



Repertoriul jurisprudenței

HOTĂRÂREA CURȚII (Camera întâi)

7 septembrie 2023 *

„Trimitere preliminară – Telecomunicații – Prelucrarea datelor cu caracter personal în sectorul comunicațiilor electronice – Directiva 2002/58/CE – Domeniu de aplicare – Articolul 15 alineatul (1) – Date reținute de furnizorii de servicii de comunicații electronice și puse la dispoziția autorităților însărcinate cu procedura penală – Utilizare ulterioară a datelor cu ocazia unei anchete privind o abatere de serviciu”

În cauza C-162/22,

având ca obiect o cerere de decizie preliminară formulată în temeiul articolului 267 TFUE de Lietuvos vyriausiasis administracinis teismas (Curtea Administrativă Supremă a Lituaniei), prin decizia din 24 februarie 2022, primită de Curte la 3 martie 2022, în procedura inițiată de

A. G.

cu participarea:

Lietuvos Respublikos generalinė prokuratūra,

CURTEA (Camera întâi),

compusă din domnul A. Arabadžiev, președinte de cameră, domnii P. G. Xuereb (raportor), T. von Danwitz, A. Kumin și doamna I. Ziemele, judecători,

avocat general: domnul M. Campos Sánchez-Bordona,

grefier: doamna A. Lamote, administratoare,

având în vedere procedura scrisă și în urma ședinței din 2 februarie 2023,

luând în considerare observațiile prezentate:

- pentru A. G., de G. Danėlius, advokatas;
- pentru guvernul lituanian, de S. Grigonis, V. Kazlauskaitė-Švenčionienė și V. Vasiliauskienė, în calitate de agenți;
- pentru guvernul ceh, de O. Serdula, M. Smolek și J. Vlácil, în calitate de agenți;

* Limba de procedură: lituaniana.

- pentru guvernul estonian, de M. Kriisa, în calitate de agent;
- pentru Irlanda, de M. Browne, A. Joyce și M. Tierney, în calitate de agenți, asistați de D. Fennelly, BL;
- pentru guvernul francez, de R. Bénard, în calitate de agent;
- pentru guvernul italian, de G. Palmieri, în calitate de agent, asistată de A. Grumetto, avvocato dello Stato;
- pentru guvernul maghiar, de Zs. Biró-Tóth și M. Z. Fehér, în calitate de agenți;
- pentru Comisia Europeană, de S. L. Kalėda, H. Kranenborg, P.-J. Loewenthal și F. Wilman, în calitate de agenți,

după ascultarea concluziilor avocatului general în ședința din 30 martie 2023,

pronunță prezenta

Hotărâre

- 1 Cererea de decizie preliminară privește interpretarea articolului 15 alineatul (1) din 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 2002, L 201, p. 37, Ediție specială, 13/vol. 36, p. 63), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 (JO 2009, L 337, p. 11) (denumită în continuare „Directiva 2002/58”).
- 2 Această cerere a fost formulată în cadrul unei proceduri inițiate de A. G. în legătură cu legalitatea unor decizii ale Lietuvos Respublikos generalinė prokuratūra (Parchetul General al Republicii Lituania, denumit în continuare „Parchetul General”) prin care a fost revocat din funcția sa de procuror.

Cadrul juridic

Dreptul Uniunii

- 3 Articolul 1 din Directiva 2002/58, intitulat „Sfera de aplicare și scopul”, prevede:

„(1) Prezenta directivă prevede armonizarea dispozițiilor naționale, lucru necesar în vederea asigurării unui nivel echivalent de protecție a drepturilor și a libertăților fundamentale, în special a dreptului la confidențialitate și la respectarea vieții private, în domeniul prelucrării de date cu caracter personal în sectorul comunicațiilor electronice și a asigurării liberei circulații a acestor date și a serviciilor și echipamentelor de comunicații electronice în interiorul Comunității.

[...]

(3) Prezenta directivă nu se aplică activităților care nu sunt cuprinse în domeniul de aplicare al Tratatului de instituire a Comunității Europene, cum sunt cele menționate la titlurile V și VI al Tratatului privind Uniunea Europeană, și în orice caz activităților legate de siguranța publică, de apărare, de siguranța statului (inclusiv de bunăstarea economică a acestuia, dacă activitățile respective sunt legate de chestiuni de siguranța statului) și activităților statului în domeniul legii penale.”

- 4 Articolul 5 din această directivă, intitulat „Confidențialitatea comunicațiilor”, prevede la alineatul (1):

„Statele membre trebuie să asigure confidențialitatea comunicațiilor și a datelor de transfer aferente transmise prin intermediul unei rețele de comunicații publice sau [al] unor servicii publice de comunicații electronice, prin legislația internă. Acestea interzic astfel în special ascultarea, înregistrarea, stocarea sau alte tipuri de interceptare sau supraveghere a comunicațiilor și a datelor de transfer aferente de către persoane altele decât utilizatorul, fără acordul utilizatorului în cauză, cu excepția cazurilor în care acest lucru este permis în temeiul articolului 15 alineatul (1). Prezentul alineat nu interzice stocarea tehnică necesară pentru transmisia comunicației care nu aduce atingere principiului confidențialității.”

- 5 Articolul 15 din directiva menționată, intitulat „Aplicarea anumitor dispoziții ale Directivei 95/46/CE”, prevede la alineatul (1):

„Statele membre pot adopta măsuri legislative pentru a restrânge sfera de aplicare a drepturilor și obligațiilor prevăzute la articolul 5, articolul 6, articolul 8 alineatele (1), (2), (3) și (4) și articolul 9 ale prezentei directive, în cazul în care restrângerea lor constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice pentru a proteja securitatea națională (de exemplu siguranța statului), apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice, în conformitate cu articolul 13 alineatul (1) al Directivei 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 (JO 1995, L 281, p. 31, Ediție specială, 13/vol. 17, p. 10)]. În acest scop, statele membre pot adopta, *inter alia*, măsuri legislative care să permită reținerea de date, pe perioadă limitată, pentru motivele arătate anterior în acest alineat. Toate măsurile menționate în acest alineat trebuie să fie conforme cu principiile generale ale legislației comunitare, inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) [TUE].”

Dreptul lituanian

Legea privind comunicațiile electronice

- 6 Articolul 65 alineatul 2 din Lietuvos Respublikos elektroninių ryšių įstatymas (Legea Republicii Lituania privind comunicațiile electronice) din 15 aprilie 2004 (Žin., 2004, nr. 69-2382), în versiunea aplicabilă faptelor din litigiul principal (denumită în continuare „Legea privind comunicațiile electronice”), obligă furnizorii de servicii de comunicații electronice să rețină datele prevăzute în anexa 1 la această lege și, dacă este cazul, să le pună la dispoziția autorităților competente pentru a fi utilizate în vederea combaterii infracționalității grave.

7 În conformitate cu anexa 1 la Legea privind comunicațiile electronice, categoriile de date care trebuie reținute sunt următoarele:

„1. Datele necesare pentru găsirea și determinarea sursei unei comunicații: [...] 2. Datele necesare pentru determinarea destinației unei comunicații: [...] 3. Datele necesare pentru determinarea datei, a orei și a duratei unei comunicații: [...] 4. Datele necesare pentru determinarea tipului de comunicație: [...] 5. Datele necesare pentru a stabili echipamentul de comunicație al utilizatorilor sau ce ar putea fi echipamentul acestora: [...] 6. Datele necesare pentru localizarea echipamentului de comunicație mobilă: [...]”

8 În temeiul articolului 77 alineatul 4 din această lege, în cazul în care există o hotărâre judecătorească motivată sau un alt temei juridic prevăzut de lege, furnizorii de servicii de comunicații electronice trebuie să facă posibil din punct de vedere tehnic, în special pentru organele însărcinate cu colectarea datelor operative în materie penală și pentru organele de cercetare penală, în conformitate cu procedurile prevăzute de Lietuvos Respublikos baudžiamojo proceso kodeksas (Codul de procedură penală al Republicii Lituania, denumit în continuare „Codul de procedură penală”), controlul conținutului informațiilor transmise prin rețelele de comunicații electronice.

Legea privind colectarea datelor operative în materie penală

9 Articolul 6 alineatul 3 punctul 1 din Lietuvos Respublikos kriminalinės žvalgybos įstatymas (Legea Republicii Lituania privind colectarea datelor operative în materie penală) din 2 octombrie 2012 (Žin., 2012, nr. 122-6093), în versiunea aplicabilă faptelor din litigiul principal (denumită în continuare „Legea privind colectarea datelor operative în materie penală”), prevede că, în cazul în care sunt îndeplinite condițiile prevăzute de această lege pentru a justifica o operațiune de colectare a datelor operative în materie penală și cu autorizarea prealabilă a unui membru al ministerului public sau a unui organ judiciar, organele însărcinate cu colectarea datelor operative în materie penală au competența, pe lângă cele enumerate la alineatele 1 și 2 ale aceluiași articol, de a colecta informații de la furnizorii de servicii de comunicații electronice.

10 Articolul 8 alineatul 1 din legea menționată prevede că organele însărcinate cu colectarea datelor operative în materie penală desfășoară o anchetă, printre altele, atunci când dispun de informații privind pregătirea sau săvârșirea unei încălcări deosebit de grave, grave ori de o gravitate scăzută sau cu privire la persoanele care pregătesc, săvârșesc ori au săvârșit o astfel de încălcare. Articolul 8 alineatul 3 din aceeași lege precizează că, dacă o astfel de anchetă indică existența unor indicii privind săvârșirea unei infracțiuni, se deschide imediat cercetarea penală.

11 Potrivit articolului 19 alineatul 1 punctul 5 din Legea privind colectarea datelor operative în materie penală, informațiile care provin din operațiuni de colectare a datelor operative în materie penală pot fi utilizate în cazurile prevăzute la alineatele 3 și 4 din acest articol și în alte situații prevăzute de lege. În temeiul alineatului 3 al articolului menționat, informațiile provenite din operațiuni de colectare a datelor operative în materie penală referitoare la un eveniment care prezintă caracteristicile unei încălcări legate de corupție pot fi declassificate, cu acordul parchetului, și utilizate în contextul unei anchete privind abateri disciplinare sau de serviciu.

Codul de procedură penală

- 12 Articolul 154 din Codul de procedură penală prevede că, prin decizia unui judecător de instrucție pronunțată la cererea unui membru al Ministerului Public, un organ de anchetă poate asculta conversațiile transmise prin rețelele de comunicații electronice, poate să le transcrie, să controleze alte informații transmise prin rețelele de comunicații electronice și să le înregistreze și să le păstreze, în cazul în care există, printre altele, motive să se considere că acest lucru va permite obținerea de informații cu privire la o încălcare deosebit de gravă sau gravă care este în curs de pregătire sau de săvârșire sau care a fost săvârșită sau cu privire la o încălcare de o gravitate scăzută sau care nu este gravă.
- 13 Articolul 177 alineatul 1 din acest cod prevede că informațiile obținute în cursul cercetării penale sunt confidențiale și că, până la judecarea cauzei, aceste informații pot fi divulgate numai cu autorizarea Ministerului Public și numai în măsura în care acest lucru este recunoscut ca justificabil.
- 14 În vederea punerii în aplicare a articolului 177 din codul menționat, se aplică *Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne Baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendacijos* (Recomandările privind transmiterea și utilizarea datelor rezultate în urma cercetării penale în alte scopuri decât urmărirea penală, precum și protecția acestor date), aprobate prin Decretul nr. I-279 al Procurorului General din 17 august 2017 (TAR, 2017, nr. 2017-13413), astfel cum au fost modificate ultima dată prin Decretul nr. I-211 din 25 iunie 2018.
- 15 Punctul 23 din aceste recomandări prevede că, atunci când primește o cerere de acces la informațiile rezultate din cercetarea penală, procurorul decide dacă este cazul să le furnizeze. În cazul în care se ia decizia de a le furniza, procurorul precizează în ce măsură pot fi furnizate informațiile vizate de cerere.

Litigiul principal și întrebarea preliminară

- 16 Parchetul General a deschis o anchetă administrativă împotriva reclamantului din litigiul principal, care exercita la acea dată funcția de procuror în cadrul unui parchet lituanian, pentru motivul că existau indicii potrivit cărora acesta furnizase în mod nelegal, în cadrul unei cercetări penale pe care o conducea, informații relevante pentru această cercetare persoanei suspectate și avocatului său.
- 17 În raportul său privind această anchetă, comisia Parchetului General a constatat că reclamantul din litigiul principal săvârșise efectiv o abatere de serviciu.
- 18 Potrivit acestui raport, abaterea de serviciu respectivă era demonstrată prin elementele obținute în cursul anchetei administrative. În special, informațiile obținute cu ocazia operațiunilor de colectare a datelor operative în materie penală și datele colectate cu ocazia a două cercetări penale ar fi confirmat existența unor comunicații telefonice între reclamantul din litigiul principal și avocatul suspectului în cadrul cercetării penale referitoare la acesta din urmă conduse de reclamantul din litigiul principal. Raportul menționat a arătat în plus că o ordonanță judiciară autorizase interceptarea și înregistrarea conținutului informațiilor transmise prin rețele de comunicații electronice privind avocatul în cauză și că o altă ordonanță judiciară autorizase aceeași măsură în ceea ce îl privește pe reclamantul din litigiul principal.

- 19 În temeiul aceluiași raport, Parchetul General a adoptat două decrete prin care, pe de o parte, a aplicat reclamantului din litigiul principal o sancțiune constând în revocarea acestuia din dosar și, pe de altă parte, l-a revocat din funcție.
- 20 Reclamantul din litigiul principal a sesizat Vilniaus apygardos administracinis teismas (Tribunalul Administrativ Regional din Vilnius, Lituania) cu o acțiune având ca obiect, printre altele, anularea acestor două decrete.
- 21 Prin hotărârea din 16 iulie 2021, această instanță a respins acțiunea reclamantului din litigiul principal, în special pentru motivul că operațiunile de colectare a datelor operative în materie penală efectuate în speță erau legale și că informațiile colectate în conformitate cu dispozițiile Legii privind colectarea datelor operative în materie penală fuseseră utilizate în mod legal pentru a aprecia existența unei abateri de serviciu săvârșite eventual de reclamantul din litigiul principal.
- 22 Reclamantul din litigiul principal a sesizat în apel Lietuvos vyriausiosios administracinis teismas (Curtea Administrativă Supremă a Lituaniei), instanța de trimitere, susținând că accesul organelor însărcinate cu colectarea datelor operative în materie penală, în cadrul unei operațiuni de colectare a datelor operative în materie penală, la datele de transfer și la conținutul însuși al comunicațiilor electronice constituia o atingere adusă drepturilor fundamentale de o asemenea gravitate încât, ținând seama de dispozițiile Directivei 2002/58 și ale Cartei drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”), acest acces nu putea fi acordat decât în scopul combaterii unor încălcări grave. Or, articolul 19 alineatul 3 din Legea privind colectarea datelor operative în materie penală ar prevedea că astfel de date pot fi utilizate pentru anchetarea nu numai a unor încălcări grave, ci și a unor abateri disciplinare sau abateri de serviciu legate de acte de corupție.
- 23 Potrivit instanței de trimitere, întrebările adresate de reclamantul din litigiul principal privesc două elemente, și anume, pe de o parte, accesul la datele reținute de furnizorii de servicii de comunicații electronice în alte scopuri decât combaterea încălcărilor grave și prevenirea amenințărilor grave la adresa siguranței publice și, pe de altă parte, după obținerea acestui acces, utilizarea acestor date pentru anchetarea unor abateri de serviciu legate de corupție.
- 24 Această instanță amintește că reiese din jurisprudența Curții, în special din Hotărârea din 6 octombrie 2020, Privacy International (C-623/17, EU:C:2020:790, punctul 39), că, pe de o parte, articolul 15 alineatul (1) din Directiva 2002/58 coroborat cu articolul 3 din aceasta trebuie interpretat în sensul că intră în domeniul de aplicare al directivei menționate nu numai o măsură legislativă care impune furnizorilor de servicii de comunicații electronice să păstreze datele de transfer și datele de localizare, ci și o măsură legislativă prin care se impune acestora să acorde autorităților naționale competente accesul la aceste date. Pe de altă parte, din această jurisprudență, în special din Hotărârea din 2 martie 2021, Prokuratuur (Condițiile de acces la datele privind comunicațiile electronice) (C-746/18, EU:C:2021:152, punctele 33 și 35), ar rezulta că, în ceea ce privește obiectivul de prevenire, investigare, detectare și de urmărire penală a infracțiunilor, în conformitate cu principiul proporționalității, numai combaterea infracționalității grave și prevenirea amenințărilor grave la adresa siguranței publice sunt de natură să justifice ingerințe grave în drepturile fundamentale consacrate la articolele 7 și 8 din cartă, precum cele pe care le implică reținerea datelor de transfer și a datelor de localizare, indiferent dacă este generalizată și nediferențiată sau direcționată.

- 25 Cu toate acestea, Curtea nu s-ar fi pronunțat încă cu privire la incidența utilizării ulterioare a datelor în discuție asupra ingerinței în drepturile fundamentale. În aceste împrejurări, instanța de trimitere ridică problema dacă trebuie să se considere că o astfel de utilizare ulterioară constituie de asemenea o ingerință de o asemenea gravitate în drepturile fundamentale consacrate la articolele 7 și 8 din cartă, încât numai combaterea infraționalității grave și prevenirea amenințărilor grave la adresa siguranței publice sunt de natură să o justifice, ceea ce ar exclude posibilitatea de a utiliza aceste date în anchete privind abateri de serviciu legate de corupție.
- 26 În aceste condiții, Lietuvos vyriausiosios administracinis teismas (Curtea Administrativă Supremă a Lituaniei) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarea întrebare preliminară:

„Articolul 15 alineatul (1) din Directiva [2002/58] coroborat cu articolele 7, 8, și 11 și cu articolul 52 alineatul (1) din [cartă] trebuie interpretat în sensul că interzice autorităților publice competente să utilizeze datele stocate de furnizorii de servicii de comunicații electronice, ce pot oferi informații privind datele unui utilizator al unui mijloc de comunicare electronică și comunicațiile efectuate de acesta, în cadrul unor investigații privind abateri în serviciu legate de fapte de corupție, indiferent dacă accesul la aceste date a fost acordat, în cazul concret, în scopul combaterii infraționalității grave și al prevenirii amenințărilor grave la adresa siguranței publice?”

Cu privire la întrebarea preliminară

- 27 Prin intermediul întrebării formulate, instanța de trimitere solicită în esență să se stabilească dacă articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că se opune ca datele personale referitoare la comunicații electronice care au fost reținute, în temeiul unei măsuri legislative adoptate în temeiul acestei dispoziții, de furnizorii de servicii de comunicații electronice și care au fost ulterior puse la dispoziția autorităților competente, în temeiul acestei măsuri, în scopul combaterii criminalității grave, să poată fi utilizate în cadrul anchetelor referitoare la abateri de serviciu legate de corupție.
- 28 Cu titlu introductiv, trebuie arătat că din decizia de trimitere reiese că, deși dosarul administrativ aferent procedurii care a condus la decretele în discuție în litigiul principal, vizate la punctul 19 din prezenta hotărâre, cuprindea de asemenea informații care fuseseră colectate de autoritățile competente datorită interceptării și înregistrării comunicațiilor electronice care fuseseră autorizate, în scopul urmăririi penale, prin două ordonanțe judiciare, nu este mai puțin adevărat că instanța de trimitere nu ridică problema utilizării datelor cu caracter personal care au fost obținute fără intervenția furnizorilor de servicii de comunicații electronice, ci a utilizării ulterioare a datelor cu caracter personal care au fost reținute de astfel de furnizori în temeiul unei măsuri legislative a statului membru care le impune o astfel de obligație de reținere, în temeiul articolului 15 alineatul (1) din Directiva 2002/58.
- 29 În această privință, din indicațiile care figurează în cererea de decizie preliminară reiese că datele vizate de întrebarea adresată sunt cele reținute în temeiul articolului 65 alineatul 2 din Legea privind comunicațiile electronice coroborat cu anexa 1 la această lege, care impune furnizorilor de servicii de comunicații electronice o obligație de a reține, în mod generalizat și nediferențiat, datele de transfer și datele de localizare aferente unor astfel de comunicații în scopul combaterii infraționalității grave.

30 În ceea ce privește condițiile în care aceste date pot fi utilizate în cadrul unei proceduri administrative privind abateri de serviciu legate de corupție, trebuie amintit mai întâi că un acces la datele respective nu poate fi acordat, în aplicarea unei măsuri adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58, decât în condițiile în care aceleași date au fost stocate de acești furnizori într-o manieră conformă cu această dispoziție [a se vedea în acest sens Hotărârea din 2 martie 2021, Prokuratuur (Condițiile de acces la datele privind comunicațiile electronice), C-746/18, EU:C:2021:152, punctul 29 și jurisprudența citată]. În continuare, o utilizare ulterioară a datelor de transfer și a datelor de localizare aferente unor astfel de comunicații în scopul combaterii criminalității grave nu este posibilă decât cu condiția, pe de o parte, ca reținerea acestor date de către furnizorii de servicii de comunicații electronice să fi fost conformă articolului 15 alineatul (1) din Directiva 2002/58, astfel cum a fost interpretat în jurisprudența Curții și, pe de altă parte, ca accesul la datele menționate acordat autorităților competente să fi fost și el conform acestei dispoziții.

31 În această privință, Curtea a statuat deja că articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, se opune unor măsuri legislative care prevăd, cu titlu preventiv, în scopul combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare (Hotărârea din 20 septembrie 2022, SpaceNet și Telekom Deutschland, C-793/19 și C-794/19, EU:C:2022:702, punctele 74 și 131, precum și jurisprudența citată). În schimb, aceasta a precizat că acest articol 15 alineatul (1), citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, nu se opune unor măsuri legislative care prevăd, în scopul combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice,

- o păstrare direcționată a datelor de transfer și a datelor de localizare care să fie delimitată, pe baza unor elemente obiective și nediscriminatorii, în funcție de categoriile de persoane vizate sau prin intermediul unui criteriu geografic, pentru o perioadă limitată la strictul necesar, dar care poate fi reînnoită;
- o păstrare generalizată și nediferențiată a adreselor IP atribuite sursei unei conexiuni, pentru o perioadă limitată la strictul necesar;
- o păstrare generalizată și nediferențiată a datelor referitoare la identitatea civilă a utilizatorilor de mijloace de comunicații electronice și
- impunerea unei obligații furnizorilor de servicii de comunicații electronice, prin intermediul unei decizii a autorității competente supuse unui control jurisdicțional efectiv, de a efectua, pentru o perioadă determinată, păstrarea rapidă a datelor de transfer și a datelor de localizare de care dispun acești furnizori de servicii,

din moment ce aceste măsuri garantează, prin norme clare și precise, că stocarea datelor în discuție este condiționată de respectarea condițiilor materiale și procedurale aferente acestora și că persoanele în cauză dispun de garanții efective împotriva riscurilor de abuz (Hotărârea din 20 septembrie 2022, SpaceNet și Telekom Deutschland, C-793/19 și C-794/19, EU:C:2022:702, punctul 75 și jurisprudența citată).

32 În ceea ce privește obiectivele care pot justifica utilizarea de către autoritățile publice a datelor păstrate de furnizorii de servicii de comunicații electronice în aplicarea unei măsuri conforme cu aceste dispoziții, trebuie amintit că articolul 15 alineatul (1) din Directiva 2002/58 permite statelor

membre să introducă excepții de la obligația de principiu, prevăzută la articolul 5 alineatul (1) din această directivă, de garantare a confidențialității datelor cu caracter personal, precum și de la obligațiile corespunzătoare, menționate în special la articolele 6 și 9 din directiva menționată, în cazul în care o astfel de restricție constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice pentru a proteja securitatea națională, apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a infracțiunilor sau a folosirii neautorizate a sistemelor de comunicații electronice. În acest scop, statele membre pot adopta, *inter alia*, măsuri legislative care să permită reținerea de date pe perioadă limitată pentru unul dintre aceste motive (Hotărârea din 6 octombrie 2020, *La Quadrature du Net și alții*, C-511/18, C-512/18 și C-520/18, EU:C:2020:791, punctul 110).

- 33 Or, articolul 15 alineatul (1) din Directiva 2002/58 nu poate să justifice ca derogarea de la obligația de principiu de a garanta confidențialitatea comunicațiilor electronice și a datelor aferente și în special de la interdicția de a stoca datele respective, prevăzută la articolul 5 din directiva menționată, să devină regula, fără a goli în mare măsură această din urmă dispoziție de conținutul său (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 40).
- 34 În ceea ce privește obiectivele susceptibile să justifice o restrângere a drepturilor și a obligațiilor prevăzute, printre altele, la articolele 5, 6 și 9 din Directiva 2002/58, Curtea a statuat deja că enumerarea obiectivelor care figurează la articolul 15 alineatul (1) prima teză din această directivă prezintă un caracter exhaustiv, așa încât o măsură legislativă adoptată în temeiul acestei dispoziții trebuie să urmărească în mod efectiv și strict unul dintre aceste obiective (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 41).
- 35 În ceea ce privește obiectivele de interes general care pot justifica o măsură adoptată în temeiul articolului 15 alineatul (1) din Directiva 2002/58, reiese din jurisprudența Curții că, în conformitate cu principiul proporționalității, există o ierarhie între aceste obiective în funcție de importanța lor respectivă și că importanța obiectivului urmărit de o asemenea măsură trebuie să se raporteze la gravitatea ingerinței care rezultă din aceasta (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 56).
- 36 În această privință, importanța obiectivului de apărare a securității naționale, interpretat în lumina articolului 4 alineatul (2) TUE, potrivit căruia apărarea securității naționale rămâne responsabilitatea exclusivă a fiecărui stat membru, o depășește pe cea a celorlalte obiective prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, în special a obiectivelor de combatere a criminalității în general, chiar grave, precum și de protejare a siguranței publice. Sub rezerva respectării celorlalte cerințe prevăzute la articolul 52 alineatul (1) din cartă, obiectivul de apărare a securității naționale poate justifica, așadar, măsuri care presupun ingerințe mai grave în drepturile fundamentale decât cele pe care le-ar putea justifica celelalte obiective (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 57, precum și jurisprudența citată).
- 37 În ceea ce privește obiectivul de prevenire, investigare, detectare și urmărire penală a infracțiunilor, Curtea a arătat că, în conformitate cu principiul proporționalității, numai combaterea criminalității grave și prevenirea amenințărilor grave la adresa siguranței publice sunt de natură să justifice ingerințe grave în drepturile fundamentale consacrate la articolele 7 și 8 din cartă, precum cele pe care le implică păstrarea datelor de transfer și a datelor de localizare. Prin urmare, numai ingerințele în drepturile fundamentale menționate care nu au

caracter grav pot fi justificate de obiectivul de prevenire, investigare, detectare și urmărire penală a infracțiunilor în general (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 59, precum și jurisprudența citată).

- 38 Din această jurisprudență reiese că, deși combaterea criminalității grave și prevenirea amenințărilor grave la adresa siguranței publice au o importanță mai redusă, în ierarhia obiectivelor de interes general, decât apărarea securității naționale (a se vedea în acest sens Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 99), importanța lor depășește totuși pe cea a combaterii infracțiunilor în general și a prevenirii unor amenințări care nu sunt grave la adresa siguranței publice.
- 39 În acest context, trebuie amintit totuși că, astfel cum reiese și din cuprinsul punctului 31 din prezenta hotărâre, posibilitatea statelor membre de a justifica o restrângere a drepturilor și a obligațiilor prevăzute printre altele la articolele 5, 6 și 9 din Directiva 2002/58 trebuie să fie apreciată măsurând gravitatea ingerinței pe care o implică o asemenea restrângere și verificând dacă importanța obiectivului de interes general urmărit prin restrângerea respectivă se raportează la această gravitate (Hotărârea din 6 octombrie 2020, La Quadrature du Net și alții, C-511/18, C-512/18 și C-520/18, EU:C:2020:791, punctul 131).
- 40 În plus, Curtea a statuat deja că accesul la datele de transfer și la datele de localizare păstrate de furnizori în aplicarea unei măsuri adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58, care trebuie să aibă loc cu respectarea deplină a condițiilor care rezultă din jurisprudența de interpretare a acestei directive, nu poate fi justificat, în principiu, decât prin obiectivul de interes general în vederea căruia această păstrare a fost impusă furnizorilor respectivi. Situația este diferită numai dacă importanța obiectivului urmărit prin acces o depășește pe cea a obiectivului care a justificat păstrarea (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 98, precum și jurisprudența citată).
- 41 Or, aceste considerații se aplică *mutatis mutandis* unei utilizări ulterioare a datelor de transfer și a datelor de localizare păstrate de furnizorii de servicii de comunicații electronice în aplicarea unei măsuri adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58 în scopul combaterii criminalității grave. Astfel, asemenea date nu pot, după ce au fost păstrate și puse la dispoziția autorităților competente în scopul combaterii criminalității grave, să fie transmise altor autorități și utilizate pentru realizarea unor obiective precum, în speță, combaterea abaterilor de serviciu legate de corupție, care au o importanță mai redusă, în ierarhia obiectivelor de interes general, decât cel al combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice. Astfel, a autoriza într-o asemenea situație accesul la datele păstrate și utilizarea lor ar contraveni acestei ierarhii a obiectivelor de interes general amintite la punctele 33, 35-37 și 40 din prezenta hotărâre (a se vedea în acest sens Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 99).
- 42 În ceea ce privește argumentul invocat de guvernul ceh și de Irlanda în observațiile lor scrise, potrivit căruia o procedură disciplinară referitoare la abateri de serviciu legate de corupție ar putea fi legată de protecția siguranței publice, este suficient să se arate că, în decizia sa de trimitere, instanța de trimitere nu a menționat o amenințare gravă la adresa siguranței publice.

- 43 Pe de altă parte, deși este adevărat că anchetele administrative privind abateri disciplinare sau abateri de serviciu legate de acte de corupție pot juca un rol important în combaterea unor astfel de acte, o măsură legislativă care prevede astfel de anchete nu răspunde în mod efectiv și strict obiectivului de urmărire și de sancționare a infracțiunilor, vizat la articolul 15 alineatul (1) prima teză din Directiva 2002/58, care nu vizează decât urmărirea penală.
- 44 Având în vedere ceea ce precedă, trebuie să se răspundă la întrebarea adresată că articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că se opune ca datele personale referitoare la comunicații electronice care au fost reținute, în aplicarea unei măsuri legislative adoptate în temeiul acestei dispoziții, de furnizorii de servicii de comunicații electronice și care au fost ulterior puse la dispoziția autorităților competente, în aplicarea acestei măsuri, în scopul combaterii criminalității grave, să poată fi utilizate în cadrul anchetelor referitoare la abateri de serviciu legate de corupție.

Cu privire la cheltuielile de judecată

- 45 Întrucât, în privința părților din litigiul principal, procedura are caracterul unui incident survenit la instanța de trimitere, este de competența acesteia să se pronunțe cu privire la cheltuielile de judecată. Cheltuielile efectuate pentru a prezenta observații Curții, altele decât cele ale părților menționate, nu pot face obiectul unei rambursări.

Pentru aceste motive, Curtea (Camera întâi) declară:

Articolul 15 alineatul (1) din 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), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene,

trebuie interpretat în sensul că

se opune ca datele personale referitoare la comunicații electronice care au fost reținute, în aplicarea unei măsuri legislative adoptate în temeiul acestei dispoziții, de furnizorii de servicii de comunicații electronice și care au fost ulterior puse la dispoziția autorităților competente, în aplicarea acestei măsuri, în scopul combaterii criminalității grave, să poată fi utilizate în cadrul anchetelor referitoare la abateri de serviciu legate de corupție.

Semnături