COMISIA
EUROPEANĂ

Bruxelles, 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI 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)

(Text cu relevanță pentru SEE)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

EXPUNERE DE MOTIVE

1. CONTEXT

1.1. Temeiurile și obiectivele propunerii

Strategia privind piața unică digitală[1] are ca obiectiv creșterea încrederii în serviciile digitale și a securității acestora. În acest sens, reforma cadrului privind protecția datelor și, în special, adoptarea Regulamentului (UE) 2016/679 - Regulamentul general privind protecția datelor („**RGPD**”)[2], au avut un rol determinant. Strategia privind piața unică digitală a anunțat, de asemenea, revizuirea Directivei 2002/58/CE („**Directiva asupra confidențialității și comunicațiilor electronice**”)[3] în vederea asigurării unui nivel ridicat de protecție a vieții private a utilizatorilor de servicii de comunicații electronice și a unor condiții de concurență echitabile pentru toți actorii de pe piață. Prezenta propunere revizuiește Directiva asupra confidențialității și comunicațiilor electronice, luând în considerare obiectivele Strategiei privind piața unică digitală și asigurând coerența cu RGPD.

Directiva asupra confidențialității și comunicațiilor electronice asigură protecția drepturilor și libertăților fundamentale, în special respectarea vieții private, a confidențialității comunicațiilor și a protecției datelor cu caracter personal în sectorul comunicațiilor electronice. De asemenea, aceasta garantează libera circulație a datelor transmise în cadrul comunicațiilor electronice, a echipamentelor și a serviciilor în Uniune. Directiva pune în aplicare în legislația secundară a Uniunii dreptul fundamental la respectarea vieții private în ceea ce privește comunicațiile, astfel cum este consacrat la articolul 7 din Carta drepturilor fundamentale a Uniunii Europene („**Carta**”).

În conformitate cu cerințele privind „o mai bună legiferare”, Comisia a efectuat o evaluare *ex post* în baza Programului privind o reglementare adecvată și funcțională („**evaluare REFIT**”) a Directivei asupra confidențialității și comunicațiilor electronice. Ca urmare a acestei evaluări, s-a constatat că obiectivele și principiile cadrului actual rămân valabile. Cu toate acestea, de la ultima revizuire, în 2009, a Directivei asupra confidențialității și comunicațiilor electronice, au avut loc pe piață o serie de evoluții tehnologice și economice importante. Consumatorii și întreprinderile utilizează tot mai mult noile servicii bazate pe internet care permit comunicațiile interpersonale, cum ar fi serviciile de telefonie prin internet, de mesagerie instantanee și de e-mail pe internet, în locul serviciilor de comunicații tradiționale. Aceste servicii de comunicații over-the-top („**OTT**”) nu intră, în general, sub incidența cadrului actual al Uniunii privind comunicațiile electronice, inclusiv a Directivei asupra confidențialității și comunicațiilor electronice. În consecință, directiva nu a ținut pasul cu evoluțiile tehnologice, ceea ce a condus la o lipsă de protecție a comunicațiilor efectuate prin intermediul noilor servicii.

---

1 Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor - O strategie privind piața unică digitală pentru Europa, COM(2015) 192 final.

2 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, 4.5.2016, p. 1-88).

3 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).

1.2. Coerența cu dispozițiile deja existente în domeniul de politică vizat

Prezenta propunere este 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. Toate aspectele care au legătură cu prelucrarea datelor cu caracter personal ce nu sunt abordate în mod specific în cadrul propunerii sunt reglementate de RGPD. Armonizarea cu RGPD a condus la abrogarea unor dispoziții, cum ar fi obligațiile în materie de securitate prevăzute la articolul 4 din Directiva asupra confidențialității și comunicațiilor electronice.

1.3. Coerența cu alte domenii de politică a Uniunii

Directiva asupra confidențialității și comunicațiilor electronice face parte din cadrul de reglementare pentru comunicațiile electronice. În 2016, Comisia a adoptat Propunerea de directivă de instituire a Codului european al comunicațiilor electronice („*European Electronic Communications Code* – **EECC**”)[4], care revizuiește acest cadru. Cu toate că prezenta propunere nu este parte integrantă din EECC, aceasta se bazează parțial pe definițiile prevăzute în acesta, inclusiv pe definiția privind „serviciile de comunicații electronice”. În mod similar cu EECC, prezenta propunere introduce, de asemenea, furnizorii de servicii OTT în domeniul său de aplicare pentru a reflecta realitatea de pe piață. În plus, prezenta propunere completează EECC prin asigurarea securității serviciilor de comunicații electronice.

Directiva 2014/53/UE privind echipamentele radio („**DER**”)[5] asigură o piață unică pentru echipamente radio. În special, aceasta prevede că, înainte de a fi introduse pe piață, echipamentele radio trebuie să includă garanții pentru asigurarea protecției datelor cu caracter personal și a confidențialității utilizatorului. În conformitate cu DER și cu Regulamentul (UE) nr. 1025/2012 privind standardizarea europeană[6], Comisia este împuternicită să adopte măsuri. Prezenta propunere nu aduce atingere DER.

Propunerea nu include dispoziții specifice în materie de păstrare a datelor. Aceasta menține conținutul de bază al articolului 15 din Directiva asupra confidențialității și comunicațiilor electronice și îl aliniază cu formularea specifică a articolului 23 din RGPD, care prezintă motivele ce permit statelor membre să restrângă sfera de aplicare a drepturilor și a obligațiilor prevăzute la articolele specifice din Directiva asupra confidențialității și comunicațiilor electronice. Prin urmare, statele membre sunt libere să mențină sau să creeze cadre naționale în materie de păstrare a datelor care prevăd, printre altele, măsuri de păstrare specifice, în măsura în care astfel de cadre sunt conforme cu legislația Uniunii, ținând seama de jurisprudența Curții de Justiție referitoare la interpretarea Directivei asupra confidențialității și comunicațiilor electronice și de Carta drepturilor fundamentale[7].

---

4 Propunerea Comisiei de directivă a Parlamentului European și a Consiliului de instituire a Codului european al comunicațiilor electronice (reformare) [(COM/2016/0590 final – 2016/0288 (COD)].

5 Directiva 2014/53/UE a Parlamentului European și a Consiliului din 16 aprilie 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a echipamentelor radio și de abrogare a Directivei 1999/5/CE (JO L 153, 22.5.2014, p. 62-106).

6 Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei nr. 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12-33).

7 A se vedea cauzele conexate C-293/12 și C-594/12, Digital Rights Ireland și Seitlinger și alții, ECLI:EU:C:2014:238; cauzele conexate C-203/15 și C-698/15 Tele2 Sverige AB și Secretary of State for the Home Department, ECLI:EU:C:2016:970.

În cele din urmă, propunerea nu se aplică activităților instituțiilor, organelor și agențiilor Uniunii. Cu toate acestea, principiile și obligațiile relevante prevăzute de propunere în ceea ce privește dreptul la respectarea vieții private și a comunicațiilor în legătură cu prelucrarea datelor transmise în cadrul comunicațiilor electronice au fost incluse în Propunerea de regulament de abrogare a Regulamentului (CE) nr. 45/2001[8].

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

2.1. Temeiul juridic

Temeiurile juridice relevante ale propunerii sunt articolele 16 și 114 din Tratatul privind funcționarea Uniunii Europene („**TFUE**”).

Articolul 16 din TFUE introduce un temei juridic specific pentru adoptarea de norme referitoare la protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile Uniunii și statele membre atunci când desfășoară activități care intră în domeniul de aplicare al dreptului Uniunii, precum și norme privind libera circulație a acestor date. Întrucât comunicațiile electronice implicând o persoană fizică sunt considerate, în mod normal, drept date cu caracter personal, protecția persoanelor fizice în ceea ce privește confidențialitatea comunicațiilor și prelucrarea unor astfel de date ar trebui să se bazeze pe articolul 16.

În plus, propunerea are ca obiectiv protejarea comunicațiilor și a intereselor legitime ale persoanelor juridice. Înțelesul și domeniul de aplicare al drepturilor în temeiul articolului 7 din Cartă trebuie, în conformitate cu articolul 52 alineatul (3) din Cartă, să fie aceleași cu cele prevăzute la articolul 8 alineatul (1) din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale. În ceea ce privește domeniul de aplicare al articolului 7 din Cartă, jurisprudența Curții de Justiție a Uniunii Europene („**CJUE**”)[9] și a Curții Europene a Drepturilor Omului[10] confirmă faptul că activitățile profesionale ale persoanelor juridice nu pot fi excluse de la protecția dreptului garantat la articolul 7 din Cartă și la articolul 8 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale.

Întrucât inițiativa urmărește un scop dublu, iar componenta privind protejarea comunicațiilor persoanelor juridice și scopul ce constă în realizarea pieței interne pentru comunicațiile electronice respective și în asigurarea funcționării sale în această privință nu pot fi considerate ca având un simplu caracter accesoriu, inițiativa ar trebui, prin urmare, să se întemeieze, de asemenea, pe articolul 114 din TFUE.

2.2. Subsidiaritatea

Respectarea comunicațiilor este un drept fundamental recunoscut în Cartă. Conținutul comunicațiilor electronice poate dezvălui informații extrem de sensibile privind utilizatorii finali implicați în comunicare. În mod similar, metadatele provenite din comunicațiile electronice pot, de asemenea, dezvălui informații extrem de sensibile și cu caracter personal, astfel cum a recunoscut în mod expres CJUE[11]. Majoritatea statelor membre recunosc, de

---

[8] Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1-22).

[9] A se vedea cauza C-450/06, Varec SA, ECLI:EU:C:2008:91, punctul 48.

[10] A se vedea, printre altele, hotărârile CEDO *Niemietz/ Germania* din 16 decembrie 1992, seria A, nr. 251-B, punctul 29; *Société Colas Est și alții/Franța*, nr. 37971/97, punctul 41; CEDO 2002-III; *Peck/Regatul Unit*, nr. 44647/98, punctul 57, CEDO 2003-I; precum și *Vinci Construction și GTM Génie Civil et Services/ Franța*, nr. 63629/10 și 60567/10, punctul 63, 2 aprilie 2015.

[11] A se vedea nota de subsol 7.

asemenea, că necesitatea de a proteja comunicațiile reprezintă un drept constituțional distinct. Deși este posibil ca statele membre să adopte politici care să garanteze că acest drept nu este încălcat, acest obiectiv nu ar putea fi atins în mod uniform în absența unor norme ale Uniunii și ar crea restricții privind fluxurile transfrontaliere de date cu caracter personal și fără caracter personal care au legătură cu utilizarea serviciilor de comunicații electronice. În final, pentru a se păstra coerența cu RGPD, este necesară revizuirea Directivei asupra confidențialității și comunicațiilor electronice și adoptarea de măsuri pentru armonizarea celor două instrumente.

Evoluțiile tehnologice și ambițiile Strategiei privind piața unică digitală au consolidat argumentele în favoarea unei acțiuni la nivelul Uniunii. Succesul pieței unice digitale a UE depinde de nivelul de eficacitate cu care UE reușește să înlăture compartimentările și barierele naționale și să valorifice avantajele și economiile oferite de o piață unică digitală europeană. În plus, având în vedere că internetul și tehnologiile digitale nu cunosc frontiere, dimensiunea problemei nu se limitează la teritoriul unui singur stat membru. Statele membre nu pot soluționa în mod eficace problemele în situația actuală. Este necesară asigurarea unor condiții de concurență echitabile pentru operatorii economici care furnizează servicii substituibile și a unui nivel de protecție uniform pentru utilizatorii finali la nivelul Uniunii pentru ca piața unică digitală să funcționeze corespunzător.

2.3. Proporționalitatea

Este necesară o extindere a domeniului de aplicare pentru a include furnizorii de servicii OTT în vederea asigurării unei protecții juridice eficace în materie de respectare a vieții private și a comunicațiilor. Cu toate că mai mulți furnizori cunoscuți de servicii OTT respectă deja, în totalitate sau parțial, principiul confidențialității comunicațiilor, protejarea drepturilor fundamentale nu poate să facă obiectul unei autoreglementări de către acest sector. De asemenea, importanța protecției efective a echipamentelor terminale din punctul de vedere al respectării vieții private crește, deoarece acestea au devenit indispensabile în viața personală și profesională pentru stocarea de informații sensibile. Punerea în aplicare a Directivei asupra confidențialității și comunicațiilor electronice nu a fost eficace din punctul de vedere al responsabilizării utilizatorilor finali. Prin urmare, pentru atingerea obiectivului este necesară punerea în aplicare a principiului prin centralizarea consimțământului în cadrul unui software și informarea utilizatorilor cu privire la setările de confidențialitate. În ceea ce privește asigurarea respectării prezentului regulament, aceasta se bazează pe autoritățile de supraveghere și pe mecanismul pentru asigurarea coerenței prevăzut în RGPD. În plus, propunerea permite statelor membre să ia măsuri de derogare la nivel național pentru anumite scopuri legitime specifice. Prin urmare, propunerea nu depășește ceea ce este necesar pentru a-și atinge obiectivele și respectă principiul proporționalității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. Obligațiile impuse serviciilor afectate sunt menținute la un nivel minim, pe cât posibil, fără a afecta drepturile fundamentale vizate.

2.4. Alegerea instrumentului

Comisia prezintă o propunere de regulament pentru a asigura coerența cu RGPD și securitatea juridică pentru utilizatori și întreprinderi, în egală măsură, evitând interpretări divergente în statele membre. Un regulament le permite utilizatorilor să beneficieze de același nivel de protecție în întreaga Uniune și întreprinderilor care desfășoară activități transfrontaliere să suporte costuri de conformitate mai reduse.

3. REZULTATE ALE EVALUĂRILOR EX POST, CONSULTĂRILOR PĂRȚILOR INTERESATE ȘI EVALUĂRII IMPACTULUI

3.1. Evaluările ex post/verificarea adecvării legislației existente

Evaluarea REFIT a examinat măsura în care Directiva asupra confidențialității și comunicațiilor electronice a contribuit în mod eficient la o protecție adecvată a respectării vieții private și a confidențialității comunicațiilor în UE. De asemenea, aceasta a urmărit să identifice posibilele redundanțe.

Evaluarea REFIT a concluzionat că obiectivele directivei menționate mai sus rămân **relevante**. În timp ce RGPD asigură protecția datelor cu caracter personal, Directiva asupra confidențialității și comunicațiilor electronice asigură confidențialitatea comunicațiilor, care pot conține, de asemenea, date fără caracter personal și date referitoare la o persoană juridică. Prin urmare, un instrument distinct ar trebui să asigure o protecție eficace a articolului 7 din Cartă. Alte dispoziții, cum ar fi normele privind transmiterea comunicărilor publicitare nesolicitate, s-au dovedit, de asemenea, relevante în continuare.

În termeni de **eficacitate și eficiență**, evaluarea REFIT a constatat că directiva nu și-a atins obiectivele pe deplin. Redactarea neclară a anumitor dispoziții și ambiguitatea unor concepte juridice au pus în pericol armonizarea, creând, astfel, provocări pentru întreprinderile care își desfășoară activitatea la nivel transfrontalier. Evaluarea a mai arătat că unele dispoziții au creat o sarcină inutilă asupra întreprinderilor și a consumatorilor. De exemplu, norma referitoare la consimțământul în vederea protejării confidențialității echipamentelor terminale nu și-a atins obiectivele întrucât utilizatorii finali se confruntă cu solicitări de a accepta cookie-urile permanente fără a înțelege ce sunt acestea și, în unele cazuri, sunt chiar expuși unor situații în care li se instalează cookie-uri fără consimțământul lor. Norma referitoare la consimțământ este excesiv de inclusivă deoarece acoperă, de asemenea, practici care nu aduc atingere vieții private și, totodată, nu este suficient de inclusivă, întrucât nu acoperă în mod clar unele tehnici de urmărire (de exemplu, prelevarea amprentelor digitale prin intermediul unui dispozitiv) care nu permit neapărat accesul la date sau stocarea de date în dispozitiv. În cele din urmă, punerea sa în aplicare poate fi costisitoare pentru întreprinderi.

În urma evaluării s-a constatat că normele prevăzute în Directiva asupra confidențialității și comunicațiilor electronice conferă în continuare o **valoare adăugată la nivelul UE** în ceea ce privește o mai bună îndeplinire a obiectivului de a asigura protecția vieții private pe internet în contextul unei piețe a comunicațiilor electronice din ce în ce mai transnațională. Aceasta a demonstrat, de asemenea, că, în general, normele sunt **coerente** cu alte acte legislative relevante, deși au fost identificate câteva redundanțe în raport cu noul RGPD (a se vedea secțiunea 1.2).

3.2. Consultările părților interesate

Comisia a organizat o consultare publică în perioada 12 aprilie – 5 iulie 2016 și a primit 421 de răspunsuri[12]. Principalele constatări sunt următoarele[13]:

[12] 162 de contribuții de la cetățeni, 33 de la organizațiile societății civile și de consumatori; 186 de la întreprinderi și 40 de la autorități publice, inclusiv autoritățile competente însărcinate cu punerea în aplicare a Directivei asupra confidențialității și comunicațiilor electronice.

[13] Textul complet al raportului este disponibil la adresa: https://ec.europa.eu/digital-single-market/news-redirect/37204.

– **Necesitatea adoptării unor norme specifice pentru sectorul comunicațiilor electronice privind confidențialitatea comunicațiilor electronice**: 83,4 % dintre cetățenii și organizațiile societății civile și de consumatori și 88,9 % dintre autoritățile publice care au oferit răspunsuri sunt de acord, în timp ce 63,4 % dintre respondenții din partea întreprinderilor nu sunt de acord.

– **Extinderea domeniului de aplicare la noile servicii de comunicații (OTT)**: 76 % dintre cetățeni și organizațiile societății civile și 93,1 % dintre autoritățile publice sunt de acord, în timp ce numai 36,2 % dintre respondenții din partea întreprinderilor sunt în favoarea unei astfel de extinderi.

– **Modificarea excepțărilor privind consimțământul pentru prelucrarea datelor privind traficul și localizarea**: 49,1 % dintre cetățeni și organizațiile societății civile și de consumatori și 36 % dintre autoritățile publice preferă să nu fie extinse excepțările, în timp ce 36 % dintre întreprinderi sunt în favoarea acestor excepțări extinse, iar 2/3 dintre întreprinderi susțin pur și simplu abrogarea dispozițiilor.

– **Sprijinul pentru soluțiile propuse cu privire la chestiunea legată de consimțământul privind cookie-urile**: 81,2 % dintre cetățeni și 63 % dintre autoritățile publice sprijină soluția care constă în a le impune producătorilor de echipamente terminale obligația de a comercializa produse în care sunt activate setările de confidențialitate implicite, în timp ce 58,3 % dintre întreprinderi preferă opțiunea de a susține autoreglementarea/coreglementarea.

În plus, Comisia Europeană a organizat în aprilie 2016 două ateliere, unul deschis tuturor părților interesate și celălalt destinat autorităților naționale competente, care au abordat principalele întrebări din cadrul consultărilor publice. Opiniile exprimate pe parcursul atelierelor reflectă concluziile consultării publice.

Pentru a obține opiniile cetățenilor, s-a organizat un sondaj Eurobarometru pe întreg teritoriul UE privind confidențialitatea și comunicațiile electronice[14]. Principalele constatări sunt următoarele[15]:

– 78 % dintre respondenți afirmă că este foarte important ca informațiile cu caracter personal de pe computerele, telefoanele inteligente sau tabletele lor să poată fi accesate numai cu permisiunea lor.

– 72 % afirmă că este foarte important să le fie garantată confidențialitatea e-mailurilor și a mesajelor instantanee online.

– 89 % sunt de acord cu opțiunea sugerată că setările implicite ale browserului folosit ar trebui să împiedice schimbul de informații care îi privesc.

3.3. Obținerea și utilizarea expertizei

Comisia s-a bazat pe consiliere de specialitate externă, și anume:

– consultări specifice ale grupurilor de experți ai UE: avizul Grupului de lucru „Articolul 29”; avizul AEPD; avizul platformei REFIT; punctele de vedere ale OAREC; punctele de vedere ale ENISA și ale membrilor Rețelei de cooperare în domeniul protecției consumatorilor;

[14] Sondaj Eurobarometru 443 din 2016 privind confidențialitatea și comunicațiile electronice (SMART 2016/079).

[15] Textul complet al raportului este disponibil la adresa: https://ec.europa.eu/digital-single-market/news-redirect/37205.

– expertiza externă, în special următoarele două studii:

  – „*ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*” (SMART 2013/007116).

  – „*Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*” (SMART 2016/0080).

3.4. Evaluarea impactului

A fost efectuată o evaluare a impactului referitoare la prezenta propunere, cu privire la care Comitetul de analiză a reglementării a emis un aviz favorabil[16] la 28 septembrie 2016. Pentru a răspunde recomandărilor comitetului, evaluarea impactului explică mai bine domeniul de aplicare al inițiativei, coerența sa cu alte instrumente juridice (RGPD, EECC, DER) și necesitatea unui instrument distinct. Scenariul de referință este mai bine dezvoltat și clarificat. Analiza impactului este consolidată și mai echilibrată, furnizând o descriere mai clară și detaliată a costurilor și a beneficiilor preconizate.

Următoarele opțiuni de politică au fost examinate pe baza criteriilor de eficacitate, eficiență și coerență:

– **opțiunea 1:** măsuri nelegislative („fără caracter obligatoriu”);

– **opțiunea 2:** consolidarea limitată a respectării vieții private/confidențialității și simplificare;

– **opțiunea 3:** consolidarea moderată a respectării vieții private/confidențialității și simplificare;

– **opțiunea 4:** consolidarea semnificativă a respectării vieții private/confidențialității și simplificare;

– **opțiunea 5:** abrogarea Directivei asupra confidențialității și comunicațiilor electronice.

Opțiunea 3 a fost desemnată ca fiind **opțiunea preferată**, în majoritatea aspectelor, pentru a atinge obiectivele, luând totodată în considerare eficiența și coerența acesteia. Principalele sale avantaje sunt:

– o mai mare protecție a confidențialității comunicațiilor electronice prin extinderea domeniului de aplicare al instrumentului juridic pentru a include noile servicii de comunicații electronice echivalente din punct de vedere funcțional. În plus, regulamentul consolidează controlul utilizatorului final, clarificând faptul că consimțământul poate fi exprimat prin setări tehnice corespunzătoare;

– consolidarea protecției împotriva comunicațiilor nesolicitate prin introducerea unei obligații de a furniza identificarea liniei apelante sau a unui prefix obligatoriu pentru apelurile în scopuri de marketing și prin posibilitățile sporite de a bloca apelurile de la numere nedorite;

– simplificarea și clarificarea cadrului de reglementare, prin reducerea marjei de manevră a statelor membre, abrogarea dispozițiilor perimate și lărgirea domeniului excepțiilor la normele privind consimțământul.

[16] http://ec.europa.eu/transparency/regdoc/?fuseaction=ia.

Impactul economic al opțiunii 3 este estimat a fi în ansamblu proporțional cu obiectivele propunerii. Serviciile de comunicații electronice tradiționale vor putea beneficia de oportunitățile de afaceri legate de prelucrarea datelor transmise în cadrul comunicațiilor, în timp ce furnizorii de servicii OTT vor face obiectul aceloraşi norme. Acest lucru implică unele costuri de conformitate suplimentare pentru operatorii în cauză. Cu toate acestea, modificarea menționată nu va afecta în mod substanțial serviciile OTT care funcționează deja pe baza consimțământului utilizatorilor. În cele din urmă, impactul opțiunii nu se va face simțit în statele membre care au extins deja aceste norme la serviciile OTT.

Prin centralizarea consimțământului în software, cum ar fi browserele de internet, prin invitarea utilizatorilor să își aleagă setările de confidențialitate și prin extinderea excepțiilor la regula consimțământului privind cookie-urile, o mare parte din întreprinderi ar fi în măsură să elimine bannerele și anunțurile privind cookie-urile, ceea ce ar putea conduce la reduceri de costuri și la simplificarea considerabilă a procedurii. Cu toate acestea, ar putea deveni mai dificil pentru anumiți difuzori de publicitate online de a obține consimțământul utilizatorilor, în cazul în care o mare parte a acestora ar opta pentru setările de „respingere a cookie-urilor de terță parte”. În același timp, centralizarea consimțământului nu îi privează pe operatorii site-urilor web de posibilitatea de a obține consimțământul prin intermediul unor cereri individuale către utilizatorii finali și, astfel, de posibilitatea de a-și menține actualul model de afaceri. Ar apărea costuri suplimentare pentru anumiți furnizori de browsere sau software similare, deoarece aceștia ar trebui să asigure setări care respectă viața privată.

Studiul extern a identificat trei scenarii distincte de punere în aplicare a opțiunii 3, în funcție de entitatea care va stabili caseta de dialog între utilizatorul care a ales setările de „respingere a cookie-urilor de terță parte” sau setările „fără monitorizare” și site-urile web vizitate care doresc ca utilizatorul de internet să își reconsidere alegerea. Entitățile care ar putea primi responsabilitatea privind această sarcină tehnică sunt: 1) software-ul, cum ar fi browserele de internet; 2) sistemele de monitorizare de terță parte; 3) site-urile web individuale (de exemplu, servicii ale societății informaționale solicitate de utilizator). În raport cu scenariul de referință, opțiunea 3 ar conduce la economii globale de 70 % în ceea ce privește costurile de conformitate (948,8 milioane EUR) în cazul primului scenariu (soluția privind browserele) prevăzut în prezenta propunere. Economiile de costuri ar fi mai reduse în alte scenarii. Întrucât economiile globale provin, în mare parte, dintr-o scădere considerabilă a numărului întreprinderilor afectate, valoarea individuală a costurilor de conformitate pe care ar trebui să le suporte o întreprindere ar fi, în medie, mai ridicată decât în prezent.

3.5. Adecvarea reglementărilor și simplificarea

Măsurile de politică propuse în cadrul opțiunii preferate abordează obiectivul de simplificare și de reducere a sarcinii administrative, în conformitate cu constatările evaluării REFIT și cu avizul platformei REFIT[17].

Platforma REFIT a emis trei seturi de recomandări adresate Comisiei:

– Protecția vieții private a cetățenilor ar trebui consolidată prin alinierea Directivei asupra confidențialității și comunicațiilor electronice la Regulamentul general privind protecția datelor;

– Eficacitatea protecției cetățenilor împotriva publicității nesolicitate ar trebui îmbunătățită prin adăugarea unor excepții de la regula consimțământului privind cookie-urile;

[17] http://ec.europa.eu/smart-regulation/refit/refit-platform/docs/recommendations/opinion_comm_net.pdf.

– Comisia abordează problemele naționale de punere în aplicare și facilitează schimbul de bune practici între statele membre.

Propunerea prevede în mod specific:

– utilizarea unor definiții neutre din punct de vedere tehnologic pentru a îngloba noile servicii și tehnologii astfel încât regulamentul să fie viabil pe termen lung;

– abrogarea normelor de securitate pentru a elimina dubla reglementare;

– clarificarea domeniului de aplicare pentru a contribui la eliminarea/reducerea riscului de implementare divergentă de către statele membre (punctul 3 din aviz);

– clarificarea și simplificarea regulii consimțământului privind cookie-urile și alți identificatori, astfel cum se explică în secțiunile 3.1 și 3.4 (punctul 2 din aviz);

– convergența autorităților de supraveghere cu autoritățile competente cu privire la punerea în aplicare a RGPD și recurgerea la mecanismul pentru asigurarea coerenței prevăzut în RGPD.

3.6. Impactul asupra drepturilor fundamentale

Propunerea urmărește să sporească eficacitatea protecției vieții private și a datelor personale prelucrate în legătură cu comunicațiile electronice și să mărească nivelul de protecție, în conformitate cu articolele 7 și 8 din Cartă, precum și să asigure o mai mare securitate juridică. Propunerea completează și detaliază RGPD. Protecția eficace a confidențialității comunicațiilor este esențială pentru exercitarea libertății de exprimare și de informare, precum și a altor drepturi conexe, cum ar fi dreptul la protecția datelor cu caracter personal sau a libertății de gândire, de conștiință și de religie.

4. IMPLICAȚII BUGETARE

Propunerea nu are nicio implicație pentru bugetul Uniunii.

5. ELEMENTE DIVERSE

5.1. Planurile de implementare și mecanismele de monitorizare, evaluare și raportare

Comisia va monitoriza punerea în aplicare a regulamentului și va prezenta Parlamentului European, Consiliului și Comitetului Economic și Social European un raport privind evaluarea sa o dată la trei ani. Aceste rapoarte vor fi publice și vor prezenta în detaliu punerea în aplicare efectivă și asigurarea respectării prezentului regulament.

5.2. Explicații detaliate cu privire la prevederile specifice ale propunerii

Capitolul I conține dispozițiile generale: obiectul (articolul 1), domeniul de aplicare (articolele 2 și 3) și definițiile din cadrul propunerii, inclusiv trimiteri la definițiile relevante din cadrul altor instrumente ale UE, cum ar fi RGPD.

Capitolul II conține principalele dispoziții referitoare la asigurarea confidențialității comunicațiilor electronice (articolul 5) și la scopurile limitate și condițiile în care este permisă prelucrarea acestor date transmise în cadrul comunicațiilor (articolele 6 și 7). Capitolul abordează, de asemenea, protecția echipamentelor terminale prin (i) garantarea integrității informațiilor stocate în acestea și (ii) protejarea informațiilor emise de echipamentele terminale, deoarece aceasta ar putea permite identificarea utilizatorilor finali ai echipamentelor (articolul 8). În cele din urmă, articolul 9 detaliază noțiunea de consimțământ

al utilizatorilor finali, care reprezintă un motiv legal central al prezentului regulament, făcând trimitere în mod expres la definiția acestuia și la condițiile prevăzute în RGPD, iar articolul 10 impune furnizorilor de software care permit comunicațiile electronice obligația de a-i ajuta pe utilizatorii finali să își aleagă în mod eficace setările de confidențialitate. Articolul 11 detaliază scopurile și condițiile în care statele membre pot restrânge dispozițiile de mai sus.

Capitolul III se referă la drepturile utilizatorilor finali de a controla transmiterea și primirea comunicațiilor electronice în vederea protejării vieții lor private: (i) dreptul utilizatorilor finali de a împiedica prezentarea identificării liniei apelante pentru garantarea anonimatului (articolul 12), cu limitările sale (articolul 13); și (ii) obligația ca furnizorii de servicii de comunicații interpersonale bazate pe numere și accesibile publicului să ofere posibilitatea de a limita primirea apelurilor nedorite (articolul 14). Acest capitol reglementează, de asemenea, condițiile în care utilizatorii finali pot fi incluși în liste de abonați accesibile publicului (articolul 15) și condițiile în care pot fi efectuate comunicațiile nesolicitate în scopuri de marketing direct (articolul 17). De asemenea, capitolul se referă la riscurile pentru securitate și prevede obligația ca furnizorii de servicii de comunicații electronice să alerteze utilizatorii finali în cazul unui risc specific care ar putea compromite securitatea rețelelor și a serviciilor. Obligațiile în materie de securitate prevăzute în RGPD și în EECC se vor aplica furnizorilor de servicii de comunicații electronice.

Capitolul IV stabilește dispozițiile în materie de supraveghere și asigurare a respectării prezentului regulament, aceste atribuții fiind conferite autorităților de supraveghere responsabile de RGPD, având în vedere sinergiile semnificative care există între aspectele generale privind protecția datelor și confidențialitatea comunicațiilor (articolul 18). Atribuțiile Comitetului european pentru protecția datelor sunt extinse (articolul 19), iar mecanismul pentru cooperare și asigurarea coerenței prevăzut în RGPD se va aplica în cazul chestiunilor transfrontaliere legate de prezentul regulament (articolul 20).

Capitolul V detaliază diversele căi de atac aflate la dispoziția utilizatorilor finali (articolele 21 și 22) și sancțiunile care pot fi aplicate (articolul 24), inclusiv condițiile generale pentru impunerea amenzilor administrative (articolul 23).

Capitolul VI se referă la adoptarea de acte delegate și acte de punere în aplicare în conformitate cu articolele 290 și 291 din tratat.

În cele din urmă, capitolul VII conține dispozițiile finale ale prezentului regulament: abrogarea Directivei asupra confidențialității și comunicațiilor electronice, monitorizarea și revizuirea, intrarea în vigoare și aplicarea. În ceea ce privește revizuirea, Comisia intenționează să evalueze, printre altele, dacă este în continuare necesar un act juridic separat, în lumina evoluțiilor juridice, tehnice sau economice și ținând seama de prima evaluare a Regulamentului (UE) 2016/679 care este prevăzută pentru 25 mai 2020.

2017/0003 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI 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)

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ŞI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolele 16 și 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European[1],

având în vedere avizul Comitetului Regiunilor[2],

având în vedere avizul Autorității Europene pentru Protecția Datelor[3],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Articolul 7 din Carta drepturilor fundamentale a Uniunii Europene („Carta”) protejează dreptul fundamental al tuturor persoanelor la respectarea vieții private și de familie, a domiciliului și a comunicațiilor acestora. Respectarea caracterului privat al comunicațiilor unei persoane constituie o dimensiune esențială a acestui drept. Confidențialitatea comunicațiilor electronice garantează faptul că schimbul de informații dintre părți și elementele externe ale unor astfel de comunicații, inclusiv cele privind momentul, locul și persoana căreia i-au fost trimise informațiile, nu trebuie dezvăluite nimănui, cu excepția părților implicate în comunicare. Principiul confidențialității ar trebui să se aplice mijloacelor de comunicare actuale și viitoare, inclusiv apelurilor telefonice, accesării internetului, aplicațiilor de mesagerie instantanee, e-mailurilor, apelurilor telefonice pe internet și mesageriei personale prin intermediul platformelor de comunicare sociale.

(2) Conținutul comunicațiilor electronice poate dezvălui informații extrem de sensibile despre persoanele fizice implicate în comunicare, de la experiențe și emoții personale, la starea de sănătate, preferințe sexuale și opinii politice, a căror divulgare ar putea conduce la prejudicii personale și sociale, pierderi economice sau situații neplăcute. În mod similar, metadatele provenite din comunicațiile electronice pot, de asemenea,

[1] JO C , , p. .
[2] JO C , , p. .
[3] JO C , , p. .

dezvălui informații extrem de sensibile și cu caracter personal. Aceste metadate includ numerele apelate, site-urile web vizitate, localizarea geografică, ora, data și durata unui apel telefonic efectuat de o persoană etc., ceea ce ar permite să se tragă concluzii precise cu privire la viața privată a persoanelor implicate în comunicațiile electronice, cum ar fi, de exemplu, cele referitoare la relațiile sociale, obiceiurile și activitățile acestora din viața de zi cu zi, interesele și preferințele lor, etc.

(3) Datele transmise în cadrul comunicațiilor electronice pot, de asemenea, să divulge informații referitoare la persoane juridice, cum ar fi secrete de afaceri sau alte informații sensibile cu valoare economică. Prin urmare, dispozițiile prezentului regulament ar trebui să se aplice atât persoanelor fizice, cât și persoanelor juridice. În plus, prezentul regulament ar trebui să asigure faptul că dispozițiile Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului[4] se aplică, de asemenea, utilizatorilor finali care sunt persoane juridice. Aceasta include definiția consimțământului în temeiul Regulamentului (UE) 2016/679. Atunci când se face trimitere la consimțământul utilizatorilor finali, inclusiv al persoanelor juridice, ar trebui să se aplice această definiție. În plus, persoanele juridice ar trebui să aibă aceleași drepturi ca și utilizatorii finali care sunt persoane fizice în ceea ce privește autoritățile de supraveghere, care ar trebui, în temeiul prezentului regulament, să fie responsabile cu monitorizarea aplicării acestuia cu privire la persoanele juridice.

(4) În conformitate cu articolul 8 alineatul (1) din Cartă și cu articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene, orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. Regulamentul (UE) 2016/679 stabilește norme referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și norme referitoare la libera circulație a datelor cu caracter personal. Datele transmise în cadrul comunicațiilor electronice pot include date cu caracter personal, astfel cum sunt definite în Regulamentul (UE) 2016/679.

(5) Dispozițiile prezentului regulament detaliază și completează normele generale privind protecția datelor cu caracter personal prevăzute în Regulamentul (UE) 2016/679 referitoare la datele transmise în cadrul comunicațiilor electronice care se încadrează în categoria datelor cu caracter personal. Prin urmare, prezentul regulament nu reduce nivelul de protecție de care beneficiază persoanele fizice în temeiul Regulamentului (UE) 2016/679. Prelucrarea datelor transmise în cadrul comunicațiilor electronice de către furnizorii de servicii de comunicații electronice ar trebui să fie permisă numai în conformitate cu prezentul regulament.

(6) În timp ce principiile și dispozițiile principale ale Directivei 2002/58/CE a Parlamentului European și a Consiliului[5] rămân în general valabile, directiva menționată nu a ținut pe deplin pasul cu evoluția tehnologică și cu realitatea de pe piață, având ca rezultat o serie de inconsecvențe sau de lipsuri legate de protecția efectivă a vieții private și a confidențialității în ceea ce privește comunicațiile electronice. Aceste evoluții includ intrarea pe piață a serviciilor de comunicații electronice care, din perspectiva consumatorului, sunt substituibile serviciilor

[4] 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, 4.5.2016, p. 1-88).

[5] 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).

tradiționale, dar nu trebuie să respecte același set de norme. Un alt aspect se referă la noile tehnici care permit urmărirea comportamentului online al utilizatorilor finali, care nu sunt reglementate de Directiva 2002/58/CE. Prin urmare, Directiva 2002/58/CE ar trebui abrogată și înlocuită cu prezentul regulament.

(7) Statele membre ar trebui să aibă posibilitatea, în limitele stabilite de prezentul regulament, să mențină sau să introducă dispoziții naționale pentru a specifica și a clarifica și mai mult normele prevăzute de prezentul regulament și punerea lor în aplicare pentru a asigura aplicarea și interpretarea eficace a acestora. Prin urmare, marja de apreciere pe care o dețin statele membre în această privință ar trebui să mențină un echilibru între protecția vieții private și a datelor cu caracter personal și libera circulație a datelor transmise în cadrul comunicațiilor electronice.

(8) Prezentul regulament ar trebui să se aplice furnizorilor de servicii de comunicații electronice, furnizorilor de liste de abonați accesibile publicului și furnizorilor de software care permite comunicațiile electronice, inclusiv obținerea și prezentarea informațiilor pe internet. De asemenea, prezentul regulament ar trebui să se aplice persoanelor fizice și juridice care utilizează serviciile de comunicații electronice pentru a trimite comunicații comerciale în scopuri de marketing direct sau pentru a colecta informații legate de echipamentele terminale ale utilizatorilor finali sau stocate în acestea.

(9) Prezentul regulament ar trebui să se aplice datelor transmise în cadrul comunicațiilor electronice care sunt prelucrate în legătură cu furnizarea și utilizarea serviciilor de comunicații electronice în Uniune, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii. În plus, pentru a nu priva utilizatorii finali din Uniune de o protecție eficace, prezentul regulament ar trebui să se aplice și în cazul datelor transmise în cadrul comunicațiilor electronice care sunt prelucrate în legătură cu furnizarea serviciilor de comunicații electronice din afara Uniunii către utilizatorii finali din Uniune.

(10) Echipamentele radio și software-ul aferent care sunt introduse pe piața internă a Uniunii trebuie să fie conforme cu Directiva 2014/53/UE a Parlamentului European și a Consiliului[6]. Prezentul regulament nu ar trebui să aducă atingere aplicabilității niciuneia dintre cerințele Directivei 2014/53/UE, nici competenței Comisiei de a adopta, în temeiul acestei directive, acte delegate care să prevadă faptul că anumite categorii sau clase de echipamente radio trebuie să includă garanții care să asigure protecția datelor cu caracter personal și a confidențialității utilizatorilor finali.

(11) Serviciile utilizate în scopuri de comunicare și mijloacele tehnice pentru furnizarea acestora au evoluat în mod considerabil. Utilizatorii finali înlocuiesc într-o măsură tot mai mare serviciile de telefonie vocală tradițională, de transmisie prin poștă electronică și de mesaje text (SMS-uri) cu servicii online echivalente din punct de vedere funcțional, cum ar fi serviciile de telefonie prin internet, de mesagerie și de e-mail pe internet. Pentru a asigura o protecție efectivă și egală a utilizatorilor finali atunci când utilizează servicii echivalente din punct de vedere funcțional, prezentul regulament utilizează definiția serviciilor de comunicații electronice prevăzută în [Directiva Parlamentului European și a Consiliului de instituire a Codului european al

[6] Directiva 2014/53/UE a Parlamentului European și a Consiliului din 16 aprilie 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a echipamentelor radio și de abrogare a Directivei 1999/5/CE (JO L 153, 22.5.2014, p. 62).

comunicațiilor electronice[7]]. Această definiție cuprinde nu numai serviciile de acces la internet și serviciile care constau, integral sau parțial, în transmiterea de semnale, ci și serviciile de comunicații interpersonale, care pot sau nu să fie bazate pe numere, ca de exemplu, servicii de telefonie prin internet, servicii de mesagerie și servicii de e-mail pe internet. Protejarea confidențialității comunicațiilor este esențială și în ceea ce privește serviciile de comunicații interpersonale care sunt auxiliare altui serviciu; prin urmare, acest tip de servicii care au, de asemenea, o funcționalitate de comunicare ar trebui să fie reglementate prin prezentul regulament.

(12) Dispozitivele și mașinile conectate comunică din ce în ce mai mult unele cu altele prin utilizarea rețelelor de comunicații electronice (internetul obiectelor). Transmiterea de comunicații de la mașină la mașină implică transmiterea de semnale într-o rețea și, prin urmare, constituie un serviciu de comunicații electronice. Pentru a se asigura protecția deplină a drepturilor la viață privată și la confidențialitatea comunicațiilor, precum și pentru a promova un internet al obiectelor sigur și de încredere în cadrul pieței unice digitale este necesar să se clarifice faptul că prezentul regulament ar trebui să se aplice în cazul transmiterii de comunicații de la mașină la mașină. Prin urmare, principiul confidențialității consacrat în prezentul regulament ar trebui să se aplice și în cazul transmiterii de comunicații de la mașină la mașină. De asemenea, ar putea fi adoptate garanții specifice, în temeiul legislației sectoriale, ca de exemplu Directiva 2014/53/UE.

(13) Dezvoltarea tehnologiilor fără fir rapide și eficiente a favorizat disponibilitatea tot mai mare pentru public a accesului la internet prin rețele fără fir accesibile tuturor în spațiile publice și semiprivate, cum ar fi „punctele de acces” (hotspots) situate în diferite locuri dintr-un oraș, magazine universale, centre comerciale și spitale. În măsura în care aceste rețele de comunicații sunt furnizate unui grup nedefinit de utilizatori finali, confidențialitatea comunicațiilor transmise prin acestea ar trebui să fie protejată. Faptul că serviciile de comunicații fără fir pot fi auxiliare altor servicii nu ar trebui să stea în calea asigurării protecției confidențialității datelor transmise în cadrul comunicațiilor și a aplicării prezentului regulament. Prin urmare, prezentul regulament ar trebui să se aplice în cazul datelor transmise în cadrul comunicațiilor electronice prin intermediul serviciilor de comunicații electronice și al rețelelor de comunicații publice. În schimb, prezentul regulament nu ar trebui să se aplice grupurilor închise de utilizatori finali, cum ar fi rețelele de întreprindere, la care accesul este limitat doar la membrii întreprinderii.

(14) Datele transmise în cadrul comunicațiilor electronice ar trebui să fie definite într-un mod suficient de larg și de neutru din punct de vedere tehnologic astfel încât să cuprindă orice informații referitoare la conținutul transmis sau schimbat (conținutul comunicațiilor electronice) și informațiile cu privire la un utilizator final de servicii de comunicații electronice prelucrate în vederea transmiterii, a distribuirii sau a schimbului de conținut al comunicațiilor electronice, inclusiv datele pentru urmărirea și identificarea sursei și a destinației unei comunicații, a localizării geografice, precum și a datei, orei, duratei și tipului de comunicare. Indiferent dacă astfel de semnale și datele conexe sunt transmise prin cablu, radio, mijloace optice sau electromagnetice, inclusiv rețelele prin satelit, rețelele terestre fixe (cu comutarea circuitelor și a pachetelor, inclusiv internetul) și mobile, precum și rețelele electrice, datele referitoare la astfel de semnale ar trebui să fie considerate drept metadate privind comunicațiile

[7] Propunerea Comisiei de directivă a Parlamentului European și a Consiliului de instituire a Codului european al comunicațiilor electronice (reformare) [(COM/2016/0590 final – 2016/0288 (COD)].

electronice și, prin urmare, să facă obiectul dispozițiilor prezentului regulament. 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.

(15) Datele transmise în cadrul comunicațiilor electronice ar trebui tratate ca fiind confidențiale. Aceasta înseamnă că orice amestec în transmiterea datelor în cadrul comunicațiilor electronice, fie direct, prin intervenție umană, fie prin intermediul prelucrării automate de către mașini, fără consimțământul tuturor părților care comunică, ar trebui interzis. Interdicția privind interceptarea datelor transmise în cadrul comunicațiilor ar trebui să se aplice în timpul transmiterii acestora, și anume până la primirea conținutului comunicațiilor electronice de către destinatar. Interceptarea datelor transmise în cadrul comunicațiilor electronice poate apărea, de exemplu, atunci când o entitate, alta decât părțile care comunică, ascultă apelurile, citește, scanează sau stochează conținutul comunicațiilor electronice sau a metadatelor asociate, în alte scopuri decât schimbul de comunicații. Interceptarea se produce și atunci când părți terțe monitorizează site-urile web vizitate, momentul vizitelor, interacțiunea cu alte persoane etc., fără consimțământul utilizatorului final în cauză. Pe măsură ce tehnologia evoluează, modalitățile tehnice de a efectua o interceptare s-au multiplicat de asemenea. Aceste modalități pot varia de la instalarea de echipamente care colectează date privind anumite domenii de la echipamentele terminale, cum ar fi așa-numiții interceptori ai identității internaționale de abonat mobil IMSI [*International Mobile Subscriber Identity (IMSI) catcher*], la programe și tehnici care permit, de exemplu, monitorizarea în mod discret a obiceiurilor de navigare pe internet în scopul creării de profiluri ale utilizatorilor finali. Alte exemple de interceptare includ captarea, din rețele și routere fără fir necriptate, a datelor referitoare la sarcina utilă sau a datelor privind conținutul inclusiv a obiceiurilor de navigare pe internet, fără consimțământul utilizatorilor finali.

(16) Interdicția stocării comunicațiilor nu vizează împiedicarea stocării automate, intermediare și tranzitorii a acestor informații, în măsura în care are loc cu unicul scop de a efectua transmisia în rețeaua de comunicații electronice. Acesta nu ar trebui să interzică nici prelucrarea datelor transmise în cadrul comunicațiilor electronice cu scopul de a asigura securitatea și continuitatea serviciilor de comunicații electronice, inclusiv verificările în vederea depistării amenințărilor la adresa securității, cum ar fi prezența unui software rău-intenționat, nici prelucrarea de metadate pentru a răspunde cerințelor în materie de calitate a serviciilor, cum ar fi timpul de așteptare, variația întârzierii de transfer a pachetelor de date etc.

(17) Prelucrarea datelor transmise în cadrul comunicațiilor electronice poate fi utilă pentru întreprinderi, consumatori și întreaga societate. În raport cu Directiva 2002/58/CE, prezentul regulament le oferă furnizorilor de servicii de comunicații electronice mai multe posibilități de prelucrare a metadatelor privind comunicațiile electronice, pe baza consimțământului utilizatorilor finali. Cu toate acestea, utilizatorii finali acordă o mare importanță confidențialității comunicațiilor în care sunt implicați, inclusiv a activităților lor online, și doresc să controleze utilizarea datelor transmise în cadrul comunicațiilor electronice în alte scopuri decât transmisia comunicației. Prin urmare, prezentul regulament ar trebui să le impună furnizorilor de servicii de comunicații electronice să obțină consimțământul utilizatorilor finali pentru prelucrarea metadatelor privind comunicațiile electronice, care ar trebui să includă datele referitoare la localizarea dispozitivului generate pentru acordarea și menținerea accesului, precum și pentru conectarea la serviciu. Datele privind localizarea care sunt

generate în alt context decât furnizarea serviciilor de comunicații electronice nu ar trebui considerate ca fiind metadate. Exemple de utilizări comerciale ale metadatelor privind comunicațiile electronice de către furnizorii de servicii de comunicații electronice pot include furnizarea de hărți termice (*heatmaps*), acestea constituind o reprezentare grafică a datelor care utilizează culori pentru a indica prezența persoanelor fizice. Pentru afișarea mișcărilor de trafic în anumite direcții pentru o anumită perioadă de timp, este necesar un element de identificare pentru a corela pozițiile persoanelor fizice la anumite intervale de timp. În cazul în care ar fi utilizate date anonime, nu s-ar dispune de acest element de identificare, iar astfel de mișcări nu ar putea fi vizualizate. Această utilizare a metadatelor privind comunicațiile electronice le-ar putea permite, de exemplu, autorităților publice și operatorilor de transport public să stabilească locurile în care să fie dezvoltate noi infrastructuri, pe baza utilizării structurii existente și a presiunii asupra acesteia. În cazul în care un tip de prelucrare a metadatelor privind comunicațiile electronice, în special care implică utilizarea de noi tehnologii, este susceptibil, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, să genereze un risc ridicat la adresa drepturilor și a libertăților persoanelor fizice, ar trebui să se efectueze o evaluare a impactului asupra protecției datelor și, după caz, o consultare a autorității de supraveghere înainte de prelucrarea metadatelor, în conformitate cu articolele 35 și 36 din Regulamentul (UE) 2016/679.

(18) Utilizatorii finali pot fi de acord cu prelucrarea metadatelor care îi privesc pentru a beneficia de anumite servicii, cum ar fi serviciile de protecție împotriva activităților frauduloase (prin analizarea în timp real a datelor privind utilizarea, a locației și a contului de client). În economia digitală, serviciile sunt adesea furnizate în schimbul unei contraprestații nepecuniare, de exemplu expunerea utilizatorilor finali la anunțuri publicitare. În sensul prezentului regulament, consimțământul unui utilizator final, indiferent dacă acesta este o persoană fizică sau juridică, ar trebui să aibă aceeași însemnătate și să fie supus acelorași condiții ca și consimțământul persoanei vizate în temeiul Regulamentului (UE) 2016/679. Accesul la internet în bandă largă de bază și serviciile de comunicații vocale trebuie considerate drept servicii esențiale pentru ca persoanele fizice să fie în măsură să comunice și să beneficieze de avantajele oferite de economia digitală. Consimțământul pentru prelucrarea datelor de pe internet sau utilizarea serviciilor de comunicații vocale nu ar fi valabil dacă persoana vizată nu ar dispune cu adevărat de libertatea de alegere sau nu ar fi în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată.

(19) Conținutul comunicațiilor electronice vizează în mod intrinsec dreptul fundamental la respectarea vieții private și de familie, a domiciliului și a comunicațiilor protejat în temeiul articolului 7 din Cartă. Orice amestec în legătură cu conținutul comunicațiilor electronice ar trebui să fie permis numai în condiții definite foarte clar, în scopuri specifice și sub rezerva unor garanții adecvate împotriva abuzurilor. Prezentul regulament prevede posibilitatea ca furnizorii de servicii de comunicații electronice să prelucreze datele transmise în cadrul comunicațiilor electronice în tranzit, cu consimțământul în cunoștință de cauză al tuturor utilizatorilor finali vizați. De exemplu, furnizorii pot oferi servicii care presupun scanarea e-mailurilor pentru a elimina anumite materiale predefinite. Dată fiind sensibilitatea conținutului comunicațiilor, prezentul regulament stabilește prezumția potrivit căreia prelucrarea unor astfel de date privind conținutul va prezenta riscuri ridicate la adresa drepturilor și libertăților persoanelor fizice. Atunci când prelucrează astfel de tipuri de date, furnizorul de servicii de comunicații electronice ar trebui să se consulte întotdeauna cu autoritatea de supraveghere în prealabil. O astfel de consultare ar trebui să fie în

conformitate cu articolul 36 alineatele (2) și (3) din Regulamentul (UE) 2016/679. Prezumția nu se aplică prelucrării de date privind conținutul în scopul furnizării unui serviciu solicitat de utilizatorul final în cazul în care acesta a fost de acord cu o astfel de prelucrare, care este efectuată în scopul și pe durata strict necesare acestui serviciu și în mod proporțional cu acesta. După ce conținutul comunicațiilor electronice a fost trimis de utilizatorul final și primit de utilizatorul final vizat sau de utilizatorii finali vizați, acesta ar putea fi înregistrat sau stocat de către utilizatorul final, utilizatorii finali sau o parte terță însărcinată de aceștia să înregistreze sau să stocheze astfel de date. Orice prelucrare a unor astfel de date trebuie să fie în conformitate cu Regulamentul (UE) 2016/679.

(20) Echipamentele terminale ale utilizatorilor finali ai rețelelor de comunicații electronice și orice informații referitoare la utilizarea unor astfel de echipamente terminale, în special în cazul în care informațiile sunt stocate în astfel de echipamente sau emise de acestea, solicitate acestora sau prelucrate în scopul de a le permite conectarea la un alt dispozitiv și/sau alte echipamente de rețea, fac parte din sfera privată a utilizatorilor finali și necesită protecție în temeiul Cartei drepturilor fundamentale a Uniunii Europene și a Convenției europene pentru apărarea drepturilor omului și a libertăților fundamentale. Având în vedere faptul că astfel de echipamente conțin sau prelucrează informații care ar putea dezvălui detalii privind complexitatea emoțională, politică sau socială a unei persoane fizice, inclusiv conținutul comunicațiilor, imagini, localizarea persoanelor prin accesarea funcțiilor GPS ale dispozitivelor, listele datelor de contact și alte informații deja stocate în dispozitiv, informațiile legate de astfel de echipamente necesită o protecție sporită a vieții private. În plus, așa-numitele programe spyware, semnalizatoare web (*web bugs*), identificatori ascunși (*hidden identifiers*), cookie-uri permanente și alte instrumente similare de urmărire nedorită pot intra în echipamentele terminale ale utilizatorului final fără cunoștința acestuia pentru a obține accesul la informații, a stoca informații ascunse și a monitoriza activitățile. Informațiile referitoare la dispozitivul utilizatorului final pot fi, de asemenea, colectate de la distanță în scopuri de identificare și urmărire, utilizând tehnici cum ar fi așa-numita „prelevare a amprentelor digitale” (*device fingerprinting*), adesea fără cunoștința utilizatorului final, ceea ce poate periclita în mod flagrant viața privată a acestor utilizatori finali. Tehnicile prin care se monitorizează în mod discret acțiunile utilizatorilor finali, de exemplu prin urmărirea activităților online ale acestora sau a localizării echipamentelor lor terminale sau care subminează funcționarea echipamentelor terminale ale utilizatorilor finali reprezintă o amenințare majoră la adresa vieții lor private. Prin urmare, orice astfel de amestec în legătură cu echipamentele terminale ale utilizatorului final ar trebui să fie permis numai cu consimțământul acestuia și în scopuri specifice și transparente.

(21) Excepțiile de la obligația de a obține consimțământul de a recurge la capacitățile de prelucrare și stocare a echipamentelor terminale sau de a accesa informațiile stocate în echipamentele terminale ar trebui să se limiteze la situațiile care nu implică periclitarea vieții private sau implică doar periclitarea foarte limitată a acesteia. De exemplu, nu ar trebui solicitat consimțământul pentru autorizarea stocării sau a accesului de natură tehnică atunci când sunt strict necesare și proporționale cu scopul legitim de a permite folosirea unui serviciu specific solicitat explicit de către utilizatorul final. Aceasta poate include stocarea de cookie-uri pe durata unei singure sesiuni stabilite pe un site web pentru a păstra datele introduse de utilizatorul final atunci când completează formulare online pe mai multe pagini. Cookie-urile pot fi, de asemenea, un instrument legitim și util, de exemplu pentru măsurarea traficului pe un site web. Faptul că un furnizor de servicii ale societății informaționale verifică o

configurație în scopul furnizării unui serviciu în conformitate cu setările utilizatorului final și simpla consemnare a faptului că dispozitivul utilizatorului final nu este în măsură să primească un conținut solicitat de utilizator nu ar trebui să constituie un acces la un astfel de dispozitiv sau o utilizare a funcțiilor de prelucrare a dispozitivului.

(22) Metodele folosite pentru a furniza informații și a obține consimțământul utilizatorului final ar trebui să fie cât mai ușor de utilizat cu putință. Având în vedere utilizarea omniprezentă a cookie-urilor permanente și a altor tehnici de urmărire, utilizatorilor finali li se solicită într-o măsură tot mai mare să își dea consimțământul privind stocarea acestor cookie-uri permanente în echipamentele lor terminale. Prin urmare, utilizatorii finali sunt supraîncărcați cu solicitări privind acordarea consimțământului. Utilizarea de mijloace tehnice pentru acordarea consimțământului, de exemplu, prin setări transparente și ușor de utilizat, poate soluționa această problemă. Prin urmare, prezentul regulament ar trebui să prevadă posibilitatea de exprimare a consimțământului prin utilizarea setărilor corespunzătoare ale unui browser sau ale altei aplicații. Alegerile făcute de utilizatorii finali atunci când își stabilesc setările de confidențialitate generale pentru un browser sau o altă aplicație ar trebui să aibă un caracter obligatoriu pentru orice parte terță și să fie opozabile acestora. Browserele sunt un tip de aplicație software care permite obținerea și prezentarea informațiilor pe internet. De asemenea, alte tipuri de aplicații, cum ar fi cele care permit efectuarea de apeluri și transmiterea de mesaje sau care oferă îndrumare rutieră, au aceleași capacități. Browserele asigură o mare parte din interacțiunile care au loc între utilizatorul final și site-ul web. Din acest punct de vedere, ele se află într-o poziție privilegiată pentru a juca un rol activ constând în sprijinirea utilizatorului final în ceea ce privește controlul fluxului de informații către și de la echipamentele terminale. Mai precis, browserele pot fi utilizate ca entități de control, ajutând astfel utilizatorii finali să împiedice accesul la informații provenind de la echipamentele lor terminale (de exemplu telefon inteligent, tabletă sau computer) și stocarea acestora.

(23) Principiile protecției datelor începând cu momentul conceperii și ale protecției implicite a datelor au fost codificate prin articolul 25 din Regulamentul (UE) 2016/679. În prezent, setările implicite pentru cookie-uri în majoritatea browserelor cunoscute prevăd „acceptarea tuturor cookie-urilor”. Prin urmare, furnizorii de software care să permită obținerea și prezentarea informațiilor pe internet ar trebui să aibă obligația de a configura software-ul astfel încât acesta să ofere opțiunea de a împiedica părțile terțe să stocheze informații în echipamentele terminale; această opțiune corespunde adesea formulei „respinge cookie-urile de terță parte”. Utilizatorilor finali ar trebui să li se ofere un set de opțiuni privind setările de confidențialitate, de la cele mai restrictive (de exemplu, „nu acceptați niciodată cookie-uri”), până la cele mai permisive (de exemplu, „acceptați întotdeauna cookie-uri”) și cele intermediare (de exemplu, „respingeți cookie-urile de terță parte” sau „acceptați numai cookie-urile originale”). Aceste setări de confidențialitate ar trebui prezentate într-un mod vizibil și inteligibil.

(24) Pentru ca browserele să poată obține consimțământul utilizatorilor finali, astfel cum este definit în Regulamentul (UE) 2016/679, de exemplu, privind stocarea cookie-urilor permanente de terță parte, acestea ar trebui, printre altele, să îi solicite utilizatorului final al echipamentelor terminale să își manifeste, printr-o acțiune afirmativă fără echivoc, acordul liber exprimat, specific, în cunoștință de cauză și univoc cu privire la stocarea și accesarea unor astfel de cookie-uri în și din echipamentele terminale. O astfel de acțiune poate fi considerată afirmativă, de

exemplu, dacă utilizatorilor finali li se solicită să selecteze în mod activ opțiunea „acceptați cookie-urile de terță parte” pentru a-și confirma acordul și li se oferă informațiile necesare pentru a face această alegere. În acest scop, este necesar ca furnizorilor de software care permit accesul la internet să li se solicite ca, în momentul instalării, să informeze utilizatorii finali în legătură cu posibilitatea de a-și alege setările de confidențialitate dintre diversele opțiuni propuse și să le solicite acestora să facă o alegere. Informațiile furnizate nu ar trebui să descurajeze utilizatorii finali să opteze pentru setările de confidențialitate cu un nivel mai ridicat și ar trebui să includă informații relevante cu privire la riscurile pe care le presupune consimțământul dat pentru stocarea în calculator a cookie-urilor de terță parte, inclusiv păstrarea pe termen lung a istoricelor de navigare ale persoanelor fizice și utilizarea acestora pentru a trimite mesaje publicitare specifice. Browserele sunt încurajate să le ofere utilizatorilor finali modalități simple de a-și modifica setările de confidențialitate în orice moment în timpul utilizării și care să le permită să prevadă excepții pentru anumite site-uri web sau să le includă pe o listă de site-uri aprobate sau să precizeze pentru ce site-uri acceptă întotdeauna sau nu acceptă niciodată cookie-urile (de terță parte).

(25) Accesul la rețelele de comunicații electronice necesită emiterea în mod regulat a anumitor pachete de date pentru a descoperi sau a menține o conexiune cu rețeaua respectivă sau cu alte dispozitive din rețea. În plus, dispozitivele trebuie să aibă o adresă unică, alocată acestora pentru a fi identificabile pe rețeaua respectivă. În mod similar, standardele privind dispozitivele fără fir și telefoanele celulare implică emiterea de semnale active care conțin identificatori unici, cum ar fi o adresă MAC, IMEI (identitatea internațională a echipamentului mobil), IMSI (identitatea internațională de abonat mobil) etc. O stație de bază fără fir izolată (de exemplu, un emițător și receptor), cum ar fi un punct de acces fără fir, are o anumită arie de acoperire în care astfel de informații pot fi colectate. Au apărut furnizori de servicii care oferă servicii de urmărire bazate pe scanarea informațiilor legate de echipamente cu diverse funcționalități, inclusiv contabilizarea persoanelor, furnizarea de date privind numărul de persoane care așteaptă la rând, stabilirea numărului de persoane aflate într-un anumit perimetru, etc. Aceste informații pot fi utilizate pentru scopuri mai intruzive, cum ar fi trimiterea de mesaje comerciale conținând oferte personalizate către utilizatorii finali, de exemplu atunci când aceștia intră în magazine. În timp ce unele dintre aceste funcționalități nu implică riscuri ridicate la adresa vieții private, altele prezintă astfel de riscuri, de exemplu cele care presupun urmărirea persoanelor fizice de-a lungul timpului, inclusiv vizitarea repetată a unor locuri specifice. Furnizorii care recurg la astfel de practici ar trebui să afișeze anunțuri foarte vizibile situate la marginea ariei de acoperire care să informeze utilizatorii finali înainte ca aceștia să intre în zona definită cu privire la prezența tehnologiei într-un anumit perimetru, la scopul urmăririi, la persoana responsabilă pentru aceasta și la existența eventualelor măsuri pe care utilizatorul final al echipamentelor terminale le poate lua pentru a minimiza sau a pune capăt colectării informațiilor. Ar trebui furnizate informații suplimentare în cazul în care datele cu caracter personal sunt colectate în temeiul articolului 13 din Regulamentul (UE) 2016/679.

(26) Atunci când prelucrarea datelor transmise în cadrul comunicațiilor electronice de către furnizorii de servicii de comunicații electronice intră în domeniul său de aplicare, prezentul regulament ar trebui să prevadă posibilitatea ca Uniunea sau statele membre să restricționeze prin lege, în anumite condiții, anumite obligații și drepturi, dacă o astfel de restricție constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja anumite interese publice, inclusiv securitatea națională, apărarea, siguranța publică, prevenirea, investigarea, depistarea sau urmărirea penală a

infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa securității publice și a altor 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, precum și prevenirea acestor amenințări, sau o funcție de monitorizare, de inspecție sau de reglementare legată de exercitarea autorității publice pentru astfel de interese. În consecință, prezentul regulament nu ar trebui să afecteze posibilitatea ca statele membre să efectueze interceptări legale ale comunicațiilor electronice sau să ia alte măsuri, dacă acest lucru este necesar și proporțional în raport cu apărarea intereselor publice menționate anterior, în conformitate cu Carta drepturilor fundamentale a Uniunii Europene și cu Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, așa cum sunt interpretate de Curtea de Justiție a Uniunii Europene și de Curtea Europeană a Drepturilor Omului. Furnizorii de servicii de comunicații electronice ar trebui să prevadă proceduri adecvate pentru a facilita cererile legitime ale autorităților competente, luând în considerare, de asemenea, în cazul în care este relevant, rolul reprezentantului desemnat în temeiul articolului 3 alineatul (3).

(27) În ceea ce privește identificarea liniei apelante, este necesară protejarea dreptului părții care efectuează apelul de a refuza prezentarea identificării liniei de pe care efectuează apelul și dreptul părții apelate de a respinge apelurile primite de pe linii neidentificate. Anumiți utilizatori finali, mai ales liniile pentru apeluri de urgență și organizațiile similare, au interesul de a păstra anonimatul apelanților lor. În ceea ce privește identificarea liniei de conectare, este necesară protejarea dreptului și a interesului legitim al părții apelate de a refuza prezentarea identificării liniei la care este efectiv conectată partea apelantă.

(28) Este justificat să nu se țină seama de eliminarea prezentării identificării liniei apelante în anumite cazuri. Dreptul la confidențialitate al utilizatorilor finali în ceea ce privește identificarea liniei apelante ar trebui restricționat în cazul în care acest lucru este necesar pentru detectarea apelurilor deranjante, iar în ceea ce privește datele de identificare și de localizare a liniei apelante, dacă este necesar, pentru a permite serviciilor de urgență, precum sistemul eCall, să își îndeplinească sarcinile într-un mod cât mai eficace cu putință.

(29) Există mijloace tehnologice care le permit furnizorilor de servicii de comunicații electronice să limiteze primirea apelurilor nedorite de către utilizatorii finali în diferite moduri, de exemplu prin blocarea apelurilor silențioase (*silent calls*) și a altor apeluri frauduloase și deranjante. Furnizorii de servicii de comunicații interpersonale bazate pe numere și accesibile publicului ar trebui să implementeze această tehnologie și să protejeze utilizatorii finali în mod gratuit împotriva apeluri deranjante. Furnizorii ar trebui să se asigure că utilizatorii finali sunt conștienți de existența unor astfel de funcționalități, de exemplu, prin promovarea acestora pe pagina lor web.

(30) Listele de utilizatori finali ai serviciilor de comunicații electronice accesibile publicului sunt distribuite pe scară largă. Listele de abonați accesibile publicului reprezintă orice listă sau serviciu care conține informații privind utilizatorii finali, cum ar fi numere de telefon (inclusiv numerele de telefon mobil) și datele de contact prin e-mail, acestea incluzând, de asemenea, servicii de informații. În virtutea dreptului la viață privată și la protecția datelor cu caracter personal ale unei persoane fizice, este necesar ca utilizatorilor finali care sunt persoane fizice să li se ceară consimțământul înainte ca datele lor personale să fie incluse într-o listă de abonați accesibilă publicului. Potrivit interesului legitim al entităților juridice, utilizatorii finali care sunt

entități juridice trebuie să aibă dreptul de a se opune includerii într-o listă de abonați accesibilă publicului a datelor care îi privesc.

(31) În cazul în care utilizatorii finali care sunt persoane fizice își dau consimțământul ca datele care îi privesc să fie incluse într-o asemenea listă, aceștia ar trebui să poată stabili, pe baza consimțământului, ce categorii de date cu caracter personal sunt incluse în lista respectivă (de exemplu numele, adresa de e-mail, adresa domiciliului, numele de utilizator, numărul de telefon). În plus, furnizorii de liste de abonați accesibile publicului ar trebui să îi informeze pe utilizatorii finali cu privire la scopul listei și la funcția de căutare în listă înainte de a-i include pe listă. Utilizatorii finali ar trebui să își poată da consimțământul referitor la categoriile de date cu caracter personal pe baza cărora pot fi căutate datele lor de contact. Categoriile de date cu caracter personal incluse în listă și categoriile de date cu caracter personal pe baza cărora pot fi căutate datele de contact ale utilizatorului final nu ar trebui să coincidă în mod necesar.

(32) În prezentul regulament, marketingul direct se referă la orice formă de publicitate prin care o persoană fizică sau juridică trimite comunicații în scopuri de marketing direct către unul sau mai mulți utilizatori finali identificați sau identificabili care utilizează servicii de comunicații electronice. În plus față de oferta de produse și servicii în scopuri comerciale, această noțiune ar trebui să cuprindă și mesajele trimise de partidele politice care contactează persoane fizice prin intermediul serviciilor de comunicații electronice cu scopul de a se promova. Același lucru ar trebui să se aplice în cazul mesajelor trimise de alte organizații nonprofit în vederea îndeplinirii obiectivelor organizației.

(33) Ar trebui prevăzute garanții pentru protecția utilizatorilor finali împotriva comunicațiilor nesolicitate în scopuri de marketing direct care reprezintă intruziuni în viața privată a acestora. Nivelul de intruziune în viața privată și de deranj este considerat ca fiind relativ similar indiferent de tipul de tehnologii și canale utilizate pentru a efectua aceste comunicații electronice, de exemplu prin folosirea sistemelor de apelare și comunicare automate, a aplicațiilor de mesagerie instantanee, a e-mailurilor, a SMS-urilor, a MMS-urilor, a tehnologiei Bluetooth etc. Prin urmare, este justificat să se solicite obținerea consimțământului utilizatorului final înainte de trimiterea comunicațiilor electronice comerciale în scopuri de marketing direct către utilizatorii finali pentru a proteja în mod eficace persoanele fizice împotriva intruziunii în viața lor privată, precum și pentru a proteja interesele legitime ale persoanelor juridice. Securitatea juridică și necesitatea de a asigura perenitatea normelor de protecție împotriva comunicațiilor electronice nesolicitate justifică nevoia de a defini un set unic de norme care nu variază în funcție de tehnologiile folosite pentru a transmite aceste comunicări nesolicitate, garantând, în același timp, un nivel echivalent de protecție pentru toți cetățenii pe întreg teritoriul Uniunii. Cu toate acestea, este rezonabil să se permită utilizarea datelor de contact prin e-mail în contextul unei relații existente cu un client pentru oferirea de produse sau servicii similare. O astfel de posibilitate ar trebui să se limiteze la întreprinderea care a obținut datele de contact electronic în conformitate cu Regulamentul (UE) 2016/679.

(34) Atunci când utilizatorii finali și-au dat consimțământul de a primi comunicări nesolicitate în scopuri de marketing direct, aceștia ar trebui să fie în continuare în măsură să își retragă cu ușurință consimțământul în orice moment. Pentru a facilita asigurarea efectivă a respectării normelor Uniunii cu privire la mesajele nesolicitate în scopuri de marketing direct, este necesar să fie interzise 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. Prin urmare, comunicările comerciale nesolicitate ar trebui să fie clar identificabile ca atare, să indice identitatea persoanei fizice sau juridice care transmite comunicarea sau în numele căreia are loc transmisia și să furnizeze informațiile necesare pentru ca destinatarii să își exercite dreptul de a se opune primirii în continuare a mesajelor în scopuri de marketing scrise și/sau orale.

(35) Pentru a facilita retragerea cu ușurință a consimțământului, persoanele juridice sau fizice care efectuează comunicații în scopuri de marketing direct prin e-mail ar trebui să prezinte un link sau o adresa de poștă electronică valabilă care să poată fi utilizate cu ușurință de către utilizatorii finali pentru a-și retrage consimțământul. Persoanele juridice sau fizice care efectuează comunicații în scopuri de marketing direct prin intermediul apelurilor vocale și al sistemelor de apelare și comunicare automate ar trebui să afișeze numărul de telefon la care societatea poate fi contactată sau să prezinte un cod specific menit să identifice faptul că apelul este efectuat în scopuri de marketing.

(36) Apelurile vocale în scopuri de marketing direct care nu implică folosirea sistemelor de apelare și comunicare automate sunt mai costisitoare pentru expeditor și nu impun costuri financiare asupra utilizatorilor finali. Prin urmare, statele membre ar trebui să fie în măsură să instituie sau să mențină sisteme naționale care să permită efectuarea acestui tip de apeluri numai către utilizatorii finali care nu au ridicat obiecții.

(37) Furnizorii de servicii care oferă servicii de comunicații electronice ar trebui să îi informeze pe utilizatorii finali cu privire la măsurile pe care le pot lua pentru protejarea securității comunicațiilor lor, de exemplu prin utilizarea unor tipuri specifice de software sau a unor tehnologii de criptare. Cerința de a informa utilizatorii finali despre un anumit risc legat de securitatea comunicațiilor nu îl scutește pe furnizorul serviciilor de obligația de a lua, pe cheltuială proprie, măsurile necesare imediate pentru a combate orice risc nou și neprevăzut și de a restabili nivelul normal de securitate al serviciilor. Informarea abonaților cu privire la riscurile legate de securitatea comunicațiilor ar trebui să fie gratuită. Securitatea este evaluată în conformitate cu articolul 32 din Regulamentul (UE) 2016/679.

(38) Pentru a se asigura coerența deplină cu Regulamentul (UE) 2016/679, asigurarea respectării dispozițiilor prezentului regulament ar trebui încredințată acelorași autorități responsabile pentru asigurarea respectării dispozițiilor Regulamentului (UE) 2016/679, prezentul regulament fiind bazat pe mecanismul de asigurare a coerenței prevăzut în Regulamentul (UE) 2016/679. Statele membre ar trebui să poată dispune de mai multe autorități de supraveghere pentru a reflecta structura lor constituțională, organizatorică și administrativă. Autoritățile de supraveghere ar trebui să fie, de asemenea, responsabile pentru monitorizarea aplicării prezentului regulament în ceea ce privește datele transmise în cadrul comunicațiilor electronice aferente persoanelor juridice. Aceste sarcini suplimentare nu ar trebui să pună în pericol capacitatea autorității de supraveghere de a-și îndeplini sarcinile în ceea ce privește protecția datelor cu caracter personal în temeiul Regulamentului (UE) 2016/679 și al prezentului regulament. 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 prezentului regulament.

(39) Fiecare autoritate de supraveghere ar trebui să aibă competența necesară pe teritoriul propriului stat membru în vederea exercitării atribuțiilor și a îndeplinirii sarcinilor prevăzute în prezentul regulament. Pentru a se asigura consecvența monitorizării și a

asigurării respectării prezentului regulament în întreaga Uniune, autoritățile de supraveghere ar trebui să aibă aceleași atribuții și competențe efective în fiecare stat membru, fără a aduce atingere competențelor autorităților de urmărire penală în temeiul dreptului intern al unui stat membru, pentru a aduce în atenția autorităților judiciare cazurile de încălcare a prezentului regulament și a acționa în justiție. Statele membre și autoritățile lor de supraveghere sunt încurajate să ia în considerare necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii în aplicarea prezentului regulament.

(40) Pentru a consolida asigurarea respectării normelor prevăzute în prezentul regulament, fiecare autoritate de supraveghere ar trebui să aibă competența de a impune sancțiuni, inclusiv amenzi administrative, pentru orice încălcare a prezentului regulament, pe lângă sau în locul oricăror alte măsuri adecvate în temeiul prezentului regulament. Prezentul regulament ar trebui să indice încălcările, precum și limita maximă și criteriile pentru stabilirea amenzilor administrative aferente, care ar trebui să fie stabilite de autoritatea de supraveghere competentă în fiecare caz în parte, ținând seama de toate circumstanțele relevante ale situației specifice, luându-se în considerare în mod corespunzător, în special, natura, gravitatea și durata încălcării, precum și consecințele acesteia și măsurile luate pentru a se asigura respectarea obligațiilor în temeiul prezentului regulament și pentru a se preveni sau atenua consecințele încălcării. În scopul stabilirii cuantumului unei amenzi, în temeiul prezentului regulament, prin întreprindere ar trebui să se înțeleagă o întreprindere în conformitate cu articolele 101 și 102 din tratat.

(41) În vederea îndeplinirii obiectivelor prezentului regulament, și anume protejarea drepturilor și libertăților fundamentale ale persoanelor fizice și, în special, a dreptului acestora la protecția datelor cu caracter personal, și pentru a se garanta libera circulație a datelor cu caracter personal pe teritoriul Uniunii, competența de a adopta acte în conformitate cu articolul 290 din tratat ar trebui să fie delegată Comisiei pentru completarea prezentului regulament. În special, ar trebui adoptate acte delegate în ceea ce privește informațiile care trebuie prezentate, inclusiv prin intermediul unor pictograme standardizate pentru a oferi o imagine de ansamblu ușor vizibilă și inteligibilă privind colectarea informațiilor emise de echipamentele terminale, scopul acesteia, persoana responsabilă în acest sens și orice măsură pe care utilizatorul final al echipamentelor terminale o poate lua pentru a reduce la minimum colectarea informațiilor. Actele delegate sunt, de asemenea, necesare în vederea definirii unui cod pentru identificarea apelurilor vocale în scopuri de marketing direct, inclusiv a celor efectuate prin sistemele de apelare și comunicare automate. Este deosebit de importantă organizarea unor consultări adecvate de către Comisie și desfășurarea acestora în conformitate cu principiile prevăzute în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016.[8] În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar aceștia au acces în mod sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate. Mai mult, în vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament, Comisia ar trebui învestită cu competențe de executare în situațiile stabilite de prezentul regulament. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011.

[8] Acordul interinstituțional între Parlamentul European, Consiliul Uniunii Europene și Comisia Europeană privind o mai bună legiferare din 13 aprilie 2016 (JO L 123, 12.5.2016, p. 1-14).

(42) Deoarece obiectivul prezentului regulament, și anume asigurarea unui nivel echivalent de protecție a persoanelor fizice și juridice, precum și libera circulație a datelor transmise în cadrul comunicațiilor electronice în întreaga Uniune, nu poate fi realizat în mod satisfăcător de către statele membre, dar, având în vedere amploarea sau efectele acțiunii, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este definit la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este enunțat la articolul menționat, prezentul regulament nu depășește ceea ce este necesar pentru atingerea respectivului obiectiv.

(43) Directiva 2002/58/CE ar trebui abrogată,

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I
DISPOZIȚII GENERALE

Articolul 1
Obiectul

1. Prezentul regulament stabilește normele referitoare la protecția drepturilor și libertăților fundamentale ale persoanelor fizice și juridice în ceea ce privește furnizarea și utilizarea serviciilor de comunicații electronice și, în special, dreptul la respectarea vieții private și a comunicațiilor și la protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal.

2. Prezentul regulament asigură libera circulație a datelor transmise în cadrul comunicațiilor electronice și a serviciilor de comunicații electronice în cadrul Uniunii, care nu poate fi restricționată sau interzisă din motive legate de respectarea vieții private și a comunicațiilor persoanelor fizice și juridice și de protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal.

3. Dispozițiile prezentului regulament aduc precizări și completări Regulamentului (UE) 2016/679 prin stabilirea unor norme specifice în scopurile menționate la alineatele (1) și (2).

Articolul 2
Domeniul de aplicare material

1. Prezentul regulament se aplică în cazul prelucrării datelor transmise în cadrul comunicațiilor electronice efectuate în legătură cu prestarea și utilizarea serviciilor de comunicații electronice și în cazul informațiilor legate de echipamentele terminale ale utilizatorilor finali.

2. Prezentul regulament nu se aplică în cazul:

(a) activităților care nu intră în domeniul de aplicare al dreptului Uniunii;

(b) activităților statelor membre care intră în domeniul de aplicare al titlului V capitolul 2 din Tratatul privind Uniunea Europeană;

(c) serviciilor de comunicații electronice care nu sunt accesibile publicului;

(d) activităților desfășurate de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale, inclusiv în scopul protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii unor asemenea amenințări.

3. Prelucrarea datelor transmise în cadrul comunicațiilor electronice de către instituțiile, organele, oficiile și agențiile Uniunii este reglementată de Regulamentul (UE) nr. 00/0000 [noul regulament care înlocuiește Regulamentul 45/2001].

4. Prezentul regulament nu aduce atingere aplicării Directivei 2000/31/CE[9], în special a normelor privind răspunderea furnizorilor intermediari de servicii prevăzute la articolele 12-15 din directiva menționată.

[9] Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (directiva privind comerțul electronic) (JO L 178, 17.7.2000, p. 1-16).

5. Prezentul regulament nu aduce atingere dispozițiilor Directivei 2014/53/UE.

Articolul 3
Domeniul de aplicare teritorial și reprezentantul

1. Prezentul regulament se aplică în cazul:

(a) furnizării de servicii de comunicații electronice către utilizatorii finali din Uniune, indiferent dacă este necesară efectuarea unei plăți de către utilizatorul final;

(b) utilizării unor astfel de servicii;

(c) protecției informațiilor aferente echipamentelor terminale ale utilizatorilor finali care se află în Uniune.

2. În cazul în care furnizorul unui serviciu de comunicații electronice nu este stabilit în Uniune, acesta își desemnează în scris un reprezentant în Uniune.

3. Reprezentantul este stabilit în unul din statele membre în care se află utilizatorii finali ai acestor servicii de comunicații electronice.

4. Reprezentantul are competența de a răspunde la întrebări și de a oferi informații, în completarea furnizorului pe care îl reprezintă sau în locul acestuia, în special, autorităților de supraveghere și utilizatorilor finali, cu privire la toate chestiunile legate de prelucrarea datelor transmise în cadrul comunicațiilor electronice pentru a asigura conformitatea cu prezentul regulament.

5. Desemnarea unui reprezentant în temeiul alineatului (2) nu aduce atingere acțiunilor în justiție care ar putea fi inițiate împotriva unei persoane fizice sau juridice care prelucrează date transmise în cadrul comunicațiilor electronice în legătură cu furnizarea de servicii de comunicații electronice din afara Uniunii către utilizatori finali din Uniune.

Articolul 4
Definiții

1. În sensul prezentului regulament, se aplică următoarele definiții:

(a) definițiile prevăzute în Regulamentul (UE) 2016/679;

(b) definițiile privind „rețeaua de comunicații electronice”, „serviciul de comunicații electronice”, „serviciul de comunicații interpersonale”, „serviciul de comunicații interpersonale bazat pe numere”, „serviciul de comunicații interpersonale care nu se bazează pe numere”, „utilizatorul final” și „apelul” de la articolul 2 alineatele (1), (4), (5), (6), (7), (14) și, respectiv, (21) din [Directiva de instituire a Codului european al comunicațiilor electronice];

(c) definiția privind „echipamentele terminale” de la articolul 1 alineatul (1) din Directiva 2008/63/CE a Comisiei[10].

2. În sensul alineatului (1) litera (b), definiția „serviciului 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.

[10] Directiva 2008/63/CE a Comisiei din 20 iunie 2008 privind concurența pe piețele echipamentelor terminale pentru telecomunicații (JO L 162, 21.6.2008, p. 20-26).

3. În plus, în sensul prezentului regulament, se aplică următoarele definiții:

(a) „date transmise în cadrul comunicațiilor electronice” înseamnă conținutul comunicațiilor electronice și metadatele privind comunicațiile electronice;

(b) „conținutul comunicațiilor electronice” înseamnă conținutul schimbat prin intermediul serviciilor de comunicații electronice, cum ar fi mesajele scrise, mesajele vocale, înregistrările video, imaginile și sunetele;

(c) „metadate privind comunicațiile electronice” înseamnă datele prelucrate într-o rețea de comunicații electronice în vederea transmiterii, a distribuirii sau a schimbului de conținut al comunicațiilor electronice; inclusiv datele utilizate pentru urmărirea și identificarea sursei și a destinației unei comunicații, datele privind locația dispozitivului generate în contextul furnizării serviciilor de comunicații electronice, precum și data, ora, durata și tipul comunicației;

(d) „listă de abonați accesibilă publicului” înseamnă o listă a utilizatorilor finali ai serviciilor de comunicații electronice, în format tipărit sau electronic, care este publicată sau pusă la dispoziția publicului sau a unei părți a publicului, inclusiv prin intermediul unui serviciu de informații privind abonații;

(e) „poștă electronică” înseamnă orice mesaj electronic conținând informații, cum ar fi mesajele scrise, mesajele vocale, înregistrările video, imaginile și sunetele, trimis prin intermediul unei rețele de comunicații electronice, care poate fi stocat în rețea sau în instalații informatice conexe sau în echipamentul terminal al beneficiarului său;

(f) „comunicații în scopuri de marketing direct” înseamnă orice tip de publicitate, în formă scrisă sau orală, trimisă unuia sau mai multor utilizatori finali identificați sau identificabili de servicii de comunicații electronice, inclusiv folosirea sistemelor de apelare și comunicare automate, cu sau fără interacțiune umană, a e-mailurilor, a SMS-urilor etc.;

(g) „apeluri vocale în scopuri de marketing direct” înseamnă apelurile efectuate în direct, care nu implică folosirea sistemelor de apelare și comunicare automate;

(h) „sisteme de apelare și comunicare automate” înseamnă sistemele capabile să efectueze în mod automat apeluri către unul sau mai mulți destinatari în conformitate cu instrucțiunile stabilite pentru sistemul respectiv și să transmită sunete care nu reprezintă un mesaj rostit în direct, inclusiv apelurile efectuate utilizând sisteme de apelare și comunicare automate care face conexiunea între destinatarul apelului și o altă persoană.

CAPITOLUL II
PROTECȚIA COMUNICAȚIILOR ELECTRONICE ALE PERSOANELOR FIZICE ȘI JURIDICE ȘI A INFORMAȚIILOR STOCATE ÎN ECHIPAMENTELE TERMINALE ALE ACESTORA

Articolul 5

Confidențialitatea datelor transmise în cadrul comunicațiilor electronice

Datele transmise în cadrul comunicațiilor electronice sunt confidențiale. Orice interferență cu datele transmise în cadrul comunicațiilor electronice, cum ar fi ascultarea, înregistrarea,

stocarea, monitorizarea, scanarea sau alte tipuri de interceptare, supravegherea sau prelucrarea datelor transmise în cadrul comunicațiilor electronice, de către alte persoane decât utilizatorii finali, este interzisă, cu excepția cazului în care acest lucru este permis prin prezentul regulament.

Articolul 6

Prelucrarea permisă a datelor transmise în cadrul comunicațiilor electronice

1. Furnizorii de rețele și servicii de comunicații electronice pot prelucra datele transmise în cadrul comunicațiilor electronice în cazul în care acest lucru:

(a) este necesar pentru efectuarea transmisiei comunicației, pe durata de timp necesară în acest scop sau

(b) este necesar pentru a menține sau a restabili securitatea rețelelor și serviciilor de comunicații electronice sau pentru a detecta defecțiuni tehnice și/sau erori de transmisie a comunicațiilor electronice, pe durata de timp necesară în acest scop.

2. Furnizorii de servicii de comunicații electronice pot prelucra metadatele privind comunicațiile electronice în cazul în care acest lucru:

(a) este necesar pentru a răspunde cerințelor obligatorii de calitate a serviciului în temeiul [Directivei de instituire a Codului european al comunicațiilor electronice] sau al Regulamentului (UE) nr. 2015/2120[11] pe durata de timp necesară în acest scop sau

(b) este necesar pentru facturare, pentru calcularea tarifelor de interconectare, pentru detectarea sau oprirea utilizării frauduloase sau abuzive a serviciilor de comunicații electronice sau pentru abonarea la acestea sau

(c) utilizatorul final în cauză și-a dat consimțământul pentru prelucrarea metadatelor privind comunicațiile sale pentru unul sau mai multe scopuri specifice, inclusiv pentru furnizarea de servicii specifice către acești utilizatori finali, cu condiția ca scopul sau scopurile în cauză să nu fi putut fi îndeplinite prin prelucrarea informațiilor anonimizate.

3. Furnizorii de servicii de comunicații electronice nu pot prelucra conținutul comunicațiilor electronice decât:

(a) exclusiv în scopul prestării unui serviciu specific pentru un utilizator final, în cazul în care utilizatorul final sau utilizatorii finali în cauză și-au dat consimțământul pentru prelucrarea conținutului comunicațiilor lor electronice și furnizarea acestui serviciu nu poate fi realizată fără prelucrarea unui astfel de conținut sau

(b) în cazul în care toți utilizatorii finali în cauză și-au dat consimțământul pentru prelucrarea conținutului comunicațiilor lor electronice pentru unul sau mai multe scopuri specifice care nu pot fi îndeplinite prin prelucrarea unor informații anonimizate, iar furnizorul a consultat autoritatea de supraveghere. Articolul 36

[11] Regulamentul (UE) 2015/2120 al Parlamentului European și al Consiliului din 25 noiembrie 2015 de stabilire a unor măsuri privind accesul la internetul deschis și de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile electronice de comunicații și a Regulamentului (UE) nr. 531/2012 privind roamingul în rețelele publice de comunicații mobile în interiorul Uniunii (JO L 310, 26.11.2015, p. 1-18).

alineatele (2) și (3) din Regulamentul (UE) 2016/679 se aplică în ceea ce privește consultarea autorității de supraveghere.

Articolul 7

Stocarea și ștergerea datelor transmise în cadrul comunicațiilor electronice

1. Fără a aduce atingere articolului 6 alineatul (1) litera (b) și articolului 6 alineatul (3) literele (a) și (b), furnizorul de servicii de comunicații electronice șterge conținutul comunicațiilor electronice sau anonimizează aceste date după primirea conținutului comunicațiilor electronice de către destinatarul sau destinatarii vizați. Aceste date pot fi înregistrate sau stocate de către utilizatorii finali sau o parte terță însărcinată de aceștia să efectueze înregistrarea, stocarea sau orice alt tip de prelucrare a datelor respective, în conformitate cu Regulamentul (UE) 2016/679.

2. Fără a aduce atingere articolului 6 alineatul (1) litera (b) și articolului 6 alineatul (2) literele (a) și (c), furnizorul de servicii de comunicații electronice șterge metadatele privind comunicațiile electronice sau anonimizează aceste date de îndată ce nu mai sunt necesare în scopul transmiterii comunicației.

3. În cazul în care prelucrarea metadatelor privind comunicațiile electronice are loc în scopul facturării, în conformitate cu 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 pot fi inițiate demersuri legale în vederea obținerii unei plăți în conformitate cu dreptul național.

Articolul 8

Protecția informațiilor stocate în echipamentele terminale ale utilizatorilor finali sau aferente acestora

1. Utilizarea capacităților de prelucrare și stocare a echipamentelor terminale și colectarea de informații de la echipamentele terminale ale utilizatorilor finali, inclusiv privind software-ul și hardware-ul acestora, de către alte persoane decât utilizatorul final în cauză sunt interzise, cu excepția următoarelor situații:

(a) dacă acest lucru este necesar cu unicul scop de a efectua transmisia unei comunicații electronice printr-o rețea de comunicații electronice; sau

(b) dacă utilizatorul final și-a dat consimțământul; sau

(c) dacă acest lucru este necesar pentru a furniza un serviciu al societății informaționale solicitat de utilizatorul final sau

(d) pentru măsurarea audienței pe internet, cu condiția ca o astfel de măsurare să fie efectuată de către furnizorul serviciului societății informaționale solicitat de utilizatorul final.

2. Colectarea informațiilor emise de echipamentele terminale care să le permită conectarea la un alt dispozitiv sau la alte echipamente de rețea este interzisă, cu excepția cazului în care:

(a) aceasta se efectuează exclusiv în vederea și în scopul stabilirii unei conexiuni, atât timp cât este necesar; sau

(b) este afișat un anunț clar și foarte vizibil în care se menționează, cel puțin, modalitățile de colectare, scopul colectării, persoana responsabilă în acest sens și celelalte informații necesare în temeiul articolului 13 din Regulamentul (UE)

2016/679, în cazul în care sunt colectate date cu caracter personal, precum și orice măsură pe care o poate lua utilizatorul final al echipamentului terminal pentru a minimiza sau a opri colectarea informațiilor.

Colectarea unor astfel de informații este condiționată de aplicarea măsurilor tehnice și organizatorice adecvate pentru a se asigura un nivel de securitate care corespunde riscurilor, astfel cum se prevede la articolul 32 din Regulamentul (UE) 2016/679.

3. Informațiile care trebuie furnizate în temeiul alineatului (2) litera (b) pot fi furnizate în combinație cu pictograme standardizate pentru a oferi o imagine de ansamblu semnificativă asupra colectării într-un mod care să fie ușor de vizualizat, de înțeles și de citit.

4. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 27 în care se stabilesc informațiile care urmează să fie prezentate de pictogramele standardizate și procedurile pentru furnizarea acestor pictograme.

Articolul 9
Consimțământul

1. Se aplică definiția consimțământului și condițiile pentru acordarea acestuia prevăzute la articolul 4 alineatul (11) și la articolul 7 din Regulamentul (UE) 2016/679.

2. Fără a aduce atingere alineatului (1), în cazul în care este posibil din punct de vedere tehnic și fezabil, în sensul articolului 8 alineatul (1) litera (b), consimțământul poate fi exprimat prin utilizarea setărilor tehnice adecvate ale unei aplicații software care să permită accesul la internet.

3. Utilizatorilor finali care și-au dat consimțământul pentru prelucrarea datelor transmise în cadrul comunicațiilor electronice, astfel cum se prevede la articolul 6 alineatul (2) litera (c) și la articolul 6 alineatul (3) literele (a) și (b), li se oferă posibilitatea de a-și retrage consimțământul în orice moment, astfel cum se prevede la articolul 7 alineatul (3) din Regulamentul (UE) 2016/679 și li se reamintește această posibilitate la intervale periodice de 6 luni, atât timp cât continuă prelucrarea datelor.

Articolul 10
Informații și opțiuni pentru setările de confidențialitate care trebuie furnizate

1. Software-ul introdus pe piață care permite efectuarea de comunicații electronice, inclusiv obținerea și prezentarea informațiilor pe internet, oferă posibilitatea de a împiedica părțile terțe să stocheze informații în echipamentele terminale ale unui utilizator final sau să prelucreze informații deja stocate în echipamentele respective.

2. La instalare, software-ul informează utilizatorul final cu privire la opțiunile legate de setările de confidențialitate și solicită acestuia, pentru a putea continua instalarea, să își dea consimțământul cu privire la una dintre setările disponibile.

3. În cazul unui software care este instalat înainte de 25 mai 2018, cerințele de la alineatele (1) și (2) trebuie îndeplinite la momentul primei actualizări a software-ului, dar nu mai târziu de 25 august 2018.

Articolul 11
Restricții

1. Dreptul Uniunii sau al statului membru pot restrânge printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la articolele 5-8, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice pentru a proteja unul sau mai multe interese publice generale menționate la articolul 23 alineatul (1) literele (a)-(e) din Regulamentul (UE) 2016/679 sau o funcție de monitorizare, inspecție sau reglementare legată de exercitarea autorității oficiale pentru astfel de interese.

2. Furnizorii de servicii de comunicații electronice stabilesc proceduri interne pentru a răspunde solicitărilor de accesare a datelor transmise în cadrul comunicațiilor electronice ale utilizatorilor finali pe baza unei măsuri legislative adoptate în temeiul alineatului (1). La cerere, aceștia oferă autorității de supraveghere competente informații despre procedurile respective, numărul de solicitări primite, justificarea legală invocată și răspunsul acestora.

CAPITOLUL III
DREPTURILE PERSOANELOR FIZICE ȘI JURIDICE PRIVIND CONTROLUL COMUNICAȚIILOR ELECTRONICE

Articolul 12
Prezentarea și restricționarea identificării liniilor apelante și a celor conectate

1. În cazul în care prezentarea identificării liniilor apelante și a celor conectate este oferită în conformitate cu articolul [107] din [Directiva de instituire a Codului european al comunicațiilor electronice], furnizorii de servicii de comunicații interpersonale bazate pe numere și accesibile publicului oferă următoarele opțiuni:

(a) utilizatorul final apelant are posibilitatea de a împiedica prezentarea identificării liniei apelante în cazul unui anumit apel, al unei anumite conexiuni sau în mod permanent;

(b) utilizatorul final apelat are posibilitatea de a împiedica prezentarea identificării liniei apelante în cazul apelurilor primite;

(c) utilizatorul final apelat are posibilitatea de a respinge apelurile primite dacă prezentarea identificării liniei apelante este împiedicată de către utilizatorul final apelant;

(d) utilizatorul final apelat are posibilitatea de a împiedica prezentarea identificării liniei conectate către utilizatorul final apelant.

2. Posibilitățile menționate la alineatul (1) literele (a), (b), (c) și (d) sunt furnizate utilizatorilor finali prin mijloace simple și în mod gratuit.

3. De asemenea, alineatul (1) litera (a) se aplică apelurilor din Uniune către țări terțe. Alineatul (1) literele (b), (c) și (d) se aplică și apelurilor primite din țări terțe.

4. În cazul în care este furnizată prezentarea identificării liniei apelante sau a liniei conectate, furnizorii de servicii de comunicații interpersonale bazate pe numere și accesibile publicului oferă publicului informații cu privire la opțiunile prevăzute la alineatul (1) literele (a), (b), (c) și (d).

Articolul 13

Excepții de la prezentarea și restricționarea identificării liniilor apelante și a celor conectate

1. Chiar dacă utilizatorul final apelant a împiedicat prezentarea identificării liniei apelante, atunci când se efectuează un apel către serviciile de urgență, furnizorii de servicii de comunicații interpersonale bazate pe numere și accesibile publicului dezactivează opțiunea apelanților de a împiedica prezentarea identificării liniei apelante și opțiunea privind refuzul sau absența consimțământului unui utilizator final pentru prelucrarea metadatelor, pentru fiecare linie în parte, astfel încât organizațiile responsabile cu comunicațiile de urgență, inclusiv centrele de preluare a apelurilor de urgență, să poată lua măsurile necesare în urma acestor comunicații.

2. Statele membre instituie dispoziții mai specifice cu privire la stabilirea procedurilor și a situațiilor în care furnizorii de servicii de comunicații interpersonale bazate pe numere și accesibile publicului dezactivează opțiunea apelanților de a împiedica prezentarea identificării liniei apelante, în mod temporar, în cazul în care utilizatorii finali solicită identificarea apelurilor răuvoitoare sau deranjante.

Articolul 14

Blocarea apelurilor primite

Furnizorii de servicii de comunicații interpersonale bazate pe numere și accesibile publicului pun în practică măsuri de ultimă generație pentru a limita primirea de apeluri nedorite de către utilizatorii finali și oferă, de asemenea, utilizatorului final apelat, în mod gratuit, următoarele posibilități:

(a) blocarea apelurilor primite de la numere specifice sau de la surse anonime;

(b) blocarea transferului automat al apelurilor de către o parte terță către echipamentul terminal al utilizatorului final.

Articolul 15

Liste de abonați accesibile publicului

1. Furnizorii de liste de abonați accesibile publicului obțin consimțământul utilizatorilor finali care sunt persoane fizice privind includerea în listă a datelor cu caracter personal ale acestora și, prin urmare, obțin consimțământul acestor utilizatori finali privind includerea datelor pentru fiecare categorie de date cu caracter personal, în măsura în care aceste date sunt relevante pentru scopul listei, astfel cum este stabilit de către furnizorul acesteia. Furnizorii pun la dispoziția utilizatorilor finali care sunt persoane fizice mijloacele necesare pentru a verifica, a corecta și a șterge datele respective.

2. Furnizorii de liste de abonați accesibile publicului informează utilizatorii finali care sunt persoane fizice și ale căror date cu caracter personal sunt incluse în listă cu privire la funcțiile de căutare disponibile în lista respectivă și obțin consimțământul utilizatorilor finali înainte de a activa astfel de funcții de căutare în legătură cu datele acestora.

3. Furnizorii de liste de abonați accesibile publicului oferă utilizatorilor finali care sunt persoane juridice posibilitatea de a se opune includerii într-o listă a datelor care îi privesc. Furnizorii pun la dispoziția utilizatorilor finali care sunt persoane juridice mijloacele necesare pentru a verifica, a corecta și a șterge datele respective.

4. Posibilitatea ca utilizatorii finali să nu fie incluși într-o listă de abonați accesibilă publicului sau de a verifica, a corecta și a șterge orice date legate de aceștia este furnizată în mod gratuit.

Articolul 16
Comunicațiile nesolicitate

1. Persoanele fizice sau juridice pot utiliza serviciile de comunicații electronice pentru trimiterea de comunicații în scopuri de marketing direct către utilizatorii finali care sunt persoane fizice și care și-au dat consimțământul în acest sens.

2. În cazul în care o persoană fizică sau juridică obține datele de contact pentru poștă electronică de la clientul său, în contextul vânzării unui produs sau a unui serviciu, în conformitate cu Regulamentul (UE) 2016/679, această persoană fizică sau juridică poate folosi respectivele date de contact pentru marketingul direct al propriilor produse sau servicii similare numai în cazul în care clienților li se oferă posibilitatea în mod clar și distinct de a se opune, în mod gratuit și facil, unei astfel de utilizări. Dreptul de a se opune este acordat la momentul colectării datelor de contact și de fiecare dată când este trimis un mesaj.

3. Fără a aduce atingere alineatelor (1) și (2), persoanele fizice sau juridice care utilizează serviciile de comunicații electronice pentru efectuarea de apeluri în scopuri de marketing direct trebuie:

(a) să prezinte identitatea unei linii unde pot fi contactate; sau

(b) să prezinte un cod specific/prefix care identifică faptul că apelul este efectuat în scopuri de marketing.

4. Fără a aduce atingere alineatului (1), statele membre pot să prevadă prin lege că efectuarea de apeluri vocale în scopuri de marketing direct către utilizatorii finali care sunt persoane fizice nu este permisă decât în ceea ce privește utilizatorii finali care sunt persoane fizice și care nu s-au opus primirii unor astfel de comunicări.

5. Statele membre se asigură că, în temeiul legislației Uniunii și a legislației naționale aplicabile, interesele legitime ale utilizatorilor finali care sunt persoane juridice beneficiază de un nivel de protecție suficient în privința comunicațiilor nesolicitate trimise prin mijloacele prezentate la alineatul (1).

6. Orice persoană fizică sau juridică ce utilizează servicii de comunicații electronice pentru transmiterea de comunicații în scopuri de marketing direct informează utilizatorii finali cu privire la caracterul comercial al comunicațiilor și la identitatea persoanei fizice sau juridice în numele căreia este transmisă comunicarea și furnizează 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.

7. Comisia este împuternicită să adopte măsuri de punere în aplicare în conformitate cu articolul 26 alineatul (2) în vederea precizării codului/prefixului pentru identificarea apelurilor în scopuri de marketing, în temeiul alineatului (3) litera (b).

Articolul 17
Informații privind riscurile de securitate detectate

În cazul unui risc specific care ar putea compromite securitatea rețelelor și a serviciilor de comunicații electronice, furnizorul unui serviciu de comunicații electronice informează utilizatorii finali cu privire la acest risc și, dacă măsurile pe care le poate lua furnizorul de servicii nu permit înlăturarea acestui risc, informează utilizatorii finali cu privire la soluțiile posibile, inclusiv prin indicarea costurilor implicate.

CAPITOLUL IV
AUTORITĂȚILE DE SUPRAVEGHERE INDEPENDENTE ȘI ASIGURAREA RESPECTĂRII LEGII

Articolul 18
Autoritățile de supraveghere independente

1. Autoritatea sau autoritățile de supraveghere independente sau autoritățile responsabile de monitorizarea aplicării Regulamentului (UE) 2016/679 sunt, de asemenea, responsabile de monitorizarea aplicării prezentului regulament. Capitolul VI și VII din Regulamentul (UE) 2016/679 se aplică *mutatis mutandis*. Autoritățile de supraveghere își exercită atribuțiile și competențele în ceea ce privește utilizatorii finali.

2. Autoritatea sau autoritățile de supraveghere menționate la alineatul (1) cooperează ori de câte ori este necesar cu autoritățile naționale de reglementare înființate în temeiul [Directivei de instituire a Codului european al comunicațiilor electronice].

Articolul 19
Comitetul european pentru protecția datelor

Comitetul european pentru protecția datelor, instituit în temeiul articolului 68 din Regulamentul (UE) 2016/679, are competența de a asigura aplicarea coerentă a prezentului regulament. În acest scop, Comitetul european pentru protecția datelor își exercită atribuțiile prevăzute la articolul 70 din Regulamentul (UE) 2016/679. De asemenea, Comitetul îndeplinește următoarele atribuții:

(a) oferă consiliere Comisiei cu privire la orice propunere de modificare a prezentului regulament;

(b) examinează, din proprie inițiativă, la cererea unuia dintre membrii săi sau la cererea Comisiei, orice chestiune referitoare la aplicarea prezentului regulament și emite orientări, recomandări și bune practici pentru a încuraja aplicarea coerentă a prezentului regulament.

Articolul 20
Proceduri ce vizează cooperarea și asigurarea coerenței

Fiecare autoritate de supraveghere contribuie la aplicarea coerentă a prezentului regulament în întreaga Uniune. În acest scop, autoritățile de supraveghere cooperează atât unele cu altele, cât și cu Comisia, în conformitate cu capitolul VII din Regulamentul (UE) 2016/679 în ceea ce privește aspectele reglementate de prezentul regulament.

CAPITOLUL V
CĂI DE ATAC, RĂSPUNDERE ȘI SANCȚIUNI

Articolul 21
Căile de atac

1. Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, fiecare utilizator final de servicii de comunicații electronice beneficiază de aceleași căi de atac precum cele prevăzute la articolele 77, 78 și 79 din Regulamentul (UE) 2016/679.

2. Orice persoană fizică sau juridică, alta decât utilizatorii finali afectați negativ de încălcări ale prezentului regulament și care au un interes legitim în încetarea sau interzicerea încălcărilor presupuse, inclusiv un furnizor de servicii de comunicații electronice care își protejează interesele comerciale legitime, are dreptul de a intenta acțiuni în justiție în ceea ce privește astfel de încălcări.

Articolul 22
Dreptul la despăgubiri și răspunderea

Orice utilizator final al serviciilor de comunicații electronice care a suferit prejudicii materiale sau morale ca urmare a unei încălcări a prezentului regulament are dreptul să obțină despăgubiri de la autorul încălcării drepturilor pentru prejudiciul suferit, cu excepția cazului în care autorul încălcării dovedește că nu este răspunzător în niciun fel pentru evenimentul care a cauzat daunele în conformitate cu articolul 82 din Regulamentul (UE) 2016/679.

Articolul 23
Condiții generale pentru impunerea amenzilor administrative

1. În sensul prezentului articol, capitolul VII din Regulamentul (UE) 2016/679 se aplică în cazul încălcării prezentului regulament.

2. Pentru încălcările următoarelor dispoziții ale prezentului regulament, în conformitate cu alineatul (1), se aplică amenzi administrative de până la 10 000 000 EUR sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare:

(a) obligațiile oricărei persoane juridice sau fizice care prelucrează date privind comunicațiile electronice, în temeiul articolului 8;

(b) obligațiile furnizorilor de software aferent serviciilor de comunicații electronice, în temeiul articolului 10;

(c) obligațiile furnizorilor de liste de abonați accesibile publicului, în temeiul articolului 15;

(d) obligațiile oricărei persoane juridice sau fizice care utilizează servicii de comunicații electronice, în temeiul articolului 16.

3. Pentru încălcările principiului confidențialității comunicațiilor, ale prelucrării permise a datelor transmise în cadrul comunicațiilor electronice și ale termenelor pentru ștergerea datelor în temeiul articolelor 5, 6 și 7 se aplică, în conformitate cu alineatul (1) din prezentul articol, amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală

anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare.

4. Statele membre stabilesc normele privind sancțiunile aplicabile în cazul încălcării articolelor 12, 13, 14 și 17.

5. Încălcarea unui ordin emis de o autoritate de supraveghere în conformitate cu articolul 18 face obiectul unor amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare.

6. Fără a aduce atingere competențelor corective ale autorităților de supraveghere în temeiul articolului 18, fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi impuse amenzi administrative autorităților publice și organismelor publice stabilite în statul membru respectiv.

7. Exercitarea de către autoritatea de supraveghere a competențelor sale în temeiul prezentului articol are loc cu condiția existenței unor garanții procedurale adecvate în conformitate cu dreptul Uniunii și cu dreptul intern al statelor membre, inclusiv a unor căi de atac judiciare eficace și a dreptului la un proces echitabil.

8. În cazul în care sistemul juridic al unui stat membru nu prevede amenzi administrative, prezentul articol poate fi aplicat astfel încât amenda să fie inițiată de autoritatea de supraveghere competentă și impusă de instanțele naționale competente, garantându-se, în același timp, faptul că aceste căi de atac sunt eficace și au un efect echivalent cu cel al amenzilor administrative impuse de autoritățile de supraveghere. În orice caz, amenzile impuse trebuie să fie eficace, proporționale și disuasive. Respectivele state membre informează Comisia cu privire la dispozițiile de drept intern pe care le adoptă în temeiul prezentului alineat până la [xxx], precum și, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară a acestora.

Articolul 24
Sancțiuni

1. Statele membre stabilesc normele privind alte sancțiunile aplicabile în caz de încălcare a prezentului regulament, în special pentru încălcări care nu fac obiectul unor amenzi administrative în temeiul articolului 23, și iau toate măsurile necesare pentru a asigura faptul că acestea sunt puse în aplicare. Sancțiunile respective sunt eficace, proporționale și disuasive.

2. Fiecare stat membru informează Comisia cu privire la dispozițiile din propria legislație pe care le adoptă în temeiul alineatului (1), cel târziu în termen de 18 luni după data stabilită în temeiul articolului 29 alineatul (2), și, fără întârziere, cu privire la orice modificare ulterioară care le afectează.

CAPITOLUL VI
ACTE DELEGATE ȘI ACTE DE PUNERE ÎN APLICARE

Articolul 25
Exercitarea delegării

1. Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

2. Se conferă Comisiei, pentru o perioadă de timp nedeterminată începând de la [data intrării în vigoare a prezentului regulament], competența de a adopta acte delegate menționată la articolul 8 alineatul (4).

3. Delegarea de competențe menționată la articolul 8 alineatul (4) poate fi revocată în orice moment de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării competenței specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Aceasta nu aduce atingere validității actelor delegate aflate deja în vigoare.

4. Înainte de adoptarea unui act delegat, Comisia îi consultă pe experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016.

5. De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

6. Un act delegat adoptat în temeiul articolului 8 alineatul (4) intră în vigoare numai în cazul în care nici Parlamentul European, nici Consiliul nu a formulat obiecții în termen de două luni de la notificarea actului respectiv Parlamentului European și Consiliului sau dacă, înainte de expirarea acestui termen, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Termenul respectiv se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 26
Comitetul

1. Comisia este asistată de Comitetul pentru comunicații instituit în conformitate cu articolul 110 din [Directiva de instituire a Codului european al comunicațiilor electronice]. Comitetul respectiv este un comitet în înțelesul Regulamentului (UE) nr. 182/2011[12].

2. Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

[12] Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13-18).

CAPITOLUL VII
DISPOZIȚII FINALE

Articolul 27
Abrogare

1. Directiva 2002/58/CE se abrogă cu efect de la 25 mai 2018.

2. Trimiterile la directiva abrogată se interpretează ca trimiteri la prezentul regulament.

Articolul 28
Monitorizare și evaluare

Până la 1 ianuarie 2018, Comisia stabilește un program detaliat pentru monitorizarea eficacității prezentului regulament.

În cel mult trei ani de la data aplicării prezentului regulament și, ulterior, o dată la trei ani, Comisia efectuează o evaluare a prezentului regulament și prezintă Parlamentului European, Consiliului și Comitetului Economic și Social European un raport conținând principalele constatări. În baza acestei evaluări, dacă este cazul, se elaborează o propunere de modificare sau abrogare a prezentului regulament, în funcție de evoluțiile juridice, tehnice sau economice.

Articolul 29
Intrare în vigoare și aplicare

1. Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

2. Se aplică de la 25 mai 2018.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președintele	*Președintele*