COMISIA
EUROPEANĂ

Bruxelles, 24.7.2019
COM(2019) 374 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Normele privind protecția datelor, factor favorizant al încrederii în UE și în afara acesteia – bilanț

Comunicare a Comisiei către Parlamentul European și Consiliu

Normele privind protecția datelor, factor favorizant al încrederii în UE și în afara acesteia – bilanț

I. Introducere

Regulamentul general privind protecția datelor[1] (denumit în continuare „regulamentul”) se aplică la nivelul Uniunii Europene de peste un an și se află în centrul unui cadru coerent și modernizat al protecției datelor în UE, care include, de asemenea, Directiva privind protecția datelor în materie de asigurare a respectării legii[2] și Regulamentul privind protecția datelor pentru instituțiile și organele UE[3]. Acest cadru urmează să fie completat cu Regulamentul privind viața privată și comunicațiile electronice, care se află, în prezent, în proces legislativ.

Existența unor norme solide privind protecția datelor este crucială pentru garantarea dreptului fundamental la protecția datelor cu caracter personal. Acestea ocupă un loc central într-o societate democratică[4] și constituie o componentă importantă a unei economii bazate tot mai mult pe date. UE aspiră să se bucure de numeroasele oportunități pe care transformarea digitală le oferă în ceea ce privește serviciile, locurile de muncă și inovarea, abordând în același timp provocările pe care acestea le aduc. Furtul de identitate, scurgerile de date sensibile, discriminarea persoanelor, prejudecățile profunde, partajarea conținutului ilegal și elaborarea unor instrumente de supraveghere intruzive reprezintă numai câteva exemple de aspecte care apar tot mai frecvent în dezbaterile publice, fiind evident faptul că cetățenii se așteaptă ca datele lor să fie protejate.

Protecția datelor a devenit un fenomen cu adevărat global, pe măsură ce, la nivel mondial, oamenii apreciază și acordă valoare tot mai mult protecției și securității datelor lor. Multe țări au adoptat sau sunt în curs de adoptare a unor norme cuprinzătoare privind protecția datelor,

---

1 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): https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679.

2 Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, JO L 119, 4.5.2016: https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=celex%3A32016L0680. Directiva trebuia să fie transpusă de statele membre până la 6 mai 2018. Rapoartele privind o uniune a securității prezintă situația transpunerii acesteia.

3 Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE, JO L 295, 21.11.2018, p. 39-98: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32018R1725. Acesta a intrat în vigoare la 11 decembrie 2018.

4 Curtea Supremă din India, în cadrul unei hotărâri de referință pronunțate la 24 august 2017, a recunoscut viața privată ca fiind un drept fundamental, o „fațetă esențială a demnității ființei umane”.

bazate pe principii similare celor din regulament, ceea ce conduce la o convergență globală a normelor privind protecția datelor. Aceasta oferă noi posibilități de facilitare a fluxurilor de date între operatorii economici sau autoritățile publice, îmbunătățind în același timp nivelul de protecție a datelor cu caracter personal în UE și în întreaga lume.

Protecția datelor este considerată acum mai importantă decât oricând și are un impact amplu asupra diferitelor părți interesate și sectoare. Comisia este hotărâtă să conducă UE către o punere reușită în aplicare a noului regim privind protecția datelor și să acorde sprijin pentru ca toate aspectele acestuia să devină pe deplin operaționale. Prin prezenta comunicare, Comisia face un bilanț al rezultatelor obținute până în prezent în legătură cu punerea consecventă în aplicare a normelor privind protecția datelor la nivelul UE, cu funcționarea noului sistem de guvernanță, cu impactul asupra cetățenilor și întreprinderilor și cu eforturile UE de promovare a convergenței globale a regimurilor de protecție a datelor. Aceasta urmează Comunicării Comisiei din ianuarie 2018[5] privind aplicarea regulamentului, și a fost fundamentată pe activitatea Grupului multipartit[6], în special pe contribuția acestuia la exercițiul de evaluare cu o durată de un an, precum și pe discuțiile derulate în cadrul evenimentului de evaluare organizat de Comisie la 13 iunie 2019[7]. Prezenta comunicare constituie, de asemenea, o contribuție la examinarea pe care Comisia intenționează să o efectueze până în mai 2020 [8].

Cadrul legislativ al UE în materie de protecție a datelor reprezintă o piatră de temelie pentru abordarea europeană centrată pe factorul uman cu privire la inovare. Acesta devine parte a bazei de reglementare pentru o gamă tot mai amplă de politici, inclusiv cu privire la sănătate și cercetare, inteligența artificială, transporturi, energie, concurență și aplicarea legii. Comisia a subliniat în mod consecvent importanța unei puneri în aplicare și a unei asigurări a respectării adecvate a noilor norme privind protecția datelor, astfel cum a evidențiat în Comunicarea sa privind aplicarea regulamentului, emisă în ianuarie 2018, și în orientările sale privind utilizarea datelor cu caracter personal în contextul alegerilor, publicate în septembrie 2018[9]. La momentul redactării prezentei comunicări, s-au înregistrat numeroase progrese în direcția atingerii acestui obiectiv, deși sunt necesare cu siguranță mai multe eforturi pentru ca regulamentul să devină pe deplin operațional.

---

5 Comunicarea Comisiei către Parlamentul European și Consiliu intitulată „Protecție sporită, noi oportunități - Orientările Comisiei privind aplicarea directă a Regulamentului general privind protecția datelor de la 25 mai 2018”, COM(2018) 43 final: https://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

6 Grupul multipartit privind regulamentul, înființat de Comisie, implică reprezentanți ai societății civile și ai întreprinderilor, mediul academic și practicieni: https://ec.europa.eu/transparency/regexpert/index.cfm?Lang=RO.

7 http://europa.eu/rapid/press-release_IP-19-2956_ro.htm.

8 Articolul 97 din regulament.

9 „Orientările Comisiei privind aplicarea legislației Uniunii în materie de protecție a datelor în contextul alegerilor”, COM(2018) 638 final: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52018DC0638&qid=1566856342213&from=EN.

II. Un continent, o legislație: statele membre au instituit cadrul de protecție a datelor

Un obiectiv-cheie al regulamentului a fost acela de a elimina peisajul fragmentat al celor 28 de legislații naționale diferite, care exista în temeiul precedentei Directive privind protecția datelor[10], și de a oferi securitate juridică pentru cetățeni și întreprinderi în întreaga UE. Acest obiectiv a fost îndeplinit în mare măsură.

Armonizarea cadrului juridic

Deși este direct aplicabil în statele membre, regulamentul le-a obligat pe acestea să ia o serie de măsuri juridice la nivel național, în special să instituie și să aloce competențe pentru autoritățile naționale de protecție a datelor[11], să prevadă norme privind aspecte specifice, cum ar fi reconcilierea protecției datelor cu caracter personal cu libertatea de exprimare și de informare și să modifice sau să abroge legislația sectorială care conține aspecte legate de protecția datelor. La momentul redactării prezentei comunicări, toate statele membre, cu excepția a trei dintre ele[12], și-au actualizat legislațiile naționale privind protecția datelor. Activitățile de adaptare a legislațiilor sectoriale sunt încă în curs la nivel național. După încorporarea sa în Acordul privind Spațiul Economic European, aplicarea regulamentului a fost extinsă la Norvegia, Islanda și Liechtenstein, care au adoptat, de asemenea, legislații naționale în materie de protecție a datelor.

Cu toate acestea, părțile interesate solicită un grad chiar și mai ridicat de armonizare în unele domenii[13]. Într-adevăr, regulamentul permite statelor membre o anumită marjă de manevră pentru a preciza și mai bine aplicarea sa în anumite domenii, cum ar fi vârsta de consimțământ a copiilor pentru serviciile online[14] sau prelucrarea datelor cu caracter personal în domenii precum medicina și sănătatea publică. În acest caz, acțiunea statelor membre este încadrată de două elemente:

i) orice legislație națională care urmărește să aducă precizări suplimentare trebuie să respecte cerințele Cartei drepturilor fundamentale[15] (și să nu depășească limitele stabilite de regulament, care se bazează pe cartă);
ii) nu poate afecta libera circulație a datelor cu caracter personal în cadrul UE[16].

---

[10] Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:31995L0046.

[11] De exemplu, competența de a impune amenzi administrative.

[12] La 23 iulie 2019, Grecia, Portugalia și Slovenia se află încă în proces de adoptare a legislațiilor lor naționale.

[13] A se vedea raportul Grupului multipartit privind regulamentul, publicat la 13 iunie 2019: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=RO.

[14] 13 ani pentru Belgia, Danemarca, Estonia, Finlanda, Letonia, Malta, Suedia și Regatul Unit; 14 ani pentru Austria, Bulgaria, Cipru, Spania, Italia și Lituania; 15 ani pentru Cehia și Franța; 16 ani pentru Germania, Ungaria, Croația, Irlanda, Luxemburg, Țările de Jos, Polonia, România și Slovacia.

[15] Articolul 8.

În unele situații, statele membre au introdus cerințe naționale în plus față de cele din regulament, în special prin multe legi sectoriale, iar acest lucru conduce la fragmentare și la crearea unor sarcini inutile. Un exemplu de cerință suplimentară introdusă de statele membre pe lângă cele din regulament constă în obligația, în temeiul legislației germane, de a desemna un responsabil cu protecția datelor în întreprinderile cu cel puțin 20 de angajați, care să fie implicat permanent în prelucrarea automată a datelor cu caracter personal.

Continuarea eforturilor în direcția unei mai bune armonizări

Comisia se implică în dialoguri bilaterale cu autoritățile naționale, în cadrul cărora acordă o atenție deosebită măsurilor naționale legate de:

- independența efectivă a autorităților de protecție a datelor, inclusiv prin resurse financiare, umane și tehnice adecvate;
- modul în care legile naționale restricționează drepturile persoanelor vizate;
- faptul că legislația națională nu ar trebui să introducă cerințe care depășesc regulamentul, atunci când nu există o marjă pentru precizări suplimentare, de exemplu condiții în plus pentru prelucrare;
- îndeplinirea obligației de a reconcilia dreptul la protecția datelor cu caracter personal cu libertatea de exprimare și de informare, ținând seama de faptul că nu ar trebui să se abuzeze de această obligație pentru a crea un efect de intimidare asupra activităților jurnalistice.

Activitatea autorităților de protecție a datelor, care cooperează în cadrul Comitetului european pentru protecția datelor („comitetul”), reprezintă un factor determinant esențial pentru o aplicare consecventă a noilor norme: acțiunile de aplicare a legii care afectează mai multe state membre se desfășoară prin intermediul mecanismului pentru cooperare și asigurarea coerenței[17] din cadrul comitetului, iar orientările adoptate de comitet contribuie la o înțelegere armonizată a regulamentului. Totuși, părțile interesate se așteaptă ca autoritățile de protecție a datelor să continue în această direcție.

Activitatea instanțelor naționale și a Curții de Justiție a Uniunii Europene contribuie, de asemenea, la asigurarea unei interpretări consecvente a normelor privind protecția datelor. Instanțele naționale au pronunțat recent hotărâri care invalidează dispozițiile din legislațiile naționale care deviază de la regulament[18].

---

[16] În concordanță cu articolul 16 alineatul (2) din Tratatul privind funcționarea Uniunii Europene.

[17] Articolul 60 din regulament prevede ca, în cooperarea dintre autoritățile de protecție a datelor, să se aplice o singură interpretare a regulamentului în cazuri concrete. Articolul 64 prevede că, în anumite situații, comitetul va emite avize, astfel încât să se asigure o aplicare consecventă a regulamentului. În fine, comitetul are competența de a adopta decizii obligatorii adresate autorităților de protecție a datelor, în cazul în care există dezacorduri între acestea.

[18] Acest lucru s-a întâmplat în Germania și în Spania.

III. Toate elementele noului sistem de guvernanță produc rezultate

Regulamentul a creat o nouă structură a guvernanței, plasând în centrul acesteia autoritățile naționale independente de protecție a datelor, ca autorități responsabile de asigurarea punerii în aplicare a regulamentului și prime puncte de contact pentru părțile interesate. Deși majoritatea autorităților de protecție a datelor au beneficiat, în anul precedent, de resurse sporite, există încă mari diferențe între statele membre[19].

Autoritățile de protecție a datelor fac uz de noile lor competențe

Regulamentul conferă autorităților de protecție a datelor competențe mai solide de aplicare a legii. Contrar temerilor exprimate de unele părți interesate înainte de luna mai 2018, autoritățile naționale de protecție a datelor au adoptat o abordare echilibrată cu privire la competențele de aplicare a legii. Acestea s-au axat pe dialog, mai degrabă decât pe sancțiuni, în special pentru cei mai mici operatori care nu prelucrează date cu caracter personal ca activitate de bază. În același timp, acestea nu au ezitat să își utilizeze noile competențe în mod eficace ori de câte ori acest lucru a fost necesar, inclusiv prin demararea unor investigații în domeniul platformelor de comunicare socială[20] și impunerea unor amenzi administrative cu valori cuprinse între câteva mii de euro și câteva milioane de euro, în funcție de gravitatea încălcărilor normelor privind protecția datelor.

Exemple de amenzi impuse de autoritățile de protecție a datelor[21]:

- amendă în valoare de 5 000 EUR aplicată unui centru de pariuri sportive din Austria, ca urmare a supravegherii video ilegale;
- amendă în valoare de 220 000 EUR aplicată unei societăți de brokeraj de date din Polonia, ca urmare a neinformării persoanelor cu privire la faptul că datele lor sunt prelucrate;
- amendă în valoare de 250 000 EUR aplicată ligii spaniole de fotbal LaLiga, pentru lipsă de transparență în conceperea aplicației sale pentru telefoane inteligente;
- amendă în valoare de 50 de milioane EUR aplicată Google din Franța, din cauza condițiilor pentru obținerea consimțământului utilizatorilor.

Atunci când desfășoară investigații, este esențial ca autoritățile de protecție a datelor să colecteze probe relevante, să respecte toate etapele procedurale prevăzute în legislația națională și să asigure respectarea garanțiilor procedurale în cazul dosarelor adesea complexe. Acest lucru necesită timp și implică un volum semnificativ de muncă, ceea ce explică motivul pentru care majoritatea investigațiilor demarate după intrarea în vigoare a regulamentului sunt încă în derulare.

---

19 https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

20 De exemplu, Comisia pentru protecția datelor din Irlanda a deschis 15 investigații oficiale legate de respectarea regulamentului de către societățile multinaționale din domeniul tehnologiei. A se vedea pagina 49 din raportul anual pe 2018 al Comisiei pentru protecția datelor din Irlanda: https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018.

21 Mai multe decizii de impunere a unor amenzi încă fac obiectul controlului judiciar.

Acestea fiind spuse, succesul regulamentului nu ar trebui măsurat prin numărul de amenzi aplicate, ci prin schimbările aduse în cultura și comportamentul tuturor actorilor implicați. În acest context, autoritățile de protecție a datelor au la dispoziție alte instrumente, precum impunerea unei limitări temporare sau definitive cu privire la prelucrare, inclusiv o interdicție sau dispunerea suspendării fluxurilor de date către un destinatar dintr-o țară terță[22].

Unele autorități de protecție a datelor au creat instrumente noi, precum linii de asistență telefonică și seturi de instrumente pentru întreprinderi, iar altele au elaborat abordări noi, precum spațiile de testare în materie de reglementare[23], pentru a ajuta întreprinderile în eforturile lor de conformare. Totuși, o serie de părți interesate consideră în continuare că nu au primit sprijin și informații suficiente, în special întreprinderile mici și mijlocii din unele state membre[24]. Pentru a contribui la remedierea acestei situații, Comisia oferă granturi autorităților de protecție a datelor pentru ca acestea să intre în contact cu părțile interesate, în special persoane fizice și întreprinderi mici și mijlocii[25].

Comitetul european pentru protecția datelor este operațional

Autoritățile de protecție a datelor și-au intensificat activitatea în cadrul Comitetului european pentru protecția datelor[26]. Această activitate intensă a permis comitetului să adopte aproximativ 20 de orientări privind aspecte-cheie ale regulamentului[27]. Viitoarele domenii de activitate ale comitetului sunt prezentate în cadrul unui program cu durata de 2 ani[28], astfel cum se prevede în regulament.

În cazurile transfrontaliere, autoritățile de protecție a datelor nu mai sunt doar autorități naționale, ci fac parte dintr-un proces cu adevărat european la nivelul tuturor etapelor, de la investigație la decizie. O astfel de cooperare strânsă a devenit o practică cotidiană: până la sfârșitul lunii iunie 2019 au fost gestionate 516 cazuri transfrontaliere prin intermediul mecanismului de cooperare.

---

22 Articolul 58 alineatul (2) literele (f) și (j).

23 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/

24 A se vedea raportul Grupului multipartit privind RGPD: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=RO

25 Suma de 2 milioane EUR alocată pentru nouă autorități de protecție a datelor în 2018, pentru activități desfășurate în perioada 2018-2019: Belgia, Bulgaria, Danemarca, Ungaria, Lituania, Letonia, Țările de Jos, Slovenia și Islanda: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;
O sumă de 1 milion EUR care urmează să fie alocată în 2019: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019.

26 Comitetul are personalitate juridică și este format din șefii autorităților naționale de supraveghere a protecției datelor și Autoritatea Europeană pentru Protecția Datelor.

27 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_ro

28 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_ro

Comisia contribuie activ la lucrările comitetului[29] pentru a promova litera și spiritul regulamentului și reamintește principiile generale ale dreptului UE[30].

Către crearea unei culturi a UE privind protecția datelor

Noul sistem de guvernanță trebuie încă să își valorifice întregul potențial. Este important ca procesul decizional al comitetului să fie simplificat în continuare și să se dezvolte o cultură comună a UE privind protecția datelor în rândul membrilor săi. Posibilitățile ca autoritățile de protecție a datelor să își cumuleze eforturile[31] privind aspecte care afectează mai mult decât un stat membru, de exemplu desfășurarea de investigații comune și măsuri comune de aplicare a legii, pot contribui la atingerea unui astfel de obiectiv, atenuând în același timp constrângerile legate de resurse.

Multe părți interesate doresc chiar mai multă cooperare și o abordare uniformă aplicată de autoritățile naționale de protecție a datelor[32]. De asemenea, acestea solicită un grad sporit de consecvență în ceea ce privește consilierea furnizată de autoritățile de protecție a datelor[33], precum și o aliniere deplină a orientărilor naționale la cele ale comitetului. Totodată, unele părți interesate așteaptă noi clarificări ale conceptelor-cheie ale regulamentului, cum ar fi abordarea bazată pe riscuri, ținând seama în special de preocupări, îndeosebi de cele ale întreprinderilor mici și mijlocii.

În acest context, este esențial să li se permită părților interesate să contribuie mai bine la activitatea comitetului. Din acest motiv, Comisia salută consultarea publică sistematică organizată de comitet cu privire la orientări. Această practică, alături de organizarea de ateliere pe subiecte specifice pentru părțile interesate într-o etapă timpurie a analizei, ar trebui continuată și amplificată pentru a se asigura caracterul transparent, incluziv și relevant al activității comitetului.

IV. Oamenii își exercită drepturile, dar activitățile de sensibilizare ar trebui să continue

Un alt obiectiv-cheie al regulamentului a fost acela de a consolida drepturile cetățenilor. În mare parte, regulamentul este considerat de asociațiile din domeniul protecției drepturilor civile și de asociațiile de consumatori drept o contribuție importantă la o societate digitală echitabilă, bazată pe încredere reciprocă.

---

29 În calitate de participant fără drept de vot.

30 De asemenea, Comisia a contribuit la facilitarea instituirii comitetului și sprijină funcționarea acestuia punându-i la dispoziție sistemul său de comunicare.

31 Articolul 62 din regulament.

32 A se vedea raportul Grupului multipartit privind regulamentul: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=RO.
De exemplu, întreprinderile consideră că listele naționale de tipuri de operațiuni de prelucrare, care necesită o evaluare a impactului asupra protecției datelor în conformitate cu articolul 35 din regulament, ar fi putut fi armonizate mai bine.

33 Inclusiv între diverse autorități din state federale.

Un nivel sporit de sensibilizare cu privire la drepturile legate de protecția datelor

Cetățenii din UE cunosc din ce în ce mai bine normele privind protecția datelor și drepturile lor: 67 % dintre respondenții la un sondaj Eurobarometru[34] efectuat în mai 2019 cunosc existența regulamentului și 57 % știu că există o autoritate națională de protecție a datelor la care pot apela pentru informații sau pentru a depune plângeri. 73 % au auzit de cel puțin unul dintre drepturile garantate de regulament. Totuși, un număr considerabil de cetățeni din UE încă nu iau măsuri active pentru a-și proteja datele cu caracter personal atunci când intră în mediul online. De exemplu, 44 % dintre cetățeni nu și-au modificat setările standard privind confidențialitatea pe rețelele sociale.

Cetățenii își exercită tot mai mult drepturile

Această conștientizare sporită a drepturilor a condus la o exercitare mai intensă a acestora de către cetățeni, prin intermediul întrebărilor adresate de clienți sau prin recurgerea mai frecventă la ajutorul autorităților de protecție a datelor pentru a solicita informații ori pentru a depune plângeri[35]. Întreprinderile raportează, de asemenea, că cererile de acces la datele cu caracter personal s-au multiplicat în mai multe sectoare, cum ar fi sectorul bancar și cel al telecomunicațiilor. Totodată, cetățenii și-au retras mai des consimțământul și și-au exercitat dreptul de a obiecta la comunicările comerciale[36].

Totuși, unii operatori au raportat neînțelegerea de către cetățeni a normelor privind protecția datelor, de exemplu ideea că cetățenii ar trebui să fie de acord cu toate prelucrările sau că dreptul la ștergerea datelor este absolut (deși, de exemplu, datele cu caracter personal trebuie păstrate uneori de operatori ca urmare a unor obligații legale)[37]. La rândul lor, organizațiile societății civile se plâng de întârzierile mari ale unor întreprinderi și autorități de protecție a datelor în a oferi răspunsuri.

Un aspect important constă în faptul că au fost lansate mai multe acțiuni reprezentative de către organizații neguvernamentale după ce au fost mandatate de cetățeni, recurgând astfel la noua posibilitate pusă la dispoziție de regulament[38]. Recurgerea la acțiuni reprezentative ar fi fost mai simplă dacă mai multe state membre ar fi utilizat posibilitatea pusă la dispoziție de regulament de a permite organizațiilor neguvernamentale să lanseze acțiuni fără un mandat[39].

---

34 http://europa.eu/rapid/press-release_IP-19-2956_ro.htm
35 https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf
36 A se vedea raportul Grupului multipartit privind Regulamentul general privind protecția datelor.
37 A se vedea raportul Grupului multipartit privind Regulamentul general privind protecția datelor.
38 Articolul 80 alineatul (1) din regulament.
39 Articolul 80 alineatul (2) din regulament.

Necesitatea continuării eforturilor de sensibilizare

Prin urmare, este necesar ca dialogul și eforturile de sensibilizare care vizează cu precădere publicul larg să continue la nivel național și la nivelul UE. În acest scop, Comisia a lansat o nouă campanie online în iulie 2019[40], pentru a încuraja cetățenii să citească declarațiile de confidențialitate și să își optimizeze setările privind confidențialitatea.

V. Întreprinderile își adaptează practicile

Regulamentul urmărește să sprijine întreprinderile în economia digitală, oferind soluții valabile în viitor. În general, întreprinderile apreciază principiul responsabilității enunțat în regulament, care se îndepărtează de împovărătoarea abordare *ex ante* anterioară (eliminarea cerințelor de notificare, scalabilitatea obligațiilor și flexibilitatea principiului protecției datelor începând cu momentul conceperii și în mod implicit, care permit concurența pe baza unor soluții care respectă viața privată). În același timp, unele întreprinderi solicită un grad sporit de securitate juridică și orientări suplimentare sau mai clare din partea autorităților de protecție a datelor[41].

Gestionare judicioasă a datelor

Deși întreprinderile raportează o serie de provocări în ajustarea la noile norme[42], multe dintre ele subliniază că aceasta a reprezentat, de asemenea, o oportunitate pentru a aduce chestiunea protecției datelor în atenția consiliilor de administrație, pentru a se organiza în mod adecvat în ceea ce privește datele deținute, pentru a îmbunătăți securitatea, pentru a fi mai bine pregătite în cazul unor incidente, pentru a reduce expunerea la riscuri inutile și pentru a crea relații bazate pe mai multă încredere cu clienții și cu partenerii lor comerciali. În ceea ce privește transparența, întreprinderile și organizațiile societății civile menționează echilibrul delicat care trebuie obținut între a oferi cetățenilor toate informațiile necesare în temeiul regulamentului și a folosi, în același timp, un limbaj clar și simplu și o formă pe care cetățenii o pot înțelege. Operatorii elaborează soluții inovatoare în această direcție.

În general, întreprinderile au indicat că au putut pune în aplicare noile drepturi ale persoanelor vizate, deși uneori le-a fost dificil să respecte termenele, din cauza unui număr sporit de solicitări și a caracterului lor mai variat[43], sau să verifice identitatea persoanei care a adresat solicitarea.

---

[40] Aceasta urmează campaniei anterioare destinate diseminării de materiale informative pentru cetățeni și întreprinderi, disponibile la adresa: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_ro.

[41] A se vedea raportul Grupului multipartit privind regulamentul.

[42] Actualizarea sistemului informatic este, adesea, menționată drept una dintre principalele provocări, îndeosebi în ceea ce privește punerea în aplicare a principiului protecției datelor începând cu momentul conceperii și a principiului protecției implicite a datelor, dreptul la ștergerea datelor în cazul copiilor de rezervă etc.

[43] De asemenea, întreprinderile solicită orientări din partea comitetului cu privire la solicitările nefondate și la cele excesive.

Impactul asupra inovării

Regulamentul nu numai că permite, dar și încurajează dezvoltarea de noi tehnologii, respectând, în același timp, dreptul fundamental la protecția datelor cu caracter personal- de exemplu, în domenii precum inteligența artificială.

Întreprinderile au început să își elaboreze oferta de noi servicii, care respectă într-o măsură mai mare viața privată. De exemplu, motoarele de căutare care nu urmăresc utilizatorii sau nu utilizează publicitatea comportamentală câștigă treptat cote de piață în unele state membre. Alte întreprinderi dezvoltă servicii care se bazează pe noi drepturi acordate cetățenilor, precum portabilitatea datelor lor cu caracter personal. Un număr tot mai mare de întreprinderi au promovat respectul față de datele cu caracter personal ca element de diferențiere la nivelul concurenței și de promovare a vânzărilor. Aceste evoluții nu sunt limitate la nivelul UE, ele caracterizând, de asemenea, economii străine foarte inovatoare[44].

Situația specifică a microîntreprinderilor și a întreprinderilor mici cu risc scăzut

Deși situația variază între statele membre, microîntreprinderile și întreprinderile mici[45], care nu prelucrează date cu caracter personal ca activitate de bază, s-au numărat printre părțile interesate cu cele mai numeroase întrebări privind aplicarea regulamentului. Deși acestea par să decurgă parțial din lipsa de cunoaștere a normelor privind protecția datelor, preocupările lor sunt, uneori, exacerbate de campanii din partea societăților de consultanță care urmăresc să ofere consultanță plătită, de răspândirea unor informații incorecte, de exemplu, cu privire la nevoia de a obține în mod sistematic consimțământul din partea cetățenilor[46], precum și de cerințe suplimentare impuse la nivel național.

În acest context, microîntreprinderile și întreprinderile mici solicită orientări care să fie adaptate la situația lor specifică și care să ofere informații foarte practice. Unele autorități de protecție a datelor au realizat deja acest lucru la nivel național[47]. Pentru a completa inițiativele naționale, Comisia a publicat materiale informative care să ajute aceste întreprinderi să respecte noile norme printr-o serie de etape practice[48].

Utilizarea setului de instrumente prevăzut de regulament

Regulamentul prevede instrumente care să demonstreze conformitatea, cum ar fi clauze contractuale standard, coduri de conduită și mecanisme de certificare nou-introduse.

---

44 De exemplu, potrivit unui raport publicat de asociația sectorului securității cibernetice din Israel, în 2018, subsectorul „Protecția datelor și viața privată” din cadrul „Securității cibernetice” a înregistrat cea mai rapidă dezvoltare, parțial ca urmare a intrării în vigoare a RGPD.

45 Potrivit definiției IMM-urilor, disponibilă la: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_ro.

46 De fapt, regulamentul nu se bazează numai pe consimțământ, ci prevede mai multe temeiuri juridice pentru prelucrarea datelor cu caracter personal.

47 De exemplu, ghidul elaborat de autoritatea de protecție a datelor din Franța: https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement.

48 https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-ro-n.pdf.

Clauzele contractuale standard sunt clauze-model care pot fi incluse în mod voluntar într-un contract, de exemplu, între un operator de date și o persoană împuternicită de operator, și care prevăd obligațiile părților contractante în temeiul regulamentului. Regulamentul extinde posibilitățile de a utiliza clauze contractuale standard atât pentru transferurile internaționale, cât și în cadrul UE[49]. În domeniul transferurilor internaționale, utilizarea lor amplă indică[50] faptul că sunt foarte utile pentru întreprinderi în ceea ce privește eforturile lor de conformare și oferă un avantaj deosebit celor care nu au resursele necesare pentru a negocia contracte individuale cu fiecare dintre contractanții lor care prelucrează date.

O serie de sectoare consideră, de asemenea, că adoptarea unor clauze contractuale standard este o modalitate utilă de a stimula armonizarea, în special atunci când Comisia este cea care le adoptă. Comisia va colabora cu părțile interesate pentru a utiliza posibilitățile oferite de regulament și a actualiza clauzele existente.

Aderarea la coduri de conduită reprezintă un alt instrument operațional și practic care se află la dispoziția sectorului pentru a facilita demonstrarea conformității cu regulamentul[51]. Aceste coduri ar trebui elaborate de asociații comerciale sau de organisme care reprezintă categorii de operatori și persoane împuternicite de operatori și ar trebui să descrie modul în care normele privind protecția datelor pot fi puse în aplicare într-un sector specific. Prin calibrarea obligațiilor cu riscurile[52], acestea se pot dovedi, de asemenea, o modalitate foarte utilă și rentabilă pentru întreprinderile mici și mijlocii în vederea îndeplinirii obligațiilor care le revin.

În fine, certificarea poate fi, de asemenea, un instrument util pentru a demonstra conformitatea cu cerințele specifice ale regulamentului. Aceasta poate spori securitatea juridică pentru întreprinderi și poate promova regulamentul la nivel global. Orientările privind certificarea și acreditarea[53], adoptate recent de Comitetul european pentru protecția datelor, vor permite elaborarea unor sisteme de certificare în UE. Comisia va monitoriza aceste evoluții și, după caz, va utiliza competențele acordate în temeiul regulamentului pentru a crea un cadru pentru cerințele de certificare. Comisia poate emite, de asemenea, o cerere de standardizare destinată organismelor de standardizare din UE, cu privire la elementele relevante pentru regulament.

---

49 A se vedea articolul 28 din regulament. Clauzele contractuale standard adoptate de Comisie sunt valabile la nivelul întregii UE. În schimb, cele adoptate în temeiul articolului 28 alineatul (8) de către o autoritate de protecție a datelor obligă doar autoritatea care le-a adoptat și, astfel, pot fi utilizate drept clauze contractuale standard pentru operațiunile de prelucrare care intră în jurisdicția autorității respective, în conformitate cu articolele 55 și 56.

50 De fapt, acestea reprezintă instrumentul principal pe care se bazează întreprinderile pentru exporturile lor de date.

51 Comitetul european pentru protecția datelor a adoptat, la 4 iunie 2019, orientări privind codurile de conduită. Acestea clarifică procedurile și normele implicate în depunerea, aprobarea și publicarea codurilor atât la nivel național, cât și al UE.

52 Considerentul 98 din regulament.

53 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_ro;
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_ro

VI. Convergența ascendentă progresează la nivel internațional

Cererea pentru protecția datelor cu caracter personal nu este limitată la UE. După cum se arată în cadrul unui sondaj global recent privind securitatea internetului, deficitul de încredere crește la nivel mondial, determinând cetățenii să își schimbe comportamentul online[54]. Un număr tot mai mare de întreprinderi abordează aceste preocupări prin extinderea , din proprie inițiativă, a drepturilor instituite de regulament la clienții lor din afara UE.

În plus, întrucât abordează tot mai mult provocări similare, țările din lume se dotează cu noi norme privind protecția datelor sau le modernizează pe cele existente. Aceste legi au adesea o serie de caracteristici comune cu regimul de protecție a datelor din UE, de exemplu o legislație generală mai degrabă decât norme sectoriale, drepturi individuale exercitabile și o autoritate de supraveghere independentă. Această tendință este cu adevărat globală, regăsindu-se în diverse țări: de la Coreea de Sud la Brazilia, de la Chile la Thailanda, de la India la Indonezia. Apartenența tot mai universală la „Convenția 108”[55] a Consiliului Europei – modernizată recent[56] cu o contribuție semnificativă din partea Comisiei – constituie un alt semnal clar al acestei tendințe către convergența ascendentă.

Promovarea unor fluxuri de date sigure și libere prin decizii privind caracterul adecvat al nivelului de protecție și dincolo de acestea

Această convergență în curs oferă noi oportunități pentru facilitarea fluxurilor de date și, prin urmare, a schimburilor comerciale, precum și a cooperării dintre autoritățile publice, îmbunătățind totodată nivelul de protecție pentru datele persoanelor din UE, atunci când sunt transferate în străinătate.

Prin punerea în aplicare a strategiei prevăzute în comunicarea sa din 2017 intitulată „Schimbul de date cu caracter personal și protecția acestora într-o lume globalizată”[57], Comisia și-a intensificat colaborarea cu țări terțe și cu alți parteneri internaționali pe baza unor elemente de convergență între sistemele de protecție a vieții private și dezvoltând în

---

[54] A se vedea Sondajul global privind securitatea și încrederea pe internet, CIGI-Ipsos 2019. Potrivit sondajului respectiv, 78 % dintre persoanele intervievate erau preocupate de protecția vieții private în mediul online, 49 % declarând că neîncrederea le-a determinat să publice mai puține informații personale online, 43 % raportând că au fost mai atente în ceea ce privește securitatea dispozitivului lor, iar 39 % răspunzând că au folosit internetul într-un mod mai selectiv, printre alte măsuri de precauție. Sondajul a fost derulat în 25 de economii: Australia, Brazilia, Canada, China, Egipt, Franța, Germania, Regatul Unit, Hong Kong, India, Indonezia, Italia, Japonia, Kenya, Mexic, Nigeria, Pakistan, Polonia, Rusia, Africa de Sud, Republica Coreea, Suedia, Tunisia, Turcia și Statele Unite.

[55] Convenția Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108) și Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor (ETS nr. 181) din 2001. Acesta este singurul instrument multilateral obligatoriu în domeniul protecției datelor. Printre ultimele țările care au ratificat convenția se numără Argentina, Mexic, Capul Verde și Maroc.

[56] Protocolul de modificare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), astfel cum a fost convenit în cadrul celei de a 128-a sesiuni a Comitetului de Miniștri, care a avut loc la Elsinore, Danemarca, în perioada 17-18 mai 2018. Textul consolidat al variantei modernizate a Convenției 108 este disponibil la: https://rm.coe.int/16808ade9d.

[57] Comunicare a Comisiei către Parlamentul European și Consiliu „Schimbul de date cu caracter personal și protecția acestora într-o lume globalizată”, COM/2017/07 final.

continuare astfel de elemente. Aceasta a inclus explorarea posibilității de a adopta constatări privind caracterul adecvat al nivelului de protecție în ceea ce privește anumite țări terțe[58]. Această activitate a generat rezultate importante, în special intrarea în vigoare, în februarie 2019, a acordului UE-Japonia privind adecvarea reciprocă, care a creat cel mai mare spațiu de liberă circulație a datelor în condiții de siguranță din lume. Negocierile cu Coreea de Sud privind caracterul adecvat al nivelului de protecție se află într-un stadiu avansat, iar activitățile de explorare sunt în curs în vederea demarării discuțiilor privind caracterul adecvat cu mai multe țări din America Latină – cum ar fi Chile sau Brazilia – în funcție de finalizarea proceselor legislative în desfășurare. Evoluțiile sunt, de asemenea, promițătoare în unele părți din Asia, cum ar fi India, Indonezia și Taiwan, precum și în vecinătatea estică și sudică europeană, ceea ce ar putea deschide calea către viitoare decizii privind caracterul adecvat al nivelului de protecție.

În același timp, Comisia salută faptul că alte țări, care au instituit instrumente de transfer similare caracterului adecvat al nivelului de protecție prevăzut în regulament, au recunoscut că UE, precum și țările recunoscute de UE ca fiind „adecvate” asigură nivelul de protecție necesar[59]. Această situație are potențialul de a crea o rețea de țări în care datele să poată circula liber.

În plus, sunt în desfășurare activități intense cu alte țări terțe, precum Canada, Noua Zeelandă, Argentina și Israel, pentru a se asigura continuitatea în temeiul regulamentului a deciziilor privind caracterul adecvat al nivelului de protecție pe baza Directivei privind protecția datelor din 1995. În același timp, Scutul de confidențialitate UE-SUA s-a dovedit un instrument util pentru a asigura fluxuri transatlantice de date pe baza unui nivel ridicat de protecție, cu peste 4 700 de întreprinderi participante[60]. Analiza sa anuală asigură că funcționarea corectă a cadrului este verificată periodic și că noile aspecte problematice pot fi soluționate în timp util.

Întrucât nu există o soluție universală pentru fluxurile de date, Comisia colaborează, de asemenea, cu părțile interesate și cu comitetul pentru a fructifica întregul potențial al setului de instrumente prevăzute în regulament pentru transferurile internaționale. Aceasta privește instrumente precum clauzele contractuale standard, crearea de sisteme de certificare, coduri de conduită sau acorduri administrative pentru organisme publice. În această privință, Comisia este interesată de schimbul de experiență și de cele mai bune practici cu alte sisteme care au dezvoltat o expertiză specifică cu privire la unele dintre aceste instrumente. Comisia va lua în considerare utilizarea competențelor acordate în temeiul regulamentului cu privire la respectivele instrumente de transfer, îndeosebi clauzele contractuale standard.

Dincolo de instrumentele pur bilaterale, ar putea fi util să se exploreze posibilitatea instituirii de către țări care împărtășesc aceeași viziune a unui cadru multinațional în acest domeniu, într-un moment în care fluxurile de date reprezintă o componentă tot mai importantă a

---

58 Regulamentul a creat, de asemenea, posibilitatea prezentării unor constatări privind caracterul adecvat al nivelului de protecție și cu privire la organizațiile internaționale, ca parte a eforturilor UE de facilitare a schimburilor de date cu astfel de entități.

59 Aceasta este abordarea adoptată, de exemplu, de Argentina, Columbia, Israel și Elveția.

60 Aceasta înseamnă că, după primii trei ani de existență, Scutul de confidențialitate are mai multe întreprinderi participante decât avea predecesorul său, *Safe Harbour* („sfera de siguranță”), după 13 ani de funcționare.

schimburilor comerciale, a comunicațiilor și a interacțiunilor sociale. Un astfel de instrument ar permite datelor să circule liber între părțile contractante, asigurând totodată nivelul necesar de protecție pe baza valorilor comune și a sistemelor convergente. Acesta ar putea fi elaborat, de exemplu, pe baza Convenției 108 modernizate sau a inițiativei „fluxuri libere de date cu încredere", lansată de Japonia la începutul acestui an.

Dezvoltarea de noi sinergii între schimburile comerciale și instrumentele de protecție a datelor

Comisia promovează convergența standardelor în materie de protecție a datelor la nivel internațional și este, de asemenea, hotărâtă să abordeze protecționismul digital. În acest scop, Comisia a elaborat dispoziții specifice privind fluxurile de date și protecția datelor în cadrul acordurilor comerciale, pe care le aduce în discuție sistematic în negocierile sale bilaterale și multilaterale, cum ar fi discuțiile actuale privind comerțul electronic din cadrul OMC. Aceste dispoziții orizontale elimină măsurile pur protecționiste, cum ar fi cerințele de localizare forțată a datelor, păstrând în același timp autonomia părților în materie de reglementare pentru a proteja dreptul fundamental la protecția datelor.

Deși trebuie să urmeze căi diferite, dialogurile privind protecția datelor și negocierile comerciale se pot completa reciproc: acordul UE-Japonia privind adecvarea reciprocă constituie cel mai bun exemplu al unor astfel de sinergii, facilitând în continuare schimburile comerciale și, astfel, amplificând beneficiile Acordului de parteneriat economic. De fapt, acest tip de convergență, bazat pe valori comune și standarde înalte și susținut de o aplicare eficace, oferă cea mai solidă fundație pentru schimbul de date cu caracter personal, aspect recunoscut într-o măsură tot mai mare de partenerii noștri internaționali[61]. Întrucât întreprinderile își desfășoară tot mai mult activitatea dincolo de frontiere și preferă să aplice seturi similare de norme în toate operațiunile lor comerciale desfășurate la nivel mondial, o astfel de convergență contribuie la crearea unui mediu care favorizează investițiile directe, facilitând schimburile comerciale și îmbunătățind nivelul de încredere dintre partenerii comerciali.

Facilitarea schimburilor de informații în vederea combaterii criminalității și a terorismului pe baza unor elemente de protecție adecvate

O compatibilitate mai mare între regimurile de protecție a datelor poate, de asemenea, să faciliteze semnificativ schimburile de informații atât de necesare dintre UE și autoritățile de reglementare, polițienești și judiciare străine și, astfel, să contribuie la o cooperare mai eficace și mai rapidă în materie de aplicare a legii[62]. În acest scop, Comisia are în vedere utilizarea posibilității de a adopta decizii privind caracterul adecvat al nivelului de protecție în temeiul Directivei privind protecția datelor în materie de asigurare a respectării legii, pentru a-și aprofunda cooperarea cu partenerii-cheie în combaterea criminalității și a terorismului. În

---

[61] După cum s-a indicat, de exemplu, în referința la conceptul de „Data Free Flow with Trust" din declarația liderilor G20 de la Osaka: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[62] A se vedea Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor intitulată „Agenda europeană privind securitatea", COM(2015) 185 final.

plus, „Acordul-cadru” UE-SUA[63], care a intrat în vigoare în februarie 2017, poate fi utilizat ca model pentru acorduri similare cu alți parteneri importanți din domeniul securității.

Alte exemple care evidențiază importanța standardelor înalte de protecție a datelor ca bază pentru o cooperare stabilă în materie de asigurare a respectării legii cu țări terțe sunt transferul registrelor cu numele pasagerilor (PNR)[64] și schimbul de informații operaționale dintre Europol și partenerii internaționali importanți. În această privință, negocierile privind acordurile internaționale sunt în prezent în desfășurare sau pregătite să demareze cu mai multe țări din vecinătatea sudică[65].

Garanțiile solide privind protecția datelor vor fi, de asemenea, o componentă esențială a oricărui acord viitor privind accesul transfrontalier la probe electronice în cadrul anchetelor penale, la nivel bilateral (acordul UE-SUA) sau multilateral (Al doilea protocol suplimentar la Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică)[66].

Promovarea cooperării între autoritățile de aplicare a legii în materie de protecție a datelor

Într-un moment în care chestiunile legate de conformitatea cu normele de protecție a vieții private sau incidentele de securitate pot afecta un număr mare de persoane în același timp, în mai multe jurisdicții, formele mai strânse de cooperare între autoritățile de supraveghere la nivel internațional pot contribui la asigurarea unei protecții mai eficace a drepturilor individuale, precum și a unui mediu mai stabil pentru operatorii economici. În acest context și în strâns contact cu comitetul, Comisia va depune eforturi pentru a găsi modalități de facilitare a cooperării în vederea asigurării respectării legii și a asistenței reciproce între autoritățile de supraveghere din UE și din străinătate, inclusiv prin utilizarea noilor competențe prevăzute de regulament pentru acest domeniu[67]. Acestea ar putea lua diferite forme de cooperare, de la elaborarea unor instrumente de interpretare sau practice comune[68] la schimbul de informații privind investigațiile în curs.

---

63 Acord între UE și SUA privind protecția datelor cu caracter personal atunci când acestea sunt transferate și prelucrate în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor, inclusiv a terorismului, în cadrul cooperării polițienești și al cooperării judiciare în materie penală: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:22016A1210(01) („Acordul-cadru”). Acordul-cadru constituie primul acord internațional bilateral în domeniul asigurării respectării legii, care prevede un catalog cuprinzător de drepturi și obligații în materie de protecție a datelor în concordanță cu acquis-ul UE. Acesta reprezintă un exemplu de succes al modului în care cooperarea în materie de asigurare a respectării legii cu un partener internațional important poate fi consolidată prin negocierea unui set solid de garanții privind protecția datelor.

64 Rezoluția (RCS) 2396 a Consiliului de Securitate al ONU din 21 decembrie 2017 solicită tuturor statelor membre ale ONU să dezvolte capabilitățile necesare pentru colectarea, prelucrarea și analiza datelor PNR, respectând pe deplin drepturile omului și libertățile fundamentale. A se vedea, de asemenea, Comunicarea Comisiei intitulată „Agenda europeană privind securitatea”, COM(2015) 185 final: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52015DC0185&qid=1566883057461&from=EN.

65 https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en

66 https://europa.eu/rapid/press-release_IP-19-2891_ro.htm

67 A se vedea articolul 50 din regulament privind cooperarea internațională în domeniul protecției datelor. Această dispoziție acoperă o gamă largă de forme de cooperare, de la informații privind legislația în materie de protecție a datelor, la transferul plângerilor și asistență în investigații.

68 De exemplu, modele comune pentru notificări privind încălcările.

În cele din urmă, Comisia intenționează, de asemenea, să-și intensifice dialogul cu organizațiile și rețelele regionale, cum ar fi Asociația Națiunilor din Asia de Sud-Est (ASEAN), Uniunea Africană, forumul autorităților de protecție a vieții private din zona Asia-Pacific (APPA) sau Rețeaua ibero-americană de protecție a datelor, care joacă un rol tot mai important în conturarea standardelor comune de protecție a datelor, promovarea schimburilor de bune practici și stimularea cooperării dintre autoritățile de aplicare a legii. De asemenea, Comisia va colabora cu Organizația pentru Cooperare și Dezvoltare Economică și cu Organizația pentru cooperare economică Asia-Pacific, pentru a consolida convergența către un nivel înalt de protecție a datelor.

VII. Legislația privind protecția datelor ca parte integrantă a unui spectru larg de politici

Protecția datelor cu caracter personal este garantată și integrată în mai multe politici ale Uniunii.

Serviciile de telecomunicații și comunicațiile electronice

Comisia a adoptat propunerea sa de regulament privind viața privată și comunicațiile electronice, în ianuarie 2017[69]. Propunerea vizează să protejeze confidențialitatea comunicațiilor, astfel cum se prevede în Carta drepturilor fundamentale, dar și datele cu caracter personal care pot face parte dintr-o comunicare, precum și echipamentele terminale ale utilizatorilor finali.

Regulamentul propus privind viața privată și comunicațiile electronice particularizează și completează regulamentul prin stabilirea unor norme specifice în scopurile menționate mai sus. Acesta modernizează normele UE actuale privind viața privată și comunicațiile electronice[70] pentru a reflecta evoluțiile pe plan tehnologic și juridic și consolidează protecția vieții private a cetățenilor prin extinderea domeniului de aplicare a noilor norme pentru a acoperi și furnizorii de servicii de comunicații *over-the-top* (OTT), creând astfel condiții de concurență echitabile pentru toate serviciile de comunicații electronice. Deși Parlamentul European a adoptat un mandat de lansare a trilogurilor în octombrie 2017, Consiliul nu a fost încă de acord cu o abordare generală. Comisia susține în continuare pe deplin Regulamentul privind viața privată și comunicațiile electronice și va sprijini eforturile colegiuitorilor de a obține o adoptare rapidă a regulamentului propus.

Sănătatea și cercetarea

Facilitarea schimburilor, între statele membre, de date privind sănătatea, care sunt date sensibile în temeiul regulamentului, devine tot mai importantă în domeniul sănătății publice, din motive de interes general. Acestea includ dispoziții privind îngrijirile medicale sau

---

69 https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52017PC0010

70 Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), JO L 201, 31.7.2002, p. 37-47.

tratamentele, protecția împotriva unor amenințări transfrontaliere grave la adresa sănătății și asigurarea unor standarde înalte de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale. Regulamentul prevede norme care asigură prelucrarea și schimburile de date privind sănătatea în UE în condiții legale și demne de încredere. Aceste norme se aplică și accesului părților terțe la datele medicale ale pacienților, inclusiv la date cuprinse în fișele pacienților, prescripții electronice și, pe termen lung, registre medicale electronice cuprinzătoare, precum și utilizării lor în scopuri de cercetare științifică. În domeniul specific al studiilor clinice, Comisia a pregătit, de asemenea, întrebări și răspunsuri specifice privind interacțiunea dintre Regulamentul privind studiile clinice[71] și Regulamentul general privind protecția datelor[72].

Inteligența artificială („IA”)

Pe măsură ce IA câștigă o importanță strategică, este esențial să se definească norme globale pentru dezvoltarea și utilizarea sa. În promovarea dezvoltării și utilizării IA, Comisia a optat pentru o abordare centrată pe factorul uman, ceea ce înseamnă că aplicațiile IA trebuie să respecte drepturile fundamentale[73]. În acest context, normele stabilite în regulament prevăd un cadru general și conțin obligații și drepturi specifice care sunt deosebit de relevante pentru prelucrarea datelor cu caracter personal în IA. De exemplu, regulamentul include dreptul de a nu fi supus numai unui proces decizional automatizat, cu excepția anumitor situații[74]. De asemenea, regulamentul include cerințe specifice privind transparența în legătură cu utilizarea procesului decizional automatizat, și anume obligația de a informa cu privire la existența unor astfel de decizii și de a furniza informații pertinente și a explica importanța acestora și consecințele preconizate ale prelucrării pentru persoana respectivă[75]. Aceste principii de bază ale regulamentului au fost recunoscute de Grupul de experți la nivel înalt privind IA[76], de Organizația pentru Cooperare și Dezvoltare Economică[77] și de G20[78] ca fiind deosebit de relevante pentru abordarea provocărilor și oportunităților generate de IA.

---

71 https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32014R0536

72 https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf

73 Comunicarea Comisiei din 8 aprilie 2019 intitulată „Cum construim încrederea cetățenilor într-o inteligență artificială centrată pe factorul uman”: https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence.
Orientări în materie de etică pentru o inteligență artificială fiabilă, prezentate de Grupul de experți la nivel înalt la 8 aprilie 2019: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. A se vedea, de asemenea, Recomandarea Consiliului OCDE privind inteligența artificială: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, Principiile IA ale G20, aprobate în cadrul Declarației liderilor G20 de la Osaka: https://www.g20.org/pdf/documents/en/annex_08.pdf și Declarația miniștrilor G20 privind comerțul și economia digitală: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

74 Articolul 22 din regulament.

75 Articolul 13 alineatul 2 litera (f) din regulament.

76 https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

77 Recomandarea Consiliului privind inteligența artificială: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

78 Declarația miniștrilor G20 privind comerțul și economia digitală: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

Comitetul european pentru protecția datelor a identificat IA ca fiind una dintre posibilele teme în programul său de lucru pentru perioada 2019-2020[79].

Transporturile

Dezvoltarea automobilelor conectate și a orașelor inteligente se bazează tot mai mult pe prelucrarea și schimburile unor volume mari de date cu caracter personal între mai multe părți, inclusiv automobile, producători de automobile, furnizori de servicii telematice și autorități publice responsabile de infrastructura rutieră. Acest mediu multipartit presupune o anumită complexitate în ceea ce privește alocarea rolurilor și a responsabilităților diverșilor actori implicați în prelucrarea datelor cu caracter personal și în ceea ce privește modalitățile prin care să se asigure legalitatea prelucrării de către toți actorii. Respectarea regulamentului și a legislației privind confidențialitatea și comunicațiile electronice este esențială pentru preluarea cu succes a sistemelor de transport inteligente la nivelul tuturor modurilor de transport și pentru răspândirea instrumentelor și a serviciilor digitale care permit o mai mare mobilitate a persoanelor și mărfurilor[80].

Energia

Dezvoltarea soluțiilor digitale în sectorul energiei se bazează tot mai mult pe prelucrarea datelor cu caracter personal. Legislația adoptată ca parte a pachetului „Energie curată pentru toți europenii”[81] include noi dispoziții care permit digitalizarea sectorului energiei electrice și norme privind accesul la date, gestionarea și interoperabilitatea prin care datele în timp real ale consumatorilor pot fi prelucrate, pentru a realiza economii și a încuraja producția proprie și participarea pe piața energiei. Prin urmare, respectarea normelor privind protecția datelor este foarte importantă pentru punerea în aplicare cu succes a acestor dispoziții.

Concurența

Prelucrarea datelor cu caracter personal reprezintă tot mai frecvent un element care trebuie luat în considerare în cadrul politicii în domeniul concurenței[82]. Dat fiind faptul că autoritățile de protecție a datelor sunt singurele autorități responsabile de evaluarea încălcării normelor privind protecția datelor, autoritățile din domeniul concurenței, al protecției consumatorului și al protecției datelor cooperează și vor continua să coopereze dacă este necesar atunci când competențelor lor interferează. Comisia va stimula această cooperare și va urmări îndeaproape evoluțiile.

---

79 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_ro.pdf

80 De exemplu, prin facilitarea planificării lor și a utilizării diverselor mijloace de transport pe parcursul întregii călătorii.

81 În special, Directiva privind energia electrică: https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX%3A32009L0072.

82 De exemplu, cauza M.8788 – Apple/Shazam și cauza M. M.8124 – Microsoft/LinkedIn.

Contextul electoral

În Orientările sale privind utilizarea datelor cu caracter personal în contextul alegerilor[83], emise în septembrie 2018, ca parte a pachetului electoral[84], Comisia a atras atenția asupra normelor de o deosebită importanță pentru actorii implicați în alegeri, inclusiv asupra aspectelor legate de acțiunile prin care li se adresează alegătorilor un conținut personalizat (*microtargeting*). Aceste orientări au fost preluate într-o declarație a Comitetului european pentru protecția datelor[85], iar o serie de autorități de protecție a datelor au emis orientări la nivel național. Pachetul electoral a inclus, de asemenea, o solicitare adresată fiecărui stat membru de a înființa o rețea națională a alegerilor, care să implice autoritățile naționale cu competențe în chestiunile electorale și pe cele responsabile de monitorizarea și aplicarea normelor, cum ar fi protecția datelor, în legătură cu activitățile online relevante pentru alegeri. Au fost adoptate, de asemenea, noi măsuri în vederea stabilirii de sancțiuni pentru încălcările normelor privind protecția datelor de către partidele și fundațiile politice europene. Comisia a recomandat ca statele membre să adopte aceeași abordare la nivel național. Evaluarea alegerilor în Parlamentul European din 2019, care urmează să fie publicată în octombrie 2019, va ține seama și de aspectele privind protecția datelor.

Aplicarea legii

O uniune a securității eficace și autentică poate fi fondată numai pe conformitatea deplină cu drepturile fundamentale consacrate în Carta UE și cu legislația secundară a UE, inclusiv pe garanții adecvate privind protecția datelor, pentru a permite schimbul de date cu caracter personal în condiții de siguranță în scopuri legate de aplicarea legii. Orice restricționare a dreptului fundamental la viață privată și protecția datelor face obiectul unui test strict privind necesitatea și proporționalitatea.

VIII. Concluzie

Pe baza informațiilor disponibile în prezent și a dialogului cu părțile interesate, evaluarea preliminară a Comisiei indică faptul că primul an de aplicare a regulamentului a fost, per ansamblu, pozitiv. Cu toate acestea, după cum se arată în prezenta comunicare, este necesar să se înregistreze în continuare progrese într-o serie de domenii.

Punerea în aplicare și completarea cadrului juridic:

- Cele trei state membre care nu și-au actualizat încă legislația națională în domeniul protecției datelor trebuie să facă urgent acest lucru. Toate statele membre ar trebui să finalizeze alinierea legislațiilor lor sectoriale la cerințele din regulament.

---

83 https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52018DC0638&qid=1566856342213&from=EN

84 https://europa.eu/rapid/press-release_IP-18-5681_ro.htm

85 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

- Comisia va utiliza toate instrumentele de care dispune, inclusiv procedurile de constatare a neîndeplinirii obligațiilor, pentru a asigura conformarea statelor membre cu regulamentul și limitarea oricărei fragmentări a cadrului de protecție a datelor.

Asigurarea fructificării la maximum a potențialului noului sistem de guvernanță:

- Statele membre ar trebui să aloce resurse umane, financiare și tehnice suficiente pentru autoritățile naționale de protecție a datelor.

- Autoritățile de protecție a datelor ar trebui să își intensifice cooperarea, de exemplu prin desfășurarea de investigații comune. Statele membre ar trebui să faciliteze desfășurarea unor astfel de investigații.

- Comitetul ar trebui să dezvolte în continuare o cultură a protecției datelor în UE și să utilizeze integral instrumentele prevăzute în regulament pentru a asigura o aplicare armonizată a normelor. Comitetul ar trebui să își continue activitatea privind orientările, în special pentru întreprinderile mici și mijlocii.

- Expertiza secretariatului comitetului ar trebui consolidată pentru a sprijini și a coordona activitatea acestuia într-un mod mai eficace.

- Comisia va continua să sprijine autoritățile de protecție a datelor și comitetul, în special prin participarea activă la lucrările comitetului și atrăgând atenția acestuia asupra cerințelor dreptului UE pe parcursul punerii în aplicare a regulamentului.

- Comisia va sprijini interacțiunea dintre autoritățile de protecție a datelor și alte autorități, îndeosebi din domeniul concurenței, respectând pe deplin competențele lor respective.

Sprijinirea și implicarea părților interesate:

- Comitetul ar trebui să consolideze modul în care implică părțile interesate în activitatea sa. Comisia va continua să sprijine financiar autoritățile de protecție a datelor, pentru a le ajuta să comunice cu părțile interesate.

- Comisia își va continua activitățile de sensibilizare și activitățile derulate împreună cu părțile interesate.

Promovarea convergenței internaționale:

- Comisia își va intensifica în continuare dialogul privind caracterul adecvat al nivelului de protecție cu partenerii-cheie care se califică, inclusiv în domeniul respectării aplicării legii. În special, aceasta intenționează să finalizeze negocierile în curs cu Coreea de Sud în lunile următoare. Comisia va raporta în 2020 cu privire la analiza celor 11 decizii privind caracterul adecvat al nivelului de protecție adoptate în temeiul Directivei privind protecția datelor.

- Comisia își va continua activitatea, inclusiv prin asistență tehnică, schimburi de informații și de bune practici cu țările interesate să adopte legi moderne privind viața privată și va stimula cooperarea cu autoritățile de supraveghere și organizații regionale din țări terțe.
- Comisia va colabora cu organizații multilaterale și regionale pentru a promova standarde înalte de protecție a datelor ca factor ce favorizează schimburile comerciale și facilitează cooperarea (de exemplu, în cadrul inițiativei „Data Free Flow with Trust” , lansată de Japonia în contextul G20).

Regulamentul[86] impune Comisiei să raporteze în 2020 cu privire la punerea în aplicare a acestuia. Aceasta va constitui o ocazie pentru a evalua progresele înregistrate și dacă, după doi ani de aplicare, diversele componente ale noului regim de protecție a datelor sunt pe deplin operaționale. În acest scop, Comisia va intra în dialog cu Parlamentul European, cu Consiliul, cu statele membre, cu Comitetul european pentru protecția datelor, cu părțile interesate și cu cetățenii.

[86] Articolul 97 din regulament.