



Repertoriul jurisprudenței

HOTĂRÂREA CURȚII (Marea Cameră)

20 septembrie 2022*

[Text îndreptat prin Ordonanța din 27 octombrie 2022]

„Trimitere preliminară – Prelucrarea datelor personale în sectorul comunicațiilor electronice – Confidențialitatea comunicațiilor – Furnizori de servicii de comunicații electronice – Păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare – Directiva 2002/58/CE – Articolul 15 alineatul (1) – Carta drepturilor fundamentale a Uniunii Europene – Articolele 6, 7, 8 și 11, precum și articolul 52 alineatul (1) – Articolul 4 alineatul (2) TUE”

În cauzele conexe C-793/19 și C-794/19,

având ca obiect cereri de decizie preliminară formulate în temeiul articolului 267 TFUE de Bundesverwaltungsgericht (Curtea Administrativă Federală, Germania), prin deciziile din 25 septembrie 2019, primite de Curte la 29 octombrie 2019, în procedurile

Bundesrepublik Deutschland, reprezentată de Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

împotriva

SpaceNet AG (C-793/19),

Telekom Deutschland GmbH (C-794/19),

CURTEA (Marea Cameră),

compusă din domnul K. Lenaerts, președinte, domnul A. Arabadjiev, doamna A. Prechal, domnii S. Rodin și I. Jarukaitis și doamna I. Ziemele, președinți de cameră, domnii T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (raportor) și N. Piçarra, doamna L. S. Rossi și domnul A. Kumin, judecători,

avocat general: domnul M. Campos Sánchez-Bordona,

grefier: domnul D. Dittert, șef de unitate,

având în vedere procedura scrisă și în urma ședinței din 13 septembrie 2021,

* Limba de procedură: germana.

luând în considerare observațiile prezentate:

- pentru Bundesrepublik Deutschland, reprezentată de Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, de C. Mögelin, în calitate de agent;
- [Astfel cum a fost îndreptat prin Ordonanța din 27 octombrie 2022] pentru SpaceNet AG, de M. Bäcker, Universitätsprofessor;
- pentru Telekom Deutschland GmbH, de T. Mayen, Rechtsanwalt;
- pentru guvernul german, de J. Möller, F. Halibi, M. Hellmann, D. Klebs și E. Lankenau, în calitate de agenți;
- pentru guvernul danez, de M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen și M. Søndahl Wolff, în calitate de agenți;
- pentru guvernul estonian, de A. Kalbus și M. Kriisa, în calitate de agenți;
- pentru Irlanda, de A. Joyce și J. Quaney, în calitate de agenți, asistați de D. Fennelly, BL, și de P. Gallagher, SC;
- pentru guvernul spaniol, de L. Aguilera Ruiz, în calitate de agent;
- pentru guvernul francez, de A. Daniel, D. Dubois, J. Illouz, E. de Moustier și T. Stéhelin, în calitate de agenți;
- pentru guvernul cipriot, de I. Neophytou, în calitate de agent;
- pentru guvernul neerlandez, de M. K. Bulterman, A. Hanje și C. S. Schillemans, în calitate de agenți;
- pentru guvernul polonez, de B. Majczyna, D. Lutostańska și J. Sawicka, în calitate de agenți;
- pentru guvernul finlandez, de A. Laine și M. Pere, în calitate de agenți;
- pentru guvernul suedez, de H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson și H. Shev, în calitate de agenți;
- pentru Comisia Europeană, de G. Braun, S. L. Kaléda, H. Kranenborg, M. Wasmeier și F. Wilman, în calitate de agenți;
- pentru Autoritatea Europeană pentru Protecția Datelor, de A. Buchta, D. Nardi, N. Stolič și K. Ujazdowski, în calitate de agenți,

după ascultarea concluziilor avocatului general în ședința din 18 noiembrie 2021,

pronunță prezenta

Hotărâre

- 1 Cererile de decizie preliminară privesc 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 [electronice] (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”), citit în lumina articolelor 6-8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”) și a articolului 4 alineatul (2) TUE.
- 2 Aceste cereri au fost formulate în cadrul unor litigii între Bundesrepublik Deutschland (Republica Federală Germania), reprezentată de Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Agenția federală a rețelelor de electricitate, gaz, telecomunicații, poștă și căi ferate, Germania), pe de o parte, și SpaceNet AG (cauza C-793/19) și Telekom Deutschland GmbH (cauza C-794/19), pe de altă parte, în legătură cu obligația impusă acestora din urmă de a păstra date de transfer și date de localizare aferente telecomunicațiilor clienților lor.

Cadrul juridic

Dreptul Uniunii

Directiva 95/46/CE

- 3 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 (JO 1995, L 281, p. 31, Ediție specială, 13/vol. 17, p. 10) a fost abrogată cu efect de la 25 mai 2018 prin 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 (Regulamentul general privind protecția datelor) (JO 2016, L 119, p. 1).
- 4 Articolul 3 alineatul (2) din Directiva 95/46 prevedea:
„Prezenta directivă nu se aplică prelucrării datelor cu caracter personal:
– puse în practică pentru exercitarea activităților din afara domeniului de aplicare a dreptului comunitar, cum ar fi cele prevăzute în titlurile V și VI din Tratatul privind Uniunea Europeană și, în orice caz, prelucrărilor care au ca obiect siguranța publică, apărarea, securitatea statului (inclusiv bunăstarea economică a statului atunci când aceste prelucrări sunt legate de probleme de securitate a statului) și a activităților statului în domeniul dreptului penal;
– efectuate de către o persoană fizică în cursul unei activități exclusiv personale sau domestice.”

Directiva 2002/58

5 Considerentele (2), (6), (7) și (11) ale Directivei 2002/58 enunță:

„(2) Prezenta directivă dorește respectarea drepturilor fundamentale și a principiilor recunoscute în special de [cartă]. Directiva caută să asigure în special respectarea deplină a drepturilor menționate la articolele 7 și 8 [din aceasta].

[...]

(6) Internetul a răsturnat structurile de piață tradiționale furnizând o infrastructură comună la nivel global pentru o gamă foarte largă de servicii de comunicare electronică. Serviciile de comunicare electronică publice prin internet deschid noi posibilități pentru utilizatori, dar reprezintă și noi riscuri pentru datele lor personale și pentru confidențialitatea comunicațiilor lor.

(7) În cazul rețelelor de comunicații publice, ar trebui adoptate acte cu putere de lege, norme administrative și norme tehnice pentru protejarea drepturilor și libertăților fundamentale ale persoanelor fizice și a intereselor legitime ale persoanelor juridice, mai cu seamă în privința capacităților în creștere de stocare automată și de prelucrare a datelor referitoare la abonați și utilizatori.

[...]

(11) La fel ca Directiva [95/46], prezenta directivă nu se referă la chestiuni de protecție a drepturilor și libertăților fundamentale legate de activități care nu sunt reglementate de legile comunitare. Prin urmare, aceasta nu aduce atingere echilibrului existent între dreptul indivizilor la confidențialitate și posibilitatea ca statele membre să ia măsurile stipulate la articolul 15 alineatul (1) al prezentei directive, posibilitate necesară în vederea protejării siguranței publice, apărării și siguranței statului (inclusiv bunăstării economice a acestuia, în cazul în care activitățile respective sunt legate de chestiuni de siguranță a statului) și întăririi legii penale. În consecință, prezenta directivă nu interzice statelor membre să efectueze interceptări legale ale comunicațiilor electronice sau să ia alte măsuri pentru atingerea scopurilor menționate anterior, dacă acest lucru este necesar și în conformitate cu Convenția Europeană pentru Protecția Drepturilor Omului și a Libertăților Fundamentale, [semnată la Roma la 4 noiembrie 1950,] așa cum este aceasta interpretată de Curtea Europeană a Drepturilor Omului. Aceste măsuri trebuie să fie corespunzătoare, strict proporționale cu scopul urmărit și necesare în cadrul unei societăți democratice și trebuie însoțite de precauțiile corespunzătoare în conformitate cu Convenția europeană pentru protecția drepturilor omului și a libertăților fundamentale.”

6 Articolul 1 din această directivă, 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.

(2) Prevederile prezentei directive precizează și completează Directiva [95/46] în scopurile menționate la alineatul (1). Mai mult, acestea sunt menite a asigura protecția intereselor legitime ale abonaților persoane juridice.

(3) Prezenta directivă nu se aplică activităților care nu sunt cuprinse în domeniul de aplicare al [Tratatului FUE], cum sunt cele menționate la titlurile V și VI ale Tratatului [UE], 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 siguranță a statului) și activităților statului în domeniul legii penale.”

7 Potrivit articolului 2 din directiva menționată, intitulat „Definiții”:

„Cu excepția cazurilor în care se precizează altfel, se aplică definițiile din Directiva [95/46] și din Directiva 2002/21/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind cadrul comun de reglementare a rețelelor și serviciilor de comunicații electronice (Directiva-cadru) [(JO 2002, L 108, p. 33, Ediție specială, 13/vol. 35, p. 195)].

Se aplică de asemenea următoarele definiții:

- (a) «utilizator» înseamnă orice persoană fizică ce folosește un serviciu public de comunicații electronice, în scopuri profesionale sau personale, fără a fi în mod necesar abonat la serviciul respectiv;
- (b) «date de transfer» înseamnă orice date prelucrate în scopul transmiterii comunicației printr-o rețea de comunicații electronice sau în vederea facturării;
- (c) «date de localizare» înseamnă orice date prelucrate într-o rețea de comunicații electronice sau prin intermediul unui serviciu de comunicații electronice, care indică poziția geografică a echipamentului terminal al unui utilizator al unui serviciu de comunicații electronice destinat publicului;
- (d) «comunicație» înseamnă orice informație trimisă sau transmisă între un număr finit de părți prin intermediul unui serviciu public de comunicații electronice. Această categorie nu include informațiile transmise în cadrul unui serviciu de radiodifuziune pentru public prin intermediul unei rețele de comunicații electronice, în măsura în care aceste informații nu pot fi relaționate cu un abonat sau cu un utilizator identificabil care primește informația;

[...]”

8 Articolul 3 din Directiva 2002/58, intitulat „Serviciile vizate”, prevede:

„Prezenta directivă se aplică prelucrării de date cu caracter personal legate de furnizarea de servicii de comunicații electronice destinate publicului prin intermediul rețelelor publice de comunicații din cadrul Comunității, inclusiv al rețelelor publice de comunicații care presupun colectarea de date și dispozitive de identificare.”

9 Potrivit articolului 5 din această directivă, intitulat „Confidențialitatea comunicațiilor”:

„(1) Statele membre trebuie să asigure confidențialitatea comunicațiilor și a datelor de transfer aferente transmise prin intermediul unei rețele de comunicații publice sau 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.

[...]

(3) Statele membre se asigură că stocarea de informații sau dobândirea accesului la informațiile deja stocate în echipamentul terminal al unui abonat sau utilizator este permisă doar cu condiția ca abonatul sau utilizatorul în cauză să își fi dat acordul, după ce a primit informații clare și complete, în conformitate cu Directiva [95/46], *inter alia*, cu privire la scopurile prelucrării. Aceasta nu împiedică stocarea sau accesul tehnic cu unicul scop de a efectua transmisia comunicării printr-o rețea de comunicații electronice sau în cazul în care acest lucru este strict necesar în vederea furnizării de către furnizor a unui serviciu al societății informaționale cerut în mod expres de către abonat sau utilizator.”

10 Articolul 6 din Directiva 2002/58, intitulat „Datele de transfer”, prevede:

„(1) Datele de transfer referitoare la abonați și utilizatori prelucrate și stocate de către furnizorul rețelei de comunicații publice sau al serviciilor publice de comunicații electronice trebuie șterse sau trecute în anonimat de îndată ce nu mai sunt necesare în scopul transmiterii comunicației, fără a aduce atingere alineatelor (2), (3) și (5) din prezentul articol sau articolului 15 alineatul (1).

(2) Datele de transfer necesare în vederea facturării serviciilor oferite abonatului sau plății conexiunii pot să fie prelucrate. Prelucrarea lor este permisă doar până la sfârșitul perioadei în care factura poate fi contestată prin lege sau plata poate fi urmărită.

(3) În scopul comercializării de servicii de comunicații electronice sau al furnizării de servicii cu valoare adăugată, furnizorul de servicii de comunicații electronice destinate publicului poate prelucra datele menționate la alineatul (1) în măsura și pe durata de timp necesare comercializării sau furnizării acestor servicii, dacă abonatul sau utilizatorul vizat de datele respective și-a dat, în prealabil, consimțământul în acest sens. Utilizatorii și abonații au posibilitatea de a-și retrace consimțământul pentru prelucrarea datelor de trafic în orice moment.

[...]

(5) Prelucrarea de date de transfer în conformitate cu alineatele (1), (2), (3) și (4) trebuie limitată la persoanele care acționează sub autoritatea furnizorilor de rețele de comunicații publice sau de servicii publice de comunicații electronice în vederea facturării sau pentru gestionarea traficului, serviciul clientelă, detectarea fraudelor, promovarea serviciilor de comunicații electronice sau furnizarea de servicii suplimentare și trebuie să se limiteze la prelucrarea strict necesară scopului respectivei activități.

[...]”

- 11 Articolul 9 din această directivă, intitulat „Datele de localizare, altele decât datele de transfer”, prevede la alineatul (1):

„În cazul în care datele de localizare, altele decât datele de transfer, referitoare la abonați sau utilizatori ai rețelelor de comunicații publice sau ai serviciilor publice de comunicații electronice pot fi prelucrate, aceste date pot fi prelucrate doar dacă sunt anonime sau cu acordul utilizatorilor sau abonaților respectivi, în măsura și pe perioada cât sunt necesare în vederea furnizării unui serviciu suplimentar. Prestatorul de servicii trebuie să informeze utilizatorii și abonații, înainte de obținerea acordului lor, despre tipul de date de localizare altele decât datele de transfer care vor fi prelucrate, despre scopul și durata prelucrării și dacă datele respective vor fi transmise unor terțe părți în scopul furnizării de servicii suplimentare. [...]”

- 12 Articolul 15 din Directiva 2002/58, intitulat „Aplicarea anumitor dispoziții ale Directivei [95/46]”, 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 [a se citi «cu alte cuvinte»] 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]. 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 german

TKG

- 13 Articolul 113a alineatul (1) prima teză din Telekommunikationsgesetz (Legea privind telecomunicațiile) din 22 iunie 2004 (BGBl. 2004 I, p. 1190), în versiunea aplicabilă litigiilor principale (denumită în continuare „TKG”), are următorul cuprins:

„Obligațiile privind păstrarea, utilizarea și securitatea datelor de transfer definite la articolele 113b-113g se referă la operatorii care furnizează utilizatorilor finali servicii publice de telecomunicații.”

- 14 Potrivit articolului 113b din TKG:

„(1) Operatorii menționați la articolul 113a alineatul (1) păstrează datele pe teritoriul național după cum urmează:

1. 10 săptămâni în cazul datelor menționate la alineatele (2) și (3),
2. 4 săptămâni în cazul datelor de localizare menționate la alineatul (4).

(2) Furnizorii de servicii publice de telefonie păstrează:

1. numărul de telefon sau alt identificator al liniei apelante și al liniei apelate, precum și al oricărei alte linii utilizate în cazul redirectionării sau al transferului apelului,
2. data și ora de început și de sfârșit al conexiunii, cu indicarea fusului orar,
3. indicațiile privind serviciul utilizat, în cazul în care în cadrul serviciului telefonic pot fi utilizate servicii diferite,
4. în plus, în cazul serviciilor de telefonie mobilă,
 - a) identificatorul internațional al utilizatorului dispozitivului mobil pentru linia apelantă și pentru linia apelată,
 - b) identificatorul internațional al terminalului de pe care se inițiază apelul și al celui apelat,
 - c) data și ora primei activări a serviciului, cu indicarea fusului orar respectiv, dacă este vorba despre servicii plătite în avans,
5. precum și, în cazul serviciilor de telefonie prin internet, adresele IP (protocol internet) ale liniei apelante și ale liniei apelate și numerele de identificare atribuite.

Primul paragraf se aplică *mutatis mutandis*

1. în cazul transmiterii de mesaje scurte, multimedia sau similare; în acest caz, indicațiile menționate la alineatul (1) punctul 2 se înlocuiesc cu momentul trimiterii și al primirii mesajului;
2. apelurilor fără răspuns sau nereușite ca urmare a intervenției operatorului de rețea [...]

(3) Furnizorii de servicii publice de acces la internet păstrează

1. adresa IP atribuită abonatului în scopul utilizării internetului,
2. identificarea clară a conexiunii care permite accesul la internet, precum și numărul de identificare atribuit,
3. data și ora de început și de sfârșit al utilizării internetului de la adresa IP atribuită, cu indicarea fusului orar.

(4) În cazul utilizării serviciilor de telefonie mobilă, se păstrează denumirea celulelor care au fost utilizate la începutul comunicației de către apelant și de către apelat. În ceea ce privește serviciile publice de acces la internet, în cazul unei utilizări mobile, se păstrează denumirea celulelor utilizate la începutul conexiunii la internet. Este necesar de asemenea să se păstreze datele care permit cunoașterea poziției geografice și a direcțiilor de radiație maximă a antenelor care deservește celula în cauză.

(5) Conținutul comunicației, datele privind site-urile internet accesate și datele serviciilor de poștă electronică nu pot fi păstrate în temeiul prezentei dispoziții.

(6) Datele care stau la baza comunicațiilor menționate la articolul 99 alineatul (2) nu pot fi păstrate în temeiul prezentei dispoziții. Acest lucru se aplică *mutatis mutandis* comunicațiilor

telefonice care provin de la entitățile indicate la articolul 99 alineatul (2). Articolul 99 alineatul (2) tezele a doua-a șaptea se aplică *mutatis mutandis*.

[...]

15 Comunicațiile menționate la articolul 99 alineatul (2) din TKG, la care face trimitere articolul 113b alineatul (6) din TKG, sunt realizate cu persoane, autorități și organizații cu caracter social sau religios care propun în exclusivitate sau în principal unor apelanți care rămân în principiu anonimi servicii de asistență telefonică în situații de urgență psihologică sau socială și care sunt ele însele supuse sau ai căror colaboratori sunt supuși unor obligații speciale de confidențialitate în această privință. Derogarea prevăzută la articolul 99 alineatul (2) a doua și a patra teză din TKG este condiționată de înscrierea apelărilor, la cererea lor, pe o listă întocmită de Agenția federală a rețelelor de electricitate, gaz, telecomunicații, poștă și căi ferate, după ce titularii numerelor de apel și-au dovedit misiunea prin prezentarea unei atestații din partea unei autorități, a unui organism, a unei instituții sau a unei fundații de drept public.

16 Potrivit articolului 113c alineatele (1) și (2) din TKG:

„(1) Datele păstrate în temeiul articolului 113b pot

1. să fie transmise unei autorități de aplicare a legii atunci când aceasta solicită transmiterea în temeiul unei dispoziții legale care o autorizează să colecteze datele menționate la articolul 113b în scopul urmăririi unor infracțiuni deosebit de grave;
2. să fie transmise unei autorități de securitate a landurilor atunci când aceasta solicită transmiterea în temeiul unei dispoziții legale care o autorizează să colecteze datele menționate la articolul 113b în scopul prevenirii unui risc concret pentru integritatea fizică, viața sau libertatea unei persoane sau pentru existența statului federal sau a landului;

[...]

(2) Datele păstrate în temeiul articolului 113b nu pot fi utilizate de persoanele supuse obligațiilor prevăzute la articolul 113a alineatul (1) în alte scopuri decât cele menționate la alineatul (1).”

17 Articolul 113d din TKG prevede:

„Debitorul obligației prevăzute la articolul 113a alineatul (1) se asigură că datele păstrate în conformitate cu articolul 113b alineatul (1) în temeiul obligației de păstrare sunt protejate împotriva controlului și a utilizării neautorizate prin măsuri tehnice și organizatorice în conformitate cu stadiul actual al tehnologiei. Aceste măsuri includ în special:

1. utilizarea unei procedeu de criptare foarte sigur,
2. stocarea în infrastructuri de stocare distincte, separate de cele destinate funcțiilor operaționale obișnuite,
3. stocarea, cu un nivel ridicat de protecție împotriva atacurilor cibernetice, în sisteme informatice de prelucrare a datelor offline,

4. limitarea accesului la instalațiile utilizate pentru prelucrarea datelor la persoanele care dețin o autorizație specială acordată de persoana responsabilă pentru îndeplinirea obligației și
 5. obligația de a asigura intervenția, cu ocazia accesării datelor, a cel puțin două persoane care dețin o autorizație specială acordată de către persoana responsabilă pentru îndeplinirea obligației.”
- 18 Articolul 113e din TKG are următorul cuprins:
- „(1) Debitorul obligației prevăzute la articolul 113a alineatul (1) se asigură că, în scopul controlului protecției datelor, se înregistrează fiecare accesare, în special citirea, copierea, modificarea, ștergerea și blocarea datelor păstrate în conformitate cu articolul 113b alineatul (1) în temeiul obligației de păstrare. Se înregistrează următoarele elemente:
1. ora accesării;
 2. persoanele care accesează datele;
 3. obiectul și natura accesului.
- (2) Datele înregistrate nu pot fi utilizate în alte scopuri decât pentru controlul protecției datelor.
- (3) Debitorul obligației prevăzute la articolul 113a alineatul (1) trebuie să se asigure că datele înregistrate sunt eliminate după un an.”
- 19 Pentru a garanta un nivel de siguranță și de calitate a datelor deosebit de ridicat, Agenția federală a rețelelor de electricitate, gaz, telecomunicații, poștă și căi ferate stabilește, conform articolului 113f alineatul (1) din TKG, un ansamblu de cerințe care, în temeiul articolului 113f alineatul (2) din aceasta, trebuie să fie evaluat în permanență și adaptat dacă este cazul. Articolul 113g din TKG impune ca măsuri de securitate specifice să fie integrate în expunerea politicii în materie de securitate care trebuie prezentată de debitor.
- StPO*
- 20 Articolul 100g alineatul (2) a doua teză din Strafprozessordnung (Codul de procedură penală, denumit în continuare „StPO”) are următorul cuprins:
- „În cazul în care anumite fapte dau naștere suspiciunii că o persoană a săvârșit, în calitate de autor sau de complice, una dintre infracțiunile deosebit de grave prevăzute în a doua teză sau în cazul în care a realizat tentativa de a săvârși o infracțiune care este de asemenea deosebit de gravă în situația respectivă, iar această tentativă se sancționează, datele privind traficul, păstrate în conformitate cu articolul 113b din [TKG], pot fi colectate dacă cercetarea faptelor sau localizarea persoanei cercetate ar fi excesiv de dificilă sau imposibil de realizat prin alte mijloace și în cazul în care colectarea datelor este proporțională cu importanța cazului.”
- 21 Articolul 101a alineatul (1) din StPO supune unei autorizări judiciare colectarea datelor de transfer în conformitate cu articolul 100g din StPO. În temeiul articolului 101a alineatul (2) din StPO, motivarea deciziei trebuie să cuprindă considerațiile esențiale referitoare la caracterul necesar și adecvat al măsurii în cazul specific în discuție. Articolul 101a alineatul (6) din StPO prevede o obligație de informare a participanților la telecomunicația vizată.

Litigiile principale și întrebarea preliminară

- 22 SpaceNet și Telekom Deutschland furnizează în Germania servicii publice de acces la internet. Cea de a doua furnizează de asemenea, tot în Germania, servicii publice de telefonie.
- 23 Acești furnizori de servicii au contestat la Verwaltungsgericht Köln (Tribunalul Administrativ din Köln, Germania) obligația care le este impusă de dispozițiile coroborate ale articolului 113a alineatul (1) și ale articolului 113b din TKG de a păstra date de transfer și date de localizare aferente telecomunicațiilor clienților lor începând cu 1 iulie 2017.
- 24 Prin hotărârile din 20 aprilie 2018, Verwaltungsgericht Köln (Tribunalul Administrativ din Köln) a statuat că SpaceNet și Telekom Deutschland nu erau obligate să păstreze datele de transfer aferente telecomunicațiilor, prevăzute la articolul 113b alineatul (3) din TKG, ale clienților cărora le furnizează acces la internet și că, în plus, Telekom Deutschland nu era obligată să păstreze datele de trafic aferente telecomunicațiilor, prevăzute la articolul 113b alineatul (2) prima și a doua teză din TKG, ale clienților cărora le furnizează acces la servicii publice de telefonie. Astfel, instanța respectivă a considerat, în lumina Hotărârii din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970), că această obligație de păstrare este contrară dreptului Uniunii.
- 25 Republica Federală Germania a formulat recursuri împotriva acestor hotărâri la Bundesverwaltungsgericht (Curtea Administrativă Federală, Germania), instanța de trimitere.
- 26 Aceasta apreciază că problema dacă obligația de păstrare impusă de dispozițiile coroborate ale articolului 113a alineatul (1) și ale articolului 113b din TKG este contrară dreptului Uniunii depinde de interpretarea Directivei 2002/58.
- 27 În această privință, instanța de trimitere arată că Curtea a stabilit deja în mod definitiv, în Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970), că reglementările privind păstrarea datelor de transfer și a datelor de localizare, precum și accesul autorităților naționale la aceste date intră, în principiu, în domeniul de aplicare al Directivei 2002/58.
- 28 Ea arată de asemenea că obligația de păstrare în discuție în litigiile principale, în măsura în care limitează drepturile care decurg din articolul 5 alineatul (1), din articolul 6 alineatul (1) și din articolul 9 alineatul (1) din Directiva 2002/58, nu ar putea fi justificată decât în temeiul articolului 15 alineatul (1) din această directivă.
- 29 În această privință, ea amintește că din Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970), reiese 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 unei reglementări naționale care prevede, în scopul combaterii criminalității, o păstrare generalizată și nediferențiată a ansamblului datelor de transfer și a datelor de localizare ale tuturor abonaților și ale utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică.
- 30 Or, potrivit instanței de trimitere, asemenea reglementărilor naționale în discuție în cauzele în care s-a pronunțat hotărârea menționată, reglementarea națională în discuție în litigiile principale nu impune niciun motiv pentru păstrarea datelor și nici vreo legătură între datele păstrate și o infracțiune sau un risc pentru siguranța publică. Astfel, această reglementare

- națională ar impune păstrarea, fără motiv, generalizată și nediferențiată din punct de vedere personal, temporal și geografic, a majorității datelor de transfer relevante care sunt aferente unor telecomunicații.
- 31 Instanța de trimitere consideră însă că nu este exclus ca obligația de păstrare în discuție în litigiile principale să poată fi justificată în temeiul articolului 15 alineatul (1) din Directiva 2002/58.
- 32 În primul rând, ea arată că, spre deosebire de reglementările naționale în discuție în cauzele în care s-a pronunțat Hotărârea din 21 decembrie 2016, *Tele2 Sverige și Watson și alții* (C-203/15 și C-698/15, EU:C:2016:970), reglementarea națională în discuție în litigiile principale nu impune păstrarea ansamblului datelor de transfer care sunt aferente telecomunicațiilor tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică. Nu numai că conținutul comunicațiilor ar fi exclus de la obligația de păstrare, dar nici datele referitoare la site-urile internet consultate, datele serviciilor de curierat electronic și datele care stau la baza comunicațiilor cu caracter social sau religios către sau provenite de la anumite linii nu ar putea fi păstrate, astfel cum reiese din articolul 113b alineatele (5) și (6) din TKG.
- 33 În al doilea rând, această instanță arată că articolul 113b alineatul (1) din TKG prevede o perioadă de păstrare de 4 săptămâni pentru datele de localizare și de 10 săptămâni pentru datele de transfer, în timp ce Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE (JO 2006, L 105, p. 54, Ediție specială, 13/vol. 53, p. 51), pe care se întemeiau reglementările naționale în discuție în cauzele în care s-a pronunțat Hotărârea din 21 decembrie 2016, *Tele2 Sverige și Watson și alții* (C-203/15 și C-698/15, EU:C:2016:970), prevedea o perioadă de păstrare cuprinsă între șase luni și doi ani.
- 34 Or, potrivit instanței de trimitere, deși excluderea anumitor mijloace de comunicare sau a anumitor categorii de date și limitarea perioadei de păstrare nu sunt suficiente pentru a elimina orice risc de stabilire a unui profil complet al persoanelor vizate, acest risc ar fi cel puțin redus în mod considerabil în cadrul punerii în aplicare a reglementării naționale în discuție în litigiile principale.
- 35 În al treilea rând, această reglementare ar cuprinde limitări stricte în ceea ce privește protecția datelor păstrate și accesul la acestea. Astfel, pe de o parte, ea ar garanta o protecție eficientă a datelor păstrate împotriva riscurilor de abuz, precum și împotriva oricărui acces ilicit la aceste date. Pe de altă parte, datele păstrate nu ar putea fi utilizate decât în scopul combaterii infracțiunilor grave sau în scopul prevenirii unui risc concret pentru integritatea fizică, pentru viața sau pentru libertatea unei persoane ori pentru existența statului federal sau a unui land.
- 36 În al patrulea rând, interpretarea articolului 15 alineatul (1) din Directiva 2002/58 în sensul unei incompatibilități generale cu dreptul Uniunii a oricărei păstrări de date fără motiv ar putea contraveni obligației de a acționa a statelor membre care decurge din dreptul la siguranță consacrat la articolul 6 din cartă.
- 37 În al cincilea rând, instanța de trimitere consideră că o interpretare a articolului 15 din Directiva 2002/58 în sensul că se opune unei păstrări generalizate a datelor ar restrânge în mod considerabil marja de manevră a legiuitorului național într-un domeniu legat de urmărirea infracțiunilor și de siguranța publică, care rămâne, conform articolului 4 alineatul (2) TUE, răspunderea exclusivă a fiecărui stat membru.

- 38 În al șaselea rând, instanța de trimitere consideră că este necesar să se țină seama de jurisprudența Curții Europene a Drepturilor Omului și arată că aceasta a statuat că articolul 8 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale (denumită în continuare „CEDO”) nu se opune unor dispoziții naționale care prevăd interceptarea masivă a fluxurilor transfrontaliere de date, având în vedere amenințările cu care se confruntă în prezent numeroase state și instrumentele tehnologice pe care se pot baza în prezent teroriștii și infractorii pentru săvârșirea de fapte ilicite.
- 39 În aceste condiții, Bundesverwaltungsgericht (Curtea Administrativă Federală) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarea întrebare preliminară:

„Articolul 15 din Directiva [2002/58], citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din [cartă], pe de o parte, și a articolului 6 din [carta menționată], precum și a articolului 4 [TUE], pe de altă parte, trebuie interpretat în sensul că se opune unei reglementări naționale care impune furnizorilor de servicii publice de comunicații electronice să păstreze datele de transfer și datele de localizare ale utilizatorilor finali ai acestor servicii atunci când

- 1) această obligație nu presupune existența unui motiv specific din punct de vedere geografic, temporal sau teritorial,
- 2) obiectul obligației de păstrare în cazul furnizării de servicii publice de telefonie – inclusiv transmiterea de mesaje scurte, multimedia sau similare, precum și apelurile pierdute sau care au rămas fără răspuns – este reprezentat de următoarele date:
 - a) numărul de telefon sau alt identificator al liniei apelante și al liniei apelate, precum și, în cazul redirectionărilor sau al transferurilor, al celorlalte linii implicate,
 - b) data și ora de început și de sfârșit al conexiunii sau – în cazul transmiterii de mesaje scurte, multimedia sau similare – momentul trimiterii și al primirii mesajului, cu indicarea fusului orar respectiv,
 - c) indicații privind serviciul utilizat, dacă în cadrul serviciului telefonic pot fi utilizate servicii diferite,
 - d) în plus, în cazul serviciilor de telefonie mobilă,
 - i) identificatorul internațional al abonatului mobil pentru linia apelantă și pentru linia apelată,
 - ii) identificatorul internațional al terminalului de pe care se inițiază apelul și al celui apelat,
 - iii) data și ora primei activări a serviciului, cu indicarea fusului orar respectiv, dacă serviciile au fost plătite în avans,
 - iv) denumirile celulelor care au fost utilizate de linia apelantă și de linia apelată la începutul conexiunii,
 - e) precum și, în cazul serviciilor telefonice prin internet, adresele de protocol internet ale liniei apelante și ale liniei apelate și identifiicatorii de utilizator,
- 3) în cadrul furnizării de servicii publice de acces la internet, obiectul obligației de păstrare este reprezentat de următoarele date:
 - a) adresa de protocol internet atribuită abonatului pentru utilizarea internetului,
 - b) un identificator clar al liniei prin intermediul căreia se utilizează internetul, precum și un identificator atribuit utilizatorului,
 - c) data și ora de început și de sfârșit al utilizării internetului de la adresa de protocol internet atribuită, cu indicarea fusului orar respectiv,
 - d) în cazul utilizării mobile, denumirea celulei utilizate la începutul conexiunii la internet,

- 4) următoarele date nu pot fi păstrate:
 - a) conținutul comunicației,
 - b) datele privind site-urile internet accesate,
 - c) datele serviciilor de poștă electronică,
 - d) datele de bază ale apelurilor către sau provenite de la anumite linii aparținând persoanelor, autorităților și organizațiilor din domeniul social sau religios,
- 5) perioada de păstrare pentru datele de localizare, și anume denumirea celulei utilizate, este de 4 săptămâni, iar pentru celelalte date, perioada de păstrare este de 10 săptămâni,
- 6) este garantată o protecție eficientă a datelor păstrate împotriva riscurilor de abuz, precum și a accesului ilicit și
- 7) datele păstrate pot fi utilizate numai în scopul urmăririi unor fapte penale deosebit de grave și al prevenirii unui pericol concret pentru integritatea corporală, pentru viața sau pentru libertatea unei persoane ori pentru existența federației sau a unui land, cu excepția adresei de protocol internet alocate unui abonat pentru utilizarea internetului, a cărei utilizare este autorizată în cadrul accesului la informații privind datele păstrate în vederea urmăririi oricăror fapte penale, prevenirii unui pericol pentru siguranța publică și ordinea publică, precum și pentru îndeplinirea sarcinilor serviciilor de informații?”

Procedura în fața Curții

- 40 Prin Decizia președintelui Curții din 3 decembrie 2019, cauzele C-793/19 și C-794/19 au fost conexe pentru buna desfășurare a fazelor scrise și orale ale procedurii, precum și în vederea pronunțării hotărârii.
- 41 Prin Decizia președintelui Curții din 14 iulie 2020, procedura în cauzele conexe C-793/19 și C-794/19 a fost suspendată, în temeiul articolului 55 alineatul (1) litera (b) din Regulamentul de procedură al Curții, până la pronunțarea hotărârii în cauza La Quadrature du Net și alții (C-511/18, C-512/18 și C-520/18).
- 42 Întrucât Curtea a pronunțat la 6 octombrie 2020 hotărârea sa în cauza La Quadrature du Net și alții (C-511/18, C-512/18 și C-520/18, EU:C:2020:791), președintele Curții a dispus, la 8 octombrie 2020, reluarea procedurii în cauzele conexe C-793/19 și C-794/19.
- 43 Instanța de trimitere, căreia grefa i-a comunicat această hotărâre, a precizat că își menține cererea de decizie preliminară.
- 44 În această privință, instanța de trimitere a arătat mai întâi că obligația de păstrare prevăzută de reglementarea în discuție în litigiile principale privește un număr mai mic de date și o perioadă de păstrare mai redusă decât ceea ce prevedeau reglementările naționale în discuție în cauzele în care s-a pronunțat 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). Aceste particularități ar reduce posibilitatea ca datele păstrate să permită deducerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate.
- 45 În continuare, ea a precizat din nou că reglementarea națională în discuție în litigiile principale asigură o protecție eficientă a datelor păstrate împotriva riscurilor de abuz și de acces ilicit.

- 46 În sfârșit, ea a subliniat că subzistă incertitudini în ceea ce privește problema compatibilității cu dreptul Uniunii a păstrării adreselor IP, prevăzută de reglementarea națională în discuție în litigiile principale, ca urmare a unei incoerențe între punctele 155 și 168 din 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). Astfel, potrivit instanței de trimitere, din această hotărâre ar rezulta o incertitudine cu privire la aspectul dacă Curtea impune, pentru păstrarea adreselor IP, un motiv de păstrare legat de obiectivul de protecție a securității naționale, de combatere a criminalității grave sau de prevenire a amenințărilor grave la adresa siguranței publice, astfel cum ar rezulta din cuprinsul punctului 168 din hotărârea menționată, sau dacă păstrarea adreselor IP este permisă chiar și în lipsa unui motiv concret, doar utilizarea datelor păstrate fiind limitată de obiectivele menționate, așa cum ar rezulta din cuprinsul punctului 155 din aceeași hotărâre.

Cu privire la întrebarea preliminară

- 47 Prin intermediul întrebării preliminare, instanța de trimitere solicită în esență să se stabilească dacă articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 6-8 și 11, precum și a articolului 52 alineatul (1) din cartă și a articolului 4 alineatul (2) TUE, trebuie interpretat în sensul că se opune unei măsuri legislative naționale care, cu anumite excepții, impune furnizorilor de servicii publice de comunicații electronice – în scopurile enumerate la articolul 15 alineatul (1) din această directivă și în special în scopul urmării infracțiunilor grave sau al prevenirii unui risc concret pentru securitatea națională – păstrarea generalizată și nediferențiată a celei mai mari părți a datelor de transfer și a datelor de localizare ale utilizatorilor finali ai acestor servicii, prevăzând o perioadă de păstrare de mai multe săptămâni, precum și norme prin care se urmărește garantarea unei protecții eficiente a datelor păstrate împotriva riscurilor de abuz și împotriva oricărui acces ilicit la aceste date.

Cu privire la aplicabilitatea Directivei 2002/58

- 48 În ceea ce privește argumentația Irlandei, ca și a guvernelor francez, neerlandez, polonez și suedez, potrivit căreia reglementarea națională în discuție în litigiile principale, în măsura în care a fost adoptată în special în scopul protejării securității naționale, nu intră în domeniul de aplicare al Directivei 2002/58, este suficient să se amintească faptul că o reglementare națională care impune furnizorilor de servicii de comunicații electronice să stocheze date de transfer și date de localizare în special în scopul protecției securității naționale și al combaterii criminalității, precum cea în discuție în litigiile principale, intră în domeniul de aplicare al Directivei 2002/58 (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 104).

Cu privire la interpretarea articolului 15 alineatul (1) din Directiva 2002/58

Evocarea principiilor rezultate din jurisprudența Curții

- 49 Rezultă dintr-o jurisprudență constantă că, pentru a interpreta o dispoziție a dreptului Uniunii, trebuie să se țină seama nu numai de formularea acesteia, ci și de contextul său și de obiectivele urmărite de reglementarea din care face parte, precum și să se ia în considerare în special geneza acestei reglementări (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 32, precum și jurisprudența citată).

- 50 Din însăși formularea articolului 15 alineatul (1) din Directiva 2002/58 reiese că măsurile legislative a căror adoptare de către statele membre este autorizată de aceasta, în condițiile pe care le stabilește, pot viza numai să „restrâng[ă] sfera de aplicare” a drepturilor și a obligațiilor prevăzute printre altele la articolele 5, 6 și 9 din Directiva 2002/58 (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 33).
- 51 În ceea ce privește sistemul instituit de această directivă și în care se înscrie articolul 15 alineatul (1), trebuie amintit că, în temeiul articolului 5 alineatul (1) prima și a doua teză din directiva menționată, statele membre sunt obligate să asigure prin legislația internă confidențialitatea comunicațiilor și a datelor de transfer aferente transmise prin intermediul unei rețele de comunicații publice sau al unor servicii publice de comunicații electronice. Acestea au obligația de a interzice în special ascultarea, înregistrarea, stocarea sau alte tipuri de interceptare sau supraveghere a comunicațiilor și a datelor de transfer aferente de către alte persoane decât utilizatorul fără acordul utilizatorului în cauză, cu excepția cazurilor în care acest lucru este permis în temeiul articolului 15 alineatul (1) din aceeași directivă (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 34).
- 52 În această privință, Curtea a statuat deja că articolul 5 alineatul (1) din Directiva 2002/58 consacră principiul confidențialității atât a comunicațiilor electronice, cât și a datelor de transfer aferente și instituie, printre altele, interdicția adresată în principiu oricăror alte persoane decât utilizatorii de a stoca fără consimțământul acestora comunicațiile și datele menționate (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 107, precum și Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 35).
- 53 Această dispoziție reflectă obiectivul urmărit de legiuitorul Uniunii la adoptarea Directivei 2002/58. Astfel, din expunerea de motive a Propunerii de directivă a Parlamentului European și a Consiliului privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor [electronice] [COM(2000) 385 final], care stă la baza Directivei 2002/58, reiese că legiuitorul Uniunii a intenționat „să facă în așa fel încât un nivel ridicat de protecție a datelor cu caracter personal și a vieții private să continue să fie garantat pentru toate serviciile de comunicații electronice, indiferent de tehnologia utilizată”. Așadar, directiva menționată are ca finalitate, după cum reiese printre altele din considerentele (6) și (7) ale acesteia, să protejeze utilizatorii serviciilor de comunicații electronice împotriva riscurilor pentru datele lor personale și pentru viața lor privată care rezultă din noile tehnologii și în special din capacitățile în creștere de stocare automată și de prelucrare automată a datelor. Așa cum enunță considerentul (2) al aceleiași directive, voința legiuitorului Uniunii este de a asigura în special respectarea deplină a drepturilor enunțate la articolele 7 și 8 din cartă, referitoare la protecția vieții private, precum și, respectiv, la protecția datelor cu caracter personal (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 36, precum și jurisprudența citată).
- 54 Prin adoptarea Directivei 2002/58, legiuitorul Uniunii a concretizat astfel aceste drepturi, așa încât utilizatorii mijloacelor de comunicații electronice sunt îndreptățiți să se aștepte ca, în principiu, comunicațiile lor și datele aferente acestora să rămână, în lipsa consimțământului lor, anonime și să nu poată face obiectul unei înregistrări (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 109, precum și Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 37).

- 55 În ceea ce privește prelucrarea și stocarea de către furnizorii de servicii de comunicații electronice a datelor de transfer referitoare la abonați și utilizatori, articolul 6 din Directiva 2002/58 prevede, la alineatul (1), că aceste date trebuie șterse sau trecute în anonimat de îndată ce nu mai sunt necesare în scopul transmiterii comunicației și precizează, la alineatul (2), că datele de transfer necesare în vederea facturării serviciilor oferite abonatului sau plății conexiunii nu pot să fie prelucrate decât până la sfârșitul perioadei în care factura poate fi contestată prin lege sau plata poate fi urmărită. În ceea ce privește datele de localizare, altele decât datele de transfer, articolul 9 alineatul (1) din directiva menționată prevede că aceste date pot fi prelucrate numai în anumite condiții și doar dacă sunt anonime sau cu acordul utilizatorilor sau al abonaților respectivi.
- 56 Prin urmare, Directiva 2002/58 nu se limitează să încadreze accesul la asemenea date prin garanții care urmăresc prevenirea abuzurilor, ci consacră totodată, în special, principiul interzicerii stocării lor de către terți (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 39).
- 57 În măsura în care articolul 15 alineatul (1) din Directiva 2002/58 permite statelor membre să adopte măsuri legislative pentru a „restrânge sfera de aplicare” a drepturilor și a obligațiilor prevăzute printre altele la articolele 5, 6 și 9 din această directivă, precum cele care decurg din principiile confidențialității comunicațiilor și interzicerii stocării datelor aferente, amintite la punctul 52 din prezenta hotărâre, dispoziția respectivă enunță o excepție de la regula generală prevăzută printre altele la aceste articole 5, 6 și 9 și trebuie astfel, conform unei jurisprudențe constante, să facă obiectul unei interpretări stricte. Așadar, o asemenea dispoziție 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, precum și jurisprudența citată).
- 58 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, precum și jurisprudența citată).
- 59 În plus, din articolul 15 alineatul (1) a treia teză din Directiva 2002/58 reiese că măsurile adoptate de statele membre în temeiul acestei dispoziții trebuie să respecte principiile generale ale dreptului Uniunii, printre care figurează principiul proporționalității, și să asigure respectarea drepturilor fundamentale garantate de cartă. În această privință, Curtea a statuat deja că obligația impusă de un stat membru printr-o legislație națională furnizorilor de servicii de comunicații electronice de a păstra datele de transfer în scopul de a le pune, dacă este cazul, la dispoziția autorităților naționale competente ridică probleme cu privire la respectarea nu numai a articolelor 7 și 8 din cartă, ci și a articolului 11 din cartă, referitor la libertatea de exprimare, această libertate constituind unul dintre fundamentele esențiale al unei societăți democratice și pluraliste și făcând parte dintre valorile pe care, conform articolului 2 TUE, se întemeiază Uniunea Europeană (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, punctele 42 și 43, precum și jurisprudența citată).

- 60 Este necesar să se precizeze în această privință că păstrarea datelor de transfer și a datelor de localizare constituie în sine, pe de o parte, o derogare de la interdicția prevăzută la articolul 5 alineatul (1) din Directiva 2002/58, impusă oricărei alte persoane decât utilizatorii, de a stoca aceste date și, pe de altă parte, o ingerință în drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal, consacrate la articolele 7 și 8 din cartă, fiind irelevant dacă informațiile vizate referitoare la viața privată prezintă sau nu un caracter sensibil, dacă persoanele interesate au suferit sau nu eventuale inconveniente ca urmare a acestei ingerințe sau dacă datele păstrate vor fi sau nu utilizate ulterior (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 44, precum și jurisprudența citată).
- 61 Această concluzie este cu atât mai justificată cu cât datele de transfer și datele de localizare pot revela informații cu privire la un număr important de aspecte ale vieții private a persoanelor vizate, inclusiv informații sensibile precum orientarea sexuală, opiniile politice, convingerile religioase, filozofice, societale sau de altă natură, precum și starea de sănătate, în condițiile în care asemenea date beneficiază, pe de altă parte, de o protecție specială în dreptul Uniunii. Considerate în ansamblu, datele menționate pot permite deducerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, precum obiceiurile din viața cotidiană, locurile de reședință permanentă sau temporară, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele. Mai precis, aceste date furnizează mijloacele de a stabili profilul persoanelor vizate, informație la fel de sensibilă, din perspectiva dreptului la respectarea vieții private, ca și conținutul însuși al comunicațiilor (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 45, precum și jurisprudența citată).
- 62 Prin urmare, pe de o parte, păstrarea datelor de transfer și a datelor de localizare în scopuri polițienești poate aduce atingere dreptului la respectarea comunicațiilor, consacrat la articolul 7 din cartă, și poate avea efecte disuasive asupra exercitării de către utilizatorii mijloacelor de comunicații electronice a libertății lor de exprimare, garantată la articolul 11 din aceasta, efecte care sunt cu atât mai grave cu cât numărul și varietatea datelor păstrate sunt ridicate. Pe de altă parte, ținând seama de cantitatea importantă de date de transfer și de date de localizare care pot fi păstrate în mod continuu printr-o măsură de păstrare generalizată și nediferențiată, precum și de caracterul sensibil al informațiilor pe care le pot furniza aceste date, simpla păstrare a datelor respective de către furnizorii de servicii de comunicații electronice presupune riscuri de abuz și de acces ilicit (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 46, precum și jurisprudența citată).
- 63 În aceste condiții, în măsura în care permite statelor membre să restrângă drepturile și obligațiile menționate la punctele 51-54 din prezenta hotărâre, articolul 15 alineatul (1) din Directiva 2002/58 reflectă împrăjirea că drepturile consacrate la articolele 7, 8 și 11 din cartă nu sunt prerogative absolute, ci trebuie luate în considerare în raport cu funcția lor în societate. Astfel, după cum reiese din articolul 52 alineatul (1) din cartă, ea admite restrângeri ale exercițiului acestor drepturi cu condiția ca respectivele restrângeri să fie prevăzute de lege, să respecte substanța drepturilor respective și, prin respectarea principiului proporționalității, să fie necesare și să răspundă efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți. Așadar, interpretarea articolului 15 alineatul (1) din Directiva 2002/58 în lumina cartei impune să se țină cont de asemenea de importanța drepturilor consacrate la articolele 3, 4, 6 și 7 din cartă și de cea a obiectivelor de protecție a securității naționale și de combatere a criminalității grave, contribuind la protecția drepturilor și libertăților celorlalți (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 48, precum și jurisprudența citată).

- 64 Astfel, în ceea ce privește în special combaterea efectivă a infracțiunilor ale căror victime sunt, printre alții, minorii și celelalte persoane vulnerabile, trebuie să se țină seama de faptul că obligații pozitive în sarcina autorităților publice pot rezulta din articolul 7 din cartă, în vederea adoptării unor măsuri juridice care vizează protejarea vieții private și de familie. Asemenea obligații pot decurge de asemenea din articolul 7 menționat în ceea ce privește protecția domiciliului și a comunicațiilor și din articolele 3 și 4 în ceea ce privește protecția integrității fizice și psihice a persoanelor, precum și interzicerea torturii și a tratamentelor inumane și degradante (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 49, precum și jurisprudența citată).
- 65 În raport cu aceste diferite obligații pozitive, este necesar deci să se realizeze o conciliere a diverselor interese legitime și drepturi în cauză și să se instituie un cadru legal care să permită această conciliere (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 50, precum și jurisprudența citată).
- 66 În acest cadru, din însuși modul de redactare a articolului 15 alineatul (1) prima teză din Directiva 2002/58 rezultă că statele membre pot adopta o măsură care să deroge de la principiul confidențialității evocat la punctul 52 din prezenta hotărâre în cazul în care o asemenea măsură este „necesară, corespunzătoare și proporțională în cadrul unei societăți democratice”, considerentul (11) al directivei menționate indicând în acest sens că o măsură de această natură trebuie să fie „strict” proporțională cu scopul urmărit.
- 67 În această privință trebuie amintit că protecția dreptului fundamental la respectarea vieții private impune, potrivit jurisprudenței constante a Curții, ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele strictului necesar. În plus, un obiectiv de interes general nu poate fi urmărit fără a se ține seama de faptul că trebuie conciliat cu drepturile fundamentale avute în vedere de măsura respectivă, prin realizarea unei ponderări echilibrate între, pe de o parte, obiectivul de interes general și, pe de altă parte, drepturile în cauză (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 52, precum și jurisprudența citată).
- 68 Mai precis, din jurisprudența Curții rezultă că 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 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 53, precum și jurisprudența citată).
- 69 Pentru a îndeplini cerința proporționalității, o legislație națională trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună 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. Această legislație trebuie să aibă forță juridică obligatorie în dreptul intern și în special să indice în ce împrejurări și în ce condiții poate fi luată o măsură care prevede prelucrarea unor asemenea date, garantând în acest mod că ingerința 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, în special în cazul în care există un risc semnificativ de acces ilicit la aceste date. Aceste considerații sunt aplicabile în special când este

- în discuție protecția categoriei speciale de date cu caracter personal pe care o reprezintă datele sensibile (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 54, precum și jurisprudența citată).
- 70 Prin urmare, o legislație națională care prevede o păstrare a datelor cu caracter personal trebuie să răspundă întotdeauna unor criterii obiective care să stabilească un raport între datele care trebuie păstrate și obiectivul urmărit (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 55, precum și jurisprudența citată).
- 71 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, în special din 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), 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).
- 72 Astfel, în ceea ce privește protecția securității naționale, a cărei importanță o depășește pe cea a celorlalte obiective prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, Curtea a constatat că această dispoziție, interpretată în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, nu se opune unor măsuri legislative care permit, în scopul protecției securității naționale, impunerea unei obligații furnizorilor de servicii de comunicații electronice de a efectua o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare în situații în care statul membru în cauză se confruntă cu o amenințare gravă la adresa securității naționale care se dovedește reală și actuală sau previzibilă, în condițiile în care decizia care prevede această obligație poate face obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă a cărei decizie are efect obligatoriu, prin care se urmărește să se verifice existența uneia dintre aceste situații, precum și respectarea condițiilor și a garanțiilor care trebuie să fie prevăzute, iar obligația menționată nu poate fi impusă decât pentru o perioadă limitată la strictul necesar, dar care poate fi reinnoită în cazul menținerii acestei amenințări (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 58, precum și jurisprudența citată).
- 73 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).
- 74 În ceea ce privește obiectivul combaterii criminalității grave, Curtea a statuat că o legislație națională care prevede în acest scop păstrarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare depășește limitele strictului necesar și nu poate fi considerată justificată într-o societate democratică. Astfel, ținând seama de caracterul sensibil al informațiilor pe care le pot furniza datele de transfer și datele de localizare, confidențialitatea acestora din urmă este esențială pentru dreptul la respectarea vieții private. Așadar, și ținând seama, pe de o parte, de

efectele disuasive asupra exercitării drepturilor fundamentale consacrate la articolele 7 și 11 din cartă, menționate la punctul 62 din prezenta hotărâre, pe care le poate cauza păstrarea acestor date și, pe de altă parte, de gravitatea ingerinței pe care o implică o asemenea păstrare, este important ca într-o societate democratică aceasta să fie, așa cum prevede sistemul instituit prin Directiva 2002/58, excepția, iar nu regula, și ca datele respective să nu poată face obiectul unei păstrări sistematice și continue. Această concluzie se impune chiar și în raport cu obiectivele de combatere a criminalității grave și de prevenire a amenințărilor grave la adresa siguranței publice, precum și în raport cu importanța care trebuie să le fie recunoscută (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 65, precum și jurisprudența citată).

75 În schimb, Curtea a precizat că articolul 15 alineatul (1) din Directiva 2002/58, interpretat 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 selectivă 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, supusă unui control jurisdicțional efectiv, de a efectua, pentru o perioadă determinată, păstrarea rapidă (*quick freeze*) a datelor de transfer și a datelor de localizare de care dispun acești furnizori de servicii,

în situația în care aceste măsuri garantează, prin norme clare și precise, că păstrarea datelor în discuție este subordonată respectării condițiilor de drept material și de drept procedural aferente acestora și că persoanele în cauză dispun de garanții efective împotriva riscurilor de abuz (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 168, precum și Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 67).

Cu privire la o măsură care prevede, pentru o perioadă de mai multe săptămâni, o păstrare generalizată și nediferențiată a majorității datelor de transfer și a datelor de localizare

76 În lumina acestor considerații de principiu trebuie examinate caracteristicile reglementării naționale în discuție în litigiile principale, evidențiate de instanța de trimitere.

77 În primul rând, în ceea ce privește conținutul datelor păstrate, din decizia de trimitere reiese că, în cadrul furnizării de servicii de telefonie, obligația de păstrare prevăzută de această reglementare privește în special datele necesare pentru a identifica sursa unei comunicații și destinația acesteia, data și ora de început și de sfârșit al comunicației sau – în cazul transmiterii de mesaje scurte, multimedia sau similare – momentul trimiterii și al primirii mesajului, precum și, în cazul

utilizării mobile, denumirea celulelor care au fost utilizate la începutul comunicației de către apelant și de către apelat. În cadrul furnizării de servicii de acces la internet, obligația de păstrare privește, printre altele, adresa IP atribuită abonatului, data și ora de început și de sfârșit al utilizării internetului de la adresa IP atribuită și, în cazul utilizării mobile, denumirea celulelor utilizate la începutul conexiunii la internet. Datele care permit cunoașterea poziției geografice și direcțiile de radiație maximă a antenelor care deservește celula în cauză sunt de asemenea păstrate.

- 78 Deși reglementarea națională în discuție în litigiile principale exclude de la obligația de păstrare conținutul comunicației și datele referitoare la site-urile internet consultate și nu impune păstrarea identificatorului celular decât la începutul comunicației, trebuie să se observe că situația era aceeași, în esență, în ceea ce privește reglementările naționale de transpunere a Directivei 2006/24 care erau în discuție în cauzele în care s-a pronunțat 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). Or, în pofida acestor limitări, Curtea a statuat în acea hotărâre că datele păstrate în temeiul directivei menționate și al acestor reglementări naționale puteau permite deducerea unor concluzii foarte precise privind viața privată a persoanelor vizate, precum obiceiurile din viața cotidiană, locurile de reședință permanentă sau temporară, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele și, în particular, furnizarea mijloacelor de stabilire a profilului persoanelor respective.
- 79 Mai mult, trebuie să se constate că, deși reglementarea în discuție în litigiile principale nu acoperă datele referitoare la site-urile internet consultate, ea prevede totuși păstrarea adreselor IP. Or, întrucât aceste adrese IP pot fi utilizate pentru a efectua printre altele reconstituirea exhaustivă a parcursului de navigare al unui utilizator de internet și, prin urmare, a activității sale online, aceste date permit stabilirea profilului detaliat al acestuia din urmă. Astfel, păstrarea și analiza adreselor IP menționate pe care le necesită o asemenea reconstituire reprezintă ingerințe grave în drepturile fundamentale ale utilizatorului de internet consacrate la articolele 7 și 8 din cartă (a se vedea în acest sens 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 153).
- 80 În plus, astfel cum a arătat SpaceNet în observațiile sale scrise, datele aferente serviciilor de curierat electronic, cu toate că nu intră sub incidența obligației de păstrare prevăzute de reglementarea în discuție în litigiile principale, nu reprezintă decât o parte infimă a datelor în cauză.
- 81 Așadar, după cum a arătat domnul avocat general în esență la punctul 60 din concluzii, obligația de păstrare prevăzută de reglementarea națională în discuție în litigiile principale se extinde la un ansamblu foarte larg de date de transfer și de date de localizare, care corespund în esență celor care au condus la jurisprudența constantă amintită la punctul 78 din prezenta hotărâre.
- 82 Totodată, în răspunsul la o întrebare adresată în ședință, guvernul german a precizat că numai 1 300 de entități erau înscrise în lista persoanelor, a autorităților sau a organizațiilor cu caracter social sau religios ale căror date aferente comunicațiilor electronice nu sunt păstrate în temeiul articolului 99 alineatul (2) și al articolului 113b alineatul (6) din TKG, ceea ce reprezintă în mod vădit o parte redusă a ansamblului utilizatorilor serviciilor de telecomunicații din Germania ale căror date intră sub incidența obligației de păstrare prevăzute de reglementarea națională în discuție în litigiile principale. Sunt astfel păstrate, printre altele, datele utilizatorilor supuși secretului profesional, precum avocații, medicii și jurnaliștii.

- 83 Din decizia de trimitere reiese deci că păstrarea datelor de transfer și a datelor de localizare prevăzută de această reglementare națională privește cvasitotalitatea persoanelor care compun populația, fără ca acestea să se regăsească, fie și în mod indirect, într-o situație care poate da naștere urmării penale. De asemenea, ea impune păstrarea, fără motiv, generalizată și nediferențiată din punct de vedere personal, temporal și geografic, a celei mai mari părți a datelor de transfer și a datelor de localizare a căror întindere corespunde în esență celei a datelor păstrate în cauzele care au condus la jurisprudența vizată la punctul 78 din prezenta hotărâre.
- 84 Prin urmare, având în vedere jurisprudența citată la punctul 75 din prezenta hotărâre, o obligație de păstrare a datelor precum cea în discuție în litigiile principale nu poate fi considerată ca fiind o păstrare selectivă a datelor, contrar celor susținute de guvernul german.
- 85 În al doilea rând, în ceea ce privește perioada de păstrare a datelor, din articolul 15 alineatul (1) a doua teză din Directiva 2002/58 rezultă că perioada de păstrare prevăzută de o măsură națională care impune o obligație de păstrare generalizată și nediferențiată este, desigur, un factor pertinent, printre alții, pentru a stabili dacă dreptul Uniunii se opune unei asemenea măsuri, teza menționată impunând ca această perioadă să fie „limitată”.
- 86 Or, în speță, este adevărat că aceste perioade, care sunt, potrivit articolului 113b alineatul (1) din TKG, de 4 săptămâni pentru datele de localizare și de 10 săptămâni pentru celelalte date, sunt sensibil mai scurte decât cele prevăzute de reglementările naționale care impun o obligație de păstrare generalizată și nediferențiată examinate de Curte în Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970), în 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), precum și în Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții (C-140/20, EU:C:2022:258).
- 87 Cu toate acestea, astfel cum reiese din jurisprudența citată la punctul 61 din prezenta hotărâre, gravitatea ingerinței decurge din riscul, în special având în vedere numărul și varietatea lor, ca datele păstrate, considerate în ansamblul lor, să permită să se deducă concluzii foarte precise cu privire la viața privată a persoanei sau a persoanelor ale căror date au fost păstrate și mai ales să furnizeze mijloacele de a stabili profilul persoanei sau al persoanelor vizate, care este o informație la fel de sensibilă, din perspectiva dreptului la respectarea vieții private, ca și conținutul însuși al comunicațiilor.
- 88 Prin urmare, păstrarea datelor de transfer sau a datelor de localizare, susceptibile să furnizeze informații cu privire la comunicațiile efectuate de un utilizator al unui mijloc de comunicare electronică sau cu privire la localizarea echipamentelor terminale pe care le utilizează, prezintă în orice caz un caracter grav, independent de durata perioadei de păstrare, de volumul sau de natura datelor păstrate, atunci când ansamblul de date menționat este susceptibil să permită să se deducă concluzii foarte precise cu privire la viața privată a persoanei sau a persoanelor vizate [a se vedea, în ceea ce privește accesul la asemenea date, Hotărârea din 2 martie 2021, Prokuratuur (Condiții de acces la datele referitoare la comunicațiile electronice), C-746/18, EU:C:2021:152, punctul 39].
- 89 În această privință, chiar și păstrarea unui volum limitat de date de transfer sau de date de localizare sau păstrarea acestor date pentru o scurtă perioadă este susceptibilă să furnizeze informații foarte precise cu privire la viața privată a unui utilizator al unui mijloc de comunicare electronică. În plus, volumul datelor disponibile și informațiile foarte precise cu privire la viața privată a persoanei vizate care decurg din acestea nu pot fi apreciate decât după consultarea datelor respective. Or, ingerința care rezultă din păstrarea datelor menționate intervine în mod

- necesar înainte ca datele și informațiile care decurg din acestea să poată fi consultate. Astfel, aprecierea gravității ingerinței pe care o constituie păstrarea se efectuează în mod necesar în funcție de riscul aferent în general categoriei de date păstrate pentru viața privată a persoanelor vizate, fără să fie necesar, pe de altă parte, să se stabilească dacă informațiile referitoare la viața privată care decurg din acestea prezintă sau nu, concret, un caracter sensibil [a se vedea în acest sens Hotărârea din 2 martie 2021, Prokuratuur (Condiții de acces la datele referitoare la comunicațiile electronice), C-746/18, EU:C:2021:152, punctul 40].
- 90 În speță, astfel cum reiese din cuprinsul punctului 77 din prezenta hotărâre și după cum s-a confirmat în ședință, un ansamblu de date de transfer și de date de localizare păstrate 10 săptămâni și, respectiv, 4 săptămâni poate permite să se deducă concluzii foarte precise cu privire la viața privată a persoanelor ale căror date sunt păstrate, precum obiceiurile din viața cotidiană, locurile de reședință permanentă sau temporară, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele și în special să se stabilească un profil al persoanelor menționate.
- 91 În al treilea rând, în ceea ce privește garanțiile prevăzute de reglementarea națională în discuție în litigiile principale, prin care se urmărește protejarea datelor păstrate împotriva riscurilor de abuz și împotriva oricărui acces ilicit, trebuie să se arate că păstrarea datelor respective și accesul la ele constituie, după cum reiese din jurisprudența amintită la punctul 60 din prezenta hotărâre, ingerințe distincte în drepturile fundamentale garantate la articolele 7 și 11 din cartă, care necesită o justificare distinctă, în temeiul articolului 52 alineatul (1) din aceasta. Reiese că legislația națională care asigură respectarea deplină a condițiilor rezultate din jurisprudența care a interpretat Directiva 2002/58 în materie de acces la datele păstrate nu poate fi susceptibilă, prin natura sa, nici să limiteze și nici măcar să remedieze ingerința gravă care ar rezulta din păstrarea generalizată a datelor respective prevăzută de această legislație națională în drepturile garantate la articolele 5 și 6 din directiva menționată și în drepturile fundamentale a căror concretizare o constituie articolele respective (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 47).
- 92 În al patrulea și ultimul rând, în ceea ce privește argumentul Comisiei Europene potrivit căruia criminalitatea deosebit de gravă ar putea fi asimilată unei amenințări la adresa securității naționale, Curtea a statuat deja că obiectivul de protecție a securității naționale corespunde interesului primordial de a proteja funcțiile esențiale ale statului și interesele fundamentale ale societății prin prevenirea și sancționarea activităților de natură să destabilizeze grav structurile constituționale, politice, economice sau sociale fundamentale ale unei țări și în special să amenințe în mod direct societatea, populația sau statul ca atare, cum ar fi activitățile de terorism (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 61, precum și jurisprudența citată).
- 93 Spre deosebire de criminalitate, fie și deosebit de gravă, o amenințare la adresa securității naționale trebuie să fie reală și actuală sau cel puțin previzibilă, ceea ce presupune apariția unor împrejurări suficient de concrete pentru a putea justifica o măsură de păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare o perioadă limitată. O asemenea amenințare se distinge, așadar, prin natura sa, prin gravitatea sa și prin caracterul specific al împrejurărilor care o constituie de riscul general și permanent care este cel de apariție a unor tensiuni sau a unor tulburări, chiar grave, ale siguranței publice sau cel de infracțiuni grave (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 62, precum și jurisprudența citată).

94 Prin urmare, criminalitatea, fie și deosebit de gravă, nu poate fi asimilată unei amenințări la adresa securității naționale. Astfel, o asemenea asimilare ar putea introduce o categorie intermediară între securitatea națională și siguranța publică în scopul de a aplica celei de a doua cerințele inerente celei dintâi (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 63).

Cu privire la măsurile care prevăd păstrarea selectivă, păstrarea rapidă sau păstrarea adreselor IP

95 Mai multe guverne, printre care guvernul francez, subliniază că numai o păstrare generalizată și nediferențiată permite realizarea eficientă a obiectivelor vizate de măsurile de păstrare, guvernul german precizând în esență că o asemenea concluzie nu este infirmată de faptul că statele membre pot recurge la măsurile de păstrare selectivă și de păstrare rapidă vizate la punctul 75 din prezenta hotărâre.

96 În această privință trebuie arătat, în primul rând, că eficacitatea urmăririi penale nu depinde în general de un singur instrument de investigație, ci de toate instrumentele de investigație de care dispun autoritățile naționale competente în acest scop (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 69).

97 În al doilea rând, 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, astfel cum este interpretat în jurisprudența amintită la punctul 75 din prezenta hotărâre, permite statelor membre să adopte, în vederea combaterii criminalității grave și a prevenirii amenințărilor grave la adresa siguranței publice, nu numai măsuri care instituie o păstrare selectivă și o păstrare rapidă, ci și măsuri care prevăd o păstrare generalizată și nediferențiată, pe de o parte, a datelor referitoare la identitatea civilă a utilizatorilor mijloacelor de comunicații electronice și, pe de altă parte, a adreselor IP atribuite sursei unei conexiuni (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 70).

98 În această privință este cert că păstrarea datelor referitoare la identitatea civilă a utilizatorilor mijloacelor de comunicații electronice poate contribui la combaterea criminalității grave cu condiția ca aceste date să permită identificarea persoanelor care au utilizat asemenea mijloace în contextul pregătirii sau al săvârșirii unui act care ține de criminalitatea gravă (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 71).

99 Or, Directiva 2002/58 nu se opune, în scopul combaterii criminalității în general, păstrării generalizate a datelor referitoare la identitatea civilă. În aceste condiții, este necesar să se precizeze că nici această directivă și niciun alt act din dreptul Uniunii nu se opune unei legislații naționale care are ca obiect combaterea criminalității grave, în temeiul căreia achiziționarea unui mijloc de comunicare electronică precum o cartelă SIM preplătită este condiționată de verificarea documentelor oficiale care stabilesc identitatea cumpărătorului și de înregistrarea de către vânzător a informațiilor care rezultă din acestea, vânzătorul fiind obligat, dacă este cazul, să permită accesul autorităților naționale competente la aceste informații (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 72).

100 În plus, trebuie amintit că păstrarea generalizată a adreselor IP ale sursei conexiunii constituie o ingerință gravă în drepturile fundamentale consacrate la articolele 7 și 8 din cartă, deoarece aceste adrese IP pot permite desprinderea unor concluzii precise asupra vieții private a utilizatorului mijlocului de comunicații electronice vizat, și poate avea efecte disuasive asupra exercitării libertății de exprimare garantate la articolul 11 din aceasta. În ceea ce privește o

- asemenea păstrare, Curtea a constatat însă că trebuie, în vederea concilierii necesare a drepturilor și a intereselor legitime în cauză impuse de jurisprudența menționată la punctele 65-68 din prezenta hotărâre, să se țină seama de faptul că, în cazul unei infracțiuni săvârșite online și în special în cazul achiziționării, diseminării, transmiterii sau punerii la dispoziție online de pornografie infantilă, în sensul articolului 2 litera (c) din Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO 2011, L 335, p. 1, rectificare în JO 2012, L 18, p. 7), adresa IP poate constitui singurul mijloc de investigare care să permită identificarea persoanei căreia îi era atribuită această adresă la momentul săvârșirii infracțiunii respective (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 73).
- 101 În aceste condiții, deși este adevărat că o măsură legislativă care prevede stocarea adreselor IP ale tuturor persoanelor fizice proprietare ale unui echipament terminal de la care se poate realiza accesul la internet ar viza persoane care nu prezintă, la prima vedere, o legătură, în sensul jurisprudenței citate la punctul 70 din prezenta hotărâre, cu obiectivele urmărite și că utilizatorii de internet dispun, în conformitate cu ceea ce s-a constatat la punctul 54 din prezenta hotărâre, de dreptul de a se aștepta, în temeiul articolelor 7 și 8 din cartă, ca identitatea lor să nu fie, în principiu, dezvăluită, o măsură legislativă care prevede păstrarea generalizată și nediferențiată numai a adreselor IP atribuite sursei unei conexiuni nu este, în principiu, contrară articolului 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, cu condiția ca această posibilitate să fie supusă respectării stricte a condițiilor de drept material și de drept procedural care trebuie să guverneze utilizarea acestor date (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 155).
- 102 Având în vedere caracterul grav al ingerinței în drepturile fundamentale consacrate la articolele 7 și 8 din cartă pe care o presupune această păstrare, numai combaterea criminalității grave și prevenirea amenințărilor grave la adresa siguranței publice sunt de natură, la fel ca protejarea securității naționale, să justifice această ingerință. În plus, durata de păstrare nu poate depăși durata strict necesară în raport cu obiectivul urmărit. În sfârșit, o măsură de această natură trebuie să prevadă condiții și garanții stricte în ceea ce privește exploatarea acestor date, în special printr-o reconstituire, în privința comunicațiilor și a activităților efectuate online de persoanele vizate (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 156).
- 103 Așadar, contrar celor subliniate de instanța de trimitere, nu există o tensiune între punctele 155 și 168 din 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). Astfel, după cum a arătat în esență domnul avocat general la punctele 81 și 82 din concluzii, reiese cu claritate din cuprinsul acestui punct 155 coroborat cu punctul 156 și cu punctul 168 din hotărârea respectivă că numai combaterea criminalității grave și prevenirea amenințărilor grave la adresa siguranței publice sunt de natură, la fel ca protejarea securității naționale, să justifice păstrarea generalizată a adreselor IP atribuite sursei unei conexiuni, independent de aspectul dacă persoanele vizate sunt susceptibile să prezinte o legătură, fie și indirectă, cu obiectivele urmărite.
- 104 În al treilea rând, în ceea ce privește măsurile legislative care prevăd o păstrare selectivă și o păstrare rapidă a datelor de transfer și a datelor de localizare, din anumite considerații expuse de statele membre împotriva unor asemenea măsuri reiese o interpretare mai restrictivă a domeniului de aplicare al acestor măsuri decât cea reținută în jurisprudența menționată la

punctul 75 din prezenta hotărâre. Astfel, deși, în conformitate cu ceea ce s-a amintit la punctul 57 din prezenta hotărâre, aceste măsuri de păstrare trebuie să prezinte un caracter derogatoriu în sistemul instituit de Directiva 2002/58, aceasta, interpretată în lumina drepturilor fundamentale consacrate la articolul 7, 8 și 11, precum și la articolul 52 alineatul (1) din cartă, nu supune posibilitatea de a impune o obligație de păstrare selectivă condiției ca în prealabil să fie cunoscute locurile susceptibile a fi scena unui act de criminalitate gravă sau persoanele suspectate de implicare într-un asemenea act. Directiva menționată nu impune nici ca obligația de păstrare rapidă să fie limitată la suspectii identificați anterior impunerii unei asemenea obligații (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 75).

- 105 În ceea ce privește, *primo*, păstrarea selectivă, Curtea a statuat că articolul 15 alineatul (1) din Directiva 2002/58 nu se opune unei legislații naționale întemeiate pe elemente obiective care permite să fie vizate, pe de o parte, persoanele ale căror date de trafic și date de localizare sunt susceptibile să prezinte o legătură, fie și indirectă, cu acte de criminalitate gravă, să contribuie la combaterea criminalității grave sau să prevină un risc grav pentru siguranța publică ori un risc pentru securitatea națională (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 76, precum și jurisprudența citată).
- 106 Curtea a precizat în această privință că, deși aceste elemente obiective pot varia în funcție de măsurile luate în scopul prevenirii, investigării, detectării și urmăririi penale a criminalității grave, persoanele astfel vizate pot fi în special cele care au fost identificate în prealabil, în cadrul procedurilor naționale aplicabile și pe baza unor elemente obiective și nediscriminatorii, ca reprezentând o amenințare la adresa siguranței publice sau a securității naționale a statului membru în cauză (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána, C-140/20, EU:C:2022:258, punctul 77).
- 107 Statele membre au deci în special posibilitatea de a lua măsuri de păstrare privind persoane care, în scopul unei atari identificări, fac obiectul unei investigații sau al altor măsuri de supraveghere actuale sau al unei înscrieri în cazierul judiciar național care menționează o condamnare anterioară pentru acte de criminalitate gravă ce pot implica un risc ridicat de recidivă. Or, atunci când o asemenea identificare se întemeiază pe elemente obiective și nediscriminatorii, definite de dreptul național, păstrarea selectivă care vizează persoane astfel identificate este justificată (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 78).
- 108 Pe de altă parte, o măsură de păstrare selectivă a datelor de transfer și a datelor de localizare poate, potrivit alegerii legiuitorului național și cu respectarea strictă a principiului proporționalității, să se întemeieze și pe un criteriu geografic atunci când autoritățile naționale competente consideră, pe baza unor elemente obiective și nediscriminatorii, că există, în una sau în mai multe zone geografice, o situație caracterizată printr-un risc ridicat de pregătire sau de săvârșire a unor acte de criminalitate gravă. Aceste zone pot fi, printre altele, locuri caracterizate printr-un număr ridicat de acte de criminalitate gravă, locuri expuse în mod deosebit săvârșirii de acte de criminalitate gravă, precum locuri sau infrastructuri frecventate în mod regulat de un număr foarte mare de persoane sau locurile strategice precum aeroporturile, gările, porturile maritime sau zonele de taxare rutieră (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 79, precum și jurisprudența citată).

- 109 Trebuie subliniat că, potrivit acestei jurisprudențe, autoritățile naționale competente pot lua, pentru zonele vizate la punctul anterior, o măsură de păstrare selectivă întemeiată pe un criteriu geografic cum este, de exemplu, rata medie a criminalității într-o zonă geografică, fără ca ele să dispună în mod necesar de indicii concrete cu privire la pregătirea sau la săvârșirea în zonele vizate a unor acte de criminalitate gravă. În măsura în care o păstrare selectivă întemeiată pe un asemenea criteriu poate afecta, în funcție de infracțiunile grave vizate și de situația proprie statelor membre respective, atât locuri caracterizate printr-un număr ridicat de acte de criminalitate gravă, cât și locuri deosebit de expuse săvârșirii unor asemenea acte, nici aceasta nu este, în principiu, de natură să dea naștere la discriminări, criteriul bazat pe rata medie a criminalității grave neavând, în sine, nicio legătură cu elemente potențial discriminatorii (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 80).
- 110 În plus și mai ales, o măsură de păstrare selectivă privind locuri sau infrastructuri frecventate în mod regulat de un număr foarte mare de persoane sau locuri strategice precum aeroporturi, gări, porturi maritime sau zone de taxare rutieră permite autorităților competente să colecteze date de transfer și în special date de localizare ale tuturor persoanelor care utilizează la un moment dat un mijloc de comunicare electronică în unul dintre aceste locuri. Așadar, o asemenea măsură de păstrare selectivă este susceptibilă să permită autorităților menționate să obțină, prin accesul la datele astfel păstrate, informații cu privire la prezența acestor persoane în locurile sau în zonele geografice vizate de măsura respectivă, precum și cu privire la deplasările lor între sau în interiorul acestora și să deducă de aici, în scopul combaterii criminalității grave, concluzii cu privire la prezența și la activitatea lor în locurile sau în zonele geografice respective la un moment dat în perioada de păstrare (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 81).
- 111 Mai trebuie arătat că zonele geografice vizate de o asemenea păstrare selectivă pot și, dacă este cazul, trebuie să fie modificate în funcție de evoluția condițiilor care au justificat selectarea lor, permițând în acest fel în special să se reacționeze la evoluțiile combaterii criminalității grave. Astfel, Curtea a statuat deja că durata măsurilor de păstrare selectivă descrise la punctele 105-110 din prezenta hotărâre nu poate depăși durata care este strict necesară în raport cu obiectivul urmărit, precum și cu împrejurările care le justifică, fără a aduce atingere unei eventuale reînnoiri ca urmare a menținerii necesității de a efectua o asemenea păstrare (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 151, precum și Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 82).
- 112 În ceea ce privește posibilitatea de a prevedea alte criterii distinctive decât un criteriu personal sau geografic pentru a pune în aplicare o păstrare selectivă a datelor de transfer și a datelor de localizare, nu se poate exclude ca alte criterii, obiective și nediscriminatorii, să poată fi luate în considerare pentru a se asigura că întinderea unei păstrări selective este limitată la strictul necesar și pentru a se stabili o legătură, fie și indirectă, între actele de criminalitate gravă și persoanele ale căror date sunt păstrate. În aceste condiții, întrucât articolul 15 alineatul (1) din Directiva 2002/58 vizează măsuri legislative ale statelor membre, acestora din urmă, iar nu Curții, le revine sarcina de a identifica asemenea criterii, înțelegându-se că nu se poate pune problema reinstaurării în acest mod a unei păstrări generalizate și nediferențiate a datelor de transfer și a datelor de localizare (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 83).

- 113 În orice caz, așa cum a arătat domnul avocat general la punctul 50 din concluzii, eventuala existență a unor dificultăți de a defini cu precizie ipotezele și condițiile în care poate fi efectuată o păstrare selectivă nu poate justifica faptul ca statele membre, făcând din excepție o regulă, să prevadă o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 84).
- 114 În ceea ce privește, *secundo*, păstrarea rapidă a datelor de transfer și a datelor de localizare prelucrate și stocate de furnizorii de servicii de comunicații electronice în temeiul articolelor 5, 6 și 9 din Directiva 2002/58 sau al măsurilor legislative adoptate în temeiul articolului 15 alineatul (1) din această directivă, trebuie amintit că asemenea date trebuie să fie, în principiu, șterse sau, după caz, anonimizate la expirarea termenelor legale în care trebuie să aibă loc, în conformitate cu dispozițiile naționale de transpunere a directivei menționate, prelucrarea și stocarea lor. Curtea a statuat însă că pe durata prelucrării și a stocării menționate pot apărea situații în care intervine necesitatea păstrării datelor respective dincolo de aceste termene în scopul elucidării unor infracțiuni grave sau a unor atingeri aduse securității naționale, atât în situația în care aceste infracțiuni sau atingeri au putut fi deja constatate, cât și în cea în care existența lor poate fi suspectată în mod rezonabil în urma unei examinări obiective a tuturor împrejurărilor relevante (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 85).
- 115 Într-o atare situație, statele membre pot, având în vedere concilierea necesară a drepturilor și a intereselor legitime în cauză menționată la punctele 65-68 din prezenta hotărâre, să prevadă, printr-o legislație adoptată în temeiul articolului 15 alineatul (1) din Directiva 2002/58, posibilitatea, prin intermediul unei decizii a autorității competente supuse unui control jurisdicțional efectiv, de a impune furnizorilor de servicii de comunicații electronice să efectueze, pentru o perioadă determinată, păstrarea rapidă a datelor de transfer și a datelor de localizare de care dispun (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 163, precum și Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 86).
- 116 În măsura în care finalitatea unei asemenea păstrări rapide nu mai corespunde celor pentru care datele au fost colectate și păstrate inițial și în măsura în care orice prelucrare de date trebuie să răspundă, în temeiul articolului 8 alineatul (2) din cartă, unor scopuri precizate, statele membre trebuie să menționeze în legislația lor finalitatea în vederea căreia poate avea loc păstrarea rapidă a datelor. Având în vedere caracterul grav al ingerinței în drepturile fundamentale consacrate la articolele 7 și 8 din cartă pe care o poate presupune o asemenea păstrare, numai combaterea criminalității grave și, *a fortiori*, protecția securității naționale sunt de natură să justifice această ingerință, cu condiția ca măsura respectivă, precum și accesul la datele astfel păstrate să respecte limitele strictului necesar, așa cum sunt enunțate la punctele 164-167 din 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) (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 87).
- 117 Curtea a precizat că o măsură de păstrare de această natură nu trebuie să fie limitată la datele persoanelor identificate în prealabil ca reprezentând o amenințare pentru siguranța publică sau securitatea națională a statului membru vizat sau ale persoanelor suspectate în mod concret că au săvârșit un act de criminalitate gravă sau o atingere adusă securității naționale. Astfel, potrivit Curții, cu respectarea cadrului stabilit prin articolul 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, și

- ținând seama de considerațiile care figurează la punctul 70 din prezenta hotărâre, o atare măsură poate, potrivit alegerii legiuitorului și cu respectarea limitelor strictului necesar, să fie extinsă la datele de transfer și la datele de localizare aferente altor persoane decât cele care sunt suspectate de planificarea sau de săvârșirea unei infracțiuni grave sau a unei atingeri aduse securității naționale, cu condiția ca aceste date să poată contribui, pe baza unor elemente obiective și nediscriminatorii, la elucidarea unei asemenea infracțiuni sau a unei asemenea atingeri aduse securității naționale, cum sunt datele victimei acesteia și cele ale anturajului său social sau profesional (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 165, precum și Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 88).
- 118 Așadar, o măsură legislativă poate autoriza impunerea unei obligații furnizorilor de servicii de comunicații electronice de a efectua păstrarea rapidă a datelor de transfer și a datelor de localizare, printre altele, ale persoanelor cu care, anterior apariției unei amenințări grave la adresa siguranței publice sau a săvârșirii unui act de criminalitate gravă, o victimă a fost în contact prin utilizarea mijloacelor sale de comunicații electronice (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 89).
- 119 O asemenea păstrare rapidă poate, potrivit jurisprudenței Curții amintite la punctul 117 din prezenta hotărâre și în aceleași condiții ca acelea vizate la acel punct, să fie extinsă și la zone geografice determinate, precum locurile săvârșirii și pregătirii infracțiunii sau ale atingerii aduse securității naționale în cauză. Trebuie precizat că mai pot face obiectul unei atari măsuri datele de transfer și datele de localizare aferente locului în care o persoană, potențial victimă a unui act de criminalitate gravă, a dispărut, cu condiția ca această măsură, precum și accesul la datele astfel păstrate să respecte limitele strictului necesar în vederea combaterii criminalității grave sau a protecției securității naționale, așa cum sunt enunțate la punctele 164-167 din 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) (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 90).
- 120 Pe de altă parte, trebuie precizat că articolul 15 alineatul (1) din Directiva 2002/58 nu se opune ca autoritățile naționale competente să dispună o măsură de păstrare rapidă încă din primul stadiu al investigației referitoare la o amenințare gravă la adresa siguranței publice sau la un eventual act de criminalitate gravă, și anume din momentul în care aceste autorități pot, potrivit dispozițiilor relevante ale dreptului național, să deschidă o asemenea investigație (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 91).
- 121 În ceea ce privește varietatea măsurilor de păstrare a datelor de transfer și a datelor de localizare vizate la punctul 75 din prezenta hotărâre, trebuie precizat că aceste diferite măsuri pot fi aplicate împreună, potrivit alegerii legiuitorului național și cu respectarea în același timp a limitelor strictului necesar. În aceste condiții, 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, astfel cum a fost interpretat de jurisprudența rezultată din 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), nu se opune unei combinări a acestor măsuri (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 92).
- 122 În al patrulea și ultimul rând, trebuie subliniat că proporționalitatea măsurilor adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58 impune, potrivit jurisprudenței constante a Curții, astfel cum a fost recapitulată în 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), respectarea nu numai a cerințelor de aptitudine și de necesitate, ci și a celei legate de caracterul proporțional al acestor măsuri în raport cu obiectivul urmărit (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 93).
- 123 În acest context, trebuie amintit că, la punctul 51 din Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238), Curtea a statuat că, deși combaterea criminalității grave prezintă o importanță primordială pentru garantarea siguranței publice, iar eficacitatea sa poate depinde într-o mare măsură de utilizarea tehnicilor moderne de investigație, un asemenea obiectiv de interes general, chiar dacă este fundamental, nu poate justifica *per se* faptul de a considera o măsură de păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare precum cea instituită de Directiva 2006/24 ca fiind necesară (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 94).
- 124 În aceeași ordine de idei, Curtea a precizat, la punctul 145 din 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), că nici măcar obligațiile pozitive ale statelor membre care pot decurge, după caz, din articolele 3, 4 și 7 din cartă și care privesc, așa cum s-a arătat la punctul 64 din prezenta hotărâre, instituirea unor norme care să permită combaterea efectivă a infracțiunilor nu pot avea ca efect justificarea unor ingerințe atât de grave în drepturile fundamentale consacrate la articolele 7 și 8 din cartă precum cele pe care le presupune o legislație națională care prevede păstrarea datelor de transfer și a datelor de localizare ale cvasitotalității populației, fără ca datele persoanelor vizate să fie susceptibile să prezinte o legătură, fie și indirectă, cu obiectivul urmărit (Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții, C-140/20, EU:C:2022:258, punctul 95).
- 125 Pe de altă parte, Hotărârea Curții EDO din 25 mai 2021, Big Brother Watch și alții împotriva Regatului Unit (CE:ECHR:2021:0525JUD 005817013), și Hotărârea Curții EDO din 25 mai 2021, Centrum för Rättvisa împotriva Suediei (CE:ECHR:2021:0525JUD 003525208), invocate de anumite guverne în ședință pentru a susține că CEDO nu se opune unor reglementări naționale care prevăd în esență o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare, nu pot repune în discuție interpretarea articolului 15 alineatul (1) din Directiva 2002/58 care decurge din considerațiile care precedă. Astfel, în aceste hotărâri erau în discuție interceptări în masă de date aferente unor comunicații internaționale. Așadar, după cum a arătat Comisia în ședință, în hotărârile menționate, Curtea Europeană a Drepturilor Omului nu s-a pronunțat cu privire la conformitatea cu CEDO a unei păstrări generalizate și nediferențiate de date de transfer și de date de localizare pe teritoriul național și nici măcar a unei interceptări de mare amploare a acestor date în scopul prevenirii, detectării și investigării infracțiunilor grave. În orice caz, trebuie amintit că articolul 52 alineatul (3) din cartă este destinat să asigure coerența necesară între drepturile prevăzute de aceasta din urmă și drepturile corespunzătoare garantate de CEDO, fără a aduce atingere autonomiei dreptului Uniunii și a Curții de Justiție a Uniunii Europene, astfel încât trebuie să se țină seama numai ca prag de protecție minimă de drepturile corespunzătoare din CEDO în vederea interpretării cartei (Hotărârea din 17 decembrie 2020, Centraal Israëlitisch Consistorie van België și alții, C-336/19, EU:C:2020:1031, punctul 56).

Cu privire la accesul la datele care au fost păstrate în mod generalizat și nediferențiat

- 126 În ședință, guvernul danez a susținut că autoritățile naționale competente ar trebui să poată avea acces, în scopul combaterii criminalității grave, la datele de transfer și la datele de localizare care au fost păstrate în mod generalizat și nediferențiat, în conformitate cu jurisprudența rezultată din

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, punctele 135-139), pentru a face față unei amenințări grave la adresa securității naționale care se dovedește reală și actuală sau previzibilă.

- 127 Trebuie arătat de la bun început că faptul de a autoriza accesul, în scopul combaterii criminalității grave, la date de transfer și la date de localizare care au fost păstrate în mod generalizat și nediferențiat ar face ca acest acces să depindă de împrejurări străine obiectivului respectiv, în funcție de existența sau nu în statul membru vizat a unei amenințări grave la adresa securității naționale, astfel cum este menționată la punctul anterior, în condițiile în care, având în vedere numai obiectivul de combatere a criminalității grave care trebuie să justifice păstrarea acestor date și accesul la ele, nimic nu ar justifica o diferență de tratament, în special între statele membre (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 97).
- 128 Așa cum Curtea deja a statuat, accesul la datele de transfer și la datele 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, 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).
- 129 Or, argumentația guvernului danez vizează o situație în care obiectivul cererii de acces avut în vedere, și anume combaterea criminalității grave, este de o importanță mai redusă, în ierarhia obiectivelor de interes general, decât cel care a justificat păstrarea, și anume protecția securității naționale. A autoriza, într-o asemenea situație, accesul la datele păstrate ar contraveni acestei ierarhii a obiectivelor de interes general amintite la punctul anterior, precum și la punctele 68, 71, 72 și 73 din prezenta hotărâre (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 99).
- 130 În plus și mai ales, conform jurisprudenței amintite la punctul 74 din prezenta hotărâre, datele de transfer și datele de localizare nu pot face obiectul unei păstrări generalizate și nediferențiate în scopul combaterii criminalității grave și, prin urmare, un acces la aceste date nu poate fi justificat în același scop. Or, atunci când aceste date au fost păstrate excepțional în mod generalizat și nediferențiat în scopul protecției securității naționale împotriva unei amenințări care se dovedește reală și actuală sau previzibilă, în condițiile menționate la punctul 71 din prezenta hotărâre, autoritățile naționale competente în materie de investigații penale nu pot avea acces la datele respective în cadrul urmăririi penale, în caz contrar fiind privată de orice efect util interdicția de a efectua o asemenea păstrare în scopul combaterii criminalității grave, amintită la punctul 74 menționat (Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, punctul 100).
- 131 Având în vedere ansamblul considerațiilor care precedă, este necesar să se răspundă la întrebarea preliminară 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 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. În schimb, articolul 15 alineatul (1) menționat, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că nu se opune unor măsuri legislative naționale:

- care permit, în scopul protecției securității naționale, impunerea unei obligații furnizorilor de servicii de comunicații electronice de a efectua o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare în situații în care statul membru în cauză se confruntă cu o amenințare gravă la adresa securității naționale care se dovedește reală și actuală sau previzibilă, în condițiile în care decizia care prevede această obligație poate face obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie are efect obligatoriu, prin care se urmărește să se verifice existența uneia dintre aceste situații, precum și respectarea condițiilor și a garanțiilor care trebuie să fie prevăzute, iar obligația menționată nu poate fi impusă decât pentru o perioadă limitată la strictul necesar, dar care poate fi reînnoită în cazul menținerii acestei amenințări;
- care prevăd, în scopul protecției securității naționale, al combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o păstrare selectivă 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;
- care prevăd, în scopul protecției securității naționale, al combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o păstrare generalizată și nediferențiată a adreselor IP atribuite sursei unei conexiuni, pentru o perioadă limitată la strictul necesar;
- care prevăd, în scopul protecției securității naționale, al combaterii criminalității și al apărării siguranței publice, o păstrare generalizată și nediferențiată a datelor referitoare la identitatea civilă a utilizatorilor de mijloace de comunicații electronice și
- care permit, în scopul combaterii criminalității grave și, *a fortiori*, al protecției securității naționale, impunerea unei obligații furnizorilor de servicii de comunicații electronice prin intermediul unei decizii a autorității competente, supusă 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,

în situația în care aceste măsuri garantează, prin norme clare și precise, că păstrarea datelor în discuție este subordonată respectării condițiilor de drept material și de drept procedural aferente acestora și că persoanele în cauză dispun de garanții efective împotriva riscurilor de abuz.

Cu privire la cheltuielile de judecată

- 132 Întrucât, în privința părților din litigiile principale, 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 (Marea Cameră) 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 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;

nu se opune unor măsuri legislative naționale:

- care permit, în scopul protecției securității naționale, impunerea unei obligații furnizorilor de servicii de comunicații electronice de a efectua o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare în situații în care statul membru în cauză se confruntă cu o amenințare gravă la adresa securității naționale care se dovedește reală și actuală sau previzibilă, în condițiile în care decizia care prevede această obligație poate face obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie are efect obligatoriu, prin care se urmărește să se verifice existența uneia dintre aceste situații, precum și respectarea condițiilor și a garanțiilor care trebuie să fie prevăzute, iar obligația menționată nu poate fi impusă decât pentru o perioadă limitată la strictul necesar, dar care poate fi reînnoită în cazul menținerii acestei amenințări;**
- care prevăd, în scopul protecției securității naționale, al combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o păstrare selectivă 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;**
- care prevăd, în scopul protecției securității naționale, al combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o păstrare generalizată și nediferențiată a adreselor IP atribuite sursei unei conexiuni, pentru o perioadă limitată la strictul necesar;**
- care prevăd, în scopul protecției securității naționale, al combaterii criminalității și al apărării siguranței publice, o păstrare generalizată și nediferențiată a datelor referitoare la identitatea civilă a utilizatorilor de mijloace de comunicații electronice și**
- care permit, în scopul combaterii criminalității grave și, *a fortiori*, al protecției securității naționale, impunerea unei obligații furnizorilor de servicii de comunicații electronice prin intermediul unei decizii a autorității competente, supusă 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,

în situația în care aceste măsuri garantează, prin norme clare și precise, că păstrarea datelor în discuție este subordonată respectării condițiilor de drept material și de drept procedural aferente acestora și că persoanele în cauză dispun de garanții efective împotriva riscurilor de abuz.

Semnături