare che i "micro" Titolari del trattamento debbano essere esentati dagli adempimenti volti alla tutela del dato dell'interessato né tantomeno che il Garante non applicherà proporzionalità nell'esercizio dei propri poteri. Tuttavia, da un lato è opportuno che tali soggetti abbiano la possibilità di accedere a strumenti facilitati di compliance, dall'altro occorre prendere atto che gli stessi siano nell'impossibilità di disporre di ingenti risorse da investire in consulenti per comprendere e gestire i complessi risvolti di azioni attivistiche, nella pratica meramente dimostrative.

3.5 Pericoli per il mercato

Le scelte dei Titolari del trattamento che acquisiscono servizi IT rischiano di essere fortemente compresse da fattori esterni per i quali gli ordinari criteri di scelta di un provider vengono frustrati e viziati da circostanze che rischiano di assumere connotati estorsivi.

Inoltre, si deve considerare quanto segue da un punto di vista di analisi economica dell'applicazione della norma che l'azione vorrebbe indurre. Innanzitutto la promozione di un presunto criterio di diritto in carenza di linee guide applicative è una circostanza che molto spesso è stata il presupposto per l'emissione di un Provvedimento Generale da parte del Garante. Rimettere alle decisioni dei Titolari l'applicazione di misure tecniche e organizzative al fine di prevenire una non conformità è senz'altro coerente con il principio di accountability ma – almeno da un'analisi preventiva – non compensa le conseguenze negative generate dalla modalità di applicazione della norma con riguardo all'ipotesi di predisposizione delle misure supplementari richieste per l'esportazione dei dati verso gli Stati Uniti.

Lo scenario che si profila genera incertezza e due comportamenti prevalenti: la dismissione di un servizio o altrimenti l'accettazione del rischio. Entrambe le ipotesi sono però viziate dalle asimmetrie informative circa le condizioni del servizio presentato da un operatore "forte" qual è Google (o altri provider, comunemente indicati come GAFAM).

Non solo: la presenza di clausole contrattuali del tipo take-it or leave-it con il riconoscimento di tali operatori "forti" come soli e semplici Responsabili del trattamento comporta di fatto un trasferimento forzoso di quei costi che andrebbero imputati in capo ai Titolari del trattamento, quali sono quelli di ricerca e sviluppo delle soluzioni di accountability per rendere il servizio conforme alle indicazioni post-Schrems II.

La distorsione sul mercato degli operatori diventa ancor più evidente se si contemplano anche i costi di transazione per la ricontrattualizzazione delle misure complementari con i provider, in una posizione di squilibrio non compensata da una riduzione effettiva di responsabilità.

L'incertezza applicativa, inoltre, richiama comportamenti predatori o opportunistici pericolosi da parte di operatori di mercato che potrebbero proporre costi aggiuntivi, che inevitabilmente andrebbero poi ad aumentare il prezzo dei servizi offerti dai singoli Titolari del trattamento o, nei casi più estremi, una riduzione dei servizi stessi.

Certamente non si vuole che l'interessato subisca il rischio imprenditoriale del Titolare, ma che l'allocazione del rischio e dei costi segua una regola di ragionevolezza e proporzionalità attribuendo all'esportatore una responsabilità pari all'effettivo controllo che questi ha sui flussi dati e sulla predisposizione di misure supplementari.

3.6 Pericoli per l'Autorità Garante

La stessa Autorità Garante, per quanto attiva, rigorosa ed autorevole, viene danneggiata da queste iniziative che la espongono a ingiuste e pretestuose critiche, che minimizzano e sviliscono il valore dell'azione regolatoria, generano enormi quantità di pratiche da gestire senza che, a questo, possa corrispondere un'utilità per l'effettivo rispetto delle norme a tutela della protezione dei dati personali.

4. Ulteriori elementi di riflessione

4.1 Chi tratta i dati? Per quali finalità?

Se, come accennato nei paragrafi precedenti, in alcuni casi questi "attivisti" stanno creando dei database partendo da dati pubblicamente accessibili, è legittimo dubitare della asserita inapplicabilità del RGPD anche ai trattamenti da costoro effettuati.

La particolare finalità di questi trattamenti è possibile evincerla in parte dal sito ufficiale del gruppo in questione, il quale si auto descrive come un "Osservatorio Automatico Distribuito sulla PA" (si veda https://monitora-pa.it/).

Posto, quindi, che l'utilizzo dei dati raccolti non rientra nella casistica di cui all'art 2, par. 2, lett. c) del RGPD, il quale prevede la non applicabilità del Regolamento in caso di uso di dati per motivi domestici, è da ritenere che anche su MonitoraPA e sui suoi componenti gravino tutti gli obblighi in materia di cui alla normativa europea, primo fra tutti l'obbligo di rendere l'informativa.

Nessuno, tra i soggetti che hanno ricevuto le richieste di accesso in esame, ha mai potuto visualizzare una informativa da cui dedurre se sono in atto, ad esempio, trattamenti automatizzati, condivisione di dati con soggetti terzi, diffusione degli stessi.

Per assurdo, i riceventi non sono stati messi al corrente della possibilità di richiedere l'accesso ai dati nei confronti del mittente.

Dall'esterno non è dato sapere se la governance di questo autoproclamato "Osservatorio" sia stata organizzata in modo coerente con il Regolamento, tuttavia, è possibile osservare che le manifestazioni esterne dello stesso lasciano dubitare di tale circostanza, mancando del tutto l'elemento fondamentale che ogni Titolare del trattamento deve rilasciare agli interessati: l'informativa.

A poco, poi, rileva il fatto che, per lo più, gli indirizzi e-mail in questione non contengano espressamente dei nomi e dei cognomi. In primo luogo, infatti, la presenza di una serie di dati di contesto porta comunque alla facile identificazione degli interessati (si pensi al meccanografico di una scuola, direttamente riconducibile al suo Dirigente). Non solo, trattandosi di raccolta e trattamento effettuato per mezzi automatizzati senza intervento di operatore, è legittimo sospettare la possibilità di applicare anche la normativa in materia di comunicazioni indesiderate la quale, come noto, trova attuazione anche nei confronti dei dati di contatto di persone giuridiche.

4.2 Abuso dell'esercizio di un diritto

L'esercizio di un diritto in modo anomalo per promuovere obiettivi non conformi con lo scopo di tutela per cui tale diritto è stato sancito esula dalla ratio della previsione del legislatore. La fattispecie astratta di abuso si configura nel momento in cui il diritto viene esperito non per realizzare l'interesse per cui è stato sancito nell'ordinamento, ma il suo esercizio è piegato per rispondere a scopi che esulano dalla ratio legis di tutela, come effettuare un'indebita pressione su altri soggetti, finendo in tal modo per costituire talvolta uno strumento ritorsivo o di intimidazione.

In tal senso è sicuramente legittimo esercitare uno dei diritti previsti dagli articoli 15 e ss. del RGPD, ma non quando, come nella fattispecie concreta, le finalità espresse e le

peculiari modalità della richiesta di esercizio non corrispondono al paradigma delle finalità e delle modalità tutelate dall'art. 15 RGPD . Nello specifico, tali finalità e modalità presupporrebbero evidentemente la tutela di un interessato – persona fisica – in relazione al trattamento dei suoi dati personali o ai consensi eventualmente espressi durante la personale navigazione in un determinato sito web, non dalle attività effettuate da un bot o da altro sistema automatizzato. In tal senso, in relazione alle menzionate operazioni condotte da tali organizzazioni di "attivisti", è possibile che la condotta assuma i connotati tipici dell'abuso nell'esercizio di un diritto.

A tale riguardo, in primis è utile considerare la sistematicità e l'organicità con cui è stato organizzato l'invio di queste richieste, che evidenzia una finalità diversa da quella che integra la ratio di tutela dell'art 15 RGPD e ss. (finalità, peraltro, espressamente dichiarata dalle organizzazioni di "attivisti").

Tali richieste, infatti, non risultano essere state avanzate da uno o più interessati – persone fisiche – intenzionati ad accedere ai loro dati personali, ma da una o più organizzazioni di "attivisti" che attribuiscono fittiziamente a una persona fisica la navigazione su un sito web compiuta da un bot o altro sistema automatizzato, la cui attività, dunque, non è idonea a generare "dati personali", ma solo "dati", poiché l'attribuzione degli stessi a una persona fisica costituisce una mera finzione al solo fine di abusare dell'esercizio del diritto di accesso, ai sensi dell'art. 15 GPR, che altrimenti non sarebbe azionabile.

Dunque, siamo dinnanzi a una organizzazione che "usa" pretestuosamente l'interessato e i diritti del RGPD. Di questo esistono prove documentali rinvenibili sul sito internet di MonitoraPA e nei canali telegram della stessa. Possiamo quindi dubitare della riconducibilità del fine concretamente perseguito con quella che è la ratio degli art. 15 e ss. RGPD. Lo scopo di tale iniziativa, come denota anche il nome del gruppo "MonitoraPA", è quello di monitorare, controllare, la pubblica amministrazione ed anche i privati.

Come detto, tuttavia, la ratio dei diritti previsti nel Regolamento non è quella di conferire un potere di controllo generalizzato, quanto riconoscere un potere al singolo al fine di consentire un maggiore controllo dei propri dati. In questo si concretizza l'abuso nell'esercizio di un diritto, come evidenziato anche dalla Giurisprudenza amministrativa con riferimento al simile – ma differente – diritto di accesso riconosciuto dall' art. 22 e ss. della l. n. 241 del 1990. Il TAR del Friuli, in particolare, con sentenza n. 145/2020, ha evidenziato come, in effetti, la Legge del 1990 riconosca indubbiamente un diritto di accesso il quale, tuttavia, non deve essere usato, in modo abusivo, al fine di portare ad un controllo generalizzato sulla Pubblica Amministrazione.

L'attività in esame, come evidenziano anche i proclami del gruppo in questione, disvela, invece, il reale interesse avuto di mira e, cioè, l'interesse a un controllo generalizzato dell'attività della P.A. Non si può, quindi, che concordare con il Tar del Friuli e con il consolidato indirizzo giurisprudenziale (cfr. C.d.S., Sez. III, 12 marzo 2018, n. 1578; id., Sez. IV, 19 ottobre 2017, n. 4838; id., Sez. V, 21 agosto 2017, n. 4043; id., Sez. IV, 9 novembre 2015, n. 5092) secondo il quale il Legislatore, mediante l'accesso agli atti ex art. 22 e ss. della l. n. 241 del 1990, non ha introdotto un'azione popolare volta a consentire un controllo generalizzato sull'attività amministrativa, ma un'azione che deve trovare giustificazione in un interesse concreto e attuale.

Da ciò, e per quanto sopra esposto circa i potenziali rischi e pericoli, si ritiene che un'azione di c.d. "DSAR weaponization" possa rientrare a pieno titolo in tale fattispecie in concreto. Di conseguenza, tale azione incontra dei limiti rispetto a una richiesta di esercizio dei diritti destinata a tutelare in concreto l'interessato, e non per promuovere o realizzare un'azione dimostrativa. Giova ricordare, infatti, che la protezione dei dati personali non è un diritto assoluto, ma deve essere contemperata con altri diritti fondamentali, secondo il principio di proporzionalità (considerando n. 4 RGPD).

V. L'AUSPICATO INTERVENTO DEL GARANTE

Tali azioni – ed eventuali future azioni analoghe – alla luce di quanto sopra esposto e per le modalità con cui sono – e potrebbero essere, se emulate o reiterate – condotte, generano diffusi allarmismi, alimentano incertezza e confusione su tematiche di primaria importanza connesse al diritto della protezione dei dati personali e sviliscono l'esercizio di un diritto ad un mero strumento propagandistico. Esse stesse, peraltro, presentano alcuni profili di dubbia liceità, e anche per questo sono potenzialmente pregiudizievoli nei confronti di diverse categorie di soggetti e in diversa misura.

Si intende, quindi, segnalare all'Autorità tale fenomeno, evidenziandone alcuni profili di possibile illiceità, o quantomeno di criticità, e i rischi sottesi per le diverse categorie di soggetti coinvolte.

Si auspica, dunque, che Codesta Autorità voglia considerare, e far rilevare anche in sede europea, quanto espresso innanzi, al fine di:

- **porre in essere qualsiasi azione che l'Autorità decida di intraprendere a seguito della Sentenza Schrems II** e nel farlo mantenendo in debita considerazione, nell'ambito del quadro normativo di riferimento, anche il **reale contesto economico e sociale**, nonché tutte le circostanze sopra brevemente illustrate, caratterizzanti l'ambito in cui i professionisti, le imprese, gli enti e le organizzazioni italiane operano;

- **voler valutare la legittimità delle azioni di "attivismo digitale" sopra descritte, nonché delle iniziative di analoga natura**, soprattutto nelle modalità di attuazione, ed **eventualmente accertata la violazione della normativa in materia di protezione dei dati personali** da parte degli attivisti Monitora-PA e del signor Federico Leva o di altri soggetti promotori, **adottare nei confronti degli stessi tutte le conseguenti iniziative necessarie e/o opportune**;

- **voler valutare l'adozione di pubbliche e autorevoli ulteriori iniziative necessarie e/o opportune affinché siano promosse puntuali verifiche** da parte dell'Autorità Garante per la protezione dei dati personali **circa le effettive misure di sicurezza organizzative e tecniche** per il trattamento dei dati personali, nonché in relazione alle **garanzie circa l'eventuale trasferimento di dati personali in Paesi extra UE, adottate dai provider IT operanti su scala globale** (c.d. "GAFAM").

Con osservanza.

Promotore e Coordinatore del Gruppo

Avv. Andrea Lisi

Redattori e primi firmatari

Dott. Christian Bernieri, Avv. Carola Caputo, Avv. Diego Dimalta, Avv. Giovanni Ferorelli, Avv. Valentina Fiorenza, Dott. Stefano Gazzella, Dott. Nicola Manzi, Avv. Sarah Ungaro.

Firmatari aderenti all'iniziativa

Dott.ssa Stefania Algerio, Avv. Adriana Augenti, Avv. Giovanni Brancalion Spadon, Avv. Sabina Bulgarelli, Dott. Franco Cardin, Dott. Matteo Colombo, Avv. Giacomo Conti, Prof. Avv. Giuseppe Corasaniti, Prof. Giovanni Crea, Avv. Antonella D'Iorio, Dott.ssa Anna Dalla Benetta, Dott. Graziano de' Petris, Avv. Luisa Di Giacomo, Avv. Sandro Di Minco, Avv. Diego Dimalta, Dott. Pierangelo Felici, Avv. Alessandra Fischetti, Avv. Luigi Foglia, Avv. Diego Fulco, Prof. Ing. Francesco Fumelli, Prof. Antonio Vittorino Gaddi, Avv. Paola Gallozzi, Avv. Graziano Garrisi, Prof.ssa Lucilla Gatt, Dott. Stefano Gazzella, Avv. Luciana Grieco, Avv. Eleonora Maria Guida, Prof. Avv. Michele Iaselli, Prof. Donato Antonio Limone, Dott. Edoardo Limone, Avv. Angela Lo Giudice, Avv. Davide Maniscalco, Dott.

Nicola Manzi , Prof. Avv. Marco Martorana, Avv. Eleonora Mataloni, Avv. Enrico Pelino, Dott. Gianni Penzo Doria, Avv. Antonino Polimeni, Avv. Matteo Pompilio, Dott. Nazzareno Prinzivalli, Dott.ssa Morena Ragone, Avv. Anna Rahinò, Dott. Roberto Reale, Dott. Alessandro Selam, Avv. Sara Sindaco, Avv. Giuseppe Vitrani, Avv. Antonio Zama.

Firmato digitalmente da: lisi andrea
Data: 22/09/2022 12:24:37