AVV. TOMMASO SCANNICCHIO Ph.D.
STUDIO LEGALE DE TOMMASI - LETIZIA - SCANNICCHIO
BARI
VIALE DELLA REPUBBLICA N.71/G· TEL. 080/5425983· FAX 080/5233773· CELL. [redacted] · E-MAIL t.scannicchio@protonmail.com· P.E.C. tommaso.scannicchio@legalmail.it

AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

P.ZZA VENEZIA, 11

00187 ROMA

***

Reclamo ex art. 77 del Regolamento (Ue) 2016/679 e artt. da 140-bis a 143 del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento

***

Per [redacted], **Coalizione Italiana per i Diritti e le Libertà Civili (CILD)**, elettivamente domiciliati in Bari al Viale della Repubblica n° 71/G, presso e nello studio dell'avv. Tommaso Scannicchio (c.f. SCN TMS 76D09 A662K) del Foro di Bari che li rappresenta e difende giusta procura in calce al presente Reclamo, il quale, ai fini del presente procedimento dichiara di voler ricevere tutte le relative comunicazioni ai seguenti recapiti:
P.E.C.: tommaso.scannicchio@legalmail.it
E-mail: t.scannicchio@protonmail.com
Ed espone quanto segue:

***

Premessa: Introduzione e Scopo del Reclamo

I Sigg. [redacted] mi hanno incaricato di sottoporre un Reclamo alla Autorità Garante per i Dati Personali per sollecitare, anche da parte della Autorità italiana, l'apertura di una indagine relativa al settore della "pubblicità comportamentale". Entrambi i reclamanti perseguono interessi personali e professionali attraverso il presente Reclamo.

- [redacted] **Coalizione Italiana per le Libertà e Diritti Civili (CILD)**, una organizzazione membro di European Digital Rights initiative (EDRi) e Open Rights Group (ORG), che lavora per preservare i diritti e le libertà digitali. CILD si batte per un mondo in cui ognuno possa controllare i propri dati digitali, decidere chi può usarli e come, e in cui i diritti dell'opinione pubblica siano riconosciuti e sostenuti. CILD è una organizzazione non governativa con sede in Roma e fondata nel 2014 che si occupa di advocacy, divulgazione, lobbying e contenzioso strategico nel settore della privacy e dei diritti digitali.

Lo scopo del presente Reclamo è finalizzato a chiedere l'intervento da parte del Garante per la Protezione dei Dati Personali per proteggere gli individui da violazioni

sistematiche e su larga scala della normativa sulla protezione dati, da parte di Google LLC e altri soggetti individuati *infra* sub lettera c). Il Reclamo trova fondamento su un rapporto tecnico in lingua inglese (c.d. "Ryan Report" – allegato 1) allegato anche in una versione sintetica tradotta in lingua italiana (allegato 2). I motivi giuridici di ricorso sono esposti sub lettera e).

Il Reclamo è finalizzato a portare a conoscenza del Garante le problematiche legate al modello di business denominato "Real Time Bidding" (RTB) ed a richiedere l'apertura di una indagine conoscitiva nei confronti dei due fornitori di tale sistema.

a) Giurisdizione e legittimazione del Garante:

[redacted]. Ai sensi dell'Articolo 3 del GDPR, il GDPR si applica a Titolari del trattamento al di fuori dell'UE, qualora il trattamento si riferisca al monitoraggio del comportamento degli interessati nell'UE.

I Titolari oggetto del presente Reclamo offrono sistemi per fornire pubblicità personalizzata di tipo "comportamentale" (i.e. basata sul monitoraggio delle abitudini degli Interessati) sui siti Web a coloro che sono all'interno del territorio UE pertinente, compresa l'Italia. Pertanto, la sede delle varie società coinvolte è irrilevante per lo scopo del GDPR e per la giurisdizione del Garante Italiano per la Protezione dei Dati Personali.

Le violazioni si sono verificate in Italia e su tutto il territorio dell'Unione Europea.

Ai sensi dell'Art. 51 GDPR il Garante per la Protezione dei Dati Personali (d'ora in avanti individuato come "Garante") è l'autorità di vigilanza in Italia. I compiti del Garante sono indicati nell'Art. 57 GDPR e artt. 154 e ss. del D.Lgs. 196/2003 come novellato dal D.Lgs 101/2018 (d'ora in avanti individuato come "Codice") e comprendono obblighi generali per monitorare e rinforzare l'applicazione del GDPR. Per adempiere a tale compito, il Garante può utilizzare i poteri previsti dall'Art. 58 GDPR per *"condurre indagini sotto forma di attività di revisione sulla protezione dei dati"*.

Rientra tra i compiti del Garante occuparsi delle questioni descritte nel presente Reclamo e nei relativi allegati tecnici.

L'Art. 4 GDPR stabilisce che per *"dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile"*. Tale definizione include *"un identificativo online"* che consente ad un individuo di essere identificato, direttamente o indirettamente [*infra* sub lettera e)]. Anche la Corte di Giustizia UE ha confermato che gli indirizzi IP costituiscono dati personali[1] e, inoltre, anche i dati "pseudonimizzati" devono essere trattati come dati personali.

La diffusione e la trasmissione di dati personali dell'interessato, durante il processo di Real Time Bidding [infra sub lettera d)] comporta il trattamento di dati personali, inclusi gli indirizzi IP o altri dati personali, anche più granulari quali, ad esempio la posizione geografica.

[1] CGUE C-582/14 Breyer

Il Garante ha, quindi, il compito ed il potere di gestire i Reclami presentati dagli Interessati ai sensi dell'Articolo 77 GDPR e 141 e ss. del Codice.
Ulteriori Reclami aventi il medesimo oggetto ed i medesimi Titolari del trattamento sono già stati presentati innanzi al Data Protection Commissioner irlandese ed all'Information Commissioner's Office inglese, ed ulteriori reclami stanno per essere presentati alle altre autorità nazionali di controllo indipendenti europee. Data la portata geografica delle problematiche e delle società-Titolari oggetto del presente Reclamo, sarebbe opportuno che un certo numero di Autorità di controllo considerino la questione in modo uniforme. Si invita, pertanto, sin da ora il Garante a collaborare con altre autorità nazionali di controllo per condurre un'indagine congiunta ai sensi dell'Articolo 62 del GDPR.

***

b) Estremi identificativi del Titolare del trattamento

Nel modello RTB, Titolari del trattamento sono tutti quei siti web che si avvalgono delle piattaforme individuate sub lettera c) per mostrare pubblicità comportamentale sulle proprie pagine, solitamente a titolo oneroso.

***

c) Estremi identificativi del Responsabile del trattamento

Nel modello di pubblicità comportamentale, possono essere individuati come Responsabili Esterni del trattamento ai sensi dell'art. 28 GDPR, sia i fornitori delle piattaforme sotto indicati, sia un numero imprecisato di destinatari di tali dati, ignoti agli Interessati i cui dati sono raccolti.
Esistono due sistemi principali che gestiscono la fornitura della "pubblicità comportamentale online", entrambi operanti tramite una specifica tecnica denominata *"real-time bidding"* (RTB), meglio descritta nel suo funzionamento tecnico negli allegati 1 e 2:

a. "OpenRTB" - Utilizzata da quasi tutte le società importanti nell'industria dei media e della pubblicità online e adottato come standard di mercato da:
   Interactive Advertising Bureau & Tech Lab
   Rond-Point Robert Schuman 11
   1040 Brussels
   Belgium
   e
   116 East 27th Street, 7th Floor
   New York, New York 10016
   USA
b. "Authorized Buyers" – (di recente rinominato da "DoubleClick Ad Exchange" (noto come "AdX") a "Authorized Buyers"). È un sistema di proprietà di:
   Google LLC
   Porta Nuova Isola, Via Federico Confalonieri 4
   20124 Milano
   Italia

e
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

I meccanismi di RTB, in palese violazione delle norme in materia di protezione dati personali, come si vedrà *infra* sub lettere d) ed e), non consentono di sapere a quali ulteriori soggetti terze parti (i.e. destinatari) vengano trasferiti i dati raccolti dal sistema. Non è, pertanto, possibile identificare con certezza ulteriori Responsabili Esterni del Trattamento come definito dall'art. 28 GDPR.

***

d) Indicazione dei fatti e delle circostanze su cui l'atto si fonda

Entrambi i sistemi RTB operano per fornire pubblicità personalizzata sui siti Web. Come dettagliatamente descritto nel rapporto tecnico "Ryan" (all. 1 e 2), *"ogni volta che una persona carica una pagina su un sito web che utilizza pubblicità comportamentale, i loro dati personali vengono trasmessi a decine - o centinaia di società"*.

Sussistono tre principali questioni chiaramente evidenziate negli allegati 1 e 2, tra loro correlate, che destano notevoli preoccupazioni in materia di tutela dei dati personali.

d.1.a) In primo luogo, quanto iniziato come un'industria focalizzata sull'assistenza con la pubblicità personalizzata, ha generato un meccanismo di trasmissione di dati di massa che:

1. raccoglie una vasta gamma di informazioni sulle persone, che vanno ben oltre le informazioni necessarie per fornire annunci pertinenti; e
2. fornisce e trasmette tali informazioni ad una serie di terze parti non identificate, per una serie di scopi che vanno ben oltre quelle finalità del trattamento che l'Interessato può comprendere, a cui può acconsentire o opporsi.

Non esiste alcuna giustificazione legale o base giuridica che consenta una simile attività di profilazione pervasiva e invasiva, tanto più quando contempli un tale trattamento dei dati personali a scopo di lucro.

d.1.b) In secondo luogo, il meccanismo di RTB non consente a chi se ne avvale di poter controllare la diffusione dei dati personali una volta che sono stati trasmessi alle terze parti. L'enorme numero dei destinatari di tali dati non permette a quelli che li trasmettono di poterli proteggere contro ulteriori trattamenti non autorizzati, né di informare adeguatamente gli Interessati, sulla identità e recapiti dei destinatari. I dati personali, una volta trasmessi dal meccanismo RTB, non sono più al sicuro e, le misure tecniche e organizzative attualmente in atto, servono esclusivamente a dimostrare che eventuali violazioni dei dati sono insite nel modello di business del settore. Tale questione crea un *vulnus* nei diritti degli Interessati che si manifesta indipendentemente dalla circostanza che il trattamento dei dati personali e la condivisione delle informazioni siano finalizzati a scopi di pubblicità personalizzata.

Un trattamento scorretto dei dati, senza le necessarie garanzie di legge, non è conforme alle normative sulla protezione dei dati.

d.1.c) In terzo luogo, i dati raccolti possono spesso includere le categorie particolari di dati personali come individuati all'art. 9 GDPR. I siti Web su cui gli Interessati navigano possono contenere indicazioni sulle loro preferenze sessuali, etnia, opinioni politiche, ecc. Tali dati potrebbero essere espliciti, ovvero dedotti efficacemente e facilmente in modo altamente preciso, attraverso moderne tecniche analitiche, che li rendono, effettivamente, espliciti[2]. La velocità con cui si verifica l'RTB, si traduce nella circostanza per cui le categorie particolari di dati possono essere diffuse senza alcun consenso o controllo dell'Interessato sulla loro diffusione.

Considerato che è molto probabile che tali dati vengano diffusi a numerose organizzazioni che cercherebbero di aggregarli con altri dati, esiste il concreto rischio che vengano prodotti profili di individui estremamente complessi, senza che l'Interessato lo sappia, vi abbia consentito o possa esercitare i diritti a sua tutela previsti dagli artt. 15-22 GDPR. I fornitori di meccanismi di RTB agevolano questa pratica e non offrono adeguate misure di sicurezza in atto a garantire l'integrità dei dati personali (comprese le categorie particolari). Inoltre, è improbabile che gli Interessati sappiano che i loro dati personali sono stati diffusi e trasmessi, a meno che non siano in qualche modo in grado di farlo in modo tale da rendere efficaci le loro richieste di accesso a una vasta gamma di società terze[3]. Non è chiaro se queste organizzazioni abbiano sviluppato o meno un percorso di compliance al GDPR che consenta di gestire le richieste degli Interessati. Senza l'intervento congiunto delle Autorità di Controllo e nuova regolamentazione, è impossibile garantire che l'intero settore / industria sia conforme alle normative sulla protezione dei dati.

***

d.2) Quanto sopra descritto è illustrato in dettaglio negli allegati 1 e 2 al presente Reclamo (c.d. rapporto "Ryan") al quale si invita il Garante a fare riferimento. Di seguito viene fornita una sintetica – per quanto possibile – descrizione del modello di business di settore e sulle questioni inerenti la protezione dei dati.

Il settore / industria del RTB è rappresentato da una associazione commerciale che definisce i parametri ed i progetti di utilizzo. Si tratta dell'associazione Interactive Advertising Bureau (IAB). La filiale europea dello IAB, IAB Europe, ha impostato una

---

[2] Si vedano sul punto le, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (wp251rev.01) "La profilazione può creare categorie particolari di dati per deduzione dai dati che non sono di categorie particolari a sé stanti, ma diventano tali quando combinati ad altri dati. Ad esempio, potrebbe essere possibile dedurre lo stato di salute di qualcuno, dai registri degli acquisti alimentari combinati ai dati sulla qualità e il contenuto energetico degli alimenti." Va anche notato (come confermato dalla CGUE in *Nowak*, C‑434/16) che perfino i dati, come le deduzioni, che si riferiscono ad un individuo ma sono inaccurate, rimangono dati personali. Se ciò non fosse vero, il "diritto alla rettifica" non potrebbe mai essere usato.

[3] Questo problema è aggravato dalla circostanza che le società terze sono in gran parte sconosciute e inaccessibili agli Interessati, poiché i Titolari, che inizialmente raccolgono le informazioni, raramente forniscono informazioni esplicite sui destinatari o persino categorie di destinatari dei dati, e, a loro volta, i destinatari non informano gli individui, su chi e come riceve questi dati secondo quanto previsto dall'Articolo 14.

politica e procedura standard per l'Europa ("IAB Europa"). Inoltre, il quasi-monopolio di Google sul mercato significa che "Authorized Buyers" hanno una propria procedura e politica distinta da quella di IAB. Tali politiche e procedure saranno ora prese in esame una per volta.

d.2.a) *IAB Europa*

IAB Europa ha creato un *"Europe Transparency & Consent Framework"* (il Framework) [4] . Questo Framework è basato sull'idea di raccogliere il consenso dell'interessato, per tutta la successiva condivisione verso i terzi durante il processo RTB.

C'è, tuttavia, un difetto fondamentale inerente alla progettazione del sistema. Il Framework riconosce espressamente che una volta trasmessi i dati di un individuo, il Titolare del trattamento (e, di conseguenza, l'Interessato) perda qualsiasi forma di controllo sul modo in cui tali dati vengono utilizzati. In effetti, il Framework consente di poter continuare a fornire dati anche quando un destinatario agisca al di fuori del dettato normativo[5]. Una volta che il Titolare del trattamento perde il controllo dei dati, l'Interessato perde ogni possibilità materiale di utilizzo di un sistema che determini come quei dati vengano poi utilizzati. Una volta perso il controllo su quei dati, gli stessi saranno persi per sempre nell'etere del brokeraggio dati. I dati vengono poi trasferiti ad un vasto ecosistema di mediatori ed inserzionisti. Successivamente, le terze parti possono, quindi, conservare e utilizzare tali dati in qualunque modo decidano, senza che l'interessato abbia voce in capitolo, conoscenza o controllo su questo utilizzo successivo. L'uso di tali dati è vario; possono essere aggregati e amalgamati ad altri dati ovvero possono essere utilizzati per profilare l'interessato per numerosi ulteriori fini. L'utilizzo finale di questi dati può, quindi, essere quello diverso da quanto espresso dal Titolare del trattamento nella sua interazione con l'Interessato. Tali usi secondari potrebbero addirittura creare disagio o danni per l'Interessato, qualora dovesse mai scoprirli[6]. Ed in effetti, non esiste un modo per il Titolare del trattamento di rendere evidenti tutti i potenziali utilizzi secondari, in quanto gli stessi Titolari del trattamento non sono più in controllo dati, una volta trasmessi. Il problema tecnico e la relativa violazione di legge sono, pertanto, inerenti alla progettazione del sistema "OpenRTB".

Inoltre, come specificato in dettaglio nel rapporto del "Ryan", i dati oggetto di trattamento potrebbero comprendere categorie particolari di dati. Che tali dati vengano trasferiti senza alcun controllo è una circostanza molto preoccupante che configura una violazione particolarmente grave.

---

[4] http://www.iabeurope.eu/tcfdocuments/documents/legal/currenttcfpolicyFINAL.pdf

[5] Il Framework sottolinea (con enfasi) "Se un CMP ritiene ragionevolmente che un Venditore non sia conforme alle specifiche, alle politiche, o alla legge, deve immediatamente sporgere denuncia al MO seguendo le procedure MO e può, come previsto dalle procedure di MO, interrompere la collaborazione con un Venditore, finché la questione non venga risolta." Ciò permette, nella realtà, al titolare del trattamento la massima discrezione di continuare a elaborare e divulgare dati personali, anche se il titolare stesso è consapevole che il destinatario sta violando le norme sulla protezione dei dati.

[6] Nel paragrafo XX del rapporto Ryan, risulta chiaro che, l'ormai famigerata *Cambridge Analytica* è solo un esempio del tipo di destinatario finale dei dati.

Un'ulteriore preoccupazione relativa al Framework è che, lo stesso, è stato progettato in modo da rimuovere le possibilità di un controllo sui dati personali una volta trasmessi. Il Framework, infatti, prevede che i Titolari possono trasmettere i dati personali a terzi, anche senza il consenso degli Interessati. Il Framework sottolinea (con enfasi):

"… un Venditore non deve trasmettere dati a un altro Venditore senza un valido motivo per ritenere che [l'altro, ndt] *Venditore non abbia una base giuridica per il trattamento dei dati personali..."*

"Se un Venditore possiede oppure ottiene dati personali e non ha le basi giuridiche per ottenere o trattare quei dati, il Venditore dovrebbe cessare rapidamente la raccolta e la conservazione dei dati e astenersi dal trasmetterli ad altre parti, anche se tali parti hanno una base giuridica."

Ai Titolari che trasmettono i dati personali viene, quindi, accordata l'ampia discrezionalità di affidarsi ad un *"valido motivo per ritenere che* [l'altro, ndt] *Venditore non abbia una base giuridica per il trattamento dei dati personali..."*. Di conseguenza, l'eventuale consenso sulle impostazioni di un Interessato potrebbe anche essere ignorato. Un Venditore potrebbe decidere in modo particolarmente discrezionale su cosa sia un *"valido motivo"* per non fornire dati personali a terzi. L'intero sistema si affida, quindi, alla discrezionalità ed alle decisioni del Venditore-Titolare in base ad una terminologia vaga e con parametri mal definiti, piuttosto che alla volontà, alla consapevolezza o al consenso dell'Interessato.
In conclusione, il Framework si affida alla totale discrezionalità del Venditore-Titolare, piuttosto che considerare la scelta dell'Interessato. Tale circostanza è contraria alle norme del GDPR e si traduce in metodologie che consentono di aggirare l'assunzione del consenso dell'Interessato, come meglio si vedrà sub lettere e.1) ed e.2). Ed in effetti, visto il possibile trattamento di categorie particolari dei dati, esiste un comprensibile interesse del sistema di fare in modo di preservare una qualche forma di discrezionalità da parte del Titolare-Venditore. Purtroppo, questo sistema non offre nulla per quanto riguarda i diritti sui dati degli individui. In sostanza, non c'è modo di trovare nel Framework un modello che affronta e protegga adeguatamente i diritti individuali degli Interessati.
Infine, si segnala che IAB Europe ha recentemente pubblicato un comunicato stampa, suggerendo una rielaborazione del Framework. Tuttavia, non c'è, ad oggi, un concreto riscontro di tali proposte e i dettagli all'interno del comunicato stampa non affrontano adeguatamente le questioni contenute in questo Reclamo.

d.2.b) *Authorized Buyers*

Authorized Buyers di Google impone una "Linea Guida" e accettazione di condizioni contrattuali per l'utilizzo. La Linea Guida[7] solleva una serie di questioni. La Linea guida

[7] https://www.google.com/doubleclick/adxbuyer/guidelines.html

sposta la responsabilità sulla protezione dei dati dal Titolare del trattamento ai terzi-destinatari che li ricevono. Ad esempio, la Guida afferma che (sic)[8]:

Restrizioni relative ai dati sui callout RTB

L'Acquirente può memorizzare l'ID cookie e l'identificatore per pubblicità su dispositivi mobili crittografati al fine di valutare le impressioni e le offerte in base ai dati sull'utente ottenuti in precedenza. L'Acquirente, dopo aver risposto a una chiamata dell'annuncio, può conservare tutti gli altri dati relativi ai callout, ad eccezione di quelli sulla posizione, al solo scopo di prevedere la disponibilità dell'inventario su Ad Exchange. L'Acquirente può conservare i dati sui callout solo per il tempo necessario per soddisfare gli scopi pertinenti sopra menzionati e, in qualsiasi caso, per non più di 18 mesi.

Se non ottiene l'impressione [così definita nelle Linee Guida di Google, nda]*, l'Acquirente non può: (i) utilizzare i dati sulle chiamate per quell'impressione per creare elenchi utenti o utenti profilo, (ii) associare a dati di terze parti i dati sulle chiamate relativi a quell'impressione o (iii) condividere con terze parti dati sui tariffari in qualsiasi forma, inclusa, a titolo esemplificativo, la forma aggregata.*

Protezione dei dati

Se l'Acquirente accede, utilizza o elabora informazioni personali rese disponibili da Google che identificano una persona in modo diretto o indiretto e provengono dallo Spazio economico europeo ("Informazioni personali"), l'Acquirente è tenuto a:

c. Rispettare tutte le leggi, direttive, regolamenti e norme vigenti riguardanti la privacy, nonché la sicurezza e la protezione dei dati.

d. Utilizzare le Informazioni personali o accedervi solo per scopi conformi al consenso rilasciato dalla persona cui tali informazioni fanno riferimento.

e. Implementare le misure organizzative e tecniche appropriate per proteggere le Informazioni personali da perdita, uso improprio, accesso non autorizzato o illegale, divulgazione, alterazione e distruzione.

f. Fornire lo stesso livello di protezione ai sensi dei principi dello scudo UE-USA per la privacy.

Verificare con regolarità di essere conforme a tale obbligo, informare immediatamente Google per iscritto qualora non possa più soddisfare (o sussista un sostanziale rischio che non possa più soddisfare) tale obbligo e, in tali casi, cessare l'elaborazione delle Informazioni personali o adottare immediatamente altre misure ragionevoli e appropriate per rimediare al mancato conseguimento di un adeguato livello di protezione.

[8] https://www.google.it/doubleclick/adxbuyer/guidelines.html

Tali passaggi suggeriscono che una volta trasferiti i dati personali ad un Acquirente, il sistema Authorized Buyer non ha più alcun controllo effettivo su come questi vengano utilizzati. Anzi, sostanzialmente si accetta che una terza parte (l'Acquirente) sia libera ed in grado di utilizzare tali dati. Le sole restrizioni imposte sono quelle contrattuali e non è chiaro fino a che punto queste vengano effettivamente applicate. Lo stesso vale per il "Google Ads Controller - Controller Data Protection Terms" (Termini contrattuali sulla protezione dei dati applicabili al Titolare del trattamento degli Annunci di Google) di Google[9].

Inoltre, anche le restrizioni imposte sono tutte da verificare. Ad esempio, nella Linea Guida non è chiaro quali restrizioni siano imposte agli Acquirenti che hanno successo nell'offerta, poiché le restrizioni vengono applicate solo agli offerenti che non vincono l'asta (ad esempio "*Se non ottiene l'impressione[10], l'Acquirente non può…*"). L'apparente assenza di controllo suscita seri dubbi in merito alla sicurezza tecnica e organizzativa dei dati pertinenti.

Infine, l'efficacia della politica di protezione dei dati dipende esclusivamente dalla volontà della terza parte di comunicare la violazione ad Authorized Buyer, senza ulteriori controlli. Ci sono quindi insufficienti misure di garanzia tecniche ed organizzative a tutela della protezione dei dati personali.

***

e) Indicazioni relative alle disposizioni del Regolamento (Ue) 2016/679 e del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento, che si presumono violate

Quanto sopra descritto sub lettera d) dimostra che il trattamento gestito dai fornitori di sistemi RTB e dai Titolari di dati del relativo settore di mercato genera un rischio sostanziale di violazioni sistematiche e continuative del Codice e del GDPR. Il Garante è invitato a considerare il Framework IAB [sub d.2.a)] e le Linee Guida di Google [sub d.2.b)] quando prenderà in considerazione eventuali provvedimenti.

Di seguito si riassumono le questioni legali fondamentali, connesse alla violazione dei principi applicabili al trattamento dati personali nel Regolamento Generale 679/2016 UE.

e.1) *Integrità e Riservatezza dei Dati [art. 5, 13-22 GDPR]*

A parere dello scrivente, la questione principale è che nè il Framework tecnico e né le politiche attuali utilizzate dal settore RTB e dai fornitori di servizi di RTB riescono a fornire protezioni e salvaguardie adeguate contro la divulgazione ed il trattamento dei dati personali non autorizzato, e potenzialmente illimitato.

L'Articolo 5, paragrafo 1, lettera f), del GDPR impone che i dati siano *"trattati in maniera da garantire una adeguata sicurezza dei dati personali, compresa la protezione"* per evitare *"trattamenti non autorizzato o illeciti"* e per evitare la perdita, la distruzione o il danno accidentale, utilizzando appropriate misure tecniche o organizzative ("integrità e riservatezza").

---

[9] https://privacy.google.com/businesses/controllerterms/

[10] Vedi, *supra* nota 8

Il Framework di IAB Europe e le Linee Guida di Google non forniscono un'adeguata "integrità e riservatezza" sui dati personali, in particolare perché:

i. Non prevedono che gli Interessati vengano informati in merito alla diffusione dei loro dati ovvero in relazione alla possibilità che vengano trasmessi a ciascun destinatario [artt. 13 a 14 GDPR];
ii. Non offrono possibilità agli Interessati di poter esercitare alcun tipo di diritto previsto dal GDPR nei confronti dei venditori/destinatari dei dati relativamente alle modalità di utilizzo dei loro dati personali [artt. 15-22 GDPR];
iii. Non consentono l'esercizio del diritto degli Interessati di opporsi all'uso dei propri dati da parte delle singole terze parti [art. 21 GDPR];
iv. Non effettuano alcun controllo, nemmeno superficiale, per impedire l'utilizzo ulteriore dei dati, sia esso illecito e/o autorizzato [art 5, par. 1, lettere a), b), c), d) ed f)].

e.2) *Liceità, Correttezza e Trasparenza [artt. 5, 6 e 9 GDPR]*

L'Articolo 5, paragrafo 1, lettera a), impone che i dati personali siano elaborati secondo i principi di liceità e correttezza. L'Articolo 6 delimita le circostanze in cui un trattamento dati personali è lecito. Esistono esclusivamente due possibili deroghe, di cui all'Articolo 6, paragrafo 1, potenzialmente applicabili al settore RTB:

i. L'Interessato ha prestato il consenso al trattamento dei propri dati personali per uno o più scopi specifici; ovvero
ii. Il trattamento è necessario ai fini degli interessi legittimi perseguiti dal titolare del trattamento o di terzi, a condizione che tali interessi non siano superati dagli interessi o diritti fondamentali e libertà dell'interessato che richiede la protezione dei dati personali, in particolare se l'interessato è un minore.

Il consenso [art. 6, par. 1, lettera a) GDPR] è – ancora oggi – il "motore principale" del trattamento. L'industria / settore RTB è intrinsecamente incapace di ottenere un adeguato consenso, esattamente come riconosciuto dal Framework IAB[11]. Tale circostanza è tanto più vera per quanto riferito alle terze parti intermediarie, che potrebbero non avere alcun contatto diretto con gli Interessati.

Allo stesso modo, anche qualsiasi tipo di utilizzo dell'interesse legittimo [art. 6, par. 1, lettera f) GDPR] quale base giuridica – oggi ampiamente diffuso nel settore RTB – sarebbe fuori luogo. Qualsiasi interesse legittimo di questo tipo non può in alcun caso essere considerato come assoluto e sarà sempre subordinato a *"gli interessi o diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali."* In particolare, la fornitura di dati personali degli Interessati ad una vasta gamma di società terze, con conseguenze sconosciute e senza adeguate salvaguardie in atto, non può mai essere giustificata in quanto necessaria e/o legittima, tenendo conto del potenziale impatto sui diritti e sulle libertà degli Interessati.

Inoltre, ai sensi dell'Art. 9 GDPR, il trattamento di "categorie speciali" di dati personali richiede sempre e senza eccezioni il consenso esplicito degli Interessati, ove questi

[11] *Supra*, nota 4 e in allegato 1.

dati “sensibili” non siano stati manifestamente resi pubblici dagli stessi Interessati. Al contrario, il Framework IAB e la Linea Guida di Authorized Buyers di Google consente di elaborare i dati ex-“sensibili” senza consenso, compresi dati reali o quelli inferiti e dedotti riferiti alla origine razziale/etnica, opinioni politiche, credi religiosi/filosofici, appartenenza sindacale, salute, vita o orientamento sessuale, dati genetici o biometrici degli Interessati. In assenza di consenso esplicito per tale trattamento, l’utilizzo dei dati infrange l'Articolo 9 del GDPR e deve, quindi, essere considerato *contra legem*.

Ad abundantiam, è richiesto un consenso esplicito laddove le decisioni significative, completamente automatizzate, vengono prese in relazione a un individuo. Il Working Party Articolo 29 [12] ha identificato alcune situazioni in cui la pubblicità comportamentale, così come attualmente gestita dall'industria del RTB, potrebbe essere considerata come avente "effetti significativi" ai sensi dell'Art. 22 GDPR. Ciò è particolarmente vero laddove gli individui più vulnerabili sono presi di mira da offerte di servizi che possono causare danno, come il gioco d'azzardo o determinati prodotti finanziari. La mancanza di capacità di ottenere questo consenso esplicito da parte dei fornitori di servizi RTB rappresenta una inosservanza assoluta di quanto previsto all'Art. 22 GDPR.

In conclusione, vi sono forti e fondati timori che i fornitori di servizi e l'industria del RTB nel suo complesso trattino dati personali e categorie particolari di dati, senza un valido consenso. In effetti, il Framework IAB contempla un sistema nel quale i dati possono essere diffusi e trasmessi senza consenso dell’Interessato. Tutto ciò non è legale e tantomeno questi trattamenti dati possono, in alcun caso, essere definiti come leciti, corretti o trasparenti.

e.3) *Adeguatezza, Pertinenza e Limitazione della Conservazione [art. 5 GDPR]*

Si dubita, altresì, che il trattamento dei dati da parte dell'industria RTB sia conforme all'Art. 5, paragrafo 1, lettera c) GDPR, dove si richiede che i dati personali siano adeguati, pertinenti e non eccessivi rispetto all’obiettivo o agli obiettivi per i quali sono elaborati. Il numero di destinatari dei dati personali e la possibilità che quei dati personali possano essere ulteriormente utilizzati dai destinatari, dà luogo a gravi conseguenze negative. L'Art. 5, paragrafo 1, lettera e) prevede, inoltre, che i dati personali elaborati per qualsiasi scopo non debbano essere conservati più a lungo di quanto sia necessario a quel preciso scopo. La Linea Guida dell’Authorized Buyers

---

[12] Supra, nota 2, a pag. 24: *" In numerosi casi tipici, la decisione di proporre pubblicità mirata basata sulla profilazione non inciderà in modo analogo significativamente sulle persone, ad esempio nel caso di una pubblicità per un outlet di moda online basato su un semplice profilo demografico: “donne nella regione di Bruxelles di età compresa tra 25 e 35 che potrebbero essere interessate alla moda e ad alcuni capi di abbigliamento”.*

Tuttavia, è possibile che ciò possa accadere, a seconda delle particolari caratteristiche del caso, tra le quali:

• l’invasività del processo di profilazione, compreso il tracciamento delle persone su siti web, dispositivi e servizi diversi;

• le aspettative e le volontà delle persone interessate;

• il modo in cui viene reso disponibile l’annuncio pubblicitario; o

• lo sfruttamento della conoscenza di vulnerabilità degli interessati coinvolti.

prevede (anche se, a causa della mancanza di controllo, non lo può garantire) la conservazione dei dati personali per 18 mesi. È, pertanto, probabile che i dati vengano conservati per lunghi periodi senza alcuno scopo correttamente identificato, in violazione della previsione di legge.

e.4) *Protezione dei Dati fin dalla Progettazione e per Impostazione Predefinita [art. 25 GDPR]*

La pubblicità comportamentale dipende dalla capacità di individuare le persone attraverso l'uso di identificatori digitali che sono legati ai dispositivi (che oggi di solito si riferiscono ad un singolo individuo) ovvero collegare gli individui attraverso dispositivi e contesti diversi. Questi identificatori includono "impronte digitali" del web, che si riferiscono all'impostazione unica di dispositivi e cookie personali collocati sui dispositivi, così come descritto nella relazione del Dr Ryan (all. 1 e 2). Per gli individui è particolarmente difficile accedere o recuperare questi identificatori, in modo da poter gestire le loro "impronte" con i Titolari del trattamento che detengono queste informazioni. Questa circostanza crea un grave squilibrio tra le parti ed una barriera significativa affinché gli Interessati possano richiedere il rispetto di importanti diritti garantiti dalle norme sulla protezione dei dati, quali l'accesso, la cancellazione, l'opposizione, la limitazione del trattamento e la portabilità.

Tutto ciò, a sua volta evidenzia una questione più ampia relativa al principio fondamentale di trasparenza e correttezza del trattamento sancito dal GDPR: i Titolari ed i destinatari terzi del trattamento hanno facile accesso agli identificatori dei singoli individui, mentre quegli stessi Interessati non hanno reali capacità o possibilità di usare o controllare quegli identificatori. Questo desta particolare preoccupazione, in particolare, ai sensi dell'Art. 25 GDPR in tema di protezione dei dati fin dalla progettazione e di default, che impone ai titolari del trattamento un obbligo positivo di creazione di modalità di gestione delle richieste degli Interessati, come l'accesso o l'opposizione, nelle loro attività e sistemi di trattamento. Tale circostanza, è anche in grado di invalidare un consenso eventualmente prestato, ai sensi della Direttiva 93/13/CEE sulle clausole abusive nei contratti stipulati con i consumatori, in quanto senza dubbio comporta un *"grave squilibrio nella posizione contrattuale delle parti"* quanto alla possibilità di esercizio dei rispettivi diritti contrattuali e/o statutari da parte dell'Interessato-Consumatore.

e.5) *Valutazione di Impatto sulla Protezione dei Dati [art. 35 GDPR]*

Data l'ampiezza e la portata dei dati personali e dei dati delle categorie particolari coinvolti, insieme alla vastissima gamma di destinatari di tali dati, il trattamento presenta con ragionevole certezza *"un rischio elevato per i diritti e le libertà delle persone fisiche"*. In tal caso, l'Art. 35 GDPR richiede che vengano svolte delle appropriate valutazioni d'impatto sui trattamenti. Al momento, per quanto risulta allo scrivente, nessuna valutazione d'impatto è stata effettuata o resa pubblica dai soggetti sopra indicati sub lettera c).

***

Tutto ciò premesso, il sottoscritto procuratore, in nome e per conto dei reclamanti, così come individuati nel presente atto

CHIEDE

al Garante per la protezione dei dati personali, esaminato il reclamo che precede e ritenutane la fondatezza, di assumere nei confronti dei soggetti individuati sub lettera c) ogni opportuno provvedimento e, in particolare di:

I. rivolgere a questi avvertimenti o ammonimenti sul fatto che detti trattamenti possono verosimilmente violare, ovvero abbiano violato, le disposizioni vigenti in materia e, specificamente, tutte quelle individuate sub lettera e);

II. considerare il presente Reclamo ai sensi dell'Art. 154 del Codice, facendo proprie le relative indicazioni di violazione di legge come meglio dettagliate sub lettera e) unitamente al rapporto "Ryan" allegato, e dare avvio ad una indagine sulle questioni specificate nei confronti dell'industria / settore della pubblicità comportamentale che si avvale dei meccanismi di "Real Time Bidding", ai sensi di quanto previsto dagli artt. 57 e 58 GDPR;

III. incoraggiare l'elaborazione di uno specifico codice di condotta per gli operatori di settore che agiscono sul mercato nazionale ed europeo;

IV. sollecitare, ai sensi dell'art. 64 GDPR, al Comitato Europeo per la Protezione dei Dati (EDPB) l'emanazione di un parere / linee guida di corretto utilizzo per l'industria RTB, in modo da assicurarsi che tali attività siano conformi al Codice della Protezione dei Dati ed al GDPR e, di conseguenza, che i diritti degli Interessati siano efficacemente sostenuti all'interno dell'Unione.

Si invita il Garante ad esercitare i suoi poteri ai sensi del Capo VII, GDPR (artt. 60-67), ed a collaborare con le altre Autorità europee per la protezione dei dati, per mettere in pratica un'indagine congiunta. Come descritto nel Reclamo, simili reclami sono stati già presentati, in altri Stati membri dell'UE, alle relative Autorità per la protezione dati.

Elenco dei documenti allegati:

1) Allegato 1: Dr Johnny Ryan – *Behavioural advertising and personal data*;
2) Allegato 2: Dr Johnny Ryan – *Pubblicità comportamentale e dati personali* (sint.).

Bari-Roma, 04.06.2019 **Avv. Tommaso Scannicchio**