



**17/RO**

**GL 247**

**Avizul 01/2017 cu privire la  
Propunerea de regulament privind viața privată și comunicațiile electronice  
(2002/58/CE)**

**Adoptat la 4 aprilie 2017**

Acest grup de lucru a fost instituit în temeiul articolului 29 din Directiva 95/46/CE și este un organ consultativ european independent privind protecția datelor și a vieții private. Atribuțiile acestuia sunt descrise la articolul 30 din Directiva 95/46/CE și la articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de Direcția C (Drepturi fundamentale și statul de drept) din cadrul Comisiei Europene, Direcția Generală Justiție și Consumatori, B-1049 Bruxelles, Belgia, biroul nr. MO-59 05/035.

Site: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

**GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE  
PRELUCRAREA DATELOR CU CARACTER PERSONAL**

instituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

având în vedere articolele 29 și 30 din directiva respectivă,

având în vedere regulamentul său de procedură,

**ADOPTĂ PREZENTUL AVIZ:**

## REZUMAT

Grupul de lucru salută propunerea Comisiei Europene din 10 ianuarie 2017 cu privire la un Regulament privind viața privată și comunicațiile electronice. Grupul de lucru apreciază în mod favorabil **alegerea regulamentului** ca instrument normativ. Astfel se asigură uniformitatea normelor în întreaga UE și claritate atât pentru autoritățile de supraveghere, cât și pentru organizații. De asemenea, se asigură coerența cu Regulamentul general privind protecția datelor. În plus, la asigurarea coerenței contribuie și opțiunea de a desemna **aceeași autoritate care răspunde de monitorizarea conformității cu RGPD** pentru a răspunde și de asigurarea respectării normelor privind viața privată și comunicațiile electronice.

În același timp, alegerea (menținerea) unui **instrument juridic complementar** este un lucru pozitiv. Protecția comunicațiilor confidențiale și a echipamentelor terminale comportă caracteristici speciale care nu sunt abordate de RGPD. Prin urmare, sunt necesare dispoziții complementare cu privire la aceste tipuri de servicii, astfel încât să se asigure protecția corespunzătoare a dreptului fundamental la viața privată și confidențialitatea comunicațiilor, inclusiv confidențialitatea echipamentelor terminale. În această privință, grupul de lucru sprijină cu fermitate **abordarea principală** adoptată în propunerea de regulament, **de extindere a interdicțiilor și de restrângere a excepțiilor**, precum și **aplicarea punctuală a conceptului de consimțământ**.

Grupul de lucru salută extinderea domeniului de aplicare al propunerii de regulament astfel încât să **includă furnizorii de servicii over-the-top (OTT)**, astfel de servicii fiind echivalente din punct de vedere funcțional cu mijloacele de comunicare tradiționale și, prin urmare, având un potențial similar de a afecta viața privată a persoanelor din UE și dreptul acestora la secretul comunicațiilor. De asemenea, este un lucru pozitiv faptul că propunerea de regulament vizează în mod clar **conținutul și metadatele asociate** și recunoaște că **metadatele pot dezvălui date foarte sensibile**.

Grupul de lucru menționează însă și patru motive de **profundă îngrijorare**. În ceea ce privește **localizarea echipamentelor terminale; condițiile în care este permisă analiza conținutului și a metadatelor; setările implicite ale echipamentelor terminale și ale programelor software, iar în ceea ce privește pereții de urmărire**, propunerea de regulament ar reduce nivelul de protecție acordat în temeiul RGPD. În prezentul aviz, grupul de lucru oferă sugestii concrete pentru a se asigura garantarea de către Regulamentul privind viața privată și comunicațiile electronice a aceluiași nivel de protecție sau a unuia mai ridicat, adecvat caracterului sensibil al datelor transmise în cadrul comunicațiilor (atât prin prisma conținutului, cât și a metadatelor).

În ceea ce privește **urmărirea prin Wi-fi**, în funcție de circumstanțele și scopurile colectării datelor, o astfel de urmărire în temeiul RGPD ar putea face obiectul consimțământului sau ar putea fi efectuată numai dacă datele cu caracter personal colectate sunt anonimizate. În acest din urmă caz, trebuie îndeplinite următoarele 4 condiții: scopul colectării datelor de la echipamentele terminale să fie limitat la simpla numărare statistică, urmărirea să fie limitată în timp și spațiu la strictul necesar acestui scop, datele să fie șterse sau anonimizate imediat după aceea și să existe posibilități efective de renunțare. Comisia Europeană este invitată să promoveze un standard tehnic pentru semnalarea automată de către dispozitivele mobile a unei obiecții împotriva unei astfel de urmăriri.

În ceea ce privește **analiza conținutului și a metadatelor**, punctul de plecare ar trebui să fie faptul că este interzisă prelucrarea datelor transmise în cadrul comunicațiilor fără consimțământul tuturor utilizatorilor finali (expeditori și destinatari). Pentru a permite furnizorilor să furnizeze serviciile solicitate în mod explicit de utilizator, cum ar fi, de exemplu, funcționalitatea de căutare și indexare sau serviciile de transformare a textului în vorbire, ar trebui să existe o excepție internă pentru prelucrarea conținutului și a metadatelor în scopurile pur personale ale utilizatorului însuși.

În ceea ce privește **consimțământul privind urmărirea**, grupul de lucru solicită interzicerea explicită a pereților de urmărire, adică a opțiunilor de tipul „acceptare sau renunțare”, care îi obligă pe utilizatori să consimtă la urmărire dacă doresc să aibă acces la serviciul respectiv.

Nu în ultimul rând, grupul de lucru recomandă ca echipamentele terminale și programele software **să ofere în mod implicit setări de protecție a vieții private** și să ofere utilizatorilor opțiuni clare de a confirma sau de a modifica aceste setări implicite în timpul instalării. Setările trebuie să fie ușor accesibile pe parcursul utilizării. Utilizatorilor trebuie să li se acorde posibilitatea să își semnaleze consimțământul concret prin setările browserului. În materie de protecție a vieții private posibilitatea de a exprima preferințe nu ar trebui să se limiteze la interferența unor terți sau la modulele cookie. Grupul de lucru recomandă cu tărie ca respectarea standardului „Do not track” (Fără monitorizare) să devină obligatorie.

Grupul de lucru a identificat și alte motive de îngrijorare, referitoare, de exemplu, la domeniul de aplicare, la protecția echipamentelor terminale și la marketingul direct. Nu în ultimul rând, grupul de lucru a identificat aspecte care necesită clarificări, pentru a proteja mai bine utilizatorii finali și pentru a asigura un nivel mai ridicat de securitate juridică pentru toate părțile interesate implicate.

## CUPRINS

<b>1. INTRODUCERE.....</b>	<b>6</b>
<b>2. ASPECTE POZITIVE ALE PROPUNERII DE REGULAMENT.....</b>	<b>6</b>
<i>Armonizarea la nivelul UE, alinierea amenzilor și asigurarea respectării exclusiv de către autoritățile pentru protecția datelor (APD).....</i>	
<i>Extinderea domeniului de aplicare în comparație cu Directiva asupra confidențialității și comunicațiilor electronice.....</i>	<i>8</i>
<i>Aplicarea punctuală a conceptului de consimțământ.....</i>	<i>11</i>
<b>3. MOTIVE DE PROFUNDĂ ÎNGRIJORARE .....</b>	<b>11</b>
<i>Protecția în temeiul RGPD este subminată de propunerea de regulament .....</i>	<i>11</i>
<b>4. ALTE MOTIVE DE ÎNGRIJORARE.....</b>	<b>19</b>
<i>Domeniul de aplicare teritorial și material trebuie extins.....</i>	<i>19</i>
<i>Este necesară consolidarea protecției echipamentelor terminale .....</i>	<i>20</i>
<i>Marketingul direct.....</i>	<i>24</i>
<i>Calendar .....</i>	<i>27</i>
<i>Alte motive de îngrijorare.....</i>	<i>27</i>
<b>5. SUGESTII DE CLARIFICARE PENTRU A ASIGURA SECURITATEA JURIDICĂ .....</b>	<b>30</b>
<i>Clarificări privind domeniul de aplicare.....</i>	<i>30</i>
<i>Clarificări privind conceptul de consimțământ și aplicarea acestuia .....</i>	<i>34</i>
<i>Clarificări privind localizarea și alte metadate.....</i>	<i>35</i>
<i>Clarificări privind comunicațiile nesolicitate.....</i>	<i>36</i>
<i>Clarificări în legătură cu aplicarea instrumentelor privind drepturile fundamentale .....</i>	<i>38</i>
<i>Alte clarificări.....</i>	<i>39</i>

## 1. INTRODUCERE

1. Grupul de lucru „Articolul 29” pentru protecția datelor (denumit în continuare „grupul de lucru” sau „GL 29”) salută propunerea Comisiei Europene (CE) de Regulament privind viața privată și comunicațiile electronice (propunerea de regulament sau Regulamentul privind viața privată și comunicațiile electronice)<sup>1</sup>, care are drept scop înlocuirea Directivei asupra confidențialității și comunicațiilor electronice (DCCE)<sup>2</sup>.
2. Propunerea de regulament cuprinde multe aspecte pozitive, iar Comisia Europeană a făcut un pas important prin prezentarea acesteia, însă i se mai pot aduce îmbunătățiri. Acestea ar fi utile nu numai pentru o mai bună protecție a utilizatorilor finali, ci și pentru asigurarea unui nivel mai ridicat de securitate juridică pentru toate părțile implicate.
3. Astfel, grupul de lucru are câteva motive de îngrijorare și recomandări de clarificări care urmează să fie abordate de Parlamentul European și de Consiliul de Miniștri în dezbaterile lor privind propunerea de regulament. Prezentul aviz va analiza mai întâi aspectele pozitive ale propunerii de regulament, apoi va evidenția motivele de îngrijorare și chestiunile de clarificat.

## 2. ASPECTE POZITIVE ALE PROPUNERII DE REGULAMENT

*ARMONIZAREA LA NIVELUL UE, ALINIAREA AMENZILOR ȘI ASIGURAREA RESPECTĂRII EXCLUSIV DE CĂTRE AUTORITĂȚILE PENTRU PROTECȚIA DATELOR (APD)*

4. Grupul de lucru apreciază în mod favorabil **alegerea regulamentului ca instrument normativ**. Astfel se asigură uniformitatea normelor în întreaga UE (cu anumite excepții, care vor fi discutate în continuare). Acest lucru oferă claritate atât pentru autoritățile de supraveghere, cât și pentru organizații. În plus, având în vedere rolul esențial pe care îl are Regulamentul general privind protecția datelor (RGPD)<sup>3</sup> în propunerea de regulament, acest lucru contribuie la asigurarea coerenței la nivelul ambelor instrumente. În același timp, **alegerea (păstrarea) unui instrument juridic**

---

<sup>1</sup> Propunere de Regulament al Parlamentului European și al Consiliului privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice și de abrogare a Directivei 2002/58/CE (Regulamentul privind viața privată și comunicațiile electronice), 2017/0003 (COD), URL: [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=41241](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241).

<sup>2</sup> Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), JO L 201, 31.7.2002, p. 37-47, URL: <http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32002L0058>.

<sup>3</sup> Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), JO L 119/1, 4.5.2016, p. 1-88, URL: <http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679>.

**complementar** este un lucru pozitiv. Protecția comunicațiilor confidențiale și a echipamentelor terminale comportă caracteristici speciale care nu sunt abordate de RGPD. Prin urmare, sunt necesare dispoziții complementare cu privire la aceste tipuri de servicii pentru a asigura o protecție adecvată a acestui drept fundamental. În acest context, grupul de lucru **sprijină și abordarea principală de extindere a interdicțiilor și de restrângere a excepțiilor, adoptată în propunerea de regulament**, și consideră că ar trebui evitată introducerea unor excepții deschise, de tipul celor de la articolul 6 din RGPD, în special cea de la articolul 6 alineatul (1) litera (f) din RGPD (temeiul privind interesul legitim).

5. **Asigurarea respectării acestor norme de către aceeași autoritate care răspunde de monitorizarea conformității cu RGPD** va susține și mai mult coerența între cele două instrumente. Având în vedere legătura dintre protecția datelor cu caracter personal și protecția comunicațiilor confidențiale și a echipamentelor terminale, este util ca asigurarea respectării dispozițiilor din propunerea de regulament să fie încredințată aceleiași autorități de supraveghere care asigură respectarea RGPD (considerentul 38 și articolul 18 din propunerea de regulament). În plus, jurisprudența Curții de Justiție a Uniunii Europene (CJUE)<sup>4</sup> confirmă faptul că este esențial ca autoritatea de supraveghere să fie independentă, astfel cum prevede articolul 7 din cartă. Totuși, din punct de vedere practic acest lucru ar însemna un important volum de activitate suplimentară pentru APD, fără garanția ducerii la bun sfârșit a acțiunii dacă nu se obține un buget suplimentar. De aceea, autoritățile pentru protecția datelor salută considerentul 38 din propunerea de regulament, care subliniază că fiecare autoritate de supraveghere ar trebui să beneficieze de resurse financiare și umane suplimentare, de sedii și de infrastructura necesare pentru îndeplinirea cu eficacitate a sarcinilor în temeiul noului regulament. De asemenea, este binevenit faptul că articolul 18 alineatul (2) furnizează temeiul juridic pentru cooperarea dintre autoritățile de supraveghere din propunerea de regulament și autoritățile naționale de reglementare din propunerea de directivă de instituire a Codului european al comunicațiilor electronice (*European Electronic Communications Code – EECC*)<sup>5</sup>.
6. De asemenea, având în vedere relația strânsă dintre propunerea de regulament și RGPD, este binevenită și **alinieră cu RGPD a amenzilor din propunerea de regulament**. Activitățile care intră sub incidența propunerii de regulament sunt destul de sensibile, implicând printre altele interferența cu comunicațiile confidențiale și cu echipamentele terminale. Nivelul amenzilor ar trebui să fie proporțional cu acest context sensibil. Acest context reprezintă și motivul pentru care este importantă armonizarea în întreaga UE, pentru a se asigura același nivel înalt de protecție în întreaga regiune. Articolul 23 din propunerea de regulament prevede pentru

---

<sup>4</sup> A se vedea, de exemplu, Hotărârea CJUE în cauza C-362/14 (Sfera de siguranță) din 6 octombrie 2015, punctul 41, și Hotărârea CJUE în cauzele conexe C-203/15 și C-698/15 (Tele2/Watson) din 21 decembrie 2016, punctul 123.

<sup>5</sup> Propunere de directivă a Parlamentului European și a Consiliului de instituire a Codului european al comunicațiilor electronice (reformare), 2016/0288 (COD), 12.10.2016, URL: [http://eur-lex.europa.eu/legal-content/RO/ALL/?uri=comnat%3ACOM\\_2016\\_0590\\_FIN](http://eur-lex.europa.eu/legal-content/RO/ALL/?uri=comnat%3ACOM_2016_0590_FIN).

încălcarea regulamentului amenzi eficace, similare ca nivel cu cele stabilite pentru încălcarea normelor din RGPD, cu excepția câtorva puncte (a se vedea observația 38).

7. De asemenea, trebuie salută **eliminarea normelor specifice de notificare privind încălcarea securității datelor** din această legislație, pentru a împiedica suprapunerea inutilă cu cerințele privind încălcarea securității datelor din RGPD.
8. De asemenea, este **de apreciat faptul că accentul se pune acum pe asigurarea unui nivel egal de protecție pentru toți utilizatorii finali**, deoarece propunerea de regulament a eliminat noțiunea de diferențiere între „abonați” și alți utilizatori ai serviciilor de comunicații electronice.

#### *EXTINDEREA DOMENIULUI DE APLICARE ÎN COMPARAȚIE CU DIRECTIVA ASUPRA CONFIDENȚIALITĂȚII ȘI COMUNICAȚIILOR ELECTRONICE*

9. Grupul de lucru salută **extinderea domeniului de aplicare al propunerii de regulament, astfel încât să includă furnizorii de servicii *over-the-top* (OTT)**, aceste servicii fiind echivalente din punct de vedere funcțional cu mijloacele de comunicare mai tradiționale și, prin urmare, având un potențial similar de a afecta viața privată a cetățenilor UE și dreptul acestora la confidențialitatea comunicațiilor. Grupul de lucru apreciază îndeosebi faptul că toate categoriile de OTT (OTT0, OTT1 și unele OTT2)<sup>6</sup> intră acum sub incidența regulamentului, deoarece acesta nu vizează numai mijloacele de comunicare tradiționale (OTT0), ci și serviciile echivalente din punct de vedere funcțional (OTT1), astfel cum se menționează la articolul 8 alineatul (1) litera (c) din propunerea de regulament. De asemenea, este pozitiv faptul că, pe lângă definițiile din EECC, sunt incluse și unele OTT2 atunci când acestea furnizează comunicații interpersonale și interactive auxiliare legate în mod intrinsec de serviciul lor, de exemplu, în cazul jocurilor, al aplicațiilor pentru găsirea unui partener sau al site-urilor de recenzii [articolul 4 alineatul (2) din propunerea de regulament]. În mod similar, este binevenită și **clarificarea faptului că protecția vizează și interacțiunea dintre mașini**. Considerentul 12 clarifică faptul că dispozitivele care comunică unele cu altele intră sub incidența protecției oferite în temeiul propunerii de regulament. Acest lucru este de dorit, deoarece astfel de comunicații conțin adesea informații protejate în temeiul drepturilor privind viața privată. Totuși, s-ar putea aduce clarificări în privința aplicabilității [a se vedea observația 40 litera (h)].
10. În plus, constituie un aspect pozitiv faptul că **propunerea de regulament vizează în mod clar conținutul și metadatele asociate**. Considerentul 14 clarifică faptul că definiția de la articolul 4 alineatul (3) litera (a) privind „datele transmise în cadrul

<sup>6</sup> Pentru o explicare suplimentară a acestor termeni, a se vedea OAREC, *Report on OTT Services*, BoR (16) 35, 29 ianuarie 2016, p. 15 și 16, URL:

[http://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/reports/5751-berec-report-on-ott-services](http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services). De asemenea, este de reținut observația din raport conform căreia categoriile sunt concepute drept noțiuni de utilizat în dezbateră despre revizuire și nu drept concepte juridice.



comunicațiilor electronice” trebuie să fie suficient de generală pentru a acoperi *toate tipurile* de conținut, precum și metadatele asociate, indiferent – de exemplu – de mijloacele de transmitere a semnalelor. Cu toate acestea, în observația 39, grupul de lucru menționează drept motiv de îngrijorare faptul că această definiție actuală a „datelor transmise în cadrul comunicațiilor electronice” este încă supusă dezbaterii. În conformitate cu această extindere a domeniului de aplicare, grupul de lucru consideră că **recunoașterea faptului că metadatele ar putea dezvălui date foarte sensibile** (a se vedea punctul 2.2 din expunerea de motive; considerentul 2) constituie o adăugire esențială. Grupul de lucru salută faptul că, prin aceasta, Comisia Europeană integrează considerațiile CJUE din hotărârile *Digital Rights Ireland* și *Tele2/Watson*. De asemenea, GL 29 apreciază **recunoașterea faptului că analiza conținutului reprezintă o prelucrare cu risc ridicat**. Considerentul 19 și articolul 6 alineatul (3) litera (b) prevăd prezumția legală logică potrivit căreia scanarea conținutului reprezintă o prelucrare cu risc ridicat conform articolul 35 din RGPD și, aparent indiferent de existența unui risc rezidual ridicat, necesită întotdeauna o consultare prealabilă cu autoritatea (principală) de protecție a datelor. În același timp, grupul de lucru este îngrijorat de sfera de aplicare a definiției metadatelor și de faptul că analiza acestora nu este supusă aceleiași cerințe obligatorii privind evaluarea impactului asupra protecției datelor (*Data Protection Impact Assessment* – DPIA) (a se vedea observațiile 33 și 46).

11. **Recunoașterea în continuare a importanței anonimizării datelor** este de asemenea binevenită. În Directiva asupra confidențialității și comunicațiilor electronice, măsurile de anonimizare au jucat deja un rol în asigurarea compatibilității [de exemplu, articolul 6 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice, care prevede că datele de trafic trebuie șterse sau trecute în anonimat de îndată ce nu mai sunt necesare în scopul transmiterii comunicației]. În conformitate cu articolul 6 alineatul (2) litera (c) și articolul 6 alineatul (3) litera (b) din propunerea de regulament, excepția de la interdicția de prelucrare a metadatelor și a conținutului este permisă pe baza consimțământului, cu condiția ca scopul sau scopurile în cauză „să nu fi putut fi îndeplinite prin prelucrarea informațiilor anonimizate”. Solicitarea unor astfel de măsuri de protecție a vieții private, pe lângă solicitarea consimțământului utilizatorilor, îi protejează pe aceștia de prelucrarea nejustificată. În același timp însă, grupul de lucru își exprimă profunda îngrijorare cu privire la faptul că adoptarea unor astfel de tehnici de anonimizare nu ar fi obligatorie în cazul localizării utilizatorilor prin intermediul echipamentelor mobile ale acestora (a se vedea observația 17). În plus, chiar și atunci când trebuie aplicate măsuri de anonimizare, furnizorii ar trebui să efectueze întotdeauna o evaluare a impactului asupra protecției datelor (DPIA) (a se vedea observațiile 33 și 46), iar grupul de lucru solicită introducerea unei obligații suplimentare, de a face public modul în care datele sunt anonimizate și aggregate [a se vedea observația 42 litera (b)].

12. Un alt aspect pozitiv îl constituie **formularea extinsă cu privire la protecția echipamentelor terminale**. În considerentul 20 și în articolul 8 se statuează că tehnologiile utilizate pentru accesul la echipamentele terminale nu sunt relevante: orice amestec în legătură cu echipamentele terminale, inclusiv utilizarea capacităților de prelucrare ale acestora, necesită consimțământul utilizatorului final (cu unele excepții). Astfel CE face precizarea utilă că „amprentarea unui echipament în rețea”

(*device fingerprinting*) intră sub incidența acestei dispoziții. În plus, grupul de lucru apreciază faptul că nerespectarea de către o terță parte a preferințelor exprimate prin **setările browserului unei anumite persoane îi este opozabilă acesteia**, astfel cum se descrie în considerentul 22. Prevederea este utilă pentru acele situații în care un terț (cum ar fi o rețea publicitară) nu respectă aceste setări, dar același lucru ar trebui prevăzut și în propunerea de regulament, printr-o dispoziție relevantă.

13. În sfârșit, trebuie salutat faptul că, în continuare, **persoanele juridice sunt incluse în domeniul de aplicare al propunerii de regulament** [a se vedea punctul 2.2 din expunerea de motive; considerentele 3, 33 și 42; articolul 1, articolul 15 și articolul 16 alineatul (5)]. Această prevedere există deja în Directiva asupra confidențialității și comunicațiilor electronice însă, dat fiind că autoritățile de protecție a datelor vor avea sarcina de a asigura respectarea noilor norme, este util să subliniem în mod precis acest lucru. Astfel, li se permite autorităților care răspund de protecția datelor să ia măsuri în cazurile în care persoanele juridice sunt victime ale unei încălcări, de exemplu atunci când corporațiile primesc mesaje spam sau comunicațiile le sunt monitorizate în mod clandestin. Totuși, grupul de lucru remarcă și unele motive de îngrijorare, cum ar fi faptul că aplicarea cerinței privind consimțământul persoanelor juridice nu este clară [a se vedea observația 41 litera (a)] și faptul că nu este clar ce se înțelege prin „interesul legitim” al persoanelor juridice în cazul marketingului direct [a se vedea observația 43 litera (c)].

14. Grupul de lucru salută o altă categorie de îmbunătățiri legate de aplicarea și interpretarea conceptului de consimțământ. În primul rând, este binevenită **clarificarea faptului că accesul la internet și telefonia (mobilă) sunt servicii esențiale, iar furnizorii acestor servicii nu își pot „forța” clienții să își dea consimțământul pentru orice prelucrare de date care nu este necesară pentru furnizarea serviciului esențial în sine.** În considerentul 18, în special, se menționează că accesul la internet în bandă largă de bază și serviciile de comunicații vocale trebuie considerate servicii esențiale, ceea ce înseamnă că, având în vedere dependența persoanelor de accesul la aceste servicii, consimțământul pentru prelucrarea datelor lor transmise în cadrul comunicațiilor în astfel de scopuri suplimentare (cum ar fi prelucrarea în scopuri publicitare sau de marketing) nu poate fi valabil. În același timp, grupul de lucru este îngrijorat de faptul că această clarificare este prea limitată. Serviciile furnizate de anumiți furnizori de OTT pot fi considerate, de asemenea, servicii esențiale, iar Regulamentul privind viața privată și comunicațiile electronice ar trebui să interzică în mod concret și opțiunile de tipul „acceptare sau renunțare” în alte circumstanțe (a se vedea observația 20).
15. În plus, **armonizarea cerinței privind consimțământul pentru includerea datelor cu caracter personal ale persoanelor fizice în listele de abonați** reprezintă un lucru pozitiv. Conform articolului 15 din propunerea de regulament, prelucrarea datelor din listele de abonați accesibile publicului este permisă numai cu consimțământul persoanelor fizice și numai dacă persoanele juridice au posibilitatea de a se opune. Acest aspect este dezvoltat și mai mult în considerentul 31, în care se afirmă că acest consimțământ trebuie să fie specific cu privire la categoriile concrete de date cu caracter personal care urmează a fi incluse în lista respectivă. Cu toate acestea, grupul de lucru consideră îngrijorător faptul că propunerea de regulament nu prevede suficient de clar solicitarea consimțământului specific separat pentru căutare și căutarea inversă (a se vedea observația 37).
16. **Noua excepție punctuală privind interferența neintruzivă cu echipamentele terminale** este, de asemenea, apreciată. GL 29 consideră utilă clarificarea prin propunerea de regulament a faptului că interdicția nu se aplică măsurării traficului pe internet [cu excepția restrânsă a cazului în care această măsurare este efectuată de către furnizorul serviciului societății informaționale solicitat de utilizatorul final, conform articolului 8 alineatul (1) litera (d) din propunerea de regulament]. A se vedea și considerentul 21. Cu toate acestea, grupul de lucru sugerează utilizarea unei definiții neutre din punct de vedere tehnologic și clarificarea aplicabilității acestei excepții (a se vedea observația 25).

### 3. MOTIVE DE PROFUNDĂ ÎNGRIJORARE

#### *PROTECȚIA ÎN TEMEIUL RGPD ESTE SUBMINATĂ DE PROPUNEREA DE REGULAMENT*

După cum s-a menționat mai sus, există o serie de îmbunătățiri esențiale în propunerea de regulament. Există însă și motive de îngrijorare, cu niveluri diferite de gravitate. În această secțiune, grupul de lucru discută cele patru aspecte în legătură cu care este **foarte**

**îngrijorat.** Acestea sunt prevederi care **subminează nivelul de protecție acordat de RGPD:**

**17. Obligațiile prevăzute în regulament referitoare la localizarea echipamentelor terminale ar trebui să respecte cerințele RGPD.** Articolul 8 alineatul (2) litera (b) din propunerea de regulament impune doar afișarea unui anunț și punerea în aplicare a unor măsuri de securitate pentru colectarea informațiilor emise de echipamentul terminal. La articolul 8 alineatul (2) litera (b) se mai menționează și faptul că persoana care răspunde de această colectare trebuie să indice măsurile pe care le pot lua utilizatorii finali pentru a minimiza sau a opri colectarea. Astfel, articolul 8 alineatul (2) litera (b) dă impresia că organizațiile pot colecta informațiile emise de echipamentele terminale pentru a urmări mișcările fizice ale persoanelor (de exemplu, „urmărirea prin Wi-fi” sau „urmărirea prin Bluetooth”) fără consimțământul persoanei în cauză. După câte se pare, partea care colectează aceste date ar putea să se conformeze prin intermediul unui anunț prin care utilizatorii sunt informați să își oprească dispozitivele atunci când nu vor să fie urmăriți. O astfel de abordare ar fi contrară unui obiectiv fundamental al politicii Comisiei Europene în domeniul telecomunicațiilor – acela de a furniza conectivitate la internet mobil de mare viteză, cu măsuri de protecție solide în ceea ce privește viața privată, la un preț redus pentru toți europenii, la nivel transfrontalier.

În plus, propunerea de regulament nu impune nicio limitare clară în ceea ce privește domeniul de aplicare al activităților de colectare a datelor sau de prelucrare ulterioară. În acest context, trebuie remarcat faptul că aceste adrese MAC sunt date cu caracter personal, chiar și după ce au fost întreprinse măsuri de securitate, cum ar fi hashingul. Neimpunând alte cerințe sau limitări, nivelul de protecție a acestor date cu caracter personal în temeiul propunerii de regulament este semnificativ mai scăzut decât în temeiul RGPD, conform căruia această urmărire ar trebui să fie echitabilă și legală, dar și transparentă. Considerentul 25 menționează în continuare – în mod inutil – că unele dintre funcționalitățile de urmărire prin Wi-fi nu implică riscuri ridicate la adresa vieții private, în timp ce altele – cum ar fi urmărirea persoanelor fizice de-a lungul timpului – prezintă astfel de riscuri. Deși grupul de lucru apreciază recunoașterea faptului că ultima situație implică riscuri ridicate la adresa vieții private, nu este util să se decidă deja în prealabil că anumite alte funcționalități nu prezintă astfel de riscuri, fără o evaluare suplimentară a circumstanțelor și a proporționalității prelucrării. O astfel de evaluare ar trebui efectuată ținând seama de următoarele condiții referitoare la urmărirea neanonimizată prin rețeaua Wi-fi.

În funcție de circumstanțele și scopurile colectării datelor, este posibil ca urmărirea în temeiul RGPD să fie supusă consimțământului sau să poată fi efectuată numai dacă datele cu caracter personal colectate sunt anonimizate. Această anonimizare se face, de preferință, imediat după colectare. Dacă nu este posibilă anonimizarea imediată, având în vedere scopurile pentru care sunt colectate datele, aceste date pot fi prelucrate într-o perioadă în care nu sunt anonimizate doar în următoarele condiții: (i) scopul colectării datelor trebuie limitat la simpla numărare statistică (a se vedea exemplele de mai jos); (ii) urmărirea să fie limitată în timp și spațiu la ceea ce este strict necesar pentru acest scop; (iii) datele să fie șterse sau anonimizate imediat după aceea; și (iv) trebuie să existe o posibilitate efectivă de renunțare. Desigur că operatorii trebuie să respecte, în orice situație, cerința de a furniza informații adecvate.

Grupul de lucru este îngrijorat de faptul că o ofertă potențială de renunțare individuală pentru fiecare organizație care colectează aceste date ar reprezenta o povară inacceptabilă pentru cetățeni, având în vedere creșterea utilizării acestor tehnologii de urmărire atât de către organizațiile din sectorul privat, cât și de cele din sectorul public. Prin urmare, grupul de lucru invită legiuitorul european să promoveze elaborarea unor standarde tehnice pentru semnalarea automată de către dispozitive a unei obiecții împotriva unei astfel de urmări și să se asigure că respectarea unui astfel de semnal este opozabilă terților.

De exemplu, consimțământul în temeiul RGPD ar fi necesar, probabil, atunci când un operator de date colectează și stochează adresele MAC ale dispozitivelor care sunt identificabile indirect (prin Wi-fi sau Bluetooth) și calculează amplasamentul utilizatorului, în vederea localizării utilizatorului de-a lungul timpului, de exemplu în mai multe magazine. Acest lucru este valabil în special în situația în care o astfel de urmărire are loc în zone publice, unde utilizatorii au așteptări legitime de a nu fi identificați sau urmăriți, dar unde se colectează adresele MAC ale trecătorilor. Consimțământul poate fi obținut, de exemplu, prin intermediul unei aplicații care să invite utilizatorii să permită localizarea lor în anumite zone în schimbul unor oferte comerciale sau prin oferirea unor puncte de check-in în anumite locuri sau prin intermediul unui modul de consimțământ în punctele de acces Wi-fi.

Doar într-un număr mic de situații li se poate permite operatorilor să prelucreze informațiile emise de echipamentele terminale pentru a le urmări mișcările fizice fără consimțământul persoanei în cauză. De exemplu, o astfel de situație ar putea fi aceea în care se numără clienții dintr-un anumit amplasament sau în care se colectează datele emise de ambele părți ale unui punct de control de securitate pentru afișarea timpului de așteptare. Totuși, în ambele exemple, datele ar trebui să fie șterse sau anonimizate imediat după îndeplinirea scopului statistic. Aceasta înseamnă că adresele MAC ale dispozitivelor vizitatorilor din interiorul unui anumit amplasament, cum ar fi un magazin, trebuie să fie anonimizate imediat după colectare, fără stocarea lor permanentă și astfel încât posibilitatea reidentificării lor să fie tehnic exclusă. În cazul calculării timpului de așteptare, adresele MAC ar trebui să fie șterse sau anonimizate imediat ce datele nu mai sunt relevante pentru calcularea duratei de așteptare (de exemplu, atunci când vizitatorul a ajuns de cealaltă parte a punctului de control de securitate sau pentru că a părăsit rândul).

În plus, operatorul ar trebui să respecte cerințele privind minimizarea datelor (de exemplu, să nu efectueze urmărirea 24 de ore pe zi, 7 zile pe săptămână dacă scopul este limitat la programul de lucru al magazinului și/sau la eșantionarea la anumite intervale). De asemenea, operatorii trebuie să ia și alte măsuri de atenuare, pentru a se asigura că impactul asupra drepturilor în materie de viață privată ale utilizatorilor este minim sau inexistent, de exemplu pentru a proteja viața privată a persoanelor care locuiesc lângă un punct de colectare.

Alegerea unei simple cerințe de afișare a unui anunț, prevăzută la articolul 8 alineatul (2) din propunerea de regulament, este cu atât mai remarcabilă având în vedere concluzia din considerentul 20, potrivit căreia informațiile referitoare la dispozitivul utilizatorului final pot fi colectate și de la distanță în scopuri de identificare și urmărire și că această prelucrare – în conformitate cu propunerea de

regulament – poate periclita în mod flagrant viața privată a acestor utilizatori finali. În plus, obligația nu depășește cerința de informare prevăzută deja la articolele 13 și 14 din RGPD. Imixtiunea gravă în viața privată prin urmărire este amplificată și mai mult de potențialul acces al altor persoane la datele colectate, cum ar fi posibilitatea ca autoritățile de aplicare a legii să identifice utilizatorii finali pe baza adresei (adreselor) MAC stocate de dispozitivele lor mobile.

**18. Trebuie să fie detaliate condițiile în care este permisă analiza conținutului și a metadatelor.**

Prin articolul 6 din propunerea de regulament, metadatelor și conținutului li se acordă niveluri diferite de protecție. GL 29 nu susține această diferențiere: ambele categorii de date sunt extrem de sensibile. Prin urmare, metadatele și conținutul ar trebui să beneficieze de același nivel ridicat de protecție. Astfel, punctul de plecare ar trebui să fie faptul că este interzisă prelucrarea metadatelor și a conținutului fără consimțământul tuturor utilizatorilor finali (cum ar fi expeditorul și destinatarul).

Totuși, în funcție de scopuri, un anumit nivel de prelucrare poate fi permis fără consimțământ, dacă este strict necesar în aceste scopuri:

- furnizorii pot prelucra datele transmise în cadrul comunicațiilor electronice în scopurile menționate la articolul 6 alineatul (1) literele (a) și (b) și la articolul 6 alineatul (2) literele (a) și (b) din propunerea de regulament<sup>7</sup>;
- ar trebui să se clarifice faptul că anumite tehnici de detectare/filtrare a mesajelor spam și de atenuare a efectelor rețelelor de tip „botnet” pot fi considerate strict necesare pentru detectarea sau oprirea utilizării abuzive a serviciilor de comunicații electronice [articolul 6 alineatul (2) litera (b)]. În ceea ce privește filtrarea mesajelor spam, ar trebui să li se ofere opțiuni de renunțare detaliate utilizatorilor finali care primesc mesaje spam, atunci când este posibil din punct de vedere tehnic;
- ar trebui să se clarifice faptul că analiza datelor transmise în cadrul comunicațiilor electronice în scopul serviciilor pentru clienți poate, de asemenea, să intre sub incidența excepției „necesar pentru facturare” [a se vedea articolul 6 alineatul (2) litera (b)]. Metadatele relevante pot fi păstrate până la sfârșitul perioadei în care o factură poate fi contestată prin lege sau în care pot fi inițiate demersuri legale în vederea obținerii unei plăți în conformitate cu dreptul național. Datele relevante (cum ar fi adresele URL) pot fi păstrate numai la cererea utilizatorului final și numai pentru o perioadă strict necesară pentru soluționarea unui litigiu legat de o factură [ceea ce înseamnă că articolul 7 alineatul (3) ar trebui modificat în consecință];

---

<sup>7</sup> În ceea ce privește necesitatea respectării cerințelor obligatorii de calitate a serviciului, astfel cum se prevede la articolul 6 alineatul (2) litera (a) din propunerea de regulament, furnizorii ar trebui să țină seama de condițiile descrise în Regulamentul (UE) nr. 15/2120 (EECS), în special la articolul 3 și în considerentele 10 și 13-15. În temeiul acestei dispoziții, este posibil ca furnizorilor să li se ceară să prelucreze datele transmise în cadrul comunicațiilor pentru a detecta și a filtra programele malware și spyware și li se poate permite să comprime datele.

- ar trebui să fie posibilă prelucrarea datelor transmise în cadrul comunicațiilor electronice în scopul furnizării de servicii solicitate în mod explicit de un utilizator final, cum ar fi funcția de căutare sau de indexare a cuvintelor-cheie, asistenței virtuali, motoarele de transformare text în vorbire și serviciile de traducere. Aceasta necesită introducerea unei exceptări pentru analiza unor astfel de date pentru uzul pur individual (casnic), precum și pentru utilizarea individuală în scopuri profesionale<sup>8</sup>. Astfel, acest lucru ar fi posibil fără consimțământul tuturor utilizatorilor finali, dar poate avea loc numai cu consimțământul utilizatorului final care solicită acest serviciu. De asemenea, un astfel de consimțământ specific ar împiedica furnizorul să utilizeze aceste date în alte scopuri.

Aceasta înseamnă că analiza conținutului și/sau a metadatelor în toate celelalte scopuri, cum ar fi analiza, crearea de profiluri, publicitatea comportamentală sau alte scopuri în beneficiul (comercial) al furnizorului, necesită consimțământul tuturor utilizatorilor finali ale căror date vor fi prelucrate. În ceea ce privește aceste situații, propunerea de regulament ar trebui să explice că simplul act de trimitere a unui e-mail sau a unei comunicări personale de altă natură de la alt serviciu către un utilizator final care a consimțit personal la prelucrarea conținutului și a metadatelor sale (de exemplu, în cursul înscrierii la un serviciu de mesagerie) nu reprezintă consimțământul valabil al expeditorului.

În cele din urmă, trebuie să se clarifice faptul că și prelucrarea datelor altor persoane decât utilizatorii finali (de exemplu, fotografia sau descrierea unui terț în cadrul unui schimb între două persoane) implicați trebuie să respecte toate dispozițiile relevante ale RGPD.

- 19. Echipamentele terminale și programele software trebuie, în mod implicit, să descurajeze, să prevină și să interzică interferențele ilegale cu acestea și să ofere informații despre opțiuni.** Deși propunerea de regulament obligă furnizorii de programe software care permit efectuarea de comunicații electronice să „ofere posibilitatea” de a împiedica o formă limitată de interferență cu echipamentele terminale și, la instalare, obligă furnizorii de software să solicite utilizatorilor finali să își dea consimțământul cu privire la una dintre setările disponibile [articolul 10 alineatele (1) și (2)], o astfel de alegere nu echivalează cu *respectarea implicită a vieții private*. În plus, „opțiunea” de a împiedica anumite interferențe există deja în prezent și până acum acest lucru nu a dus la soluționarea în mod suficient a problemei urmăririi nejustificate. Acesta este chiar motivul pentru care, în cadrul RGPD, a fost adoptată o alegere conștientă în materie de politici de a introduce principiile protecției datelor și a vieții private, începând cu momentul conceperii și în mod implicit (articolul 25 din RGPD). Propunerea de regulament subminează aceste principii în ceea ce privește datele transmise în cadrul comunicațiilor și datele dispozitivelor.

---

<sup>8</sup> Deși considerentul 13 din propunerea de regulament exclude în mod explicit rețelele corporatiste din domeniul de aplicare al regulamentului, această nouă excepție pentru utilizarea individuală ar trebui să abordeze și utilizarea serviciilor cloud de către angajați, în scop profesional, cum ar fi pentru căutarea în e-mailurile lor.



Între timp, Directiva 2014/53/UE privind echipamentele radio<sup>9</sup> (menționată în considerentul 10) prevede doar o obligație foarte limitată în materie de securitate, care impune ca echipamentele radio să încorporeze „sisteme pentru asigurarea protecției datelor cu caracter personal și a vieții private a utilizatorilor și a abonaților” [Articolul 3 alineatul (3) litera (e)]. Acest lucru nu poate înlocui setările specifice privind respectarea implicită a vieții private în propunerea de regulament. În acest sens, merită remarcat, de asemenea, că Sondajul Eurobarometru privind confidențialitatea și comunicațiile electronice, publicat în decembrie 2016, arată că „[aproape] șapte din zece (69 %) persoane sunt total de acord că setările prestabilite ale browserului lor ar trebui să împiedice partajarea informațiilor”<sup>10</sup>. Grupul de lucru are un motiv separat de îngrijorare cu privire la setările browserului și la definiția „terților”. A se vedea observația 24. În plus, trebuie avut în vedere faptul că această prevedere nu se referă numai la browserele utilizate pe calculatoare, ci se extinde și la alte tipuri de software care permit comunicarea (inclusiv sistemele de operare, aplicațiile și interfețele software pentru dispozitivele conectate la internetul obiectelor). În concluzie, echipamentele terminale și programele software trebuie să ofere *în mod implicit* setări de protecție a confidențialității și să ghideze utilizatorii prin meniurile de configurare pentru a modifica aceste setări implicite la instalare. Aceste meniuri de configurare trebuie să fie întotdeauna ușor accesibile în timpul utilizării. Grupul de lucru încurajează legiuitorul european să clarifice domeniul de aplicare al articolului 10 în acest sens.

- 20. Regulamentul privind viața privată și comunicațiile electronice ar trebui să interzică în mod explicit pereții de urmărire**, adică practica prin care accesul la un site sau la un serviciu este refuzat dacă persoanele nu sunt de acord să fie urmărite pe alte site-uri sau servicii. După cum s-a menționat deja în avizele precedente ale grupului de lucru cu privire la Directiva asupra confidențialității și comunicațiilor electronice<sup>11</sup>, astfel de abordări de tipul „acceptare sau renunțare” sunt rareori legitime<sup>12</sup>. Atunci când utilizarea capacităților de prelucrare și stocare ale echipamentelor terminale sau colectarea de informații de la echipamentele terminale ale utilizatorilor finali permite urmărirea activităților utilizatorului în timp sau la nivelul mai multor servicii (de exemplu, site-uri sau aplicații diferite), aceste activități de prelucrare pot afecta serios viața privată a acestor utilizatori. Având în vedere importanța fundamentală a internetului în validarea dreptului fundamental la libertatea de exprimare, inclusiv a dreptului de acces la informații, capacitatea persoanelor de a accesa conținutul online nu ar trebui să depindă de acceptarea urmăririi activităților pe dispozitive și site-uri/aplicații. Prin urmare, viitorul Regulament privind viața privată și comunicațiile electronice ar trebui să precizeze că

---

<sup>9</sup> Directiva 2014/53/UE privind echipamentele radio.

<sup>10</sup> A se vedea Eurobarometrul Flash 443, Raport privind confidențialitatea și comunicațiile electronice (publicat în decembrie 2016), p. 5.

<sup>11</sup> A se vedea, de exemplu, GL 240 (analiză privind confidențialitatea în mediul electronic), p. 16. GL 208 (exceptările de la obținerea consimțământului), p. 5.

<sup>12</sup> Această poziție nu aduce atingere articolului 7 alineatul (4) din RGPD, care poate exclude „opțiunile de tipul acceptare sau renunțare” și în alte situații în care acest lucru este adecvat.

accesul la conținut, de exemplu în site-uri și aplicații, nu poate fi condiționat de acceptarea unor astfel de activități de prelucrare intruzive, indiferent de tehnologia de urmărire aplicată, cum ar fi modulele cookie, amprentarea echipamentelor în rețea, introducerea identificatorilor unici sau alte tehnici de monitorizare. Necesitatea acestei interdicții este subliniată de ultimul sondaj Eurobarometru privind confidențialitatea și comunicațiile electronice, care arată că „aproape două treimi dintre respondenți declară că este inacceptabilă monitorizarea activităților lor online în schimbul accesului nerestricționat la un anumit site (64 %)”.

21. Pe scurt, în ceea ce privește cele patru aspecte menționate anterior, **propunerea de regulament ar trebui să își respecte promisiunea de a oferi un nivel de protecție egal sau mai ridicat decât RGPD**. În considerentul 5 se afirmă în mod concret că propunerea de regulament nu reduce nivelul de protecție de care beneficiază RGPD. Însă, așa cum este formulată în prezent propunerea de regulament, această constatare este incorectă, în special în ceea ce privește urmărirea dispozitivelor (observația 17), lipsa principiului respectării implicite a vieții private (observația 19) și consimțământul (observația 18). Acest lucru este deosebit de important, întrucât în același considerent se menționează că propunerea de regulament va constitui „o *lex specialis* în raport cu RGPD. Aceasta detaliază și completează prevederile regulamentului referitoare la datele transmise în cadrul comunicațiilor electronice care se încadrează în categoria datelor cu caracter personal”. Grupul de lucru sugerează că, cel puțin, textul Regulamentului privind viața privată și comunicațiile electronice clarifică faptul că:

(i) interdicțiile din Regulamentul privind viața privată și comunicațiile electronice prevalează asupra permisiunilor din RGPD [de exemplu, interdicția prevăzută la articolul 5 din Regulamentul privind viața privată și comunicațiile electronice prevalează asupra drepturilor furnizorilor de servicii de comunicații electronice de a prelucra în continuare datele personale în temeiul articolului 5 alineatul (1) litera (b) și al articolului 6 alineatul (4) din RGPD];

(ii) atunci când prelucrarea este permisă în temeiul oricărei excepții (inclusiv privind consimțământul) de la interdicțiile din Regulamentul privind viața privată și comunicațiile electronice, această prelucrare, în cazul în care se referă la date cu caracter personal, trebuie să respecte, totuși, toate dispozițiile relevante din RGPD;

(iii) atunci când prelucrarea este permisă în temeiul oricărei excepții de la interdicțiile din Regulamentul privind viața privată și comunicațiile electronice, este interzisă orice altă prelucrare pe baza RGPD, inclusiv prelucrarea într-un alt scop în temeiul articolului 6 alineatul (4) din RGPD. Acest lucru nu ar împiedica operatorii să solicite consimțământul suplimentar pentru noi operațiuni de prelucrare, nici nu ar împiedica legiuitorii să ofere excepții suplimentare, limitate și specifice în Regulamentul privind viața privată și comunicațiile electronice, de exemplu, pentru a permite prelucrarea în scopuri științifice sau statistice în temeiul articolului 89 din RGPD sau pentru a proteja „interesele vitale” ale persoanelor în temeiul articolului 6 alineatul (d) din RGPD.

În plus, Regulamentul privind viața privată și comunicațiile electronice ar trebui interpretat astfel încât să se asigure că oferă cel puțin același nivel și, acolo unde este cazul, un nivel mai ridicat de protecție decât cel prevăzut în RGPD.

#### 4. ALTE MOTIVE DE ÎNGRIJORARE

Pe lângă punctele menționate mai sus, Grupul de lucru „Articolul 29” este **îngrijorat** de următoarele aspecte.

##### *DOMENIUL DE APLICARE TERITORIAL ȘI MATERIAL TREBUIE EXTINS*

22. **Termenul „metadata” este definit prea restrictiv.** Acesta este definit la articolul 4 alineatul (c) astfel: „datele prelucrate într-o rețea de comunicații electronice în vederea transmiterii, a distribuirii sau a schimbului de conținut al comunicațiilor electronice” (sublinierea noastră). Utilizarea cuvântului „rețea” pare să sugereze că numai datele generate pe parcursul furnizării de servicii la nivelul „inferior” al rețelei s-ar califica drept „metadata”. Acest lucru ar putea însemna că datele generate pe parcursul furnizării unui serviciu OTT ar fi excluse din acest domeniu de aplicare, ceea ce ar fi indezirabil și, probabil, neintenționat, având în vedere intenția de a extinde domeniul de aplicare al propunerii de regulament la furnizorii de servicii OTT. Pentru a elimina această îngrijorare, definiția „metadatelor privind comunicațiile electronice” ar trebui modificată astfel încât să includă toate datele prelucrate în vederea transmiterii, a distribuirii sau a schimbului de conținut al comunicațiilor electronice.
23. În plus, un alt motiv de îngrijorare este faptul că **domeniul de aplicare teritorial al propunerii de regulament în ceea ce privește organizațiile care nu sunt stabilite în UE se adresează numai furnizorilor de servicii de comunicații electronice.** În conformitate cu propunerea de regulament, furnizorul unui serviciu de comunicații electronice care nu este stabilit în UE își desemnează în scris un reprezentant în Uniune [articolul 3 alineatul (2)]. De asemenea, în considerentul 9 se menționează că regulamentul s-ar aplica prelucrării de către furnizorii serviciilor de comunicații electronice, indiferent unde are loc prelucrarea. Grupul de lucru apreciază această clarificare. Totuși, întrucât formularea este limitată la furnizorii de servicii de comunicații electronice, nu se știe în ce măsură acest domeniu de aplicare teritorial se aplică altor tipuri de părți (de exemplu, părților care intervin asupra echipamentelor terminale ale utilizatorilor finali sau colectează informații difuzate de acestea, în conformitate cu articolul 3 alineatul (1) litera (c) coroborat cu articolul 8 din propunerea de regulament). Prin urmare, grupul de lucru sugerează modificarea alineatelor (2) și (5) ale articolului 3 astfel încât să includă furnizorii de liste de abonați accesibile publicului, furnizorii de programe software care permit comunicațiile electronice și persoanele care trimit comunicații comerciale în scopuri de marketing direct sau colectează (alte) informații referitoare la echipamentele

terminale ale utilizatorilor finali sau stocate în acestea, ori de câte ori activitățile lor vizează utilizatorii din UE (a se vedea considerentul 8 al propunerii de regulament)<sup>13</sup>.

#### *ESTE NECESARĂ CONSOLIDAREA PROTECȚIEI ECHIPAMENTELOR TERMINALE*

O altă categorie de motive de îngrijorare se referă la protecția insuficientă a echipamentelor terminale în propunerea de regulament.

24. În primul rând, **propunerea de regulament sugerează în mod incorect că acordul valabil poate fi dat prin setări nespecifice ale browserului**. Grupul de lucru recunoaște faptul că utilizatorii finali sunt în prezent supraîncărați cu cereri de acordare a consimțământului (considerentul 22). Setările browserului (și ale programelor software comparabile) au un rol important în abordarea acestei probleme. Cu toate acestea, deoarece setările generale ale browserului nu sunt menite să se aplice în cazul utilizării unei tehnologii de urmărire într-un caz individual, acestea nu sunt potrivite pentru acordarea consimțământului în conformitate cu articolul 7 și considerentul 32 din RGPD (deoarece consimțământul nu este suficient de specific și nu este dat în cunoștință de cauză).

Utilizatorul final trebuie să poată să își dea consimțământul separat pe fiecare site sau aplicație pentru urmărirea în scopuri diferite (cum ar fi partajarea pe platformele de comunicare socială sau publicitatea). Un operator de date care răspunde de mai multe site-uri sau aplicații poate să solicite consimțământul și pentru toate celelalte site-uri cu aplicații pe care le controlează, atâta timp cât această solicitare de consimțământ este prezentată separat.

În plus, operatorul trebuie să respecte toate celelalte obligații legate de consimțământ, inclusiv obligația de a oferi informații adecvate utilizatorilor. Și pentru browsere, și pentru operatorii de date acest lucru înseamnă că consimțământul nu ar fi valabil dacă aceștia ar oferi doar opțiunea „de a accepta toate cookie-urile”, deoarece astfel nu li s-ar permite utilizatorilor să își dea consimțământul detaliat necesar. Cu toate acestea, browserele ar trebui să le permită utilizatorilor să aleagă în mod conștient și în cunoștință de cauză acceptarea tuturor modulelor cookie, împiedicând astfel eventuale solicitări de consimțământ viitoare de la site-urile pe care le vizitează.

Grupul de lucru recomandă ferm ca Regulamentul privind viața privată și comunicațiile electronice să impună obligația ca browserele să pună în aplicare mecanisme tehnice, cum ar fi standardul „Do not track” (Fără monitorizare), pentru a se asigura că utilizatorilor li se dă cu adevărat posibilitatea de alegere și control în ceea ce privește intervenția asupra dispozitivelor lor<sup>14</sup>.

---

<sup>13</sup> A se vedea articolul 3 alineatul (2) din RGPD: „Prezentul regulament se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activitățile de prelucrare sunt legate de: (a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată; sau (b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.” Această obligație ar putea include și excepții asemănătoare celor prevăzute la articolul 27 alineatul (2) din RGPD.

<sup>14</sup> A se vedea adresa URL: <https://www.w3.org/TR/tracking-compliance/>. Punctul 7 explică modelul de excepție și diferența între excepțiile de la nivel de site și cele de la nivelul internetului. Punctul 6 conține informațiile lizibile

Chiar mai important este faptul că Regulamentul privind viața privată și comunicațiile electronice ar trebui să se asigure că atât opțiunea referitoare la stocarea informațiilor în dispozitiv, cât și semnalul DNT de la un browser sunt acceptate de toți operatorii de date drept o indicație obligatorie din punct de vedere juridic privind consimțământul sau refuzul. Acest lucru nu aduce atingere orientărilor suplimentare ale Grupului de lucru privind conformitatea standardului DNT, printre altele, cu principiul limitării scopului, atunci când standardul va fi fost finalizat (lucru programat pentru sfârșitul anului 2017).

Tipurile implicite de „consimțământ”, cum ar fi un clic pe un site sau derularea paginii, nu pot prevala asupra opțiunilor privind stocarea și semnalul DNT. Un avantaj important al utilizării acestui standard este faptul că nu se limitează la tehnologia de urmărire a modulelor cookie, ci se adresează și altor tipuri de urmărire, cum ar fi amprentarea.

Dacă acest standard devine obligatoriu din punct de vedere juridic, se va rezolva astfel și o altă problemă, aceea a utilizării actuale a termenului „părțile terțe” la articolul 10. O pagină web sau o aplicație conține, în general, multe elemente, atât din site-ul în sine, cât și elemente externe. Iar codul extern poate rula și în contextul site-ului vizitat, în timp ce raportează către un server unor terți. Un modul cookie de urmărire poate apărea, de la o primă parte, atunci când un utilizator vizitează, de exemplu, un site de socializare în rețea. Acest site de socializare poate fi și o terță parte atunci când utilizatorul respectiv vizitează un alt site care conține interacțiuni cu acel site de socializare în rețea. În toate aceste cazuri, indiferent dacă este vorba despre „accesul la” sau despre „stocarea” informațiilor în dispozitivul utilizatorului final, aceasta reprezintă o intervenție asupra dispozitivului, pentru care este necesar consimțământul (cu excepția cazului în care se aplică una dintre excepții). În standardul DNT, această chestiune este tratată prin utilizarea termenilor „la nivelul de site” și „la nivelul internetului”. Prin urmare, pentru a îmbunătăți securitatea juridică a tuturor părților interesate, ar trebui reformulată trimiterea din Regulamentul privind viața privată și comunicațiile electronice cu privire la „terțele părți”, pentru a se referi la toate entitățile cu care interacționează un dispozitiv (deoarece acestea stochează sau accesează informații din dispozitiv).

Pentru a face standardul Do Not Track compatibil cu nivelul ridicat de protecție a confidențialității comunicațiilor și de protecție a datelor acordat în temeiul cartei, regulamentul privind viața privată și comunicațiile electronice ar trebui să precizeze că, spre deosebire de urmărirea la nivel de site, cererile de urmărire la nivelul internetului trebuie să fie prezentate separat, iar utilizatorii să fie liberi să accepte sau să respingă astfel de solicitări. În plus, pentru a proteja utilizatorii împotriva solicitărilor frecvente de consimțământ, Regulamentul privind viața privată și comunicațiile electronice ar trebui să se asigure că refuzul de a accepta urmărirea la nivelul internetului de la o anumită organizație (prin standardul Do Not Track sau printr-o listă neagră separată) blochează posibilitatea organizației respective de a face alte solicitări de consimțământ timp de minimum 6 luni. Această regulă nu împiedică respectiva organizație, atunci când este vizitată direct de către utilizator (deci ca

---

automat pe care operatorii de date le pot furniza din punctul de vedere al cererii de informații pentru obținerea consimțământului.

primă parte), să solicite consimțământul pe site-ul propriu (adică să facă o solicitare de consimțământ la nivel de site). În practică, aceasta înseamnă că, de exemplu, un site de transmisie video prin flux continuu care prezintă module cookie de urmărire poate solicita consimțământul atunci când utilizatorul vizitează site-ul de transmisie video, dar nu poate solicita din nou consimțământul timp de 6 luni dacă acel utilizator a refuzat să își dea consimțământul și vizitează alte site-uri care conțin videoclipuri difuzate de pe site-ul respectiv.

25. În plus, **excepția privind „măsurarea audienței pe internet” este formulată imprecis.** Articolul 8 alineatul (1) litera (d) din propunerea de regulament prevede o excepție pentru măsurarea audienței pe internet. Primul motiv de îngrijorare este faptul că acest termen nu este definit și poate fi confundat cu stabilirea profilului utilizatorilor. Definiția trebuie să clarifice faptul că această excepție nu poate fi utilizată în scopuri de creare a profilurilor. Excepția ar trebui să se aplice numai analizelor de utilizare necesare pentru evaluarea performanței serviciului solicitat de utilizator, dar nu și pentru analiza utilizatorilor (adică analiza comportamentului utilizatorilor identificabili ai unui site, ai unei aplicații sau ai unui dispozitiv). Prin urmare, excepția nu poate fi utilizată în situațiile în care datele pot fi corelate cu date ale utilizatorilor identificabili prelucrate de furnizor sau de alți operatori de date. În plus, descrierea sa sugerează o aplicare foarte axată pe tehnologie. Prin urmare, termenul „măsurarea audienței pe internet” ar trebui să fie redefinit într-o manieră neutră din punct de vedere tehnologic, astfel încât să includă și informațiile similare referitoare la analizele de utilizare recuperate din aplicații, dispozitive portabile și dispozitive ce țin de internetul obiectelor.

Grupul de lucru sugerează folosirea ca sursă de inspirație a excepției olandeze, care se aplică în cazul în care este strict necesar pentru obținerea informațiilor privind calitatea tehnică sau eficacitatea unui serviciu furnizat de societatea informațională și care are un impact minim sau inexistent asupra vieții private a abonatului sau a utilizatorului final [a se vedea articolul 11.7a alineatul (3) litera (b) din Legea neerlandeză a telecomunicațiilor]. Această excepție ține cont de faptul că majoritatea datelor colectate prin analiza site-urilor sau a aplicațiilor sunt în continuare date cu caracter personal, ceea ce înseamnă că prelucrarea acestor date este, de asemenea, supusă RGPD. Aceasta presupune, de exemplu, că analizele de utilizare ar putea fi efectuate și de o organizație externă, dar numai dacă:

- (i) organizația respectivă acționează în calitate de persoană împuternicită de operator;
- (ii) este încheiat de către persoana împuternicită de operator un acord conform cu RGPD;
- (iii) tehnologia de analiză folosită împiedică reidentificarea, incluzând, printre altele, anonimizarea adreselor IP de la utilizatori;
- (iv) modulele cookie specifice sau alte date utilizate în scop analitic pot fi utilizate numai pentru site-ul, aplicația sau dispozitivul portabil respectiv și nu pot fi corelate cu alte date identificabile;
- (v) utilizatorii au dreptul de a renunța (a se vedea, de asemenea, observațiile 17 și 50 din prezentul aviz).

Chiar dacă nu s-ar solicita consimțământul în cazul îndeplinirii acestor condiții, operatorii de date trebuie să furnizeze, totuși, informații adecvate utilizatorilor, de

exemplu prin câmpurile de reprezentare a stării de urmărire în standardul Do Not Track<sup>15</sup>.

26. Regulamentul privind viața privată și comunicațiile electronice **ar trebui să asigure excepții restrânse și precis formulate în ceea ce privește solicitările de consimțământ**. Formularea excepției de la cerința de acordare a consimțământului pentru intervenția asupra dispozitivelor prevăzută la articolul 8 alineatul (1) litera (c) este aproape identică cu formularea actuală din Directiva asupra confidențialității și comunicațiilor electronice, articolul 5 alineatul (3), „*strict necesar în vederea furnizării unui serviciu al societății informaționale cerut în mod explicit de către abonat sau utilizator*”, dar cuvântul „strict” este omis fără nicio explicație. Acest lucru reprezintă un motiv de îngrijorare din două motive. În primul rând, dispoziția din Directiva asupra confidențialității și comunicațiilor electronice a dus deja la o discuție amplă privind domeniul său de aplicare în rândul autorităților de supraveghere și al organizațiilor, iar eliminarea cuvântului „strict” va oferi un nivel și mai scăzut de securitate juridică. Acest lucru este îngrijorător și pentru că grupul de lucru a oferit deja îndrumări cu privire la interpretarea termenului „strict” în acest context. Grupul de lucru a sugerat următoarele clarificări în Avizul cu privire la exceptările de la consimțământul privind modulele cookie (GL 194):

*„cookie-ul este strict necesar pentru a furniza o anumită funcționalitate utilizatorului (sau abonatului): în cazul în care cookie-urile sunt dezactivate, funcționalitatea nu este disponibilă, iar această funcționalitate a fost cerută în mod explicit de către utilizator (sau abonat), ca parte a unui serviciu al societății informaționale.”*<sup>16</sup>

În plus, grupul de lucru a precizat că:

*cookie-urile de „terță parte” nu sunt, în general, „strict necesare” pentru utilizatorul care accesează un site, dat fiind că aceste cookie-uri sunt de obicei legate de un serviciu care este diferit de cel care a fost „cerut în mod expres” de către utilizator*<sup>17</sup>. Grupul de lucru a adăugat că, în egală măsură, folosirea pluginurilor sociale care vizează persoanele care nu utilizează o platformă sau un site nu ar fi considerată strict necesară.

În plus, deși articolul 6 alineatul (1) litera (b) din propunerea de regulament permite prelucrarea datelor transmise în cadrul comunicațiilor electronice dacă este „necesar” în scopuri de securitate, considerentul 49 din RGPD impune ca acest lucru să fie strict necesar. Este posibil ca omiterea cuvântului „strict” să nu fi fost intenționată, deoarece în considerentul 21 al propunerii de regulament se menționează că nu ar trebui solicitat consimțământul pentru intervenții atunci când este „strict” necesar. Cu toate acestea, propunerea de regulament oferă ocazia de a clarifica suplimentar faptul

<sup>15</sup> A se vedea: Tracking Preference Expression (Exprimarea preferințelor în ceea ce privește urmărirea) (DNT), Versiunea editorului, 7 martie 2016.

<sup>16</sup> Grupul de lucru „Articolul 29”, GL 194, Avizul 04/2012 cu privire la exceptările de la consimțământul privind modulele cookie, adoptat la 7 iunie 2012, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194\\_ro.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_ro.pdf).

<sup>17</sup> Ibid.

că testul necesității în contextul acestui regulament ar trebui interpretat în mod restrictiv în privința tuturor excepțiilor. Prin urmare, grupul de lucru sugerează că, în privința tuturor excepțiilor de la articolul 6 și articolul 8 alineatul (1) din propunerea de regulament, înaintea cuvântului „necesar” ar trebui adăugat cuvântul „strict”.

Pe de altă parte, Regulamentul privind viața privată și comunicațiile electronice ar trebui să permită în mod explicit intervențiile asupra echipamentelor pentru instalarea actualizărilor de securitate. Trimiterea actualizărilor de securitate prin internet este metoda preferată pentru instalarea acestora pe majoritatea dispozitivelor utilizatorilor finali. Instalarea actualizărilor este considerată o intervenție asupra echipamentelor terminale. Există un interes legitim în a garanta că securitatea acestor dispozitive este actualizată. Prin urmare, un furnizor de patch-uri de securitate ar trebui, în general, să poată instala actualizările de securitate strict necesare fără consimțământul utilizatorului final. Cu toate acestea, nu este sigur dacă această intervenție poate beneficia de excepția de la interdicția de intervenție legată de societatea informațională [articolul 8 alineatul (1) litera (c)]. Ar trebui să se clarifice faptul că instalarea actualizărilor de securitate este permisă în cadrul acestei excepții, dar numai în măsura în care: (i) actualizările de securitate sunt ambalate discret și nu modifică în niciun fel funcționalitatea programului software pe echipament (inclusiv interacțiunea cu alte programe sau setări alese de utilizator); (ii) utilizatorul final este informat în prealabil de fiecare dată când se instalează o actualizare; și (iii) utilizatorul final are posibilitatea de a dezactiva instalarea automată a acestor actualizări.

## *MARKETINGUL DIRECT*

O altă categorie de îngrijorări se referă la protecția insuficientă împotriva marketingului direct.

27. În primul rând, este îngrijorător faptul că **sfera de aplicare a marketingului direct este prea limitată**. La articolul 4 alineatul (3) litera (f) din propunerea de regulament, prin „comunicații în scopuri de marketing direct” se înțelege „orice tip de publicitate, în formă scrisă sau orală, trimisă unuia sau mai multor utilizatori finali identificați sau identificabili de servicii de comunicații electronice”. Folosirea cuvântului „trimisă” implică utilizarea mijloacelor tehnologice de comunicații care implică în mod necesar transmiterea unei comunicări, în timp ce marea parte a publicității pe internet (prin intermediul platformelor sociale sau pe site-uri) nu ar implica „trimiterea” de reclame în sensul strict. Acest lucru este subliniat și mai mult prin exemplele care urmează în cadrul acestei definiții (SMS, e-mail) și în considerentul 33. Toate acestea se referă la forme destul de tradiționale ale comunicării în scopuri de marketing și, chiar și în acest caz, se poate spune că utilizarea sistemelor de apelare – destul de tradiționale – nu intră în sfera de aplicare. Articolul și considerentul trebuie modificate astfel încât să includă toate reclamele *trimise, direcționate sau prezentate* unuia sau mai multor utilizatori finali identificați sau identificabili. În plus, în continuare, ar trebui să se asigure și că reclamele comportamentale (bazate pe profilurile utilizatorilor finali) sunt, de asemenea, considerate comunicații în scopuri de marketing direct care



vizează „unul sau mai mulți utilizatori finali identificați sau identificabili” (deoarece aceste reclame sunt direcționate către utilizatori concreți, identificabili).

În plus, în cadrul domeniului de aplicare propus al „comunicațiilor în scopuri de marketing direct”, protecția de la articolul 16 alineatul (1) s-ar limita la mesaje care conțin materiale publicitare și nu ar proteja persoanele de alte mesaje trimise, direcționate sau prezentate în scopuri de marketing [cum ar fi mesajele generatoare de oportunități comerciale (*lead-generation messages*) prin care se solicită consimțământul, promovarea opiniilor politice sau a preferințelor în materie de vot, promovarea organizațiilor caritabile sau a altor organizații non-profit sau brandingul general al unei organizații]. În plus, faxurile sunt încă folosite ca metodă de marketing direct, deși nu sunt menționate în definiție. Prin urmare, articolul 4 alineatul (3) litera (f) ar trebui să includă orice formă de publicitate, de prospectare sau de promovare, inclusiv pentru organizațiile non-profit și ar trebui să includă în mod explicit faxurile alături de e-mailuri și SMS-uri [a se vedea și propunerea de clarificare din observația 43 punctul (a)]. În sfârșit, în considerentul 32 se afirmă că marketingul direct include și mesajele promoționale trimise de partidele politice. Acesta ar trebui actualizat astfel încât să includă politicienii și candidații la alegeri care își promovează candidatura.

28. În al doilea rând, **retragerea consimțământului pentru marketingul direct nu este gratuită și nici nu se face la fel de ușor ca acordarea acestuia**. Opțiunea de retragere a consimțământului în temeiul propunerii de regulament trebuie să fie clarificată pentru a asigura coerența și pentru a îmbunătăți protecția beneficiarilor. Conform articolului 16 alineatul (6) din propunerea de regulament, beneficiarii marketingului direct trebuie să fie informați cu privire la „informațiile necesare pentru ca beneficiarii să își exercite dreptul de a-și retrage cu ușurință consimțământul privind primirea în continuare de comunicații în scopuri de marketing” (sublinierea noastră). Acest lucru este confirmat în considerentul 34. Totuși, din considerentul 70 din RGPD rezultă că persoanele vizate în temeiul RGPD ar trebui să aibă nu numai dreptul de a se opune cu ușurință prelucrării în scopuri de marketing direct, ci și de a face acest lucru „în mod gratuit”. Acest termen este utilizat și la articolul 16 alineatul (2) din propunerea de regulament, însă numai în ceea ce privește renunțarea la mesajele de marketing direct pe baza datelor de contact obținute în contextul unei vânzări.

Articolul 7 alineatul (3) din RGPD prevede că retragerea este la fel de ușoară ca și acordarea consimțământului și că persoanele trebuie să își poată retrage consimțământul în orice moment. În plus, în Avizul 04/2010 privind Codul de conduită european al FEDMA (GL 174), grupul de lucru a recunoscut deja importanța de a oferi „o metodă simplă, eficientă, gratuită, directă și ușor accesibilă de a se dezabona” de la marketingul direct<sup>18</sup>. Acest standard în materie de retragere a

---

18 Grupul de lucru „Articolul 29”, GL 174, Avizul 04/2010 privind Codul de conduită european al FEDMA pentru utilizarea datelor cu caracter personal în cadrul marketingului direct, adoptat la 13 iulie 2010, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174\\_ro.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_ro.pdf).

consimțământului ar trebui să fie inclus în normele privind marketingul direct din propunerea de regulament. Același lucru este valabil și pentru cerința de la articolul 7 alineatul (3) din RGPD conform căreia retragerea consimțământului ar trebui să se facă la fel de simplu ca acordarea acestuia în orice moment.

29. În acest sens, **ar trebui clarificat modul de retragere a consimțământului sau de renunțare la apelurile de marketing direct.** În temeiul articolului 16 alineatul (4) din propunerea de regulament, statele membre pot opta pentru un regim de renunțare pentru apelurile vocale în scopuri de marketing direct. Regulamentul privind viața privată și comunicațiile electronice ar trebui să precizeze modalitățile de retragere a consimțământului și de renunțare la apelurile în scopuri de marketing. Considerentul 36 specifică faptul că statele membre *ar trebui să poată* stabili și/sau menține sisteme naționale de renunțare. În temeiul acestei dispoziții, statele membre ar putea permite astfel chiar și o situație în care un utilizator ar trebui să renunțe la furnizorii individuali de comunicații. O astfel de punere în aplicare nu protejează utilizatorii împotriva neplăcerilor legate de comunicările nesolicitate<sup>19</sup> și nu oferă un mecanism compatibil cu RGPD pentru retragerea consimțământului cu ușurință și în orice moment. În consecință, regulamentul ar trebui să precizeze că fiecare stat membru *trebuie* să creeze un registru național „Do Not Call”. În plus, regulamentul ar trebui să precizeze că destinatarilor apelurilor vocale ar trebui să li se ofere două posibilități de retragere a consimțământului: pentru apelurile viitoare de la acea companie sau organizație și posibilitatea ca în timpul acestor apeluri să se înregistreze într-un registru național Do Not Call.
30. Un alt motiv de îngrijorare este faptul că **nu este explicit interzisă utilizarea identităților false atunci când se trimit comunicații în scopuri de marketing direct.** În considerentul 34 se menționează că este interzisă „mascarea identității sau folosirea de identități false, precum și de adrese sau de numere de telefon de răspuns false la trimiterea de mesaje comerciale nesolicitate în scopuri de marketing direct”. Însă la articolul 16 alineatul (4) se menționează pur și simplu că utilizatorii finali sunt informați despre „identitatea persoanei fizice sau juridice în numele căreia este transmisă comunicarea”. Această obligație de informare a beneficiarilor cu privire la identitate ar trebui completată cu o interdicție clară de utilizare a adreselor de contact mascate sau false în scopuri de marketing direct.
31. Acest punct are legătură cu un alt motiv de îngrijorare: **cerința privind prefixul pentru apelurile de marketing direct este prezentată ca o alternativă la cerința de identificare a liniei de contact.** În conformitate cu articolul 16 alineatul (3), apelurile de marketing direct sunt permise dacă apelantul: ori (i) prezintă identitatea unei linii unde poate fi contactată persoana fizică sau juridică care a efectuat apelul [articolul 16 alineatul (3) litera (a)]; ori (ii) utilizează un cod specific/prefix care identifică faptul că apelul este efectuat în scopuri de marketing [articolul 16 alineatul (3) litera (b)]. Deși grupul de lucru salută obligația prevăzută la articolul 16 alineatul (3) litera (b) de utilizare a unui prefix, consideră că această cerință nu

<sup>19</sup> De exemplu, în Regatul Unit, operatorul de telecomunicații BT a înregistrat 31 de milioane de apeluri deranjante într-o singură săptămână. A se vedea: <http://www.bbc.com/news/business-38635921>.

tratează aceeași problemă abordată de obligația de identificare a liniei de contact de la articolul 16 alineatul (3) litera (a). În timp ce cerința privind prefixul are rolul de a permite beneficiarului să identifice un apel în mod clar drept apel efectuat în scopuri de marketing (și să pună în aplicare măsuri de blocare a acestor apeluri), cerința de identificare a liniei de contact are rolul de a oferi destinatarilor (și autorităților de supraveghere) modalități de identificare și contactare a instigatorului apelului de marketing. Acest lucru este deosebit de relevant pentru apelurile automate, în care există un puternic dezechilibru între posibilitățile comerciantului de a trimite apeluri deranjante și posibilitățile destinatarului de a evita aceste apeluri. Prin urmare, cerințele nu trebuie să fie alternative, ci să se completeze reciproc.

#### CALENDAR

32. Grupul de lucru „Articolul 29” felicită Comisia Europeană pentru recunoașterea necesității ca propunerea de regulament să intre în vigoare alături de RGPD în mai 2018, pentru a evita neconcordanțele dintre cele două acte legislative. Cu toate acestea, este încă îngrijorător faptul că acest calendar este unul ambițios, care impune și finalizarea proiectului Codului european al comunicațiilor electronice. Prin urmare, GL 29 solicită ca toate părțile interesate din cadrul procesului legislativ să se angajeze să respecte termenul limită din mai 2018.

#### ALTE MOTIVE DE ÎNGRIJORARE

Această secțiune prezintă o serie de alte motive de îngrijorare.

33. În primul rând, GL 29 este îngrijorat de **sugestia că măsurile nespecifice de păstrare a datelor sunt acceptabile**. În expunerea de motive se menționează că, în temeiul propunerii de regulament, statele membre sunt libere să mențină sau să creeze cadre naționale în materie de păstrare a datelor care să prevadă, printre altele, măsuri de păstrare specifice (punctul 1.3). După Hotărârea în cauza Tele2/Watson<sup>20</sup>, în mod clar, cadrele în materie de păstrare a datelor care prevăd altceva decât măsuri de păstrare specifice nu sunt permise în temeiul cartei (și chiar și atunci sunt supuse unor condiții importante precum supravegherea), iar accesul generalizat la metadate va trebui să se considere că încalcă esența articolului 7 în același mod ca accesul generalizat la conținutul comunicațiilor electronice (a se vedea Hotărârea CJUE în cauza Schrems și considerentul 94). Formularea acestui enunț sugerează astfel o anumită marjă acordată statelor membre în ceea ce privește măsurile de păstrare a datelor, care nu există. Referitor la acest aspect, **metadatele nu beneficiază de un nivel suficient de protecție** în propunerea de regulament. După cum se menționează în observația 10, Grupul de lucru „Articolul 29” salută recunoașterea faptului că metadatele ar putea dezvălui date foarte sensibile. Cu toate acestea, în propunerea de regulament metadatele nu beneficiază de protecția care ar trebui să decurgă din această recunoaștere. Având în vedere sensibilitatea metadatelor, în special, înaintea

---

<sup>20</sup> ECLI:EU:C:2016:970, URL: <http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203>.

unei analize în temeiul articolului 6 alineatul (2) litera (c) ar trebui efectuată o evaluare a impactului asupra protecției datelor (a se vedea și observația 46).

34. În al doilea rând, **propunerea de regulament ar extinde în mod nedorit posibilitățile în materie de păstrare a datelor**. Articolul 11 din propunerea de regulament face trimitere la articolul 23 alineatul (1) literele (a)-(e) din RGPD în descrierea scopurilor în care statele membre pot limita obligațiile și drepturile prevăzute la articolele 5-8 din regulament. RGPD nu prevede astfel de restricții privind categorii speciale de date, în conformitate cu riscurile ridicate pentru persoanele vizate. Deși articolul 15 din Directiva asupra confidențialității și comunicațiilor electronice permite în prezent o restricție similară, scopurile sunt mai limitate. Noul regulament propus ar face posibile noi restricții pentru „executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora” [articolul 23 alineatul (1) litera (d) din RGPD] și „alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale” [articolul 23 alineatul (1) litera (e) din RGPD]. Nu numai că aceste scopuri sunt noi în comparație cu Directiva asupra confidențialității și comunicațiilor electronice, dar ultimul scop al articolului 23 alineatul (1) litera (d) și întregul scop al articolului 23 alineatul (1) litera (e) sunt formulate într-o manieră extrem de generală. Prin urmare, se sugerează eliminarea trimiterii la articolul 23 alineatul (1) literele (a)-(e) din RGPD și menționarea în schimb doar a scopurilor menționate în prezent la articolul 15 din Directiva asupra confidențialității și comunicațiilor electronice.
35. **Obligația de a informa utilizatorii cu privire la riscurile de securitate are un domeniu de aplicare minimalist**. Grupul de lucru salută faptul că furnizorii de servicii trebuie să informeze utilizatorii cu privire la riscurile de securitate și măsurile de combatere a acestor riscuri, cum ar fi criptarea (articolul 17 și considerentul 37). Cu toate acestea, titlul articolului este: „Informații privind riscurile de securitate detectate”. Faptul că titlul menționează riscurile detectate sugerează că această dispoziție se referă numai la (potențiale) încălcări ale securității, în timp ce formularea dispoziției și a considerentului indică mai mult educația generală a utilizatorilor finali. De exemplu, dacă un furnizor de servicii detectează faptul că dispozitivul unui utilizator este infectat cu programe malware și a devenit parte a unei rețele botnet, această dispoziție pare să impună furnizorului obligația directă de a informa utilizatorul cu privire la riscurile care rezultă. Cu toate acestea, domeniul de aplicare al acestei dispoziții ar putea fi clarificat și nu ar trebui să se limiteze la acest scenariu specific. Dispoziția ar trebui să acopere cel puțin riscurile de securitate detectate în toate echipamentele furnizate utilizatorului final de către furnizor ca parte a abonamentului, cum ar fi, de exemplu, routerele și dispozitivele mobile, și să includă educația cu privire la riscurile schimbării setărilor care au fost stabilite pentru protecția vieții private în conformitate cu principiul respectării vieții private începând cu momentul conceperii.

Grupul de lucru recomandă extinderea domeniului de aplicare astfel încât să cuprindă furnizorii de programe software care permit comunicațiile electronice (conform

considerentului 8) și, eventual, o nouă categorie: furnizorii de tehnologii esențiale pentru securizarea comunicațiilor, care nu sunt furnizori de servicii (de exemplu, furnizorii de tehnologie de criptare). În cazul acestei din urmă extinderi, ar trebui să se acorde atenție nesuprapunerii acestei obligații cu obligațiile de notificare privind încălcarea securității din alte instrumente, cum ar fi Directiva privind securitatea rețelor și a informațiilor<sup>21</sup> și alte instrumente juridice privind furnizorii de certificate. Întrucât furnizorii de tehnologie din ultima categorie nu au, de obicei, un contact direct cu utilizatorii finali, trebuie explicat și modul în care aceștia își pot respecta obligațiile de informare în temeiul acestei dispoziții.

36. Grupul de lucru salută dispozițiile articolelor 2 și 13 care se vor aplica serviciilor de comunicații interpersonale bazate pe numere. Însă nu este clar de ce un **nivel similar de protecție a vieții private nu ar trebui să fie disponibil și pentru serviciile de apelare prin OTT echivalente din punct de vedere funcțional**.
37. Grupul de lucru este, de asemenea, îngrijorat de **lipsa de claritate cu privire la consimțământul detaliat pentru căutarea inversă în listele de abonați**. Articolul 15 alineatul (2) din propunerea de regulament prevede că furnizorii trebuie să obțină consimțământul utilizatorilor finali înainte de a permite funcțiile de căutare legate de date (a se vedea, de asemenea, considerentul 31). Grupul de lucru apreciază armonizarea cerinței de obținere a consimțământului în ceea ce privește includerea în listele de abonați, dar regretă lipsa detalierii în ceea ce privește diferitele tipuri de căutări. Actuala Directivă asupra confidențialității și comunicațiilor electronice permite statelor membre să solicite o cerință separată de obținere a consimțământului pentru căutarea inversă, în temeiul articolului 12 alineatul (3). Acest articol prevede că *„[s]tatele membre pot cere ca, pentru orice alt scop al unei liste publice altul decât căutarea detaliilor de contact al persoanelor în funcție de nume sau de un minimum de alți identificatori, să fie obligatorie obținerea acordului abonatului pentru fiecare scop suplimentar”*. În temeiul acestei dispoziții, în multe state membre este necesară obținerea consimțământului separat pentru funcțiile de căutare inversă, luând în considerare diferitele niveluri ale posibilității de identificare și, prin urmare, caracterul intruziv al celor două funcționalități.
38. Dintr-o perspectivă mai formală, **nivelul amenziilor nu este armonizat pentru toate încălcările regulamentului**. În propunerea de regulament, statele membre stabilesc normele privind sancțiunile pentru încălcarea articolului 23 alineatul (4), a articolului 23 alineatul (6) și a articolului 24 din propunerea de regulament. O abordare mai consecventă ar fi să se prevadă acest lucru și în Regulamentul privind viața privată și comunicațiile electronice.
39. În fine, **propunerea de regulament se bazează pe definiții care pot deveni „ținte în mișcare”**. Pentru o serie de concepte-cheie, propunerea de regulament face trimitere la un alt instrument juridic, care este în prezent în formă de proiect:

---

<sup>21</sup> Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelor și a sistemelor informatice în Uniune, JO L 194, 19.7.2016, p. 1-30, URL: <http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L1148>

propunerea de Cod european al comunicațiilor electronice [a se vedea, de exemplu, articolul 4 alineatul (1) litera (b)]. Două exemple importante sunt, pe de o parte definiția „utilizatorului final”, care include în prezent persoanele fizice și juridice, , și, pe de altă parte definiția „serviciilor de comunicații electronice” și a „serviciilor de comunicații interpersonale”, care se reflectă în propunerea de regulament la articolul 4 alineatul (1) litera (b), cea din urmă fiind detaliată suplimentar la articolul 4 alineatul (2), astfel încât să cuprindă tipurile de servicii excluse în mod special din Codul european al comunicațiilor electronice<sup>22</sup>. Prezentul aviz se bazează pe definițiile în forma lor actuală, însă este destul de probabil ca propunerea de EECC și/sau conceptele sale esențiale să se modifice. Acest lucru ar avea implicații imediate și pentru Regulamentul privind viața privată și comunicațiile electronice. În mod ideal, toți termenii care provin din EECC ar trebui definiți independent în Regulamentul privind viața privată și comunicațiile electronice, sau, cel puțin, propunerea de regulament ar trebui să includă clarificări în cazul în care există termeni ale căror definiții sunt diferite față de cele cuprinse în EECC (de exemplu, includerea mai sus menționată a „serviciilor auxiliare” în definiția „serviciilor de comunicații interpersonale”). Însă dacă acest lucru nu este posibil, grupul de lucru dorește să propună tuturor părților implicate în procesul legislativ să se asigure că atât propunerea de regulament, cât și EECC sunt discutate și votate simultan, pentru a permite părților interesate să evalueze în mod corect domeniul de aplicare și implicațiile noilor instrumente.

## **5. SUGESTII DE CLARIFICARE PENTRU A ASIGURA SECURITATEA JURIDICĂ**

Pe lângă punctele discutate mai sus, grupul de lucru dorește, de asemenea, să evidențieze anumite dispoziții din propunerea de regulament pentru care ar fi utile unele clarificări. Astfel de clarificări sunt considerate necesare pentru îmbunătățirea nivelului de securitate juridică pentru toate părțile interesate în legătură cu înțelegerea și aplicarea uniformă a Regulamentul privind viața privată și comunicațiile electronice în întreaga UE.

### *CLARIFICĂRI PRIVIND DOMENIUL DE APLICARE*

40. În ceea ce privește domeniul de aplicare al propunerii de regulament, GL 29 sugerează următoarele clarificări:

- a. **termenul „utilizator final” ar trebui să includă toți utilizatorii individuali.** Articolul 2 alineatul (14) din EECC definește „utilizatorul final” drept un utilizator care nu furnizează rețele publice de comunicații publice sau servicii de comunicații electronice accesibile publicului. Ar trebui să se

---

<sup>22</sup> De exemplu, articolul 4 alineatul (2) din propunerea de regulament prevede că un serviciu de comunicații interpersonale „include serviciile care permit comunicarea interpersonală și interactivă doar ca un simplu element auxiliar minor care este legat în mod intrinsec de un alt serviciu”, în timp ce articolul 2 alineatul (5) din EECC exclude în mod special aceste servicii din definiția respectivă. [EECC include „serviciile de comunicații interpersonale” în cadrul categoriei mai mari a „serviciilor de comunicații electronice” de la articolul 2 alineatul (4).]

clarifice faptul că persoanele care contribuie la rețele – de exemplu, pentru formarea rețelelor plasă (mesh) prin routerul Wi-fi – nu sunt excluse din domeniul de aplicare a protecției din propunerea de regulament;

- b. **ar trebui să se clarifice faptul că domeniul de aplicare teritorial se referă la toți utilizatorii finali din Uniune.** Articolul 3 alineatul (1) litera (a) prevede că propunerea de regulament se aplică furnizării de servicii de comunicații electronice către utilizatorii finali „din Uniune”, în timp ce articolul 3 alineatul (1) litera (c) prevede că aceasta se aplică protecției echipamentelor terminale ale utilizatorilor finali „care se află în Uniune” (sublinierea noastră). Acest lucru a fost tradus diferit. Varianta în limba germană nu conține această distincție, în timp ce în altele, cum ar fi cele în franceză, spaniolă și neerlandeză, distincția respectivă se face. Din considerentul 9 rezultă clar că s-a dorit ca domeniul de aplicare teritorial să fie amplu, indiferent dacă serviciile sunt furnizate din afara Uniunii sau dacă prelucrarea are loc în Uniune. Prin urmare, se sugerează eliminarea sintagmei „se află în” din articolul 3 alineatul (1) litera (c) pentru a sublinia acest larg domeniu de aplicare;
- c. **propunerea de regulament pare să protejeze doar comunicațiile confidențiale în tranzit, nu și pe cele stocate.** Abordarea actuală din propunerea de regulament se axează pe protejarea transmiterii comunicațiilor. A se vedea, de exemplu, considerentul 15, care prevede că interdicția de interceptare a datelor transmise în cadrul comunicațiilor ar trebui să se aplice în timpul transmiterii acestora, și anume până la primirea conținutului comunicațiilor de către destinatar. Domeniul de aplicare al acestei protecții se bazează pe un cadru conceptual depășit în materie de comunicații. Majoritatea datelor transmise în cadrul comunicațiilor rămân stocate la furnizorii de servicii, chiar și după primire. Ar trebui să se asigure protejarea în continuare a confidențialității acestor date. În plus, comunicațiile dintre abonații acelorași servicii bazate pe cloud (de exemplu, furnizorii de servicii de tip „webmail”) adesea implică un serviciu de transmitere nesemnificativ: în majoritatea cazurilor, trimiterea unui e-mail înseamnă reflectarea acestui fapt în baza de date a furnizorului și nu un serviciu efectiv de comunicație între două părți. Argumentul că acest aspect ar fi deja acoperit de RGPD nu este convingător, deoarece scopul propunerii de regulament este tocmai acela de a proteja toate comunicațiile confidențiale, indiferent de mijloacele tehnice ale acestora. Este posibil ca aceasta să fie o simplă eroare de redactare, deoarece interdicția de la articolul 5 se referă la „stocare” și „prelucrare”;
- d. **toate punctele publice de acces la internet fără fir ar trebui să intre sub incidența domeniului de aplicare.** Deoarece utilizarea punctelor de acces la internet fără fir este ceva obișnuit, este logic să nu existe nicio îndoială cu privire la protejarea confidențialității comunicațiilor transmise prin astfel de puncte de acces. Regulamentul conține o încercare nereușită de a clarifica acest aspect, deoarece domeniul de aplicare cuprinde doar rețelele furnizate unui „grup nedefinit de utilizatori finali” (considerentul 13). Este necesar să se definească termenii „grup nedefinit de utilizatori finali” și „grup închis de utilizatori finali”. În special, ar trebui să se precizeze că rețelele fără fir securizate (cu o parolă) intră și ele sub incidența domeniului de aplicare, dacă

această parolă este oferită unui grup teoretic nedefinit de utilizatori a căror identitate nu poate fi stabilită în prealabil (de exemplu, clienții unei cafenele sau vizitatorii unui aeroport). Principiul fundamental în acest context este acela că, în conformitate cu avizul anterior al GL 29 privind revizuirea Directivei asupra confidențialității și comunicațiilor electronice, „*numai serviciile care se desfășoară într-o situație oficială sau legată de locul de muncă doar în scopuri profesionale sau oficiale sau comunicațiile tehnice între organisme private sau cele publice numai pentru a controla munca sau procesele de afaceri, precum și utilizarea serviciilor exclusiv în scopuri casnice, pot fi exceptate din instrumentul privind viața privată și comunicațiile electronice*” (p. 8);

- e. **datele colectate pe parcursul furnizării de servicii de televiziune digitală ar trebui să facă obiectul propunerii de regulament.** Având în vedere caracterul sensibil al comportamentului legat de vizionare, dat fiind că dezvăluie interesele personale și caracteristicile telespectatorilor, Regulamentul privind viața privată și comunicațiile electronice ar trebui să specifice (poate printr-un considerent) că excluderea serviciilor care furnizează „conținut transmis prin intermediul rețelelor de comunicații electronice” din definiția „serviciului de comunicații electronice” nu înseamnă că furnizorii de servicii care oferă atât servicii de comunicații electronice, cât și servicii de conținut se situează în afara domeniului de aplicare al dispozițiilor Regulamentului privind viața privată și comunicațiile electronice care vizează furnizorii de servicii de comunicații electronice. Acest lucru este deosebit de relevant deoarece furnizarea de servicii care constau în furnizarea de „conținuturi prin intermediul rețelelor de comunicații electronice” este exclusă din definiția „serviciilor de comunicații electronice” în propunerea de Cod european al comunicațiilor electronice [articolul 2 alineatul (4)];
- f. **datele transmise în cadrul comunicațiilor sunt în general date cu caracter personal.** În considerentul 4 se face observația că este posibil ca datele transmise în cadrul comunicațiilor să includă date cu caracter personal. În fapt, majoritatea datelor transmise în cadrul comunicațiilor sunt date cu caracter personal<sup>23</sup> și, în mare parte, unele destul de intime și de sensibile, de aceea considerentul respectiv ar trebui modificat pentru a preciza că ele sunt, în general, date cu caracter personal;
- g. **în categoria comunicațiilor confidențiale intră și mesajele trimise prin intermediul platformelor.** Considerentul 1 explică faptul că principiul confidențialității se aplică „mijloacelor de comunicare actuale și viitoare”. Acest considerent continuă cu o listă de exemple de astfel de mijloace, inclusiv „mesageri[a] personal[ă] prin intermediul platformelor de comunicare sociale”. Această formulare are probabil rolul de a include

---

<sup>23</sup> A se vedea, de exemplu, Hotărârea CJUE din 6 noiembrie 2003 în cauza C-101/01, punctul 24 (cu privire la un număr de telefon), Hotărârea CJUE din 19 octombrie 2016 în cauza C-582/14 (Breyer), punctul 49 (cu privire la adresele IP dinamice) și Hotărârea CJUE din 8 aprilie 2014 în cauzele conexate C-239/12 și C-594/12 (Digital Rights Ireland), punctele 26-27 (cu privire la sensibilitatea metadatelor).



mesajele private schimbate între utilizatorii unei rețele de socializare (cum ar fi Facebook sau Twitter) sau mesajele postate pe o cronologie care sunt accesibile unui număr limitat de persoane, însă formularea nu este suficient de clară;

- h. **modul în care Regulamentul privind viața privată și comunicațiile electronice se aplică interacțiunii de la mașină la mașină.** După cum se menționează la punctul 9, grupul de lucru salută extinderea protecției la interacțiunea de la mașină la mașină. Totuși, acest lucru este menționat doar în considerentul 12 și nu într-un articol corespunzător. Această protecție este de dorit, deoarece astfel de comunicații conțin adesea informații protejate în temeiul drepturilor privind viața privată. Pe de altă parte, o categorie restrânsă de comunicații exclusiv de la mașină la mașină ar trebui excluse dacă nu au niciun impact asupra vieții private sau asupra confidențialității comunicațiilor, cum ar fi, de exemplu, cazurile în care astfel de comunicații au loc în cadrul executării unui protocol de transmisie între elementele din rețea (de exemplu, servere, comutatoare), în vederea informării reciproce asupra stării lor de activitate.

Un context specific în care este necesară clarificarea aplicării Regulamentului privind viața privată și comunicațiile electronice este domeniul sistemelor de transport inteligente. Se preconizează că vehiculele vor transmite în mod continuu date care conțin un identificator unic, prin radio. În lipsa protecției suplimentare din Regulamentul privind viața privată și comunicațiile electronice cu privire la datele transmise în cadrul comunicațiilor, acest lucru ar putea conduce la urmărirea continuă a obiceiurilor privind modul în care șofează conducătorii auto, a itinerariilor și a vitezei acestora. Cu toate acestea, articolul 2 alineatul (1) din EECC conține o definiție nouă și extinsă a rețelelor de comunicații. Ele includ sistemele de transmisie care nu dispun de o capacitate de administrare centralizată și care permit transmiterea de semnale prin radio. Considerentul 14 din Regulamentul privind viața privată și comunicațiile electronice specifică faptul că aceste date reprezintă date transmise în cadrul comunicațiilor electronice. În temeiul articolului 5 din propunerea de regulament, orice interceptare, monitorizare sau stocare a acestor date de comunicații este interzisă, cu excepția cazului în care se aplică una dintre excepții. Cu toate acestea, există un interes față de prelucrarea acestor date, prin care li s-ar permite unor obiecte precum automobilele și dispozitivele autonome să se avertizeze reciproc cu privire la apropierea unele față de altele sau la alte riscuri. Astfel, întrebarea este ce excepție s-ar aplica în acest caz. Consimțământul utilizatorilor finali nu este o excepție admisibilă, deoarece ar putea deveni necesar să existe întotdeauna posibilitatea de a prelucra aceste date. Prin urmare, furnizorii ar trebui să se poată baza pe o excepție specifică, care să le permită obiectelor precum automobilele și dispozitivele autonome să se avertizeze reciproc cu privire la apropierea unele față de altele sau la alte riscuri.

41. În ceea ce privește conceptul de consimțământ și aplicarea acestuia în prezenta propunere de regulament, GL 29 sugerează următoarele clarificări:

- a. **modul în care urmează să se aplice conceptul de consimțământ în contextul persoanelor juridice.** În considerentul 3 se menționează că regulamentul ar trebui să garanteze că dispozițiile RGPD se aplică și utilizatorilor finali care sunt persoane juridice. Aceasta, conform considerentului, include definiția consimțământului în temeiul RGPD (a se vedea, de asemenea, considerentul 18). După cum se menționează în observația 13, grupul de lucru salută includerea explicită a persoanelor juridice în domeniul de aplicare al regulamentul. Totuși, aplicarea practică a acestui principiu nu este clară. Definiția consimțământului conform RGPD cere ca acesta să fie „în cunoștință de cauză”, iar indicarea dorințelor persoanei vizate trebuie să fie făcută „printr-o declarație sau printr-o acțiune fără echivoc” [articolul 4 alineatul (11) din RGPD]. Trebuie să se clarifice când se poate considera de fapt că o persoană juridică este „în cunoștință de cauză” și când are loc o astfel de expresie a voinței din partea unei persoane juridice;
- b. în acest context, trebuie precizat faptul că, în majoritatea cazurilor, angajatorul nu își poate da consimțământul în numele angajaților săi deoarece, în cazul în care un angajator cere consimțământul unui angajat și, având în vedere echilibrul inegal al puterii, există un prejudiciu relevant real sau potențial care rezultă din neacordarea consimțământului, un astfel de consimțământ nu este valabil deoarece nu este acordat în mod liber<sup>24</sup>. În ceea ce privește **societățile care furnizează dispozitive sau echipamente unor persoane fizice, propunerea de regulament nu conține vreo excepție (adekvată)** la interdicția de intervenție. Un exemplu îl constituie cazul în care un angajator dorește să actualizeze un telefon al companiei. Un al doilea exemplu este acela în care un angajator oferă angajaților mașini de serviciu și, în scopuri administrative, permite unui terț să colecteze date privind localizarea prin intermediul unității aflate la bordul unei mașini. În ambele cazuri, angajatorul are interesul de a interveni asupra acestor dispozitive. Această intervenție nu poate fi considerată necesară pentru furnizarea unui serviciu al societății informaționale [articolul 8 alineatul (1) litera (c)] sau necesară pentru măsurarea audienței web [articolul 8 alineatul (1) litera (d)]. Această problemă ar putea fi rezolvată prin crearea unei noi excepții, care să includă o situație în care: (i) angajatorul furnizează anumite echipamente în contextul unei relații de muncă; (ii) angajatul este utilizatorul acestui echipament; și (iii) intervenția este strict necesară pentru operarea echipamentului de către angajat (ceea ce implică aplicarea principiilor proporționalității și subsidiarității în privința colectării datelor). Doar dacă

---

<sup>24</sup> A se vedea Avizul 15/2011 privind definiția consimțământului (GL 187), Avizul 8/2001 privind prelucrarea datelor cu caracter personal în contextul ocupării forței de muncă (GL 48) și noul Aviz privind prelucrarea datelor la locul de muncă (adoptat simultan cu prezentul aviz).

aceste condiții sunt îndeplinite ar trebui să fie posibil ca angajatorul să intervină asupra dispozitivului folosit de utilizatorul final;

- c. **îmbunătățirea controalelor în vederea opririi redirecționării automate a apelurilor.** Articolul 14 oferă un mecanism de control important pentru ca utilizatorii finali să poată opri redirecționarea automată a apelurilor de către un terț. Această protecție poate fi îmbunătățită și mai mult, solicitând, în plus, obținerea prealabilă a consimțământului utilizatorului final pentru inițierea redirecționării apelurilor.

#### CLARIFICĂRI PRIVIND LOCALIZAREA ȘI ALTE METADATE

42. Grupul de lucru propune clarificarea următoarelor aspecte legate de datele privind localizarea și de alte metadate:

- a. în considerentul 17, ar trebui să se clarifice sensul enunțului **„datele privind localizarea care sunt generate în alt context decât furnizarea serviciilor de comunicații electronice”**. Nu este clar dacă aceasta se referă la datele privind localizarea colectate, de exemplu, prin aplicații care utilizează datele din funcționalitatea GPS a dispozitivelor inteligente și/sau generează date privind localizarea bazate pe routerele Wi-Fi din apropiere și/sau la datele privind localizarea colectate prin asistenții de navigare de la bord și/sau prin alte modalități de generare a datelor despre localizare. Această lipsă de claritate creează insecuritate juridică în ceea ce privește sfera de aplicare a obligației. În orice caz, datele privind localizarea dispozitivului terminal al unei persoane fizice sunt date cu caracter personal și, prin urmare, prelucrarea acestora este supusă obligațiilor din RGPD;
- b. ar trebui să se clarifice faptul că **majoritatea prelucrărilor legitime ale datelor privind localizarea și ale altor metadate nu necesită un identificator unic**. Considerentul 17 menționează hărțile termice (heatmaps) drept exemplu de utilizări comerciale ale metadelor privind comunicațiile electronice de către furnizorii de servicii de comunicații electronice. Cu toate acestea, pentru a crea o hartă termică de bază nu sunt necesari identificatori unici, ci simpla numărare statistică este suficientă. Un alt exemplu menționat în considerent – utilizarea infrastructurii și presiunea asupra acesteia – poate fi, de asemenea, luat în calcul de anumite puncte de măsurare, de exemplu prin crearea unor statistici agregate privind utilizarea turnurilor de control al traficului pentru a indica o presiune într-un anumit loc și la un anumit moment, fără a fi nevoie să se cunoască și identitatea persoanelor conectate.

În plus, considerentul menționează ca exemplu afișarea mișcărilor din trafic în anumite direcții pe o anumită perioadă, în care un identificator unic ar fi necesar pentru corelarea pozițiilor persoanelor la anumite intervale de timp. Cu acest exemplu, considerentul pare să ofere legitimitate prelucrării ulterioare a acestor date pentru a susține analiza „volumelor mari de date”. Singura condiție prevăzută de propunerea de regulament pentru acest tip de prelucrare este obligația de a efectua o evaluare a impactului asupra protecției datelor, în cazul în care prelucrarea *este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice*. Această

condiție nu este suficientă. De asemenea, este contrar obligației prevăzute la articolul 6 faptul că acest tip de prelucrare poate fi efectuat numai cu consimțământul utilizatorilor și numai dacă datele nu pot fi anonimizate, adică fără identificatori unici. Adesea, utilizatorii nu pot refuza colectarea datelor privind geolocalizarea de către furnizorii de servicii de comunicații electronice, în cazul în care o astfel de colectare este necesară din punct de vedere tehnic pentru a transmite comunicațiile către utilizator sau în cazul în care o astfel de prelucrare este necesară pentru livrarea serviciului solicitat (cum ar fi navigarea). În avizele anterioare, grupul de lucru a concluzionat că astfel de date privind localizarea, obținute de la dispozitive inteligente, constituie date cu caracter personal de natură sensibilă și că avantajele conferite în urma analizării acestor date nu prevalează asupra drepturilor utilizatorilor la protecția confidențialității metadatelor lor transmise prin comunicații și nici asupra drepturilor lor generale de protecție a datelor în temeiul RGPD. Prin urmare, considerentul trebuie să precizeze cel puțin că furnizorii trebuie să respecte obligațiile de la articolul 25 din RGPD în cazul prelucrării ulterioare a datelor de localizare sau a altor metadate. Acest lucru presupune cel puțin luarea următoarelor măsuri:

- (i) utilizarea unor pseudonime temporare;
- (ii) ștergerea oricărui tabel de căutare inversă între aceste pseudonime și datele inițiale de identificare;
- (iii) agregarea la un nivel la care utilizatorii individuali nu mai pot fi identificați prin itinerariile lor specifice; și
- (iv) ștergerea valorilor excepționale în privința cărora identificarea ar fi în continuare posibilă (toate aceste măsuri trebuie aplicate cumulativ).

În fine, Regulamentul privind viața privată și comunicațiile electronice trebuie să oblige părțile implicate în prelucrarea localizării și a altor metadate să facă publice metodele de anonimizare și de agregare ulterioară, fără a aduce atingere secretului garantat prin lege. Acest lucru ar permite atât autorităților de supraveghere, cât și publicului larg să verifice cu ușurință dacă metoda aleasă este potrivită.

#### *CLARIFICĂRI PRIVIND COMUNICAȚIILE NESOLICITATE*

43. Grupul de lucru propune clarificarea următoarelor aspecte privind comunicațiile nesolicitate:

- a. **formularea interdicției privind marketingul direct fără consimțământ.** Articolul 16 alineatul (1) din propunerea de regulament menționează în prezent că serviciile de comunicații electronice „pot” fi utilizate în scopul trimiterii de mesaje de marketing direct (cu consimțământul persoanei), dar nu conține o interdicție explicită privind trimiterea (direcționarea sau prezentarea) mesajelor de marketing direct fără consimțământ. Acest aspect se află în contradicție cu abordarea din celelalte dispoziții, în care mai întâi se formulează o interdicție, iar aceasta este urmată de anumite excepții concrete. Formularea actuală sugerează o abordare mai îngăduitoare (care probabil nu este intenționată). Grupul de lucru propune o formulare puțin diferită a

actualului articol 13 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice: „Folosirea de către persoanele fizice sau juridice a serviciilor de comunicații electronice, inclusiv a apelurilor vocale, a sistemelor automate de apelare și de comunicații, inclusiv a sistemelor semiautomate care fac conexiunea între destinatarul apelului și o altă persoană, a faxurilor, a poștei electronice sau alte utilizări ale serviciilor de comunicații electronice în scopul prezentării unor comunicațiilor în scopuri de marketing direct către utilizatorii finali poate fi permisă numai în legătură cu acei utilizatori finali care și-au dat consimțământul în prealabil.”

- b. **domeniul de aplicare al dispozițiilor privind comunicațiile și apelurile în scopuri de marketing efectuate către contactele existente.** Articolul 16 alineatul (2) prevede că, în cazul în care o persoană obține datele de contact de la un client existent prin e-mail, aceasta poate folosi respectivele date de contact pentru marketingul direct ulterior al propriilor produse și servicii, în cazul în care se oferă o posibilitate clară, gratuită și facilă de a se opune la momentul colectării și în fiecare mesaj. În prezent, acest lucru se limitează la datele de contact comerciale obținute „în contextul vânzării unui produs sau a unui serviciu” și pentru marketingul ulterior al propriilor produse sau servicii similare. Având în vedere că dispozițiile privind marketingul direct se aplică în egală măsură activităților promoționale necomerciale (de exemplu, ale organizațiilor caritabile sau ale partidelor politice), această dispoziție ar trebui modificată pentru a se aplica în egală măsură organizațiilor necomerciale pentru a contacta susținătorii din trecut atunci când aceștia își promovează propriile scopuri sau idealuri similare; același drept de a se opune ar trebui să se aplice apelurilor în scopuri de marketing direct. În plus, ar trebui să se stabilească un termen de valabilitate a „datelor de contact ale clienților existenți” în comunicațiile electronice în scopuri comerciale, caritabile sau politice, iar acest termen ar trebui să se aplice și în cazul apelurilor în scopuri de marketing direct. În cazul în care statele membre au optat pentru un sistem de opoziție față de apelurile vocale în scopuri de marketing, prezența unei relații de contact cu un client existent prevalează asupra înregistrării într-un registru Do Not Call. În aceste condiții, utilizatorii finali nu au nicio posibilitate efectivă de a preveni apelurile nesolicitate din partea companiilor sau a organizațiilor cu care au intrat în contact la un anumit moment, dar cu care nu mai doresc să aibă legături. Prin urmare, ca regulă generală, regulamentul ar trebui să precizeze perioada de valabilitate a acestei excepții privind „clienții existenți”, de exemplu unul sau doi ani, în raport cu așteptările legitime ale utilizatorilor finali vizați;
- c. **aplicarea normelor de marketing direct în cazul persoanelor juridice.** Articolul 16 alineatul (5) din propunerea de regulament prevede că statele membre se asigură că interesele legitime ale utilizatorilor finali care sunt persoane juridice beneficiază de un nivel de protecție suficient în privința comunicațiilor nesolicitate. Articolul 13 alineatul (5) din actuala Directivă asupra confidențialității și comunicațiilor electronice descrie interesele legitime ale abonaților, alții decât persoanele fizice. Nu este clar care sunt implicațiile acestei modificări a formulării. Ar trebui să se clarifice în considerente faptul că această modificare nu reflectă intenția de a oferi un

nivel mai scăzut de protecție. În acest sens, interzicerea marketingului direct fără consimțământ se referă la „utilizatorii finali care sunt persoane fizice și care și-au dat consimțământul în acest sens” (sublinierea noastră). Ar trebui să se clarifice faptul că aici sunt incluse și persoanele fizice *care lucrează* pentru persoane juridice. Pe de altă parte, consimțământul nu ar fi necesar pentru abordarea persoanelor juridice prin detalii de contact generice pe care le-au făcut publice în acest scop (cum ar fi „info@companynome.eu”);

- d. **aplicarea normelor în materie de marketing direct în cazul celor care acționează într-o capacitate de reprezentare (politică):** Articolul 16, așa cum a fost redactat, poate împiedica trimiterea către reprezentanții aleși a unor comunicații legate de preocupări sau interese comerciale. Ar trebui să se clarifice faptul că regulamentul nu împiedică astfel de comunicații.

#### *CLARIFICĂRI ÎN LEGĂTURĂ CU APLICAREA INSTRUMENTELOR PRIVIND DREPTURILE FUNDAMENTALE*

44. **Aplicarea cartei și a Convenției europene a drepturilor omului (CEaDO) în legislațiile naționale privind păstrarea datelor** ar trebui clarificată mai mult. Considerentul 26 prevede că orice măsură luată de statele membre pentru protejarea interesului public, cum ar fi măsurile de interceptare legală, trebuie să fie în conformitate cu cartă (pe lângă CEaDO). Acest lucru este de dorit, deoarece este în conformitate cu motivarea din Hotărârea Tele2/Watson, potrivit căreia orice excepții naționale de la legislația europeană în materie de protecții privind prelucrarea datelor fac obiectul cartei (și, astfel, încălcările prin intermediul legislației naționale pot face obiectul unor acțiuni la Curtea de Justiție a UE). Însă la articolul 11 din propunerea de regulament se constată doar că restricțiile privind sfera de aplicare a articolelor 5-8 din propunerea de regulament trebuie să respecte esența drepturilor și a libertăților fundamentale și să constituie o măsură necesară și proporțională. Ar trebui inclusă aici și o trimitere explicită la cartă și la Convenția europeană a drepturilor omului.

45. **Confidențialitatea comunicațiilor este protejată și prin articolul 8 din Convenția europeană a drepturilor omului.** La punctul 1.1 din expunerea de motive și în considerentul 1 se explică faptul că propunerea de regulament pune în aplicare articolul 7 din cartă. Această idee se repetă în considerentul 19. Cu toate acestea, dreptul fundamental la comunicații confidențiale este protejat nu numai prin această prevedere, ci și în temeiul articolului 8 din CEaDO. Includerea unei trimiteri explicite într-un articol din propunerea de regulament ar confirma și mai mult faptul că orice jurisprudență relevantă a Curții Europene a Drepturilor Omului va trebui luată în considerare la evaluarea regulamentului (final). Această trimitere este, de altfel, cuprinsă deja în considerentele 20 (referitor la echipamentele terminale) și 26 (referitor la interceptarea legală) și susținută suplimentar de considerațiile de la punctul 2.1 din expunerea de motive (referitoare la relația dintre cartă și CEaDO în contextul persoanelor juridice), dar nu și în vreunul dintre articolele relevante, cum ar fi articolul 11 alineatul (1).

46. Ar trebui să se clarifice faptul că **obligățiile care decurg din RGPD, cum ar fi cele privind regimul încălcării securității datelor cu caracter personal și evaluarea impactului asupra protecției datelor, rămân aplicabile** atunci când părțile prelucreează date cu caracter personal în contextul datelor transmise în cadrul comunicațiilor electronice. Deoarece se menționează în considerentul 5 că propunerea de regulament este *lex specialis* pentru RGPD și că prelucrarea datelor transmise în cadrul comunicațiilor electronice ar trebui permisă numai în conformitate cu propunerea de regulament, s-ar putea pune problema dacă anumite obligații din RGPD se aplică și în contextul propunerii de regulament. Aceasta este situația mai ales în cazul în care s-ar putea interpreta că propunerea de regulament introduce o anumită obligație, cu toate că ea este prevăzută și de RGPD. În continuare sunt prezentate câteva exemple elocvente:

- (i) propunerea de regulament impune obligația unei anumite notificări a riscurilor de securitate „detectate” (articolul 17) (a se vedea și observația 35), dar RGPD conține un regim de notificare a încălcării securității datelor (articolele 33 și 34);
- (ii) propunerea de regulament prevede că efectuarea unei evaluări a impactului asupra protecției datelor și consultarea cu autoritatea de supraveghere în conformitate cu RGPD sunt obligatorii în anumite circumstanțe [considerentele 17 și 19 și articolul 6 alineatul (3) litera (b)], în timp ce RGPD stabilește deja când trebuie să se realizeze o evaluare a impactului asupra protecției datelor și când este necesară consultarea (articolele 35 și 36); și
- (iii) nu se precizează că, dacă sunt întrunite condițiile necesare pentru o excepție de la interdicția de prelucrare prevăzută la articolul 5 din propunerea de regulament, trebuie să se respecte, totuși, toate obligațiile relevante în temeiul RGPD referitoare la prelucrarea datelor cu caracter personal, iar orice altă prelucrare în temeiul RGPD este interzisă. Prin urmare, ar trebui să se clarifice faptul că nu se aplică testul de compatibilitate prevăzut la articolul 6 alineatul (4) din RGPD.
- (iv) Propunerea de regulament privind viața privată și comunicațiile electronice nu prevede mecanisme de certificare similare cu cele de la articolele 42 și 43 din RGPD. Întrucât domeniul de aplicare al articolului 42 din RGPD se limitează strict la instituirea de mecanisme de certificare în domeniul protecției datelor, precum și de sigilii și mărci în acest domeniu, care să permită demonstrarea conformității cu RGPD, ar trebui să se analizeze dacă nu ar trebui introdusă o dispoziție comparabilă care să permită certificarea operațiunilor, a standardelor, a produselor sau a serviciilor de prelucrare în vederea respectării de către acestea a Regulamentului privind viața privată și comunicațiile electronice.

Pentru a se împiedica utilizarea acestei lipse de claritate ca argument pentru reducerea nivelului de protecție prevăzut de propunerea de regulament, trebuie să se clarifice faptul că, în toate aceste cazuri, operatorii trebuie să se conformeze și RGPD.

47. În plus, ar trebui să se clarifice faptul că **cerința privind retragerea consimțământului se aplică și în contextul intervențiilor asupra echipamentelor terminale**. Articolul 8 alineatul (1) litera (b) din propunerea de regulament prevede posibilitatea de a interveni asupra echipamentelor terminale ale utilizatorilor finali, cu consimțământul acestora. Articolul 9 alineatul (3) impune ca utilizatorii finali să aibă posibilitatea de a-și retrage consimțământul în orice moment, însă acest lucru se aplică doar pentru consimțământul pentru analiza metadatelor și a conținutului. Ar trebui să se clarifice faptul că această obligație este valabilă și pentru intervenția asupra echipamentelor terminale.
48. În acest sens, trebuie să se clarifice faptul că **reamintirea faptului că există posibilitatea de retragere a consimțământului se aplică și pentru consimțământul acordat prin setările browserului**. Articolul 9 alineatul (3) impune ca utilizatorilor finali să li se reamintească, la intervale regulate de 6 luni, posibilitatea de a-și retrage consimțământul în orice moment. Deși grupul de lucru consideră că setările generale ale browserelor și ale altor programe software, inclusiv ale sistemelor de operare, aplicațiilor și interfețelor programelor software pentru dispozitivele conectate la internetul obiectelor (adică nu pe baza unor controale detaliate specifice) nu pot constitui o măsură valabilă pentru acordarea consimțământului, deoarece setările generale nu sunt adecvate pentru acordarea consimțământului specific pentru scenarii specifice (a se vedea observația 24), setările implicite ar trebui să fie ușor de utilizat (a se vedea observația 19). *Dacă* acest aspect va rămâne menționat în propunerea de regulament, setările vor trebui să fie suficient de detaliate pentru a controla toate procesele de prelucrare a datelor pentru care utilizatorul își dă consimțământul și pentru a acoperi toate funcționalitățile echipamentelor care ar putea conduce la prelucrarea datelor. În plus, utilizatorului final ar trebui să i se amintească cel puțin la intervale periodice (de 6 luni) posibilitatea de a modifica aceste setări.
49. Este binevenită dispoziția din propunerea de regulament de a impune programelor software deja introduse pe piață să informeze utilizatorul final cu privire la opțiunile pe care le are cu privire la setările de confidențialitate (articolul 10). **Cu toate acestea, nu este clar modul în care această dispoziție poate fi aplicată eficient produselor vechi** și altor produse, pentru care nu se mai asigură asistență. În plus, ar trebui să se furnizeze clarificări suplimentare cu privire la modul în care această obligație se va aplica programelor software cu sursă deschisă, dezvoltate în mod deschis și descentralizat.
50. Ar trebui să se clarifice faptul că **oferirea posibilității de a bloca modulele cookie (de terță parte) în temeiul articolului 10 din propunerea de regulament prevalează asupra excepției pentru măsurarea audienței pe internet** de la articolul 8 alineatul (1) litera (d). Cu alte cuvinte, chiar dacă un site poate utiliza date analitice pentru măsurarea audienței pe internet în conformitate cu articolul 8 alineatul (1) litera (d), utilizatorii ar trebui să aibă, totuși, dreptul de a bloca aceste tehnologii de urmărire în browserul lor.
51. Ar trebui clarificată **definiția sistemelor de apelare și de comunicare (semi)automate**. Definiția acestui termen, prevăzută la articolul 4 alineatul (3)



litera (h) din propunerea de regulament, conține o trimitere la termenul în sine în a doua parte a propoziției („inclusiv apelurile efectuate utilizând sisteme de apelare și comunicare automate care fac conexiunea între destinatarul apelului și o altă persoană”). Se recomandă ștergerea ultimei propoziții din definiție și modificarea definiției de la articolul 4 alineatul (3) litera (g) pentru a include apelurile efectuate prin intermediul sistemelor de comunicare semiautomate, ca de exemplu dispozitivele automate de formare a numerelor care fac conexiunea între destinatarul apelului și o altă persoană.

52. **Ar trebuie clarificate informațiile care fac parte din abonamentul la un serviciu**”. În considerentul 14 se menționează că metadatele privind comunicațiile electronice „pot include informații care fac parte din abonamentul la un serviciu atunci când astfel de informații sunt prelucrate în scopul transmiterii, al distribuirii sau al schimbului de conținut al comunicațiilor electronice”. Nu este clară intenția din spatele acestei formulări.
53. **Ar trebui clarificată aplicabilitatea mecanismelor de asigurare a coerenței și a cooperării**. În considerentul 38 se remarcă faptul că propunerea de regulament se bazează pe mecanismul de asigurare a coerenței prevăzut în RGPD. În plus, articolul 18 alineatul (1) prevede că se aplică *mutatis mutandis* capitolele VI și VII din RGPD. La articolul 19 se mai remarcă faptul că Comitetul european pentru protecția datelor (*European Data Protection Board* – EDPB) își exercită atribuțiile prevăzute la articolul 70 din RGPD. Deși aplicarea acestor prevederi este relativ clară, există posibilitatea să apară probleme de interpretare cu privire la conceptele-cheie ale mecanismelor de asigurare a coerenței și a cooperării în temeiul RGPD. De exemplu, mecanismul autorității principale se aplică în cazurile în care există „prelucrare transfrontalieră” [articolul 56 alineatul (1) din RGPD]: nu se știe cum se aplică acest lucru în cazul intervenției asupra echipamentelor terminale sau al analizei conținutului sau a metadatelor în temeiul propunerii de regulament. Prin urmare, se recomandă să se clarifice aplicarea acestor concepte-cheie în cadrul unui considerent și să se sublinieze că orice întrebări rămase privind aplicabilitatea acestor capitole ale RGPD în contextul propunerii de regulament vor fi soluționate prin interpretarea dispozițiilor acestor capitole în conformitate cu intenția lor. În plus, se recomandă să fie exprimat clar faptul că articolul 70 se aplică *mutatis mutandis* Comitetului european pentru protecția datelor în contextul propunerii de regulament (acest lucru lipsește acum din considerent).

\* \* \*