Recomandările 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere

Adoptate la 10 noiembrie 2020

Cuprins

Comitetul European pentru Protecția Datelor,

având în vedere articolul 70 alineatul (1) litera (e) din Regulamentul 2016/679/UE 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 (denumit în continuare „RGPD")[1],

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[2],

având în vedere articolele 12 și 22 din Regulamentul său de procedură,

având în vedere documentul de lucru al Grupului de lucru „Articolul 29" privind justificarea ingerințelor în drepturile fundamentale la viață privată și la protecția datelor prin măsuri de supraveghere atunci când se transferă date cu caracter personal (garanții esențiale europene denumite în continuare „GEE"), WP 237,

ADOPTĂ URMĂTOARELE RECOMANDĂRI:

1. INTRODUCERE

1. În urma hotărârii pronunțate în cauza Schrems I, autoritățile UE pentru protecția datelor reunite în cadrul Grupului de lucru 29 s-au inspirat din jurisprudență pentru a identifica garanțiile esențiale europene, care trebuie respectate pentru a se asigura că ingerințele în drepturile la viață privată și la protecția datelor cu caracter personal, prin măsuri de supraveghere, când se transferă date cu caracter personal, nu depășesc ceea ce este necesar și proporțional într-o societate democratică.

2. CEPD ar dori să sublinieze faptul că garanțiile esențiale europene se bazează pe jurisprudența Curții de Justiție a Uniunii Europene (denumită în continuare „CJUE") în legătură cu articolele 7, 8, 47 și 52 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta") și, după caz, pe jurisprudența Curții Europene a Drepturilor Omului (denumită în continuare „CEDO") în legătură cu articolul 8 din Convenția europeană a drepturilor omului (denumită în continuare „convenția") care abordează aspecte legate de supraveghere în statele părți la convenție[3].

[1] Prezentul document nu abordează situațiile de transfer sau de partajare ulterioară care intră în domeniul de aplicare al Directivei privind protecția datelor în materie de aplicare a legii [Directiva (UE) 2016/680].

[2] Referirile la „statele membre" din acest document trebuie înțelese ca referiri la „statele membre ale SEE".

[3] În aceste recomandări, termenul „drepturi fundamentale" derivă din Carta drepturilor fundamentale a Uniunii Europene. Cu toate acestea, este utilizat pentru a acoperi și „drepturile omului", astfel cum sunt incluse în Convenția europeană a drepturilor omului.

3. Actualizarea acestui document este menită să dezvolte în continuare garanțiile esențiale europene, elaborate inițial ca răspuns la hotărârea pronunțată în cauza Schrems I[4], reflectând clarificările furnizate de CJUE (și de CEDO) de la prima sa publicare, în special în hotărârea sa de referință în cauza Schrems II[5].

4. În hotărârea pronunțată în cauza Schrems II, CJUE a afirmat că examinarea Deciziei 2010/87/UE a Comisiei privind clauzele contractuale standard pentru transferul de date cu caracter personal către persoanele împuternicite de către operator stabilite în țări terțe, în lumina articolelor 7, 8 și 47 din cartă, nu a evidențiat niciun element care să afecteze validitatea deciziei respective, dar a invalidat Decizia privind Scutul de confidențialitate. CJUE a considerat că Decizia privind Scutul de confidențialitate era incompatibilă cu articolul 45 alineatul (1) din RGPD, având în vedere articolele 7, 8 și 47 din cartă. Prin urmare, hotărârea poate servi drept exemplu în cazul în care măsurile de supraveghere dintr-o țară terță (în acest caz, SUA, cu secțiunea 702 din FISA și ordinul executiv 12 333) nu sunt suficient de limitate și nici nu fac obiectul unei căi de atac eficiente disponibile persoanelor vizate pentru a-și exercita drepturile, astfel cum se prevede în legislația UE, pentru a considera că nivelul de protecție dintr-o țară terță este „în esență, echivalent” cu cel garantat în Uniunea Europeană în sensul articolului 45 alineatul (1) din RGPD.

5. Motivele pentru invalidarea Scutului de confidențialitate au, de asemenea, consecințe asupra altor instrumente de transfer[6]. Chiar dacă Curtea a interpretat articolul 46 alineatul (1) din RGPD în contextul validității clauzelor contractuale standard (denumite în continuare „CCS”), interpretarea se aplică oricărui transfer către țări terțe care se bazează pe oricare dintre instrumentele menționate la articolul 46 din RGPD[7].

6. În cele din urmă, este de competența CJUE să hotărască dacă ingerințele într-un drept fundamental pot fi justificate. Cu toate acestea, în absența unei astfel de hotărâri și în aplicarea jurisprudenței permanente, autoritățile de protecție a datelor au obligația de a evalua fiecare caz în parte, ex officio sau în urma unei plângeri, și fie de a sesiza o instanță națională, în cazul în care suspectează că transferul nu este în conformitate cu articolul 45 dacă există o decizie privind caracterul adecvat adoptată, fie de a suspenda sau de a interzice transferul, în cazul în care constată că articolul 46 din RGPD nu poate fi respectat, iar protecția datelor transferate impusă prin dreptul UE nu poate fi asigurată prin alte mijloace.

7. Scopul garanțiilor esențiale europene actualizate este de a furniza elemente care să permită să se examineze dacă măsurile de supraveghere care permit accesul autorităților publice dintr-o țară terță la date cu caracter personal, în calitate de agenții naționale de securitate sau de autorități de aplicare a legii, pot fi considerate sau nu o ingerință justificată.

[4] Hotărârea CJUE din 6 octombrie 2015, Maximillian Schrems/Data Protection Commissioner, cauza C-362/14, EU:C:2015:650 (denumită în continuare „Schrems I”).

[5] Hotărârea CJUE din 16 iulie 2020, Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, cauza C-311/18, ECLI:EU:C:2020:559 (denumită în continuare „Schrems II”).

[6] Vezi punctul 105 din Schrems II.

[7] Vezi punctul 92 din Schrems II.

8. Într-adevăr, garanțiile esențiale europene fac parte din evaluarea care trebuie efectuată pentru a stabili dacă o țară terță asigură un nivel de protecție în esență echivalent cu cel garantat în cadrul UE, dar nu urmăresc, în sine, să definească toate elementele care sunt necesare pentru a considera că o țară terță asigură un astfel de nivel de protecție în conformitate cu articolul 45 din RGPD. De asemenea, acestea nu urmăresc, în sine, să definească toate elementele care ar trebui să fie avute în vedere atunci când se evaluează dacă regimul juridic al unei țări terțe împiedică exportatorul de date și importatorul de date să asigure garanții adecvate în conformitate cu articolul 46 din RGPD.

9. Prin urmare, elementele furnizate în prezentul document ar trebui considerate drept garanțiile esențiale care trebuie să se regăsească în țara terță atunci când se evaluează ingerința, pe care o implică măsurile de supraveghere ale unei țări terțe, în dreptul la viață privată și la protecția datelor, nu o listă de elemente care demonstrează că regimul juridic al unei țări terțe în ansamblu asigură un nivel de protecție în esență echivalent.

10. Articolul 6 alineatul (3) din Tratatul privind Uniunea Europeană prevede că drepturile fundamentale consacrate în convenție constituie principii generale ale dreptului Uniunii. Cu toate acestea, astfel cum reamintește CJUE în jurisprudența sa, aceasta din urmă nu constituie, atât timp cât Uniunea Europeană nu a aderat la ea, un instrument juridic integrat formal în ordinea juridică a Uniunii[8]. Astfel, nivelul de protecție a drepturilor fundamentale prevăzut la articolul 46 alineatul (1) din RGPD trebuie să fie determinat pe baza dispozițiilor acestui regulament, interpretate în lumina drepturilor fundamentale consacrate în cartă. Acestea fiind spuse, în conformitate cu articolul 52 alineatul (3) din cartă, drepturile cuprinse în aceasta, corespuzătoare drepturilor garantate prin convenție, trebuie să aibă același înțeles și aceeași întindere ca și cele prevăzute de convenția amintită și, prin urmare, astfel cum a reamintit CJUE, jurisprudența CEDO privind drepturile care sunt prevăzute și în Carta drepturilor fundamentale a Uniunii Europene trebuie să fie luată în considerare ca prag minim de protecție pentru interpretarea drepturilor corespunzătoare din cartă[9]. Cu toate acestea, în conformitate cu articolul 52 alineatul (3) ultima teză din cartă, „[a]ceastă dispoziție nu împiedică dreptul Uniunii să confere o protecție mai largă".

11. Prin urmare, în fond, garanțiile esențiale vor continua să se bazeze parțial pe jurisprudența CEDO, în măsura în care carta, astfel cum a fost interpretată de CJUE, nu prevede un nivel mai ridicat de protecție care să specifice alte cerințe decât jurisprudența CEDO.

12. Prezentul document explică contextul și detaliază în continuare cele patru garanții esențiale europene.

[8] Vezi punctul 98 din Schrems II.

[9] Vezi punctul 124 din cauzele conexate C-511/18, C-512/18 și C-520/18, La Quadrature du Net și alții (denumite în continuare „La Quadrature du Net și alții").

2. INGERINȚE ÎN DREPTURILE FUNDAMENTALE

13. Drepturile fundamentale la respectarea vieții private și de familie, inclusiv a comunicațiilor, și la protecția datelor cu caracter personal sunt prevăzute la articolele 7 și 8 din cartă și se aplică tuturor. În plus, articolul 8 stabilește condițiile pentru legalitatea prelucrării datelor cu caracter personal și recunoaște dreptul de acces și de rectificare, precum și impune ca aceste norme să facă obiectul controlului unei autorități independente.

14. „(O)perațiunea care constă în transferul datelor cu caracter personal dintr-un stat membru către o țară terță constituie, în sine, o prelucrare a datelor cu caracter personal”[10]. Astfel, articolele 7 și 8 din cartă se aplică acestei operațiuni specifice, iar protecția lor se extinde la datele transferate, motiv pentru care persoanele vizate ale căror date cu caracter personal sunt transferate către o țară terță trebuie să beneficieze de un nivel de protecție în esență echivalent cu cel garantat în cadrul Uniunii Europene[11].

15. Potrivit CJUE, atunci când dreptul fundamental la respectarea vieții private consacrat la articolul 7 din cartă este afectat, prin prelucrarea datelor cu caracter personal ale unei persoane, este afectat și dreptul la protecția datelor, întrucât o astfel de prelucrare intră în domeniul de aplicare al articolului 8 din cartă și, prin urmare, trebuie să îndeplinească în mod obligatoriu cerința privind protecția datelor prevăzută la articolul respectiv[12].

16. Prin urmare, în ceea ce privește o eventuală ingerință în drepturile fundamentale în temeiul dreptului Uniunii, obligația impusă furnizorilor de servicii de comunicații electronice (...) de a păstra datele de trafic în scopul de a le pune, dacă este cazul, la dispoziția autorităților naționale competente ridică probleme legate de compatibilitatea cu articolele 7 și 8 din cartă[13]. Același lucru este valabil și pentru alte tipuri de prelucrare a datelor, cum ar fi transmiterea de date către alte persoane decât utilizatorii sau accesul la aceste date în vederea utilizării lor[14], ceea ce implică, prin urmare, o ingerință în drepturile fundamentale menționate. În plus, potrivit unei jurisprudențe constante, accesul unei autorități publice la date constituie o ingerință suplimentară[15].

17. Pentru a se constata o ingerință, nu contează „dacă informațiile vizate referitoare la viața privată prezintă sau nu prezintă un caracter sensibil sau dacă persoanele interesate au suferit sau nu au suferit eventuale inconveniente ca urmare a acestei ingerințe”[16]. CJUE a subliniat, de asemenea, că utilizarea ulterioară a datelor păstrate este irelevantă[17].

18. Cu toate acestea, articolele 7 și 8 din cartă nu sunt drepturi absolute, ci trebuie luate în considerare în raport cu funcția lor în societate[18].

---

[10] CJUE, Schrems II, punctul 83.
[11] CJUE, Schrems II, punctul 96.
[12] CJUE, Schrems II, punctele 170-171.
[13] CJUE, cauza C-623/17, Privacy International (denumită în continuare „Privacy International”), punctul 60.
[14] CJUE, Privacy International, punctul 61.
[15] CEDO, Leander, punctul 48; CEDO, Rotaru punctul 46; CJUE, Digital Rights Ireland, punctul 35.
[16] CJUE, Schrems II, punctul 171, inclusiv jurisprudența citată.
[17] CJUE, Schrems II, punctul 171, inclusiv jurisprudența citată.
[18] CJUE, Privacy International, punctul 63.

19. Carta include un test de necesitate și proporționalitate pentru a încadra limitările drepturilor pe care le protejează. Articolul 52 alineatul (1) din cartă precizează domeniul de aplicare al posibilelor limitări ale articolelor 7 și 8, precizând că „orice restrângere a exercițiului drepturilor și libertăților recunoscute prin prezenta cartă trebuie să fie prevăzută de lege și să respecte substanța acestor drepturi și libertăți. Prin respectarea principiului proporționalității, pot fi impuse restrângeri numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți”.

20. CJUE a reiterat faptul că legislația UE care implică ingerințe în drepturile fundamentale garantate prin articolele 7 și 8 din cartă „trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime astfel încât persoanele ale căror date cu caracter personal sunt vizate să dispună de garanții suficiente care să permită protejarea în mod eficient a acestor date împotriva riscurilor de abuz”, în special în cazul în care datele cu caracter personal sunt supuse unei prelucrări automate și „există un risc important privind un acces ilicit la aceste date”[19].

21. Potrivit CJUE, protecția dreptului la viață privată impune ca derogările de la protecția datelor și limitările acesteia „să se aplice în limitele strictului necesar”. În plus, un obiectiv de interes general trebuie să fie compatibil cu drepturile fundamentale vizate de măsură, „prin realizarea unui just echilibru” între obiectiv și drepturile în cauză[20].

22. În consecință, accesul, păstrarea și utilizarea ulterioară a datelor cu caracter personal de către autoritățile publice în cadrul măsurilor de supraveghere nu trebuie să depășească limitele strictului necesar, evaluate în lumina cartei, în caz contrar „nu pot fi considere justificate, într-o societate democratică”[21].

23. Cele patru garanții esențiale europene, astfel cum sunt prezentate în capitolul următor, urmăresc să specifice mai în detaliu modul de evaluare a nivelului de ingerință în drepturile fundamentale la viață privată și la protecția datelor în contextul măsurilor de supraveghere adoptate de autoritățile publice dintr-o țară terță atunci când transferă date cu caracter personal, precum și cerințele legale care trebuie să se aplice în consecință pentru a evalua dacă astfel de ingerințe ar fi acceptabile în temeiul cartei.

3. GARANȚIILE EUROPENE ESENȚIALE

24. În urma analizei jurisprudenței, CEPD consideră că cerințele legale aplicabile pentru ca limitările drepturilor la viață privată și la protecția datelor recunoscute de cartă să poată fi justificate pot fi clasificate în patru garanții esențiale europene:

A. Prelucrarea ar trebui să se bazeze pe norme clare, precise și accesibile.

[19] CJUE, Privacy International, punctul 68 și jurisprudența citată.

[20] CJUE, Privacy International, punctul 68 și jurisprudența citată.

[21] CJUE, Privacy International, punctul 81.

B. Trebuie să se demonstreze necesitatea și proporționalitatea în raport cu obiectivele legitime urmărite.
C. Ar trebui să existe un mecanism independent de supraveghere.
D. Persoanele fizice trebuie să dispună de căi de atac eficiente.

25. Garanțiile se bazează pe drepturile fundamentale la viață privată și la protecția datelor care se aplică tuturor, indiferent de naționalitate.

Garanția A – Prelucrarea ar trebui să se bazeze pe norme clare, precise și accesibile

26. În temeiul articolului 8 alineatul (2) din cartă, datele cu caracter personal ar trebui, printre altele, să fie prelucrate „în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege”[22], astfel cum a reamintit CJUE în hotărârea în cauza Schrems II. În plus, potrivit articolului 52 alineatul (1) din cartă, orice restrângere a exercitării drepturilor și libertăților recunoscute prin cartă în cadrul UE trebuie să fie prevăzută de lege. Astfel, o ingerință justificată trebuie să fie în conformitate cu legea.

27. Acest temei juridic ar trebui să stabilească norme clare și precise care să reglementeze conținutul și aplicarea măsurii în cauză și să impună o serie de cerințe minime[23]. În plus, Curtea a reamintit că „legislația trebuie să fie obligatorie din punct de vedere juridic în dreptul intern”[24]. În această privință, CJUE a clarificat faptul că evaluarea legislației aplicabile a țării terțe ar trebui să se concentreze asupra posibilității ca persoanele fizice să o invoce și să o exercite în fața unei instanțe[25]. Prin urmare, Curtea indică faptul că drepturile acordate persoanelor vizate pot face obiectul unei acțiuni în justiție; în cazul în care persoanelor fizice nu le sunt acordate drepturi executorii împotriva autorităților publice, nivelul de protecție garantat poate fi considerat în esență echivalent cu cel care decurge din cartă, contrar cerinței prevăzute la articolul 45 alineatul (2) litera (a) din RGPD[26].

28. În plus, Curtea a subliniat că legislația aplicabilă trebuie să indice în ce împrejurări și în ce condiții poate fi luată o măsură care prevede prelucrarea unor astfel de date[27] (vezi relația dintre aceste cerințe și principiile necesității și proporționalității în secțiunea Garanția B de mai jos).

29. În plus, CJUE a indicat, de asemenea, că „cerința ca orice restrângere a exercitării drepturilor fundamentale să fie prevăzută de lege presupune ca temeiul juridic care permite ingerința în aceste drepturi să definească el însuși întinderea restrângerii exercitării dreptului vizat”[28].

[22] Vezi punctul 173 din Schrems II.

[23] Vezi punctele 175 și 180 din Schrems II și Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, punctul 139 și jurisprudența citată.

[24] Vezi punctul 68 din Privacy International – de asemenea, ar trebui să fie clar că, în versiunea în limba franceză a hotărârii, Curtea utilizează termenul „réglementation”, care nu se limitează doar la actele Parlamentului.

[25] Vezi punctul 181 din Schrems II, la acest punct CJUE face trimitere la Directiva nr. 28 privind politica prezidențială din SUA.

[26] Vezi punctul 181 din Schrems II.

[27] Vezi punctul 68 din Privacy International, în legătură cu legislația statelor membre.

[28] Vezi Schrems II, punctul 175 și jurisprudența citată, precum și Privacy International, punctul 65.

30. În cele din urmă, Curtea Europeană a Drepturilor Omului „consideră că nu există niciun temei pentru aplicarea unor principii diferite care să reglementeze accesibilitatea și claritatea normelor care reglementează interceptarea comunicațiilor persoanelor fizice, pe de o parte, și programe mai generale de supraveghere”[29]. CEDO a clarificat, de asemenea, că temeiul juridic ar trebui să includă cel puțin o definiție a categoriilor de persoane care ar putea face obiectul supravegherii, o limitare a duratei măsurii, procedura care trebuie urmată pentru examinarea, utilizarea și stocarea datelor obținute și precauțiile care trebuie luate la comunicarea datelor către alte părți[30].

31. În sfârșit, ingerința trebuie să fie previzibilă în ceea ce privește efectul său asupra persoanei fizice, pentru a-i oferi o protecție adecvată și eficientă împotriva ingerințelor arbitrare și a riscului de abuz. Prin urmare, prelucrarea trebuie să se bazeze pe un temei juridic precis, clar, dar și accesibil (adică public)[31]. CEDO, cu privire la această chestiune, a reamintit în cauza Zakharov că „trimiterea la «previzibilitate» în contextul interceptării comunicațiilor nu poate fi înțeleasă în același mod ca în multe alte domenii”. Aceasta a precizat că, în contextul măsurilor secrete de supraveghere, cum ar fi interceptarea comunicațiilor, „previzibilitatea nu poate însemna că o persoană trebuie să fie pusă în posibilitatea de a prevedea când autoritățile pot intercepta comunicațiile sale, astfel încât să își poată adapta comportamentul în consecință”. Cu toate acestea, având în vedere că, în acest tip de situație, riscul arbitrariului este evident, „existența unor norme clare și detaliate cu privire la interceptarea convorbirilor telefonice este așadar indispensabilă, mai ales că procedeele tehnice utilizabile evoluează în permanență. Legislația națională trebuie să fie elaborată cu suficientă claritate pentru a indica cetățenilor în mod corespunzător în ce împrejurări și în ce condiții abilitează autoritățile publice să adopte astfel de măsuri secrete”[32].

Garanția B – Trebuie să se demonstreze necesitatea și proporționalitatea în raport cu obiectivele legitime urmărite

32. În conformitate cu articolul 52 alineatul (1) prima teză din cartă, orice restrângere a exercitării drepturilor și libertăților recunoscute prin cartă trebuie să respecte substanța acestor drepturi și libertăți. În conformitate cu articolul 52 alineatul (1) a doua teză din cartă, prin respectarea principiului proporționalității, pot fi impuse restrângeri drepturilor și libertăților respective numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.[33]

33. În ceea ce privește **principiul proporționalității**, Curtea a statuat, cu privire la legislația statelor membre, că problema dacă o limitare a drepturilor la viață privată și la protecția datelor cu caracter personal poate fi justificată trebuie să fie analizată, pe de o parte, prin evaluarea **gravității ingerinței** pe care o implică o astfel de limitare[34] și prin verificarea faptului dacă **importanța obiectivului de**

[29] CEDO, Liberty, punctul 63.

[30] CEDO, Weber și Saravia, punctul 95.

[31] CEDO, Malone, punctele 65, 66.

[32] CEDO, Zakharov, punctul 229.

[33] Schrems II, punctul 174.

[34] În acest context, Curtea constată, de exemplu, că „ingerința pe care o implică colectarea în timp real a datelor care permit localizarea echipamentelor terminale pare deosebit de gravă, întrucât datele respective oferă autorităților naționale competente un mijloc de a urmări cu exactitate și în permanență mișcările utilizatorilor de telefoane mobile (...)” (La Quadrature du Net și alții, punctul 187, inclusiv jurisprudența citată).

interes general urmărit de limitarea respectivă este proporțională cu această gravitate, pe de altă parte.[35]

34. În cauza La Quadrature du Net și alții, se poate observa că CJUE a statuat, în raport cu legislația unui stat membru, și nu cu legislația unei țări terțe, că obiectivul de a proteja securitatea națională poate, datorită importanței sale, justifica măsuri care implică ingerințe mai grave în drepturile fundamentale decât cele care ar putea fi justificate de alte obiective, cum ar fi combaterea criminalității. Cu toate acestea, Curtea a constatat că acesta este cazul atât timp cât există temeiuri suficient de solide pentru a considera că statul în cauză se confruntă cu o amenințare gravă la adresa securității naționale care se dovedește a fi reală, prezentă sau previzibilă și sub rezerva îndeplinirii celorlalte cerințe prevăzute la articolul 52 alineatul (1) din cartă[36].

35. În această privință, potrivit jurisprudenței constante a Curții, derogările de la protecția datelor cu caracter personal și limitările acesteia trebuie să se aplice numai în limitele strictului necesar[37]. Pentru a îndeplini această cerință, pe lângă stabilirea unor norme clare și precise care să reglementeze conținutul și aplicarea măsurii în cauză, legislația în cauză trebuie să impună o serie de cerințe minime, astfel încât persoanele ale căror date au fost transferate să dispună de garanții suficiente pentru a-și proteja în mod eficient datele cu caracter personal împotriva riscului de abuz. „Această reglementare trebuie în special să indice în ce împrejurări și în ce condiții o măsură care prevede prelucrarea unor asemenea date poate fi luată, garantând în acest mod că o ingerință este limitată la strictul necesar. Necesitatea de a dispune de astfel de garanții este cu atât mai importantă atunci când datele cu caracter personal sunt supuse unei prelucrări automatizate”[38].

36. În cauza Schrems II, CJUE a subliniat că legislația unei țări terțe care nu indică nicio limitare a competenței pe care o conferă pentru a pune în aplicare programe de supraveghere în scopul colectării de informații externe nu poate asigura un nivel de protecție în esență echivalent cu cel garantat de cartă. Într-adevăr, în conformitate cu jurisprudența, un temei juridic care permite ingerința în drepturile fundamentale trebuie, pentru a îndeplini cerințele principiului proporționalității, să definească el însuși întinderea restrângerii exercitării dreptului în cauză[39].

37. În ceea ce privește **principiul necesității**, CJUE a clarificat faptul că legislațiile „care autorizează în mod generalizat stocarea integrală a datelor cu caracter personal ale tuturor persoanelor ale căror date au fost transferate din Uniune (...), fără a se face vreo diferențiere, limitare sau excepție în funcție de obiectivul urmărit și fără a se prevedea un criteriu obiectiv care să permită delimitarea

[35] La Quadrature du Net și alții, punctul 131.

[36] Punctele 136 și 137. Vezi, de asemenea, Privacy International, astfel cum a precizat Curtea, astfel de amenințări se pot distinge, prin natura și prin gravitatea lor deosebită, de riscul general de apariție a unor tensiuni sau perturbări, chiar grave, ale siguranței publice. Punctul 75. De exemplu, în cauza La Quadrature du Net și alții, Curtea a observat că analiza automatizată a datelor de transfer și de localizare care acoperă în general și nediferențiat datele persoanelor care utilizează sisteme de comunicații electronice constituie o ingerință deosebit de gravă, astfel încât o astfel de măsură nu poate îndeplini cerința proporționalității decât în situațiile în care statul membru în cauză se confruntă cu o amenințare gravă la adresa securității naționale care se dovedește a fi reală, prezentă sau previzibilă și, printre alte condiții, cu condiția ca durata păstrării să fie limitată la strictul necesar (punctele 174-177).

[37] Schrems II, punctul 176, inclusiv jurisprudența citată.

[38] Schrems II, punctul 175.

[39] Schrems II, punctul 180.

accesului autorităților publice la date și utilizarea lor ulterioară în scopuri precise, strict restrânse și susceptibile să justifice ingerința pe care o implică atât accesarea, cât și utilizarea acestor date", nu respectă acest principiu[40]. În special, CJUE a considerat că o reglementare care permite autorităților publice să aibă acces în mod generalizat la conținutul comunicărilor electronice aduce atingere substanței dreptului fundamental la respectarea vieții private, astfel cum este garantat la articolul 7 din cartă[41].

38. Cu toate acestea, de data aceasta, atunci când a evaluat legislația unui stat membru, și nu legislația unei țări terțe, CJUE a statuat în cauza La Quadrature du Net și alții, că „legislația care impune păstrarea datelor cu caracter personal trebuie să îndeplinească întotdeauna criterii obiective care să stabilească o legătură între datele păstrate și obiectivul urmărit"[42]. În același context, în cauza Privacy International, Curtea a statuat, de asemenea, că legiuitorul „trebuie să se întemeieze pe criterii obiective pentru a defini împrejurările și condițiile în care trebuie să se acorde autorităților naționale competente accesul la datele în cauză"[43].

Garanția C – Ar trebui să existe un mecanism independent de supraveghere

39. CEPD reamintește că are loc o ingerință în momentul colectării datelor, dar și în momentul accesării datelor de către o autoritate publică în scopul prelucrării ulterioare. CEDO a precizat de mai multe ori că orice ingerință în dreptul la viață privată și la protecția datelor ar trebui să facă obiectul unui sistem de supraveghere eficace, independent și imparțial, care trebuie să fie asigurat fie de un judecător, fie de un alt organism independent[44] (de exemplu, de o autoritate administrativă sau de un organism parlamentar). Supravegherea independentă a punerii în aplicare a măsurilor de supraveghere a fost, de asemenea, luată în considerare de CJUE în hotărârea pronunțată în cauza Schrems II[45].

---

[40] Schrems I, punctul 93 cu trimiterile suplimentare. Vezi însă, de această dată, în raport cu legislația unui stat membru, și nu cu legislația unei țări terțe, Privacy International, punctul 71, inclusiv jurisprudența citată. În această cauză, Curtea a afirmat că legislația unui stat membru care impune furnizorilor de servicii de comunicații electronice să divulge date de trafic și date de localizare serviciilor de securitate și de informații printr-o măsură de transmitere generalizată și nediferențiată depășește limitele strictului necesar și nu poate fi considerată justificată, în cadrul unei societăți democratice, astfel cum prevede Directiva privind viața privată și comunicațiile electronice, interpretată în lumina cartei (punctul 81).

[41] Schrems I, punctul 94.

[42] La Quadrature du Net și alții, punctul 133. În acest context, Curtea a confirmat că măsurile legislative care prevăd, ca măsură preventivă, păstrarea generalizată și nediferențiată a datelor de trafic și de localizare sunt interzise de Directiva privind viața privată și comunicațiile electronice, interpretată în lumina cartei. În schimb, Curtea a hotărât că, în situații în care există o amenințare gravă la adresa securității naționale care se dovedește a fi reală, prezentă sau previzibilă, legiuitorul poate permite, în scopul apărării securității naționale, recurgerea la o instrucțiune care impune furnizorilor de servicii de comunicații electronice să păstreze, în general și nediferențiat, datele de trafic și de localizare. Cu toate acestea, o astfel de măsură trebuie să îndeplinească anumite condiții. În special, instrucțiunea poate fi acordată numai pentru o perioadă limitată în timp la ceea ce este strict necesar, care poate fi prelungită în cazul în care amenințarea persistă (punctul 168).

[43] Privacy International, punctul 78, inclusiv jurisprudența citată. În cauza Privacy International, în ceea ce privește accesul unei autorități la datele cu caracter personal furnizate în temeiul legislației unui stat membru, Curtea a hotărât că „un acces general la toate datele păstrate, în lipsa oricărei legături, chiar indirectă, cu scopul urmărit, nu poate fi considerat limitat la strictul necesar" (punctele 77-78).

[44] CEDO, Klass, punctele 17, 51.

[45] Schrems II, punctele 179, 183.

40. CEDO precizează că, deși autorizarea prealabilă (judiciară) a măsurilor de supraveghere reprezintă o garanție importantă împotriva arbitrariului, trebuie să se țină seama și de funcționarea efectivă a sistemului de interceptare, inclusiv de sistemul de control și echilibru al exercitării puterii, precum și de existența sau absența abuzului real[46]. În cauza Schrems II, CJUE a luat în considerare, de asemenea, domeniul de aplicare al rolului de control al mecanismului de supraveghere, care nu a acoperit măsurile individuale de supraveghere[47].

41. În ceea ce privește legislația statelor membre, CJUE a identificat o serie de măsuri care sunt în conformitate cu legislația UE numai dacă fac obiectul unui control efectiv efectuat de o instanță sau de o autoritate administrativă independentă a cărei decizie este obligatorie. Scopul acestui control este de a verifica existența unei situații care justifică măsura și respectarea condițiilor și a garanțiilor care trebuie stabilite[48]. Pentru colectarea în timp real a datelor de trafic și de localizare, controlul ar trebui să permită verificarea ex ante, printre altele, a faptului dacă aceasta este autorizată numai în limitele strictului necesar. În cazuri de urgență justificate în mod corespunzător, măsurile pot fi puse în aplicare fără un astfel de control prealabil; cu toate acestea, Curtea impune totuși ca controlul ulterior să aibă loc într-un termen scurt[49].

42. În ceea ce privește independența mecanismelor de supraveghere în raport cu supravegherea, ar putea fi luate în considerare constatările CJUE privind independența unui organism în contextul căilor de atac (vezi mai jos garanția D). În plus, jurisprudența CEDO poate oferi elemente suplimentare. Curtea și-a exprimat preferința ca un judecător să fie responsabil de menținerea supravegherii. Cu toate acestea, nu este exclus ca un alt organism să fie responsabil, „atât timp cât este suficient de independent față de executiv”[50] și „de autoritățile care efectuează supravegherea și [este] învestit cu puteri și competențe suficiente pentru a exercita un control efectiv și continuu”[51]. CEDO a adăugat că „modul de numire și statutul juridic al membrilor organului de control”[52] trebuie luate în considerare atunci când se evaluează independența. Aceasta include „persoane cu calificările necesare pentru accesul la magistratură, numite fie de parlament, fie de prim-ministru. În schimb, Curtea a considerat insuficient de independent un ministru de Interne care nu doar că era numit de puterea politică și membru al executivului, ci mai era și direct implicat în conducerea mijloacelor speciale de supraveghere”[53]. De asemenea, CEDO „constată că este esențial ca organul de control să aibă acces la toate documentele relevante, inclusiv la informații confidențiale”[54]. În cele din urmă, CEDO ia în considerare „dacă activitățile organului de control sunt deschise controlului public”[55].

[46] CEDO, Big Brother Watch atacată, punctele 319-320.

[47] Schrems II, punctul 179.

[48] CEUE, La Quadrature du Net și alții, punctele 168, 189.

[49] CEUE, La Quadrature du Net și alții, punctul 189.

[50] CEDO, Zakharov, punctul 258, Iordachi și alții c. Moldovei, punctele 40 și 51 și Dumitru Popescu c. României, punctele 70-73.

[51] CEDO, Klass punctul 56 și Big Brother Watch atacată, punctul 318

[52] CEDO, Zakharov, punctul 278.

[53] CEDO, Zakharov, punctul 278.

[54] CEDO, Zakharov, punctul 281.

[55] CEDO, Zakharov, punctul 283.

Garanția D – Persoanele fizice trebuie să dispună de căi de atac eficiente

43. Garanția esențială europeană finală se referă la căile de atac aflate la dispoziția persoanelor fizice. Acestea trebuie să dispună de o cale de atac eficientă pentru a-și exercita drepturile atunci când consideră că acestea nu sunt sau nu au fost respectate. De asemenea, CJUE a explicat în Schrems I că „o reglementare care nu prevede nicio posibilitate a persoanei fizice de a exercita căi legale pentru a avea acces la date cu caracter personal care o privesc sau pentru a obține rectificarea sau ștergerea unor astfel de date nu respectă substanța dreptului fundamental la o protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din cartă. Astfel, articolul 47 primul paragraf din cartă impune ca orice persoană ale cărei drepturi și libertăți garantate de dreptul Uniunii sunt încălcate să aibă dreptul la o cale de atac efectivă în fața unei instanțe judecătorești, în conformitate cu condițiile stabilite de acest articol”[56].

44. Atunci când evaluează legislația unui stat membru care permite colectarea în timp real a datelor de trafic și de localizare, Curtea a considerat că notificarea este necesară „pentru a permite persoanelor afectate să își exercite drepturile care le revin în temeiul articolelor 7 și 8 din cartă de a solicita accesul la datele lor cu caracter personal care au făcut obiectul acestor măsuri și, după caz, rectificarea sau ștergerea acestora din urmă, precum și să se prevaleze, în conformitate cu articolul 47 primul paragraf din cartă, de o cale de atac eficientă în fața unei instanțe judecătorești”[57]. Cu toate acestea, Curtea a recunoscut, de asemenea, că notificarea persoanelor ale căror date au fost colectate sau analizate trebuie să intervină numai în măsura în care și imediat ce notificarea nu mai pune în pericol sarcinile pentru care sunt responsabile autoritățile respective[58].

45. De asemenea, pentru CEDO, problema unei căi de atac eficiente este indisolubil legată de notificarea persoanei în cauză cu privire la o măsură de supraveghere, după încheierea supravegherii. În special, Curtea a constatat că „persoana vizată cu greu poate, în principiu, să conteste retroactiv în instanță legalitatea măsurilor întreprinse fără știrea sa, dacă nu este informată despre acestea sau, dacă – în altă ipoteză –, bănuind că îi sunt ori i-au fost interceptate comunicațiile, persoana are posibilitatea de a sesiza instanțele, acestea având competență chiar dacă subiectul interceptării nu a fost informat despre această măsură”[59]. CEDO a recunoscut astfel că, în anumite cazuri, ar putea să nu existe nicio notificare, însă trebuie prevăzută o cale de atac eficientă. În această cauză, Curtea a clarificat, de exemplu în cauza Kennedy, că o instanță oferă suficiente căi de atac dacă îndeplinește o serie de criterii, și anume un organism independent și imparțial, care și-a adoptat propriul regulament de procedură, compus din membri care trebuie să dețină sau să fi deținut o funcție judiciară importantă ori să fie avocați experimentați și că nu există nicio sarcină probatorie pentru a depune o cerere la aceasta[60]. Atunci când examinează plângerile depuse de persoane fizice, instanța ar trebui să aibă acces la toate informațiile relevante[61], inclusiv la informații confidențiale. În cele din urmă, aceasta ar trebui să aibă competența de a remedia situația de nerespectare[62].

---

[56] CJUE, Schrems I, punctul 95.
[57] Vezi punctul 190 din cauza La Quadrature du Net și alții și CJUE, Avizul 1/15, punctul 220.
[58] Vezi punctul 191 din cauza La Quadrature du Net și alții.
[59] CEDO, Zakharov, punctul 234.
[60] CEDO, Kennedy, punctul 190.
[61] CEPD constată că Comisarul pentru drepturile omului al Consiliului Europei consideră că așa-numita „regulă a terțului” – în temeiul cărora agențiile de informații dintr-o țară care furnizează date agențiilor de informații dintr-o altă țară pot impune agențiilor beneficiare obligația de a nu transmite datele transferate niciunui terț –

46. Articolul 47 din cartă se referă la un tribunal, chiar dacă în alte versiuni lingvistice decât engleza se preferă cuvântul „instanță”[63], în timp ce Convenția europeană a drepturilor omului obligă statele membre să se asigure doar că „orice persoană ale cărei drepturi și libertăți sunt încălcate are dreptul să se adreseze efectiv unei instanțe naționale”[64], care nu trebuie să fie neapărat o autoritate judiciară[65].

47. CJUE, în contextul hotărârii pronunțate în cauza Schrems II atunci când a evaluat caracterul adecvat al nivelului de protecție al unei țări terțe, a reiterat faptul că „persoanele vizate trebuie să dispună de posibilitatea de a exercita căi legale în fața unei instanțe judecătorești independente și imparțiale pentru a avea acces la date cu caracter personal care le privesc sau de a obține rectificarea sau ștergerea unor astfel de date”[66]. În același context, CJUE consideră că o protecție jurisdicțională efectivă împotriva unor astfel de ingerințe poate fi asigurată nu numai de o instanță, ci și de un organism[67] care oferă garanții în esență echivalente cu cele prevăzute la articolul 47 din cartă. În hotărârea sa pronunțată în cauza Schrems II, CJUE a subliniat că trebuie asigurată independența instanței sau a organismului, în special față de puterea executivă, cu toate garanțiile necesare, inclusiv în ceea ce privește condițiile de anulare sau de revocare a numirii sale[68], și că competențele care ar trebui acordate unei instanțe trebuie să respecte cerințele articolului 47 din cartă. În acest sens, organismului[69] i se conferă competența de a adopta decizii obligatorii pentru serviciile de informații, în conformitate cu garanțiile legale de care s-ar putea prevala persoanele vizate[70].

4. OBSERVAȚII FINALE

48. Cele patru garanții esențiale europene trebuie considerate principalele elemente care trebuie să fie identificate atunci când se evaluează nivelul de ingerință în drepturile fundamentale la viață privată și la protecția datelor. Acestea nu ar trebui să fie evaluate în mod independent, deoarece sunt strâns legate între ele, ci în mod global, revizuind legislația relevantă în ceea ce privește măsurile de supraveghere, nivelul minim de garanții pentru protecția drepturilor persoanelor vizate și căile de atac prevăzute de legislația națională a țării terțe.

49. Aceste garanții necesită un anumit grad de interpretare, cu atât mai mult cu cât legislația țărilor terțe nu trebuie să fie identică cu cadrul juridic al UE.

50. Astfel cum a afirmat CEDO în cauza Kennedy, o „apreciere depinde de toate împrejurările cauzei, de exemplu natura, întinderea și durata eventualelor măsuri, motivele necesare pentru a le dispune,

---

nu ar trebui să se aplice organismelor de supraveghere pentru a nu submina posibilitatea unei căi de atac eficiente (Document tematic privind supravegherea democratică și eficientă a serviciilor de securitate națională).

[62] CEDO, Kennedy punctul 167.

[63] Cuvântul „tribunal” este, de exemplu, tradus ca „Gericht” în limba germană și „gerecht” în limba olandeză.

[64] Articolul 13 din Convenția europeană a drepturilor omului.

[65] CEDO, Klass, punctul 67.

[66] Vezi punctul 194 din Schrems II.

[67] Vezi punctul 197 din Schrems II, în care Curtea utilizează în mod expres acest termen.

[68] Vezi punctul 195 din Schrems II.

[69] Vezi punctul 197 din Schrems II, în care Curtea utilizează în mod expres acest termen.

[70] Vezi punctul 196 din Schrems II.

autoritățile competente pentru a le permite, a le executa și a le controla, tipul de cale de atac oferit de dreptul național”[71].

51. În consecință, evaluarea măsurilor de supraveghere ale țărilor terțe în raport cu GEE poate conduce la două concluzii:

- Legislația țării terțe în cauză nu asigură cerințele GEE: în acest caz, legislația țării terțe nu ar oferi un nivel de protecție în esență echivalent cu cel garantat în cadrul UE.

- Legislația țării terțe în cauză îndeplinește garanțiile esențiale europene.

52. Atunci când evaluează caracterul adecvat al nivelului de protecție, în temeiul articolului 45 din RGPD, Comisia va trebui să aprecieze dacă garanțiile esențiale europene sunt satisfăcute ca parte a elementelor care trebuie luate în considerare pentru a garanta că legislația țării terțe în ansamblu oferă un nivel de protecție în esență echivalent cu cel garantat în UE.

53. Atunci când exportatorii de date se bazează, împreună cu importatorii de date, pe garanții adecvate în temeiul articolului 46 din RGPD, având în vedere cerințele legislației țării terțe aplicabile în mod specific datelor transferate, aceștia ar trebui să se asigure că se atinge în mod eficient un nivel de protecție echivalent în esență. În special, în cazul în care legislația țării terțe nu respectă cerințele GEE, acest lucru ar implica asigurarea faptului că legislația în cauză nu va afecta garanțiile și măsurile de protecție aferente transferului, astfel încât să se asigure în continuare un nivel de protecție în esență echivalent cu cel garantat în UE.

54. CEPD a emis orientări și recomandări suplimentare de care trebuie să se țină seama la realizarea evaluării, în funcție de instrumentul de transfer care urmează să fie utilizat și de necesitatea de a oferi garanții adecvate, inclusiv, după caz, măsuri suplimentare[72].

55. În plus, ar trebui remarcat faptul că garanțiile esențiale europene se bazează pe cerințele prevăzute de legislație. CEPD subliniază că garanțiile esențiale europene se bazează pe drepturile fundamentale care se aplică tuturor, indiferent de naționalitate.

56. CEPD reiterează faptul că garanțiile esențiale europene reprezintă un standard de referință atunci când se evaluează ingerința pe care o implică măsurile de supraveghere ale țărilor terțe, în contextul transferurilor internaționale de date. Aceste standarde decurg din legislația UE și din jurisprudența CJUE și a CEDO, care este obligatorie pentru statele membre.

[71] CEDO, Kennedy, punctul 153.

[72] Criterii de referință privind caracterul adecvat al nivelului de protecție (Adequacy Referential), WP 254 rev. 01, revizuite și adoptate la 6 februarie 2018; Recomandările 01/2020 ale Comitetului european pentru protecția datelor din 10 noiembrie 2020 privind măsurile care completează instrumentele de transfer pentru a asigura conformitatea cu nivelul UE de protecție a datelor cu caracter personal.