Către

AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

B-dul G-ral Gh. Magheru nr. 28-31 sector 1 București
anspdcp@dataprotection.ro

Subiect: Sesizare Regulamentul UE 679/2016 (RGPD) - încălcări sistematice la scară largă privind regimul protecției datelor personale de către sistemele de publicitate online

Având în vedere atribuțiile Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal cu privire la protecția datelor cu caracter personal conform Regulamentului UE 679/2016, a legii 102/2005 și a legii 190/2018

Având în vedere faptul că Asociația pentru Tehnologie și Internet (ApTI) acționează în România și în Uniunea Europeană pentru drepturile civile digitale, în conformitate cu obiectivele sale de susținere a unei lumi digitale liberă prin promovarea vieții private, libertății de exprimare și a tehnologiilor deschise pe Internet și a susținut importanța unui regim funcțional pentru protecția datelor cu caracter personal de la înființare până acum.

Vă trimitem sesizarea anexată cu privire la principalele aspecte care stau la baza încălcării sistematice la scară largă privind regimul protecției datelor personale de către sistemele de publicitate online identificate mai jos.

Demersul nostru face parte dintr-un context mai larg în care organizații aparținând societății civile din diverse state membre ale Uniunii Europene (și nu numai) încearcă să sesizeze autoritățile naționale cu privire la aceste aspecte încă din 2018. O parte dintre acestea au primit deja răspunsuri preliminare de la autoritățile respective, de care probabil deja știți, și facem referire la ele în detaliile de mai jos. O altă parte dintre acestea sesizează astăzi, 10 decembrie 2020, autoritățile competente din 6 state membre ale Uniunii Europene cu același probleme de principiu.

Deși, după cum veți vedea problemele sunt aproape identice pe întreg teritoriul Uniunii Europene, sunt două aspecte pe care considerăm importante pentru situația din România.

În primul rând considerăm de o gravitate deosebită prelucrarea datelor din categoriile speciale (art. 9 RGPD) prin aceste sisteme de publicitate online fără un temei legal adecvat, în special cele cu privire la interesele politice. Atât observațiile empirice, cât și rezultate unui sondaj[1] făcut în septembrie 2020, ne arată că toate partidele politice folosesc sistemele de publicitate online într-un mod neadecvat, iar interesele politice ale utilizatorilor de Internet sunt prelucrate de operatorii sau

1 Vedeți analiza ApTI după campania electorală de la alegerile locale din 2020, disponibilă la https://apti.ro/sites/default/files/Analiz%C4%83%20date%20personale%20si%20reclame%20politice%20alegeri%20locale%202020.pdf

brokerii de date în mod constant, fără vreun temei legal adecvat.

În al doilea rând, dacă luăm în calcul profilul utilizatorilor de Internet din România este clar ca avem de-a face cu o colectare sistematică de date personale pe scară largă. Conform datelor DESI 2020, 72% din populația României între 16 și 74 de ani a accesat Internetul și deci probabil este persoana vizată de această prelucrare.[2]

Considerăm că RGPD este o unealtă legislativă foarte bună, dar aplicarea corectă a Regulamentului este crucială pentru a garanta o reală protecția a datelor personale, în special în astfel de cazuri. În același timp este evident că avem de-a face cu o problemă care nu poate avea doar o rezolvare națională, poate nici doar la nivelul Uniunii Europene.

De aceea, scopul principal al acestei sesizări este de a fi rezolvată **în mod colaborativ de autoritățile competente din statele membre ale Uniunii Europene**. În acest context, sugerăm să trimiteți această plângere către autoritățile competente de supraveghere din Belgia și Irlanda, care la momentul acestei plângeri efectuează o anchetă cu privire la prelucrarea datelor personale de către sistemele de publicitate online și să solicitați asocierea cu omologi din alte state membre pentru a desfășura o anchetă comună în conformitate cu articolul 62 din RGPD.

București, 10 decembrie 2020

Asociația pentru Tehnologie și Internet

Bogdan Manolea
Director executiv

2 Date disponibile la https://ec.europa.eu/digital-single-market/en/scoreboard/romania

A <u>Introducere și scopul acestei sesizări</u>

1 Ne adresăm către ANSPDCP pentru a evidenția plângerile noastre cu privire la sistemul de reclame online referitor la oferta în timp real - Real-Time Bidding (RTB), utilizat de industria RTB ("industria").

2 Respondenții sunt responsabili pentru aspectele care mijlocesc încălcarea în mod sistematic de către industrie a Regulamentului General privind Protecția Datelor (RGPR). Respondenții au sediul în Uniunea Europeană după cum urmează:

2.1 **Google Irlanda** – Casa Gordon, Barrow St, Dublin 4, Irlanda

2.2 **IAB Europe**– IAB Europe, Robert Schuman 11, 1000 Bruxelles, Belgia.

3 Scopul acestei plângeri este de a solicita acțiuni din partea ANSPDCP și a altor autorități competente pentru protecția drepturilor persoanelor fizice împotriva încălcărilor sistematice la scară largă privind regimul protecției datelor personale, de către Google și IAB Europe. Această plângere este susținută inclusiv prin următoarele anexe, care sunt disponibile în limba originală – limba engleză:

- Anexa 1: Un raport cu privire la industria de publicitare online a dr. Johnny Ryan (**"Raportul Ryan"**)

- Anexa 2: "Raport revizuit privind industria publicității online și a ofertei în timp real (*real-time-bidding)*" al Comisarului Britanic de Protecție a Datelor (Information Commissioner's Office - ICO) (iunie 2019)

- Anexa 3: Dovezi suplimentare din partea dr. Ryan privind distribuirile neautorizate ale datele personale din oferta în timp real (RTB) către cei care tranzacționează date și despre nivelul încălcărilor.

B Informații generale

4 Sistemul RTB operează în fundal pe majoritatea site-urilor comerciale și a aplicațiilor pentru telefon. Acesta declanșează licitații rapide și automate prin care companiile de tehnologie care reprezintă agențiile de publicitate pot licita pentru a avea reclamele lor prezentate în spațiul de reclamă al unui website sau al unei aplicații. Aceste licitații RTB operează în mod curent prin transmiterea datelor personale despre o persoană care vizualizează website-ul sau aplicația către sute de companii pentru a solicita oferte de la aceștia, așa cum este detaliat în Raportul Ryan. Aceste distribuiri de date sunt cunoscute sub denumirea de solicitări de ofertă - “bid requests”.

5 Respondenții, și anume Google și IAB, definesc “protocoale” (sau reguli) pentru ce tipuri de date pot și trebuie să fie oferite despre o anumită persoană care a accesat un website sau o aplicație . Respondenții rulează diferite versiuni de RTB: (1) Sistemul de ofertă în timp real al IAB se numește “OpenRTB” – RTB deschis și (2) Sistemul Google este numit “Authorized Buyers”- Cumpărători autorizați.[3] Miile de companii din industria RTB trebuie să se supună acestor reguli pentru a participa la piața RTB în valoare de miliarde de euro.

6 Sistemele RTB ale IAB și Google difuzează informații despre aspecte ce țin de viața privată, ce vizionăm online și cum ne poziționăm în lumea reală,[4] către o gamă largă de companii, de sute de miliarde de ori în fiecare zi.[5] Sistemul RTB al Google este activ pe peste 13.5 milioane de website-uri.[6] Sistemul RTB al IAB este activ pe nenumărate alte website-uri. Nu există vreo cale pentru utilizator pentru a limita ceea ce se întâmplă cu aceste date. Sistemele RTB ale IAB și Google conduc așadar la o încălcare vastă și continuă a datelor. Facem trimitere către Raportul Ryan (Anexa 1) pentru o explicație detaliată a ofertei în timp real, cum funcționează și ce date personale pune în pericol acest sistem.

3 Anterior se numea sistemul “DoubleClick”.

4 Vedeți Raportul Ryan pentru detalii despre ce date pot fi difuzate.

5 De exemplu, For example, o licitație RTB numită Index Exchange, a desfășurat 120 miliarde de licitații pe zi. Vedeți "IX Traffic Filter: Meeting 2020’s Business Challenges with Machine Learning", Index Exchange, 6 August 2020 (URL: https://www.indexexchange.com/ix-traffic-filter-meeting-2020s-business-challenges-with-machine/, last accessed 12 September 2020). Vedeți mai mult în Anexa 3.

6 Doubleclick.net a detectat 13.5 milioane de website-uri (5,002,707 și încă 8,823,691 website-uri associate cu primele). Date de la BuiltWith.com (URL: https://trends.builtwith.com/ads/DoubleClick.Net, 11 September 2020).

7 Există patru probleme esențiale ce sunt interconectate:

1.i **În primul rând**, nu există “măsuri tehnice sau organizatorice corespunzătoare” precum mijloacele de protecție, așa cum este cerut în Articolul 5(1)(f) RGPD, pentru a controla diseminarea datelor personale prin RTB odată ce au fost difuzate. Numărul real de Beneficiari sugerează că aceia care difuzează nu se pot proteja împotriva ulterioarelor prelucrări de date neautorizate, așa cum solicită Articolul 5(1)(f) RGPD. IAB Europe a luat la cunoștință, în mai 2018, faptul că “nu există o soluție tehnică pentru a limita felul în care sunt folosite datele după ce sunt primite”.[7] Eșecul respondenților de a proteja aceste date este descris în paragrafele de mai jos.

1.ii **În al doilea rând**, pentru că sistemele RTB ale Google și IAB transferă date personale fără protecții tehnice, este imposibil pentru companiile care folosesc sistemul RTB să transmită persoanelor vizate informațiile cerute în Articolele 13 și 14 din RGPD. De asemenea nu există mijloace adecvate de protecție pentru a preveni ca cei care primesc datele inițial să le folosească pentru alte scopuri, în mod ilegal, sau să distribuie acele date către alte companii. Mai mult, nu există o cale posibilă pentru operatori să explice toate scopurile utilizării, având în vedere că nu se mai află în controlul operatorilor o dată ce datele au fost transmise. În acest sens, operatorul nu se poate supune regulilor din Articolul 13(1)(c) și 14(1)(c) din RGPD.

1.iii **În al treilea rând**, datele includ deseori categorii speciale de date personale.[8] Paginile web sau aplicațiile folosite de indivizi pot indica orientarea lor sexuală, etnia, opiniile politice etc. Acești indicatori pot fi expliciți, sau determinați efectiv și ușor prin tehnici analitice moderne.[9] În

7 "pubvendors.json v1.0: Transparency & Consent Framework", IAB Europe & IAB TechLab, Mai 2018 (URL: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md#liability).

8 Vedeți Anexa: Dovezi suplimentare privind scurgerile de date RTB către brokerii de date, și despre dimensiunea încălcărilor RTB

9 Vedeți Ghidul privind Luarea deciziilor individuale în mod automat și profilarea conform scopurilor Regulamentului 2016/679 (wp251rev.01) “Profiling can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data. For example, it may be possible to infer someone’s state of health from the records of their food shopping combined with data on the quality and energy content of foods.” Este de notat, de asemenea, (cum a fost confirmat și de CJUE în cazul Nowak) că datele, cum ar fi interferențele, care au

acest sens, Anexa 3 arată că datele RTB sunt diseminate către organizații care produc profiluri extrem de complexe ale indivizilor fără cunoștința persoanei vizate, despre consimțământ nepunându-se nici măcar problema. Exemplele în Anexa 3 includ un broker de date care a folosit date RTB să profileze persoane LGBTQ+ în Polonia, pentru a le influența decizia de vot pentru alegerile parlamentare din 2019. În plus, este improbabil ca indivizii să știe faptul că datele lor au fost diseminate și difuzate, decât dacă și-ar exercita dreptul de acces la date către o gamă foarte largă de firme. [10] O asemenea sarcină este aproape imposibilă pentru persoanele vizate, limitând scopul GDPR de a oferi protecție efectivă și completă pentru persoanele vizate.

1.iv **În al patrulea rând**, sistemele RTB ale IAB Europe și Google RTB:

1.a Colectează o gamă largă de informații despre indivizi, mergând mult mai departe decât informațiile *cerute* pentru a oferi reclame relevante;

1.b Colectează și diseminează acele date pentru numeroase scopuri, care depășesc scopurile pe care persoana vizată le poate înțelege, consimți la acestea sau obiecta împotriva lor.

Anexele evidențiază faptul că nu există justificare legală, iar aceste profilări invazive sunt făcute cu un scop comercial evident.

8 Considerând toate acestea, sistemele RTB ale Google și IAB conduc la abuzuri ale datelor persoanelor vizate în mod sistematic și larg întâlnit. ANSPDCP este sesizată pentru a lua acțiuni care să asiste încetarea acestor abuzuri. Acțiunea solicitată din partea ANSPDCP este detaliată în paragrafele 67-69 de mai jos.

legătură cu un individ dar sunt inexacte rămân date personale. Dacă nu ar fi fost astfel, dreptul la rectificare nu ar fi putut fi niciodată utilizat.

10 Această problem este agravată de faptul că aceste companii sunt de obiecei necunoscute și inaccesibile pentru persoanele vizate, având în vedere că operatorii care colectează initial informațiile doar rareori oferă informații explicite despre companiile care primesc datele, sau chiar despre categoriile de companii care primesc informații și companiile nu informează persoanele vizate despre recepția datelor conform obligațiilor din Articolul 14.

9 Alte autorități de supraveghere au făcut pași pentru a răspunde la încălcările RGPD inerente în sistemele RTB după cum urmează:

i **IAB Europe** – În octombrie 2020, Autoritatea Belgiană pentru Protecția Datelor (APD) a descoperit că politica de transparență și modalitatea dezvoltată de IAB Europe pentru acordarea consimțământului încalcă RGPD, din pricina lipsei de siguranță, transparență și a bazelor legale inadecvate.[11]

ii **Google** – În martie 2019, Autoritatea Irlandeză pentru Protecția Datelor a deschis o investigație privind posibile încălcări ale RGPD de către sistemul cumpărătorilor pentru "presupuse încălcări" ale RGPD.[12] O actualizare a stadiului investigației va fi publicată în curând.

10 Astfel, autoritățile de supraveghere relevante au deschis anchete cu privire la funcționarea RTB și la politicile și procedurile care stau la baza utilizării acestuia.

C <u>Politici și proceduri</u>

1.I Politici și proceduri

11 IAB Europe[13] a stabilit "Cadrul de Transparență și Consimțământ" (TCF),[14] care dorește să fie o măsură de respectare a GDPR. Google folosește de asemenea TCF, și mai utilizează ceea ce numește o garanție contractuală. Le vom prezenta pe acestea mai jos:

1.a <u>IAB Europe – Cadrul de Transparență și Consimțământ (TFC)</u>

11 https://www.iccl.ie/human-rights/info-privacy/apd-iab-findings/

12 Secțiunea 110 din Actul Irlandez privind Protecția Datelor, în baza căruia se desfășoară ancheta, se referă la cazuri de încălcare suspectată.

13 A se vedea trimiterea la memorandumul lor de înțelegere privind TCF la „TCF Governance", IAB Europe (URL: https://iabeurope.eu/tcf-governance/).

14 https://iabeurope.eu/wp-content/uploads/2020/08/TCF_v2-0_FINAL_2020-08-24-3.2.pdf.

12 TCF se bazează pe ideea de a colecta consimțământul de la o persoană vizată sau de a-i notifica interesul legitim ca bază legală pentru toate transferurile ulterioare de date și prelucrarea de către sutele (în prezent 628)[15] de companii care s-au înregistrat în TCF - și către un număr necunoscut de companii suplimentare cu care aceste 628 pot partaja date.

13 Autoritatea Belgiană pentru Protecția Datelor (APD), autoritatea principală de supraveghere a TCF, a ajuns la concluzii preliminare cu privire la încălcările RGPD de către TCF. Referindu-se la TCF, consideră că:

> "Serviciul de inspecție estimează că abordarea IAB Europe arată că neglijează riscurile care pot afecta drepturile și libertățile persoanelor în cauză."

14 Această constatare a APD nu este surprinzătoare. Există un defect fundamental în proiectarea sistemului. TCF recunoaște în mod expres că, odată ce datele unei persoane sunt transmise, operatorul (și, implicit, persoana vizată) își pierde tot controlul asupra modului în care aceste date sunt utilizate. Într-adevăr, TCF acceptă faptul că, chiar și atunci când un destinatar acționează în afara legii, acesta poate continua să prelucreze date. TCF precizează:

> > "Dacă un CMP - Consent Management Platform [„platforma de gestionare a consimțământului"] consideră în mod rezonabil că un furnizor [companie care primește date RTB] nu respectă specificațiile și / sau politicile, trebuie să notifice imediat IAB Europe în conformitate cu procedurile sale și acesta **poate** (...) întrerupe activitatea cu furnizorul în timp ce problema este verificată".

Acest lucru oferă discreție operatorului să continue prelucrarea și diseminarea datelor cu caracter personal, chiar dacă operatorul respectiv știe că destinatarul acționează cu încălcarea reglementărilor privind protecția datelor.

15 Documentația proprie a IAB atestă faptul că „mii de furnizori" pot primi datele dintr-o singură licitație RTB și că „nu există o modalitate tehnică de a limita modul în care

15 IAB Europe Lista globală a furnizorilor TCF (URL: https://iabeurope.eu/vendor-list-tcf-v2-0/, last 5 noiembrie 2020).

datele sunt utilizate după ce datele sunt primite de către un furnizor”.[16]

16 Din acest motiv, CEO-ul IAB Europe scrisese Comisiei Europene în 2017, cu un an înainte de lansarea TCF, pentru a recunoaște că „este tehnic imposibil ca utilizatorul să aibă informații prealabile despre fiecare operator de date implicat într-un scenariu de ofertă în timp real (RTB)”.[17] În consecință, RTB ar fi „incompatibil cu consimțământul conform RGPD”. Din acest motiv, ea a solicitat o excepție pentru RTB în viitorul Regulament ePrivacy.

17 Nici nu există nicio modalitate de a verifica sau audita ceea ce au făcut companiile care primesc date personale prin RTB. Politicile TCF doar sugerează, dar nu încearcă să definească, o posibilitate ca IAB să încerce o formă de revizuire a ceea ce au făcut aceste companii cu datele personale.[18] Desigur, nu ar fi posibil să se descopere ceea ce s-a întâmplat într-un sistem care transmite pe scară largă date personale către atâtea companii, de sute de miliarde de ori pe zi.

18 Mai mult, și așa cum este detaliat într-un raport recent al dr. Ryan, în Anexa 3, datele prelucrate includ adesea date încadrate în categorii speciale [19]. Constatarea preliminară a APD este că:

“TCF nu prevede reguli adecvate pentru prelucrarea unor categorii speciale de date cu caracter personal. Cu toate acestea, standardul OpenRTB, guvernat de TCF al

16 https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md

17 Document de lobby trimis de CEO al IAB Europe înalților oficiali ai Comisiei Europene, “The EU’s proposed new cookie rules: digital advertising, European media, and consumer access to online news, other content and services”, IAB Europe, iunie 2017. Această lucrare a fost trimisă Comisiei Europene - DG Connect (și a fost obținută printr-o cerere de acces la informații). Consultați pagina 3 din atașamentul la e-mail la URL: https://www.iccl.ie/wp-content/uploads/2020/10/IAB-to-Commission-email-and-attachment-26-June-2017.pdf.

18 “The MO [IAB Europe] may adopt procedures for periodically reviewing and verifying a Vendor’s compliance with the Policies.”, în “Transparency & Consent Framework – Policies Version 2020-08-24.3.2” IAB Europe, 2020 (URL: https://iabeurope.eu/wp-content/uploads/2020/08/TCF_v2-0_FINAL_2020-08-24-3.2.pdf), p. 21

19 Vedeți, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf și https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf

IAB Europe, permite prelucrarea unor categorii speciale de date cu caracter personal."

19 O altă problemă în legătură cu TCF este că anticipează că cei care primesc date personale prin RTB pot să le difuzeze către terți, indiferent dacă persoană vizată a folosit caracteristicile TCF care pretind că oferă o bază legală adecvată. TCF spune că o companie poate partaja date RTB cu oricine, la propria sa discreție: se poate baza pe ceea ce TCF numește „o bază justificată pentru faptul că destinatarul furnizorului are o bază legală pentru prelucrarea datelor cu caracter personal".[20] Un furnizor ar putea adopta o opinie discreționară privind o „bază justificată" nespecificată pentru a considera că există un temei legal pentru a furniza date cu caracter personal unei terțe părți, chiar și în cazul în care o persoană a refuzat în mod specific consimțământul. TCF se bazează pe discreția a sute de companii pentru care tranzacționarea rapidă a datelor cu caracter personal este un model de afaceri. Unei persoane vizate i se poate arăta o cerere de a accepta prelucrarea datelor sale (opt-in) la vizitarea unei pagini, dar dacă este de acord nu este important.

20 Nu există nicio interpretare plauzibilă a TCF care să abordeze și să protejeze în mod adecvat drepturile persoanei vizate.

1.b Google – Cumpărătorii autorizați

21 Google folosește sistemul TCF și este un membru important al IAB. În plus, companiile RTB care doresc să primească difuzări RTB de la Google trebuie să semneze „Ghidul" Google[21]. Ghidul ridică o serie de probleme.

22 Ghidul Google transferă responsabilitatea pentru protecția datelor către 964 companii[22] care primesc date personale din sistemul său RTB. Documentația Google

20 Pagina 21, paragraful 18

21 https://www.google.com/doubleclick/adxbuyer/guidelines.html

22 Alte 1.218 companii sunt listate ca „furnizorii externi certificați" de la Google, care, probabil, primesc direct date de la Google în afara Spațiului Economic European. Consultați „Furnizorii de tehnologie publicitară", politicile programului Ad Manager și Ad Exchange, Google (URL: https://support.google.com/admanager/answer/9012903, 12 septembrie 2020), și „Furnizori externi certificați", certificări de difuzare a anunțurilor terților-părți, Google (URL:

face referire la aceste companii drept „Cumpărători” și se referă la datele solicitării ofertelor RTB ca „date de apelare” (call out data). Sub titlul „Restricționarea datelor RTB”, regulile Google menționează:

> „Cumpărătorul ... nu trebuie: (i) să utilizeze „date de apelare” pentru acea afișare pentru a crea liste de utilizatori sau profila utilizatorii; (ii) să asocieze „datele de apelare” pentru acea afișare cu date de la terți”.

Sub titlul „Protecția datelor”, regulile Google informează companiile care primesc difuzările RTB ale Google că trebuie să anunțe Google dacă intenționează să încalce regulile sale:

> *“Cumpărătorul va monitoriza în mod regulat respectarea acestei obligații și va notifica imediat Google în scris dacă Cumpărătorul nu mai poate îndeplini (sau dacă există un risc semnificativ ca Cumpărătorul să nu mai poată îndeplini) această obligație și, în astfel de cazuri, Cumpărătorul va înceta prelucrarea datelor personale sau va lua imediat alte măsuri rezonabile și adecvate pentru remedierea eșecului de a oferi un nivel adecvat de protecție.”*

Protecția Google depinde în totalitate de discreția a aproape o mie de companii, cărora li se cere să ofere voluntar informații prealabile despre comportamentul lor nepotrivit față de Google.

23 Acest pasaj demonstrează faptul că Google nu are control asupra datelor personale pe care le difuzează de sute de miliarde de ori pe zi. Mai mult, sistemul RTB privind Cumpărătorii Autorizați, proiectat și controlat de Google, nu oferă niciun control eficient asupra modului în care aceste date sunt apoi utilizate. Singurele restricții sunt contractuale și nu este clar în ce măsură acestea sunt sau ar putea fi puse în aplicare. Același lucru este valabil și pentru „Termenii de protecție a datelor pentru operator – Google Ads Controller ”.[23]

https://developers.google.com/third-party-ads/adx-vendors, 12 septembrie 2020).

23 https://privacy.google.com/businesses/controllerterms/

24 În plus, chiar și aceste restricții sunt insuficiente. De exemplu, în Ghid nu este clar ce restricții sunt impuse dacă un Cumpărător câștigă oferta, deoarece restricțiile sunt aplicate numai ofertanților care nu au câștigat licitația (de exemplu, „Cu excepția cazului în care Cumpărătorul câștigă o ofertă, acesta nu trebuie: (i) să utilizeze „date de apelare" pentru ...").

25 Prin urmare, nu există garanții tehnice suficiente pentru a proteja datele cu caracter personal și datele cu caracter personal din categorii speciale în sistemul RTB al Google.

D <u>Probleme juridice cu privire la prelucrarea datelor personale</u>

26 Contextul prezentat mai sus demonstrează că prelucrarea efectuată de industrie dă naștere unui risc substanțial de încălcare continuă a RGPD.

27 Considerăm că o serie de principii de protecție a datelor prevăzute la Articolul 5 RGPD ar trebui să fie respectate de RTB și de politicile și procedurile relevante.

●*.i Integritate și confidențialitate*

28 Îngrijorarea principală despre protocoalele RTB ale Google și ale IAB Europe este faptul că permit includerea datelor personale și a datelor din categoriile speciale în difuzările RTB, dar nu au nicio modalitate de a proteja aceste date împotriva divulgării și prelucrării neautorizate și potențial nelimitate.

29 Articolul 5 alineatul (1) litera (f) din RGPD prevede „prelucrarea datelor cu caracter personal într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale, utilizând tehnici adecvate sau măsuri organizaționale („integritate și confidențialitate"). "

30 Sistemul respondenților nu oferă mecanisme de „integritate și confidențialitate"

adecvate asupra datelor personale, în special deoarece nu sunt în măsură să protejeze împotriva prelucrării ilegale și / sau autorizate de către mii de companii care primesc date cu caracter personal în difuzările RTB și care nu sunt împiedicate să partajeze în continuare aceste date.

31 În plus, respondenții nu pot să:

a Ofere transparență cu privire la amploarea deplină a transmiterii și a altor prelucrări de date cu caracter personal, o dată ce acestea sunt difuzate.

b Ofere persoanelor vizate un drept formal să se opună utilizării datelor lor de către fiecare entitate care primește datele lor din sistemul RTB, deoarece sistemul este conceput astfel încât datele să ajungă la părți care nu pot fi identificate. Ca atare, persoanele vizate nu pot ști cine sunt aceste părți și nu pot obiecta cu privire la utilizarea datelor de către acele părți dacă nu știu cine sunt acele părți.

●*.ii Legalitatea și corectitudinea procesării*

32 Articolul 5 alineatul (1) litera (a) prevede prelucrarea legală și echitabilă a datelor cu caracter personal. Articolul 6 delimitează circumstanțele în care are loc prelucrarea legală a datelor cu caracter personal. Există doar două excepții în temeiul articolului 6 alineatul (1) care pot fi aplicate industriei:

1.i persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale personale pentru unul sau mai multe scopuri specifice; sau

1.ii prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o terță parte, cu excepția cazului în care aceste interese sunt depășite de interesele sau drepturile și libertățile fundamentale ale persoanei vizate care necesită protecția datelor cu caracter personal, în special atunci când subiectul este un copil.

33 Industria este inerent incapabilă să obțină consimțământul adecvat, după cum a recunoscut IAB Europe în scrisoarea sa din 2017 adresată Comisiei Europene, menționată mai sus.

34 Orice temei al interesului legitim pentru cererile de ofertă RTB difuzate la scară largă nu poate fi oportun. Orice astfel de interes legitim nu este absolut și ar fi depășit de „interesele sau drepturile și libertățile fundamentale ale persoanei vizate care necesită protecția datelor cu caracter personal". În special, furnizarea datelor personale ale persoanelor vizate către o gamă largă de companii terțe, cu consecințe necunoscute și fără garanții adecvate, nu poate fi justificată ca fiind necesară și / sau legitimă, luând în considerare impactul potențial asupra drepturilor și libertăților persoanelor vizate. Constatarea preliminară a APD cu privire la utilizarea de către TCF a interesului legitim ca posibilă bază legală pentru RTB confirmă acest lucru:

> "IAB Europe nu demonstrează că interesul legitim prevalează asupra intereselor fundamentale, libertăților și drepturilor persoanei relevante care necesită protecția datelor cu caracter personal; aceste drepturi nu au fost echilibrate ".

35 În plus, în conformitate cu articolul 9 din RGPD, prelucrarea „categoriilor speciale" de date cu caracter personal necesită consimțământul explicit în cazul în care datele respective nu au fost „făcute publice" în mod evident de către persoana vizată și nu se aplică nicio altă excepție. Cu toate acestea, TCF și restul documentelor permit industriei să proceseze date fără consimțământ, inclusiv date reale sau care dezvăluie originea rasială / etnică, opiniile politice, credințele religioase / filosofice, apartenența la sindicat, sănătatea, viața sexuală sau orientarea sexuală, date genetice sau date biometrice prelucrate în scopuri unice de identificare. În absența consimțământului explicit pentru o astfel de prelucrare sau a oricărei alte baze legale pentru prelucrarea acestor date, practicile ar încălca articolul 9 din RGPD. În acest scop, APD a remarcat în constatările sale preliminare despre TCF, că singurul temei juridic prin care se poate invoca procesarea datelor aparținând categoriilor speciale este consimțământul explicit.

36 Mai mult, este necesar consimțământul explicit atunci când se iau decizii

semnificative, automatizate, referitoare la o persoană. European Data Protection Board (denumit anterior Grupul de Lucru al Articolului 29)[24] identifică ocaziile în care publicitatea comportamentală, astfel cum este aplicată de industrie, ar putea fi considerată ca având „efecte semnificative” în sensul articolului 22 din RGPD. Acest lucru este valabil mai ales în cazul în care persoanele vulnerabile sunt vizate de servicii care le pot aduce prejudicii, cum ar fi jocurile de noroc sau anumite produse financiare. Lipsa capacității de a obține acest consimțământ explicit reprezintă o ignorare a articolului 22 din RGPD.

37 În consecință, se ridică probleme cu privire la faptul că industria prelucrează date personale și date din categorii speciale, fără consimțământul valid al utilizatorilor. Într-adevăr, cadrul prevede un sistem în care datele pot fi diseminate și difuzate fără consimțământul persoanei vizate. Acest lucru nu este legal și nu în toate cazurile această prelucrare a datelor nu poate fi descrisă ca fiind „corectă” sau „transparentă”.

●.*iii Oportunitate, relevanță și limitarea în timp*

38 Se ridică o serie de probleme cu privire la prelucrarea datelor de către industrie și respectarea articolul 5 alineatul (1) litera (c) din RGPD, care impune ca datele cu caracter personal să fie adecvate, relevante și nu excesive scopului sau scopurilor pentru care sunt prelucrate. Google și IAB ar putea modifica regulile sistemelor lor RTB astfel încât să nu fie difuzate date personale. Cu toate acestea, deoarece industria RTB lucrează în prezent cu numeroase companii care primesc date cu caracter personal și existând potențialul ca aceste date cu caracter personal să fie utilizate în continuare de către companii, există consecințe negative foarte importante.[25]

24 Supra, nota de subsol 1, la 22: „În multe cazuri obișnuite, decizia de a prezenta publicitate direcționată pe baza profilării nu va avea un efect semnificativ similar asupra persoanelor, de exemplu, o reclamă pentru un magazin de modă online care se bazează pe un profil demografic simplu: 'femeile din regiunea Bruxelles cu vârste cuprinse între 25 și 35 de ani, care sunt susceptibile de a fi interesate de modă și anumite articole vestimentare". Cu toate acestea, este posibil să aibă un impact semnificativ, în funcție de caracteristicile specifice ale cazului, inclusiv:
• intruzivitatea procesului de profilare, inclusiv urmărirea persoanelor pe diferite site-uri web, dispozitive și servicii;
• așteptările și dorințele indivizilor în cauză;
• modul în care este livrată reclama; sau
• utilizarea cunoașterii vulnerabilităților persoanelor vizate.

25 A se vedea, de exemplu, videoclipul: declarația și remarcile doctorului Johnny Ryan la Marele Comitet internațional pentru dezinformare și „Știri false”, 7 noiembrie 2019 (URL: https://vimeo.com/371652420).

39 Articolul 5 alineatul (1) litera (e) impune, de asemenea, ca datele cu caracter personal prelucrate în orice scop sau scopuri să nu fie păstrate mai mult decât este necesar în acest scop sau în aceste scopuri. Ghidul pentru cumpărătorii autorizați are în vedere (deși, din cauza lipsei de control, nu poate garanta) păstrarea datelor cu caracter personal timp de 18 luni. Prin urmare, este probabil ca datele să fie păstrate pentru perioade lungi de timp, fără niciun scop adecvat identificabil.

●*.iv Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit*

40 RTB depinde de abilitatea de a determina individual persoane prin utilizarea unor identificatori digitali care sunt legați de dispozitivele folosite și comportament (care astăzi se referă de obicei la un singur individ) sau de a conecta indivizi între dispozitive și contexte. Acești identificatori includ „amprente digitale”, care se referă la setări unice a dispozitivelor[26] și cookie-urilor individuale plasate pe dispozitive, așa cum este elaborat în raportul dr. Ryan. Acești identificatori sunt dificil de accesat de către indivizi pentru a-și gestiona profilul deținut/datele deținute de operatori, creând un dezechilibru și o barieră semnificativă pentru ca persoanele vizate să-și poată exercita drepturile lor privind protecția datelor, cum ar fi accesul, ștergerea, obiecția, restricția de procesare și portabilitatea.

41 La rândul său, acest lucru evidențiază o preocupare mai largă legată de principiul general al corectitudinii din RGPD: operatorii au acces ușor la identificatori pentru persoanele vizate, în timp ce aceiași indivizi nu au abilitatea reală de a utiliza sau de a controla acei identificatori. Acest lucru ridică probleme, în special în temeiul articolului 25 RGPD, ceea ce impune operatorilor de date obligația pozitivă de a crea modalități de a permite accesul sau ridica obiecții cu privire la activitățile și sistemele lor de prelucrare.

●*.v Evaluarea impactului asupra protecției datelor*

42 Având în vedere amplitudinea datelor cu caracter personal și a datelor din categoriile

26A se vedea câteva exemple la https://en.wikipedia.org/wiki/Device_fingerprint

speciale implicate, împreună cu o gamă largă de destinatari ai acestor date, prelucrarea va duce probabil la „un risc ridicat pentru drepturile și libertățile persoanelor fizice”. În consecință, articolul 35 solicită evaluări adecvate ale impactului asupra protecției datelor. În prezent, din câte știm, nu a fost efectuată sau făcută publică nicio evaluare adecvată a impactului.

E Responsabilitatea pentru operatori

43 Cei care organizează și controlează RTB sunt operatori. Aceasta include IAB Europe, pentru TCF și Google pentru Cumpărătorii Autorizați.

Principii legale

44 Există suficiente dovezi care să sugereze că structura organizată, coordonată și încurajată de respondenți face ca aceste entități să fie operatori [27]. Un operator este definit în RGPD[28] ca (sublinierea noastră)

> *“persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;”*

45 CJUE a constatat în mod constant că conceptul de „operator” trebuie să aibă o interpretare largă [29]. Într-adevăr, ghidul European Data Protection Board (anterior Grupul de Lucru pentru Articolul 29)[30] confirmă faptul că acest control „poate fi găsit [în] medii complicate, folosind adesea noile tehnologii informaționale, unde actorii relevanți sunt adesea înclinați să se vadă pe ei înșiși ca „facilitatori” și nu ca operatori responsabili”. Acest lucru se aplică chiar și atunci când aceste entități sunt

27 Într-adevăr, structura în sine ar putea fi considerată un „corp” care definește scopurile și mijloacele de procesare. Cu toate acestea, clienții nu trebuie să ia în considerare această problemă în continuare în scopurile actuale.

28 Exact aceeași formulare este utilizată la articolul 2 din Directiva 95

29 C-25/17 - *Jehovan todistajat* la [21]

30 Opnia 1/2010 privind conceptele de „operator” și „persoană împuternicită de operator”. Adoptat la 16 februarie 2010 (disponibil la https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf)

integrate într-un proces mai mare, cum ar fi cele ale unei platforme.[31]

46 În plus, dacă respondenții au sau nu acces la date este irelevant. După cum a constatat CJUE, „responsabilitatea comună a mai multor actori pentru aceeași prelucrare, în temeiul acelei dispoziții, nu impune ca fiecare dintre ei să aibă acces la datele cu caracter personal în cauză.”[32]

47 Orice sugestie conform căreia RTB este doar un protocol tehnic care nu solicită și nu direcționează nicio organizație să prelucreze date cu caracter personal este greșită. O astfel de poziție ar fi, de asemenea, inexactă. Structura facilitează prelucrarea și difuzarea datelor cu caracter personal, întrucât structura și protocoalele aferente conțin câmpuri concepute pentru a prelucra date cu caracter personal și categorii speciale.

48 Astfel, conceptului de operator asociat trebuie să i se ofere o interpretare largă și extinsă pentru a oferi o protecție eficientă și completă persoanelor vizate.

Aplicarea legislației la faptele concrete

49 Cei care determină mijloacele (protocoalele RTB) și scopurile (implicarea în sistemul RTB) sunt responsabili pentru RTB ca operatori asociați. În cazul de față, respondenții, prin crearea și determinarea specificațiilor API și a cadrului de consimțământ și a ghidurilor aferente, sunt operatori de date în sensul RGPD. În special:

49.1 Structurile RTB IAB Europe și Google (care conțin protocoalele RTB și politicile lor respective) au fost create fără a ține seama în mod suficient de preocupările privind protecția datelor personale. Atât structurile IAB Europe, cât și Google ar putea - și ar trebui - să fie corectate pentru a ține seama în mod corespunzător de drepturile persoanei vizate. Acest lucru se află în controlul IAB Europe și al Google.

31 Cazul C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388 at [76-77].

32 C-25/17 - *Jehovan todistajat* at [69]

49.2 În cazul *Jehovan todistajat*[33], CJUE (Marea Cameră) a constatat că Comunitatea Martorilor lui Iehova are responsabilitatea în calitate de operator asociat pentru furnizarea de îndrumări, crearea hărților și prin păstrarea înregistrărilor despre membri (diferiți de persoanele vizate). Comunitatea este un operator, în ciuda faptului că nu interacționează cu persoana vizată. CJUE a considerat că Comunitatea are „nu numai ... cunoștințe la nivel general despre faptul că o astfel de prelucrare se efectuează pentru a-și răspândi credința, ci Comunitatea organizează și coordonează activitățile de predicare ale membrilor săi".

49.3 Acest caz este direct comparabil cu situația respondenților, deoarece acele entități corporative furnizează linii directoare, o hartă digitală sub forma specificației RTB și au o listă de membri (IAB Europe operează, de asemenea, un „program de conformitate" care permite membrilor să devină certificați de către IAB Europe). Pârâții au, de asemenea, „cunoștințe la nivel general despre faptul că o astfel de prelucrare se efectuează" pentru a disemina oferte în timp real RTB și IAB Europe / Google „organizează și coordonează activitățile [RTB] ale membrilor săi"[34] prin funcționarea structurii.

49.4 IAB Europe recunoaște că în prezent nu există „nici o modalitate tehnică de a limita modul în care datele sunt utilizate după ce datele sunt primite de către un furnizor pentru luarea deciziilor / licitarea / după livrarea unui anunț, dar au nevoie de o modalitate de a semnaliza în mod clar restricția pentru utilizările permise într-un mod care poate fi verificat"[35]. Aceste defecte inerente sunt cauzate de modalitatea de proiectare a sistemelor respondenților.

33 C-25/17 - *Jehovan todistajat*

34 *Ibid*

35 "pubvendors.json v1.0: Transparency & Consent Framework", IAB Europe și IAB Tech Lab, Proiect pentru comentariu public, mai 2018 https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/414b8e23737209f37c018611af299003d167a270/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md

49.5 IAB Europe și Google furnizează politici (TCF și, respectiv, liniile directoare pentru cumpărători autorizați) și protocoale (OpenRTB și Cumpărători Autorizați) pentru ca utilizatorii să le respecte și să adere la ele. Aceste ghiduri și protocoale sunt un sistem cu un deficit inerent și sistematic de protecție a datelor.

49.6 Statutul IAB Europe afirmă că scopul său este „să dezvolte și să promoveze publicitate interactivă și marketing", precum și diferite scopuri care susțin acest scop.[36] Actul constitutiv al IAB Europe afirmă că scopul său este „promovarea comercializării și vânzării de publicitate interactivă și de altă natură și sponsorizare pe și prin intermediul internetului în medii online și interactive", inclusiv „Furnizarea de sprijin pentru creșterea utilizării publicității în media interactivă"[37]

49.7 Lista membrilor generali ai IAB Europe („cercul interior" al membrilor) include organizații cheie din industrie precum Google, Amazon, Facebook etc.[38]

49.8 O analogie poate fi realizată cu conceptul de „asociație de întreprinderi" în dreptul UE privind concurența. În temeiul articolului 101 alineatul (1) din Tratatul privind funcționarea Uniunii Europene („TFUE"), deciziile luate de asociația de întreprinderi pot fi anticoncurențiale. În timp ce TFUE nu definește termenul, Concluzia avocatului general Leger din C-309/99 J.C.J. Wouters EU: C: 2001: 390 a declarat la §61 că „[o] regulă generală, o asociație este formată din întreprinderi de același tip general și se responsabilizează pentru reprezentarea și apărarea intereselor lor comune față de alți operatori economici, organele guvernamentale și publicul în general."[39] Această descriere se potrivește IAB

36 3.1 din „Statutul modificat și reformulat al Interatctive Advertising Bureau, Inc.", 29 septembrie 2014 (https://www.iab.com/wp-content/uploads/2015/05/IABBylaws20140929A.pdf).

37 Secțiunea 3 a Actului constitutiv al IAB Europe

38 Vedeți "Despre IAB ", pagina 1 la: https://www.iab.com/wp-content/uploads/2018/05/IAB_Programmatic-In-Housing-Whitepaper_v7a.pdf

39 A se vedea, de exemplu, abordarea adoptată în ceea ce privește Mastercard în contextul deciziei Comisiei și litigiilor ulterioare privind comisioanele de schimb (a se vedea, în special, Decizia Comisiei din 2007 în cazurile COMP / 34.579 MasterCard, COMP / 36.518 Eurocommerce și COMP / 38.580 Carduri comerciale). În special, Comisia (și instanțele europene) au respins argumentul potrivit căruia asociația băncilor, reprezentată de companiile MasterCard, ar putea scăpa de răspunderea pentru normele adoptate de asociație prin externalizarea procesului decizional către organele MasterCard. Nu li s-a permis să se sustragă prin „externalizarea" responsabilităților lor în acest mod. Organismele reprezentative MasterCard, precum și băncile membre, ar putea fi responsabile pentru efectele anticoncurențiale ale normelor adoptate de

Europe, iar principiul care stă la bază sa (conform căruia companiile nu ar trebui să poată scăpa de responsabilitățile lor legale acționând prin asociații de tip „arm's length") se aplică la fel în contextul protecției datelor.

49.9 Mai mult, IAB Europe acționează nu doar ca un set de standarde independente, ci ca un reprezentant / agent care acționează în numele membrilor săi. Având în vedere personalitatea sa juridică distinctă, este un organism adecvat să își asume responsabilitatea în calitate de reprezentant.

50 Având în vedere diferitele probleme ridicate mai sus, concluzia inevitabilă trebuie să fie că cei care controlează structurile acționează ca operatori.

Doar un cod cu sursă deschisă?

51 Orice sugestie că respondenții sunt creatori pasivi și benigni ai protocoalelor și cadrelor care controlează RTB este greșită. Aceștia sunt operatori autorizați ai acelei structuri și, ca atare, sunt operatori în sensul RGPD.[40] Orice sugestie conform căreia încadrarea respondenților drept operatori ar avea un „efect de autocenzurare asupra dezvoltării standardelor de conformitate cu sursă deschisă care servesc la sprijinirea jucătorilor din industrie și la protejarea consumatorilor"[41] ar fi greșit. În mod concret:

51.1 Protocoalele RTB și cadrele și îndrumările aferente depășesc furnizarea unui standard de sursă deschisă. Mai degrabă, cei care participă la industria RTB sunt obligați să utilizeze mijloacele dictate de respondenți pentru a putea participa la RTB. Nu există nicio posibilitate de a se abate de la aceste sisteme dacă un actor dorește să lucreze prin RTB. Astfel, respondenții determină mijloacele și scopurile RTB și acționează ca operatori asociați ai acestor sisteme.

51.2 Protocolul RTB are un efect răspândit și semnificativ asupra drepturilor

organizația de plăți.

40 De exemplu, a se vedea următorul caz așteptat Fashion-ID (C-40/17), a se vedea și Wirtschaftsakademie, unde Curtea confirmă că entitățile pot fi operatori de date fără a vedea vreodată prelucrarea datelor cu caracter personal.

41 https://iabeurope.eu/all-news/iab-europe-comments-on-belgian-dpa-report/

persoanelor vizate. Singurii actori cu capacitatea de a schimba acest sistem sunt IAB Europe și Google. După cum a constatat în mod constant CJUE, este necesară o interpretare extinsă a „operatorilor asociați” pentru a asigura protecția „eficientă și completă” a persoanelor vizate[42]. Fără o astfel de interpretare, drepturile persoanelor vizate nu ar fi protejate în mod adecvat.

51.3 Spre deosebire de majoritatea protocoalelor cu sursă deschisă, RTB are ca rezultat încălcări generalizate și sistemice ale RGPD. Niciun alt protocol cu sursă deschisă nu duce la abuzuri ale drepturilor omului pe această scară. În caz contrar, cei responsabili pentru acele încălcări ale drepturilor omului ar trebui să fie responsabili pentru remedierea încălcărilor pe care le-au creat.

52 Astfel, respondenții sunt capabili de și responsabili pentru remedierea abuzurilor pe scară largă ale drepturilor omului cauzate de protocoalele lor.

Concluzii

53 În consecință, solicităm ANSPDCP să ia măsuri cu privire la cadrele de guvernare și structura sistemului RTB în sine. Fără o astfel de acțiune, actorii individuali care utilizează și se bazează pe structura RTB vor continua să acționeze încălcând principiile protecției datelor. Aceste companii se confruntă cu o alegere de neinvidiat: ori se bazează pe ilegalitatea latentă în structură, ori nu participă la industria RTB din Europa. ANSPDCP poate remedia acest deficit legal printr-un audit asupra problemelor și poate lua măsuri de aplicare pentru a se asigura că sunt remediate.

54 În situația în care un organism este cel puțin potențial un operator (adică un operator de date „presupus”) ANSPDCP are puteri adecvate pentru a interveni. Fără a aduce atingere acestui fapt, reclamanții consideră că, în lumina deciziei CJUE din *Tietosuojavaltuutettu*[43], respondenții sunt în fapt operatori de date asociați.

F Jurisdicție

42 Vedeți cazurile *Google Spain*, *Weltimmo, Schrems, Wirtschaftsakademie and Jehovan todistajat* etc.

43 La fel ca și Comunitatea Martorilor lui Iehova în acest caz, IAB este standardul, care exercită o influență asupra modului în care datele sunt prelucrate.

55 ANSPDCP are jurisdicție asupra activităților ridicate în aceste comunicări și descrise în Raportul Ryan.

●*.i Procesarea datelor personale*

56 Articolul 4 din RGPD menționează că „date cu caracter personal înseamnă orice informație referitoare la o persoană fizică identificată sau identificabilă.” Aceasta include „un identificator online” în care permite identificarea unei persoane, direct sau indirect. Curtea de Justiție a Uniunii Europene a confirmat că adresele IP pot constitui date cu caracter personal.[44] Mai mult, datele cu caracter personal „pseudonimizate” vor fi tratate în continuare ca date cu caracter personal.

57 Diseminarea și difuzarea datelor personale ale unei persoane vizate în timpul procesului RTB implică prelucrarea datelor cu caracter personal, inclusiv adrese IP sau date personale mai granulare, cum ar fi locația.

●*.ii Reclamantul*

58 Sesizarea este depusă de către Asociația pentru Tehnologie și Internet, București, România

●*.iii Respondenții*

59 În conformitate cu articolul 3 al RGPD, RGPD se va aplica operatorilor de date din afara UE în cazul în care prelucrarea lor se referă la monitorizarea comportamentului persoanelor vizate în UE.

60 Industria acționează pentru a oferi reclame celor de pe teritoriul relevant. Ca atare, locul înființării diferitelor companii implicate este irelevant pentru domeniul de aplicare al RGPD și al jurisdicției ANSPDCP.

44 Cazul C-582/14 *Breyer*

61 A se nota pentru exhaustivitate că autoritățile de supraveghere principale iau deja în considerare sediul respondenților în Europa:

61.1 Comisarul Irlandez pentru Protecția Datelor are în vedere activitățile Google

61.2 Autoritatea Belgiană pentru Protecția Datelor a făcut deja constatări inițiale cu privire la IAB Europe

62 Având în vedere sfera geografică a problemelor și a companiilor avute în vedere în această plângere, ar fi potrivit ca autoritățile de supraveghere să ia în considerare această problemă în ansamblu, deoarece RTB afectează toți utilizatorii internetului. **Prin urmare, invităm ANSPDCP să:**
(1) să trimită această plângere autorităților de supraveghere principale, și anume Comisarului Irlandez pentru Protecția Datelor pentru Google și Autorității Belgiene pentru Protecția Datelor, care efectuează deja o investigație cu privire la conformitatea respondenților cu RGPD; și
(2) să ia legătura cu alte autorități naționale de supraveghere în vederea lansării unei anchete comune în conformitate cu articolul 62 din RGPD.

G <u>Următoarele etape</u>

63 Activitățile descrise mai sus sunt la o asemenea scară și complexitate încât oricine ar putea fi afectat în orice moment. Afectează persoanele vizate, inclusiv persoanele vulnerabile, din toate categoriile sociale, în întreaga UE. Prin urmare, invităm ANSPDCP să trimită această plângere împotriva IAB Europe și Google către autoritățile competente de supraveghere din Belgia și Irlanda, care la momentul acestei plângeri efectuează o anchetă și să se asocieze cu omologii lor din alte state membre pentru a desfășura o anchetă comună în conformitate cu articolul 62 din RGPD.

64 Dacă este cazul, vom completa această plângere cu alte dovezi și argumente. Între timp, dacă putem oferi ajutor suplimentar, vă rugăm să nu ezitați să ne contactați.

65 V-am fi recunoscători dacă ne-ați putea ține la curent cu măsurile luate ca răspuns la această comunicare, în conformitate cu articolul 77 alineatul (2) din RGPD.