Repertoriul jurisprudenței

HOTĂRÂREA CURȚII (Marea Cameră)

6 octombrie 2020*

„Trimitere preliminară – Prelucrarea datelor cu caracter personal în sectorul comunicațiilor electronice – Furnizori de servicii de comunicații electronice – Transmitere generalizată și nediferențiată a datelor de transfer și a datelor de localizare – Apărarea securității naționale – Directiva 2002/58/CE – Domeniu de aplicare – Articolul 1 alineatul (3) și articolul 3 – Confidențialitatea comunicațiilor electronice – Protecție – Articolul 5 și articolul 15 alineatul (1) – Carta drepturilor fundamentale a Uniunii Europene – Articolele 7, 8 și 11, precum și articolul 52 alineatul (1) – Articolul 4 alineatul (2) TUE”

În cauza C-623/17,

având ca obiect o cerere de decizie preliminară formulată în temeiul articolului 267 TFUE de Investigatory Powers Tribunal (Tribunalul cu competențe de investigare, Regatul Unit), prin decizia din 18 octombrie 2017, primită de Curte la 31 octombrie 2017, în procedura

Privacy International

împotriva

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

CURTEA (Marea Cameră),

compusă din domnul K. Lenaerts, președinte, doamna R. Silva de Lapuerta, vicepreședintă, domnii J.-C. Bonichot și A. Arabadjiev, doamna A. Prechal, domnii M. Safjan și P. G. Xuereb și doamna L. S. Rossi, președinți de cameră, domnii J. Malenovský, L. Bay Larsen și T. von Danwitz (raportor), doamnele C. Toader și K. Jürimäe și domnii C. Lycourgos și N. Piçarra, judecători,

avocat general: domnul M. Campos Sánchez-Bordona,

grefier: doamna C. Strömholm, administratoare,

având în vedere procedura scrisă și în urma ședinței din 9 și din 10 septembrie 2019,

* Limba de procedură: engleza.

luând în considerare observațiile prezentate:

– pentru Privacy International, de B. Jaffey, T. de la Mare, QC, D. Cashman, solicitor, și H. Roy, avocat;

– pentru guvernul Regatului Unit, de Z. Lavery, D. Guðmundsdóttir și S. Brandon, în calitate de agenți, asistați de G. Facenna, D. Beard, QC, C. Knight și R. Palmer, barristers;

– pentru guvernul belgian, de P. Cottin și J.-C. Halleux, în calitate de agenți, asistați de J. Vanpraet, advocaat, și E. de Lophem, avocat;

– pentru guvernul ceh, de M. Smolek, J. Vláčil și O. Serdula, în calitate de agenți;

– pentru guvernul german, inițial de M. Hellmann, R. Kanitz, D. Klebs și T. Henze și ulterior de J. Möller, M. Hellmann, R. Kanitz și D. Klebs, în calitate de agenți;

– pentru guvernul estonian, de A. Kalbus, în calitate de agent;

– pentru guvernul irlandez, de M. Browne, G. Hodge și A. Joyce, în calitate de agenți, asistați de D. Fennelly, barrister;

– pentru guvernul spaniol, inițial de L. Aguilera Ruiz și M. J. García-Valdecasas Dorrego și ulterior de L. Aguilera Ruiz, în calitate de agenți,

– pentru guvernul francez, inițial de E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas și D. Dubois și ulterior de E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune și D. Dubois, în calitate de agenți;

– pentru guvernul cipriot, de E. Symeonidou și E. Neofytou, în calitate de agenți;

– pentru guvernul leton, inițial de V. Soņeca și I. Kucina și ulterior de V. Soņeca, în calitate de agenți;

– pentru guvernul maghiar, inițial de G. Koós, M. Z. Fehér, G. Tornyai și Z. Wagner și ulterior de G. Koós și M. Z. Fehér, în calitate de agenți;

– pentru guvernul neerlandez, de C. S. Schillemans și M. K. Bulterman, în calitate de agenți;

– pentru guvernul polonez, de B. Majczyna, J. Sawicka și M. Pawlicka, în calitate de agenți;

– pentru guvernul portughez, de L. Inez Fernandes, M. Figueiredo și F. Aragão Homem, în calitate de agenți;

– pentru guvernul suedez, inițial de A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren și A. Alriksson și ulterior de H. Shev, C. Meyer-Seitz, L. Zettergren și A. Alriksson, în calitate de agenți;

– pentru guvernul norvegian, de T. B. Leming, M. Emberland și J. Vangsnes, în calitate de agenți;

– pentru Comisia Europeană, inițial de H. Kranenborg, M. Wasmeier, D. Nardi și P. Costa de Oliveira și ulterior de H. Kranenborg, M. Wasmeier și D. Nardi, în calitate de agenți;

– pentru Autoritatea Europeană pentru Protecția Datelor, de T. Zerdick și A. Buchta, în calitate de agenți,

după ascultarea concluziilor avocatului general în ședința din 15 ianuarie 2020,

pronunță prezenta

Hotărâre

1 Cererea de decizie preliminară privește interpretarea articolului 1 alineatul (3) și a articolului 15 alineatul (1) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva privind confidențialitatea și comunicațiile 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”), interpretate în lumina articolului 4 alineatul (2) TUE, precum și a articolelor 7 și 8 și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”).

2 Această cerere a fost formulată în cadrul unui litigiu între Privacy International, pe de o parte, și Secretary of State for Foreign and Commonwealth Affairs (ministrul pentru Afaceri Externe și Commonwealth, Regatul Unit), Secretary of State for the Home Departement (ministrul pentru Afaceri Interne, Regatul Unit), Government Communications Headquarters (Cartierul General pentru Comunicații, Regatul Unit) (denumit în continuare „GCHQ”), Security Service (Serviciul de Securitate, Regatul Unit, denumit în continuare „MI5”) și Secret Intelligence Service (Serviciul Secret de Informații, Regatul Unit, denumit în continuare „MI6”), pe de altă parte, în legătură cu legalitatea unei reglementări care autorizează achiziția și utilizarea de către agențiile de securitate și de informații a datelor referitoare la comunicații colectate în masă (*bulk communications data*).

Cadrul juridic

Dreptul Uniunii

Directiva 95/46

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 începere de la 25 mai 2018 prin Regulamentul (UE) 2016/679 al Parlamentul European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (JO 2016, L 119, p. 1). Articolul 3 din directiva menționată, intitulat „Domeniul de aplicare”, avea următorul cuprins:

„(1) Prezenta directivă se aplică prelucrării automate, în totalitate sau parțial, precum și prelucrării neautomate a datelor cu caracter personal, conținute sau care urmează să fie conținute într-un sistem de evidență a datelor cu caracter personal.

(2) Prezenta directivă nu se aplică prelucrării datelor cu caracter personal:

– puse în practică pentru exercitarea activităților din afara domeniului de aplicare al dreptului comunitar, cum ar fi cele prevăzute în titlurile V și VI [TUE], 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 activitățile statului în domeniul dreptului penal;

– efectuate de către o persoană fizică în cursul unei activități exclusiv personale sau domestice.”

Directiva 2002/58

4 Considerentele (2), (6), (7), (11), (22), (26) și (30) 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 [dreptul Uniunii]. 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 siguranța 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.

[…]

(22) Interdicția stocării comunicațiilor și a datelor de transfer aferente de către alte persoane decât utilizatorul sau fără acordul acestuia nu înseamnă interzicerea oricărei stocări automate, intermediare sau tranzitorii a acestor informații, în cazul în care acest lucru se întâmplă cu unicul scop al efectuării transmisiei prin rețeaua de comunicații electronice și cu condiția ca informațiile să nu fie stocate pentru o perioadă mai lungă decât este necesar în vederea transmiterii sau în scopuri legate de gestionarea traficului și ca în timpul perioadei de stocare să fie garantată confidențialitatea datelor. Atunci când acest lucru este necesar pentru eficientizarea transmisiei informațiilor publice către alți destinatari a serviciilor la cerere, prezenta directivă nu trebuie să împiedice stocarea acestor informații, cu condiția ca acestea să fie accesibile fără restricții publicului larg și ca orice date referitoare la abonații sau utilizatorii individuali să fie șterse.

[…]

(26) Datele referitoare la abonați prelucrate în cadrul rețelei de comunicații electronice pentru a stabili conexiuni sau pentru a transmite informații conțin informații despre viața personală a persoanelor fizice și intră sub incidența dreptului la respectarea confidențialității corespondenței sau a dreptului la protejarea intereselor legitime ale persoanelor juridice. Aceste date pot fi stocate doar pe timpul necesar furnizării serviciului sau facturării și pentru plăți on-line și numai pentru o perioadă limitată de timp. Orice altă prelucrare a acestor date […] este permisă numai în cazul în care abonatul își dă acordul la aceasta după o informare corectă și completă din partea prestatorului de servicii publice de comunicații electronice cu privire la modul de prelucrare ulterioară a datelor pe care intenționează să o efectueze și la dreptul abonatului de a nu acorda sau de a-și retrage acordul pentru această prelucrare. Datele de transfer folosite pentru comercializarea serviciilor de comunicații […] trebuie de asemenea șterse sau trecute în anonimat […]

[…]

(30) Sistemele de furnizare de servicii și rețele de comunicații electronice trebuie astfel construite încât să limiteze cantitatea de date personale necesare la un minimum strict. […]”

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

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

(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 [TFUE], cum sunt cele menționate în titlurile V și VI ale Tratatului privind Uniunea Europeană, și în orice caz activităților legate de siguranța publică, de apărare, de siguranța statului (inclusiv de bunăstarea economică a acestuia, dacă activitățile respective sunt legate de chestiuni de siguranța statului) și activităților statului în domeniul legii penale.”

6 Potrivit articolului 2 din această directivă, 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;

[…]”

7 Articolul 3 din directiva menționată, 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 [Uniunii], inclusiv al rețelelor publice de comunicații care presupun colectarea de date și dispozitive de identificare.”

8 Potrivit articolului 5 din Directiva 2002/58, 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, interceptarea, 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.”

9 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 retrage 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.”

10 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. […]”

11 Articolul 15 din directiva menționată, 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, 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 [Uniuni], inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) al Tratatului privind Uniunea Europeană.”

Regulamentul 2016/679

12 Articolul 2 din Regulamentul 2016/679 prevede:

„(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.

(2) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:

(a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;

(b) de către statele membre atunci când desfășoară activități care intră sub incidența capitolului 2 al titlului V din Tratatul UE;

[…]

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

[…]"

13 Articolul 4 din regulamentul menționat prevede:

„În sensul prezentului regulament:

[…]

2) «prelucrare» înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

[…]"

14 Potrivit articolului 23 alineatul (1) din același regulament:

„Dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la articolele 12-22 și 34, precum și la articolul 5 în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la articolele 12-22, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică pentru a asigura:

(a) securitatea națională;

(b) apărarea;

(c) securitatea publică;

(d) prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;

(e) alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale;

(f) protejarea independenței judiciare și a procedurilor judiciare;

(g) prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate;

(h) funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazurile menționate la literele (a)-(e) și (g);

(i) protecția persoanei vizate sau a drepturilor și libertăților altora;

(j) punerea în aplicare a pretențiilor de drept civil."

15 Potrivit articolului 94 alineatul (2) din Regulamentul 2016/679:

„Trimiterile la directiva abrogată se interpretează ca trimiteri la prezentul regulament. Trimiterile la Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal instituit prin articolul 29 din Directiva [95/46] se interpretează ca trimiteri la Comitetul european pentru protecția datelor instituit prin prezentul regulament."

Dreptul Regatului Unit

16 Articolul 94 din Telecommunications Act 1984, în versiunea aplicabilă faptelor din litigiul principal (denumită în continuare „Legea din 1984"), intitulat „Instrucțiuni în interesul securității naționale etc.", prevede:

„(1) Ministrul poate da persoanei căreia îi este aplicabil acest articol, după consultarea acesteia, instrucțiuni generale necesare, în opinia sa, în interesul securității naționale sau al relațiilor cu guvernul unei țări sau al unui teritoriu situat în afara Regatului Unit.

(2) În cazul în care ministrul consideră necesar să procedeze astfel în interesul securității naționale sau al relațiilor cu guvernul unei țări sau al unui teritoriu situat în afara Regatului Unit, acesta poate da persoanei căreia îi este aplicabil acest articol, după consultarea acesteia, instrucțiuni prin care să îi solicite (în funcție de împrejurările speței) să pună sau nu în aplicare o măsură specifică menționată în instrucțiuni.

(2A) Ministrul poate da instrucțiuni în temeiul alineatelor (1) sau (2) numai în cazul în care apreciază că comportamentul impus prin instrucțiuni este proporțional cu obiectivul care trebuie atins prin acest comportament.

(3) Persoana căreia i se aplică acest articol trebuie să pună în aplicare toate instrucțiunile care îi sunt date de ministru în temeiul prezentului articol, sub rezerva oricărei alte obligații care îi revine în temeiul părții 1 sau 2 din capitolul 1 din Communications Act 2003 [Legea din 2003 privind comunicațiile] și, în cazul instrucțiunilor date furnizorului unei rețele publice de comunicații electronice, chiar dacă instrucțiunile respective i se aplică în temeiul unei alte calități decât aceea de furnizor de acces la o asemenea rețea.

(4) Ministrul depune la fiecare dintre camerele Parlamentului o copie a tuturor instrucțiunilor date în temeiul prezentului articol, cu excepția situației în care apreciază că divulgarea instrucțiunilor respective ar fi contrară intereselor securității naționale sau relațiilor cu guvernul unei țări sau al unui teritoriu situat în afara Regatului Unit ori intereselor comerciale ale unei persoane.

(5) O persoană nu trebuie să divulge sau nu poate fi obligată să divulge, în temeiul unei legi sau în alt mod, anumite informații privind măsurile adoptate în conformitate cu prezentul articol în cazul în care ministrul i-a notificat că divulgarea acestor informații este considerată contrară intereselor securității naționale sau relațiilor cu guvernul unei țări sau al unui teritoriu situat în afara Regatului Unit ori intereselor comerciale ale unei alte persoane.

[…]

(8) Prezentul articol se aplică [Office of communications (OFCOM)] și furnizorilor de rețele publice de comunicații electronice.”

17 Articolul 21 alineatele (4) și (6) din Regulation of Investigatory Powers Act 2000 (Legea din 2010 de reglementare a competențelor de investigare, denumită în continuare „RIPA”) prevede:

„(4) «[D]ate privind comunicațiile» înseamnă oricare dintre următoarele:

(a) orice date de transfer incluse în sau anexate la o comunicație (fie de către expeditor, fie în alt mod) pentru orice serviciu poștal sau sistem de telecomunicații prin intermediul căruia este transmisă sau poate fi transmisă;

(b) orice informație care nu include nimic din conținutul unei comunicații [cu excepția oricărei informații care intră în domeniul de aplicare al literei (a)] și care se referă la utilizarea de către orice persoană:
(i) a oricărui serviciu poștal sau de telecomunicații sau
(ii) în legătură cu furnizarea sau cu utilizarea de către orice persoană a oricărui serviciu de telecomunicații sau a oricărei părți dintr-un sistem de telecomunicații;

(c) orice informație care nu intră în domeniul de aplicare al literelor (a) sau (b), care este deținută sau obținută în legătură cu persoanele destinatare ale serviciului de către o persoană care furnizează un serviciu poștal sau un serviciu de telecomunicații.

[…]

(6) [N]oțiunea de «date de transfer» în legătură cu orice comunicație se referă la:

(a) orice date de identificare sau care permit identificarea unei persoane, a unui aparat sau a locului către care sau de la care este transmisă sau poate fi transmisă o comunicație;

(b) orice date de identificare sau de selecționare sau care permit identificarea sau selecționarea echipamentului prin care este transmisă sau poate fi transmisă comunicația;

(c) orice date care conțin semnale pentru operarea aparatului utilizat într-un sistem de comunicații cu scopul de a transmite orice comunicație și

(d) orice date de identificare a datelor incluse în sau anexate la o comunicație particulară sau alte date, în măsura în care sunt incluse în sau anexate la o comunicație particulară.

[…]”

18 Articolele 65-69 din RIPA stabilesc normele privind funcționarea și competențele Investigatory Powers Tribunal (Tribunalul cu competențe de investigare, Regatul Unit). În conformitate cu articolul 65 din această lege, se pot formula plângeri la această instanță dacă există motive să se considere că datele au fost colectate în mod necorespunzător.

Litigiul principal și întrebările preliminare

19 La începutul anului 2015, existența unor practici de colectare și de utilizare a datelor referitoare la comunicații colectate în masă de către diferitele agenții de securitate și de informații din Regatul Unit, și anume GCHQ, MI5 și MI6, a fost făcută publică printre altele într-un raport al Intelligence and Security Committee of Parliament (Comisia pentru Informații și Securitate a Parlamentului, Regatul Unit). La 5 iunie 2015, Privacy International, o organizație non-guvernamentală, a sesizat Investigatory Powers Tribunal (Tribunalul cu competențe de investigare, Regatul Unit) cu o acțiune împotriva ministrului pentru Afaceri Externe și Commonwealth, a ministrului pentru Afaceri Interne, precum și a acestor agenții de securitate și de informații, contestând legalitatea practicilor respective.

20 Instanța de trimitere a examinat legalitatea practicilor menționate în raport mai întâi cu dreptul intern și cu prevederile Convenției europene pentru apărarea drepturilor omului și a libertăților fundamentale, semnată la Roma la 4 noiembrie 1950 (denumită în continuare „CEDO”), apoi cu dreptul Uniunii. Într-o hotărâre din 17 octombrie 2016, această instanță a constatat că pârâții din litigiul recunoscuseră că agențiile de securitate și de informații respective colectau și utilizau, în cadrul activităților lor, toate datele privind particularii și încadrate în diferite categorii (*bulk personal data*), cum ar fi date biografice sau referitoare la călătorii, informații de natură financiară sau comercială, date legate de comunicații și care puteau conține date sensibile, supuse secretului profesional, sau chiar material jurnalistic. Aceste date, obținute pe diverse căi, eventual secrete, ar fi analizate prin suprapunere, precum și prin prelucrări automate, ar putea fi divulgate altor persoane și autorități și partajate cu parteneri străini. În acest cadru, agențiile de securitate și de informații ar utiliza și date referitoare la comunicații colectate în masă de la furnizorii de rețele publice de comunicații electronice în special în temeiul instrucțiunilor ministeriale adoptate în temeiul articolului 94 din Legea din 1984. GCHQ și MI5 ar proceda astfel încă din anii 2001 și, respectiv, 2005.

21 Instanța menționată a apreciat că aceste măsuri de colectare și de utilizare a datelor erau conforme cu dreptul intern și, din anul 2015, cu articolul 8 din CEDO, sub rezerva unor aspecte încă neexaminate referitoare la proporționalitatea măsurilor menționate și la transferurile de date către terți. În această din urmă privință, ea a precizat că i-au fost prezentate probe privind garanțiile aplicabile, în special în ceea ce privește procedurile de acces și de divulgare în afara agențiilor de securitate și de informații, modalitățile de păstrare a datelor și existența unor controale independente.

22 În ceea ce privește legalitatea măsurilor de colectare și de utilizare în discuție în litigiul principal din perspectiva dreptului Uniunii, instanța de trimitere a examinat, într-o hotărâre din 8 septembrie 2017, dacă aceste măsuri intrau în domeniul de aplicare al acestui drept și, în caz afirmativ, dacă erau compatibile cu dreptul menționat. Această instanță a constatat, în ceea ce privește datele referitoare la comunicații colectate în masă, că furnizorii de rețele de comunicații electronice erau obligați, în temeiul articolului 94 din Legea din 1984, în cazul unor instrucțiuni în acest sens emise de un ministru, să furnizeze agențiilor de securitate și de informații datele colectate în cadrul activității lor economice care intră sub incidența dreptului Uniunii. În schimb, situația era diferită pentru culegerea celorlalte date, obținute de aceste servicii fără a recurge la asemenea competențe obligatorii. Pe baza acestei constatări, instanța menționată a considerat necesar să solicite Curții să stabilească dacă un regim precum cel care rezultă din acest articol 94 intră sub incidența dreptului Uniunii și, în cazul unui răspuns afirmativ, dacă și în ce mod se aplică acestui regim cerințele impuse de jurisprudența rezultată din Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, denumită în continuare „Hotărârea Tele2”, EU:C:2016:970).

23 În această privință, în cererea sa de decizie preliminară, instanța de trimitere arată că, potrivit articolului 94 menționat, ministrul poate da furnizorilor de servicii de comunicații electronice instrucțiuni generale sau specifice necesare în interesul securității naționale sau al relațiilor cu un guvern străin. Făcând trimitere la definițiile care figurează la articolul 21 alineatele (4) și (6) din RIPA, această instanță precizează că datele în cauză includ date de transfer, precum și informații privind serviciile utilizate în sensul acestei din urmă dispoziții, fiind exclus numai conținutul comunicațiilor.

Aceste date și aceste informații ar permite printre altele să se cunoască „cine, unde, când și cum” în privința unei comunicări. Datele menționate ar fi transmise agențiilor de securitate și de informații și păstrate de acestea în scopul desfășurării activităților lor.

24 Potrivit instanței menționate, regimul în discuție în litigiul principal diferă de cel rezultat din Data Retention and Investigatory Powers Act 2014 (Legea din 2014 privind păstrarea datelor și competențele de investigare), în discuție în cauza care a condus la pronunțarea Hotărârii din 21 decembrie 2016, Tele2 (C-203/15 și C-698/15, EU:C:2016:970), întrucât acest din urmă regim prevede păstrarea datelor de către furnizorii de servicii de comunicații electronice și punerea acestora nu numai la dispoziția agențiilor de securitate și de informații, în interesul securității naționale, ci și a altor autorități publice, în funcție de nevoile lor. Pe de altă parte, această hotărâre ar fi privit o anchetă penală, iar nu securitatea națională.

25 Instanța de trimitere adaugă că bazele de date constituite de agențiile de securitate și de informații fac obiectul unei prelucrări de masă și automate, nespecifică, prin care se urmărește descoperirea unor eventuale amenințări necunoscute. În acest scop, instanța menționată arată că toate metadatele astfel constituite ar trebui să fie cât mai complete posibil pentru a putea dispune de un „car cu fân” pentru a găsi „acul” care se ascunde acolo. În ceea ce privește utilitatea colectării de date în masă de către serviciile menționate și a tehnicilor de consultare a acestor date, instanța amintită se referă în special la concluziile raportului întocmit la 19 august 2016 de domnul David Anderson, QC, pe atunci United Kingdom Independent Reviewer of Terrorism Legislation (controlor independent din Regatul Unit al legislației privind terorismul), care, pentru a întocmi acest raport, s-a întemeiat pe o examinare efectuată de o echipă de specialiști în informații și pe mărturia agenților serviciilor de securitate și de informații.

26 Instanța de trimitere precizează de asemenea că, potrivit Privacy International, regimul în discuție în litigiul principal este nelegal în raport cu dreptul Uniunii, în timp ce pârâții din litigiul principal apreciază că obligația de transmitere a datelor prevăzută de acest regim, accesul la aceste date, precum și utilizarea lor nu intră în sfera de competență a Uniunii, în conformitate în special cu articolul 4 alineatul (2) TUE, potrivit căruia securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru.

27 În această privință, instanța de trimitere consideră, pe baza Hotărârii din 30 mai 2006, Parlamentul/Consiliul și Comisia (C-317/04 și C-318/04, EU:C:2006:346, punctele 56-59), referitoare la transferul de date PNR (*Passenger Name Record*) în scopul protecției securității publice, că activitățile societăților comerciale în cadrul prelucrării și al transferului de date în vederea protejării securității naționale nu par să intre în domeniul de aplicare al dreptului Uniunii. Ar fi necesar să se examineze nu dacă activitatea în cauză constituie o prelucrare de date, ci numai dacă, în esența și prin efectele sale, obiectul unei asemenea activități este de a susține o funcție esențială a statului, în sensul articolului 4 alineatul (2) TUE, prin intermediul unui cadru stabilit de autoritățile publice cu privire la siguranța publică.

28 În ipoteza în care măsurile în discuție în litigiul principal ar intra totuși sub incidența dreptului Uniunii, instanța de trimitere apreciază că cerințele care figurează la punctele 119-125 din Hotărârea din 21 decembrie 2016, Tele2 (C-203/15 și C-698/15, EU:C:2016:970), sunt inadecvate în contextul securității naționale și ar fi de natură să împiedice capacitatea agențiilor de securitate și de informații de a controla anumite amenințări la adresa securității naționale.

29 În aceste condiții, Investigatory Powers Tribunal (Tribunalul cu competențe de investigare, Regatul Unit) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„ În condițiile în care:

a) capacitatea [agențiilor de securitate și de informații] de a utiliza [datele referitoare la comunicații colectate în masă] furnizate este esențială pentru a proteja securitatea națională a Regatului Unit, inclusiv în domeniul combaterii terorismului, al contraspionajului și al combaterii proliferării nucleare;

b) o trăsătură fundamentală a utilizării de către [agențiile de securitate și de informații] a [datelor referitoare la comunicații colectate în masă] este descoperirea amenințărilor până atunci necunoscute la adresa securității naționale prin intermediul unor tehnici nespecifice în bloc care se bazează pe agregarea [datelor referitoare la comunicații colectate în masă] într-un singur loc. Principala sa utilitate constă în identificarea și investigarea rapidă a țintei, precum și în furnizarea unei baze de acțiune în situații de amenințare iminentă;

c) furnizorul unei rețele de comunicații electronice nu are apoi obligația de a păstra [datele referitoare la comunicații colectate în masă] (dincolo de perioada în care trebuie să le păstreze în vederea exercitării activității sale obișnuite), care sunt păstrate numai de către stat ([agențiile de securitate și de informații]);

d) instanța națională a constatat (sub rezerva anumitor aspecte rămase în pronunțare) că garanțiile legate de utilizarea [datelor referitoare la comunicații colectate în masă] de către [agențiile de securitate și de informații] sunt conforme cu dispozițiile CEDO și

e) instanța națională a constatat că impunerea cerințelor specificate la punctele 119-125 din Hotărârea [din 21 decembrie 2016, Tele2 (C-203/15 și C-698/15 (EU:C:2016:970)], ar submina, prin aplicarea lor, măsurile luate pentru protejarea securității naționale de către [agențiile de securitate și de informații] și ar periclita astfel securitatea națională a Regatului Unit;

1) Având în vedere articolul 4 TUE și articolul 1 alineatul (3) din Directiva [2002/58], o cerință inclusă într-o instrucțiune transmisă de ministru furnizorului unei rețele de comunicații electronice, conform căreia trebuie să furnizeze agențiilor de securitate și de informații ale unui stat membru date referitoare la comunicații colectate în masă, intră în domeniul de aplicare al dreptului Uniunii și al Directivei [2002/58]?

2) În cazul în care răspunsul la prima întrebare este afirmativ, unei astfel de instrucțiuni transmise de ministru i se aplică vreuna dintre cerințele [aplicabile datelor privind comunicațiile păstrate, specificate la punctele 119-125 din Hotărârea din 21 decembrie 2016, Tele2 (C-203/15 și C-698/15, EU:C:2016:970)], sau orice altă cerință suplimentară față de cele impuse de CEDO? Dacă răspunsul este afirmativ, în ce mod și în ce măsură se aplică aceste cerințe, luând în considerare nevoia absolută a [agențiilor de securitate și de informații] de a utiliza tehnicile de obținere în masă și de prelucrare automată pentru a proteja securitatea națională și măsura în care astfel de capacități, deși conforme cu CEDO din alte puncte de vedere, pot fi grav afectate de impunerea acestor cerințe?”

Cu privire la întrebările preliminare

Cu privire la prima întrebare

30 Prin intermediul primei întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolul 1 alineatul (3) din Directiva 2002/58 coroborat cu articolul 4 alineatul (2) TUE trebuie interpretat în sensul că intră în domeniul de aplicare al acestei directive o reglementare națională care permite unei autorități a statului să impună furnizorilor de servicii de comunicații electronice să transmită agențiilor de securitate și de informații date de transfer și date de localizare în vederea apărării securității naționale.

31 În această privință, Privacy International susține în esență că, având în vedere concluziile care decurg din jurisprudența Curții în ceea ce privește domeniul de aplicare al Directivei 2002/58, atât colectarea datelor de către agențiile de securitate și de informații de la acești furnizori, în temeiul articolului 94 din Legea din 1984, cât și utilizarea lor de către agențiile menționate intră în domeniul de aplicare al acestei directive, indiferent dacă datele menționate sunt colectate prin intermediul unei transmiteri amânate în timp sau sunt colectate în timp real. În special, faptul că obiectivul protejării securității naționale este enumerat în mod expres la articolul 15 alineatul (1) din directiva menționată nu ar avea drept consecință inaplicabilitatea acesteia din urmă în asemenea situații, iar articolul 4 alineatul (2) TUE nu ar afecta această apreciere.

32 În schimb, guvernul Regatului Unit, guvernele ceh și estonian, Irlanda, precum și guvernele francez, cipriot, maghiar, polonez și suedez arată în esență că Directiva 2002/58 nu se aplică reglementării naționale în discuție în litigiul principal, în măsura în care are ca finalitate apărarea securității naționale. Activitățile agențiilor de securitate și de informații țin de funcțiile esențiale ale statelor membre, care privesc menținerea ordinii publice, precum și apărarea securității interne și a integrității teritoriale, și, în consecință, sunt de competența exclusivă a acestora din urmă, după cum ar demonstra în special articolul 4 alineatul (2) a treia teză TUE.

33 Potrivit acestor guverne, Directiva 2002/58 nu poate fi, așadar, interpretată în sensul că măsurile naționale care vizează apărarea securității naționale intră în domeniul său de aplicare. Articolul 1 alineatul (3) din directiva menționată ar delimita acest domeniu de aplicare și ar exclude de aici, la fel cum se prevede deja la articolul 3 alineatul (2) prima liniuță din Directiva 95/46, activitățile privind siguranța publică, apărarea și siguranța statului. Aceste dispoziții ar reflecta repartizarea competențelor prevăzute la articolul 4 alineatul (2) TUE și ar fi lipsite de efect util în cazul în care măsurile care se încadrează în domeniul securității naționale ar trebui să respecte cerințele Directivei 2002/58. Pe de altă parte, jurisprudența Curții rezultată din Hotărârea din 30 mai 2006, Parlamentul/Consiliul și Comisia (C-317/04 și C-318/04, EU:C:2006:346), privind articolul 3 alineatul (2) prima liniuță din Directiva 95/46, ar fi aplicabilă articolului 1 alineatul (3) din Directiva 2002/58.

34 În această privință, trebuie arătat că, potrivit articolului 1 alineatul (1) din Directiva 2002/58, ea prevede printre altele 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.

35 Articolul 1 alineatul (3) din Directiva 2002/58 exclude din domeniul de aplicare al acesteia „activitățile statului” în domeniile menționate în articol, printre care se numără activitățile statului în domeniul penal și cele privind siguranța publică, apărarea, siguranța statului, inclusiv bunăstarea economică a statului atunci când este vorba despre activități legate de siguranța statului. Activitățile astfel menționate cu titlu de exemplu sunt, în toate cazurile, activități proprii statelor sau autorităților statale, străine de domeniile de activitate ale particularilor (Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctul 32 și jurisprudența citată).

36 În plus, articolul 3 din Directiva 2002/58 prevede că directiva menționată 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 Uniunii, inclusiv al rețelelor publice de comunicații care presupun colectarea de date și dispozitive de identificare (denumite în continuare „servicii de comunicații electronice”). Prin urmare, trebuie considerat că directiva menționată reglementează activitățile furnizorilor de astfel de servicii (Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctul 33 și jurisprudența citată).

37 În acest cadru, articolul 15 alineatul (1) din Directiva 2002/58 permite statelor membre să adopte, cu respectarea condițiilor pe care le prevede, „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 din [această] directivă” (Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 71).

38 Or, articolul 15 alineatul (1) din Directiva 2002/58 presupune în mod necesar că măsurile legislative naționale prevăzute la acest articol intră în domeniul de aplicare al directivei menționate, din moment ce aceasta din urmă permite în mod expres statelor membre să le adopte numai cu respectarea condițiilor prevăzute de directivă. În plus, asemenea măsuri guvernează, în scopurile menționate la această dispoziție, activitatea furnizorilor de servicii de comunicații electronice (Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctul 34 și jurisprudența citată).

39 În special în raport cu aceste considerații, Curtea a statuat că articolul 15 alineatul (1) din Directiva 2002/58 coroborat cu articolul 3 din aceasta trebuie interpretat în sensul că intră în domeniul de aplicare al directivei menționate nu numai o măsură legislativă care impune furnizorilor de servicii de comunicații electronice să păstreze datele de transfer și datele de localizare, ci și o măsură legislativă prin care se impune acestora să acorde autorităților naționale competente accesul la aceste date. Astfel, asemenea măsuri legislative implică în mod obligatoriu o prelucrare, de către acești furnizori, a datelor respective și, întrucât guvernează activitățile acelorași furnizori, nu pot fi asimilate unor activități proprii statelor, vizate la articolul 1 alineatul (3) din directiva menționată (a se vedea în acest sens Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctele 35 și 37, precum și jurisprudența citată).

40 În ceea ce privește o măsură legislativă precum articolul 94 din Legea din 1984, pe baza căreia autoritatea competentă poate da furnizorilor de servicii de comunicații electronice instrucțiunea de a comunica transmițând agențiilor de securitate și de informații date colectate în masă, trebuie să se arate că, potrivit definiției prevăzute la articolul 4 punctul 2 din Regulamentul 2016/679, care este aplicabil în conformitate cu articolul 2 din Directiva 2002/58 coroborat cu articolul 94 alineatul (2) din regulamentul menționat, noțiunea de „prelucrarea datelor cu caracter personal” înseamnă „orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, […], stocarea, […], consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod […]”.

41 Rezultă că o comunicare a datelor cu caracter personal prin transmitere constituie, la fel ca reținerea de date sau orice altă formă de punere la dispoziție, o prelucrare, în sensul articolului 3 din Directiva 2002/58, și, în consecință, se încadrează în domeniul de aplicare al directivei menționate (a se vedea în acest sens Hotărârea din 29 ianuarie 2008, Promusicae, C-275/06, EU:C:2008:54, punctul 45).

42 În plus, având în vedere considerațiile care figurează la punctul 38 din prezenta hotărâre și economia generală a Directivei 2002/58, o interpretare a acestei directive potrivit căreia măsurile legislative prevăzute la articolul 15 alineatul (1) ar fi excluse din domeniul de aplicare al directivei menționate, dat fiind că finalitățile la care trebuie să răspundă astfel de măsuri se pliază în esență pe finalitățile

urmărite de activitățile menționate la articolul 1 alineatul (3) din aceeași directivă, ar priva acest articol 15 alineatul (1) de orice efect util (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctele 72 și 73).

43 Prin urmare, noțiunea de „activități” care figurează la articolul 1 alineatul (3) din Directiva 2002/58 nu poate fi interpretată, astfel cum a arătat în esență domnul avocat general la punctul 75 din Concluziile prezentate în cauzele conexate La Quadrature du Net și alții (C-511/18 și C-512/18, EU:C:2020:6), la care face trimitere la punctul 24 din Concluziile prezentate în prezenta cauză, în sensul că se aplică măsurilor legislative prevăzute la articolul 15 alineatul (1) din această directivă.

44 Dispozițiile articolului 4 alineatul (2) TUE, la care s-au referit guvernele menționate la punctul 32 din prezenta hotărâre, nu pot infirma această concluzie. Astfel, potrivit jurisprudenței constante a Curții, deși definirea intereselor esențiale de securitate și adoptarea măsurilor apte să asigure siguranța lor internă și externă este de competența statelor membre, simplul fapt că o măsură națională a fost adoptată în vederea protecției securității naționale nu poate determina inaplicabilitatea dreptului Uniunii și nu poate exonera statele membre de respectarea necesară a acestui drept [a se vedea în acest sens Hotărârea din 4 iunie 2013, ZZ, C-300/11, EU:C:2013:363, punctul 38 și jurisprudența citată, Hotărârea din 20 martie 2018, Comisia/Austria (Imprimeria statului), C-187/16, EU:C:2018:194, punctele 75 și 76, precum și Hotărârea din 2 aprilie 2020, Comisia/Polonia, Ungaria și Republica Cehă (Mecanismul temporar de transfer al solicitanților de protecție internațională), C-715/17, C-718/17 și C-719/17, EU:C:2020:257, punctele 143 și 170].

45 Este adevărat că, în Hotărârea din 30 mai 2006, Parlamentul/Consiliul și Comisia (C-317/04 și C-318/04, EU:C:2006:346, punctele 56-59), Curtea a statuat că transferul de date cu caracter personal de către companiile aeriene către autoritățile publice dintr-un stat terț în scopul prevenirii, precum și al combaterii terorismului și al altor infracțiuni grave nu intră, în temeiul articolului 3 alineatul (2) prima liniuță din Directiva 95/46, în domeniul de aplicare al acestei directive, întrucât un asemenea transfer s-ar înscrie într-un cadru instituit de autoritățile publice privind siguranța publică.

46 Totuși, având în vedere considerațiile care figurează la punctele 36, 38 și 39 din prezenta hotărâre, această jurisprudență nu este aplicabilă pentru a interpreta articolul 1 alineatul (3) din Directiva 2002/58. Astfel, după cum a arătat în esență domnul avocat general la punctele 70-72 din Concluziile prezentate în cauzele conexate La Quadrature du Net și alții (C-511/18 și C-512/18, EU:C:2020:6), articolul 3 alineatul (2) prima liniuță din Directiva 95/46, la care se raportează jurisprudența menționată, excludea din domeniul de aplicare al acestei din urmă directive în general „prelucrăril[e] care au ca obiect siguranța publică, apărarea, securitatea statului” și nu efectua nicio distincție între persoane din perspectiva subiectului prelucrării datelor în cauză. În schimb, în cadrul interpretării articolului 1 alineatul (3) din Directiva 2002/58, o asemenea distincție se dovedește necesară. Astfel, după cum reiese din cuprinsul punctelor 37-39 și 42 din prezenta hotărâre, toate prelucrările de date cu caracter personal efectuate de furnizorii de servicii de comunicații electronice intră în domeniul de aplicare al directivei menționate, inclusiv prelucrările care decurg din obligațiile care le sunt impuse de autoritățile publice, în timp ce aceste din urmă prelucrări pot eventual intra în domeniul de aplicare al excepției prevăzute la articolul 3 alineatul (2) prima liniuță din Directiva 95/46, ținând seama de formularea mai largă a acestei dispoziții care privește ansamblul prelucrărilor, indiferent de autorul acestora, având ca obiect siguranța publică, apărarea sau securitatea statului.

47 Pe de altă parte, este necesar să se arate că Directiva 95/46, în discuție în cauza în care s-a pronunțat Hotărârea din 30 mai 2006, Parlamentul/Consiliul și Comisia (C-317/04 și C-318/04, EU:C:2006:346), a fost, potrivit articolului 94 alineatul (1) din Regulamentul 2016/679, abrogată și înlocuită de acesta începând de la 25 mai 2018. Or, deși regulamentul menționat precizează la articolul 2 alineatul (2) litera (d) că nu se aplică prelucrării „de către autoritățile competente” în scopul, printre altele, al prevenirii și depistării infracțiunilor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, din articolul 23 alineatul (1) literele (d) și (h) din același regulament reiese că prelucrarea datelor cu caracter personal efectuate de particulari în aceleași scopuri intră în

domeniul de aplicare al acestuia. Rezultă că interpretarea articolului 1 alineatul (3), a articolului 3 și a articolului 15 alineatul (1) din Directiva 2002/58 care precedă concordă cu delimitarea domeniului de aplicare al Regulamentului 2016/679 pe care această directivă îl completează și îl precizează.

48 În schimb, atunci când statele membre pun în mod direct în aplicare măsuri care derogă de la confidențialitatea comunicațiilor electronice, fără a impune obligații de prelucrare furnizorilor de astfel de servicii de comunicații, protecția datelor persoanelor vizate nu intră sub incidența Directivei 2002/58, ci doar a dreptului național, sub rezerva aplicării Directivei (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO 2016, L 119, p. 89), astfel încât măsurile în cauză trebuie să respecte printre altele dreptul național la nivel constituțional și cerințele CEDO.

49 Având în vedere considerațiile care precedă, trebuie să se răspundă la prima întrebare că articolul 1 alineatul (3), articolul 3 și articolul 15 alineatul (1) din Directiva 2002/58, prin raportare la articolul 4 alineatul (2) TUE, trebuie interpretate în sensul că o reglementare națională care permite unei autorități statale să impună furnizorilor de servicii de comunicații electronice să transmită agențiilor de securitate și de informații date de transfer și date de localizare în scopul apărării securității naționale intră în domeniul de aplicare al acestei directive.

Cu privire la a doua întrebare

50 Prin intermediul celei de a doua întrebări, instanța de trimitere urmărește în esență să afle dacă articolul 15 alineatul (1) din Directiva 2002/58, prin raportare la articolul 4 alineatul (2) TUE, precum și la articolele 7, 8 și 11 și la articolul 52 alineatul (1) din cartă, trebuie interpretat în sensul că se opune unei reglementări naționale care permite unei autorități statale să impună, în scopul apărării securității naționale, ca furnizorii de servicii de comunicații electronice să transmită în mod generalizat și nediferențiat date de transfer și date de localizare agențiilor de securitate și de informații.

51 Cu titlu introductiv, trebuie amintit că, potrivit indicațiilor care figurează în cererea de decizie preliminară, articolul 94 din Legea din 1984 permite ministrului să impună furnizorilor de servicii de comunicații electronice, prin instrucțiuni, atunci când consideră că este necesar în interesul securității naționale sau al relațiilor cu un guvern străin, să transmită agențiilor de securitate și de informații datele referitoare la comunicații colectate în masă, aceste date incluzând datele de transfer și datele de localizare, precum și informații privind serviciile utilizate, în sensul articolului 21 alineatele (4) și (6) din RIPA. Această din urmă dispoziție acoperă printre altele datele necesare pentru identificarea sursei unei comunicații și a destinației acesteia, stabilirea datei, a orei, a duratei și a tipului comunicației, identificarea materialului utilizat, precum și localizarea echipamentelor terminale și a comunicațiilor, date printre care figurează în special numele și adresa utilizatorului, numărul de telefon al apelantului și numărul apelat, adresele IP ale sursei și destinatarului comunicării, precum și adresele paginilor de internet vizitate.

52 O asemenea comunicare prin transmiterea datelor îi privește pe toți utilizatorii mijloacelor de comunicații electronice, fără să se precizeze dacă această transmitere trebuie să intervină în timp real sau cu întârziere. Odată transmise, aceste date sunt, potrivit indicațiilor care figurează în cererea de decizie preliminară, păstrate de agențiile de securitate și de informații și rămân la dispoziția acestora din urmă în scopul desfășurării activităților lor, precum celelalte baze de date pe care le dețin aceste agenții. În special, datele astfel colectate, care sunt supuse prelucrării și analizelor de masă și automate, se pot suprapune cu alte baze de date care cuprind diferite categorii de date cu caracter

personal colectate în masă sau pot fi divulgate în afara acestor servicii și unor state terțe. În sfârșit, aceste operațiuni nu sunt condiționate de autorizarea prealabilă a unei instanțe sau a unei autorități administrative independente și nu conduc la o informare a persoanelor vizate.

53 Directiva 2002/58 are drept scop, astfel cum reiese în special din considerentele (6) și (7) ale acesteia, să protejeze utilizatorii serviciilor de comunicații electronice împotriva riscurilor pentru datele lor personale și pentru confidențialitatea comunicațiilor lor care rezultă din noile tehnologii și în special din capacitățile în creștere de stocare automată și de prelucrare a datelor. În special, directiva menționată caută, astfel cum enunță considerentul (2) al acesteia, să asigure respectarea deplină a drepturilor menționate la articolele 7 și 8 din cartă. În această privință, din expunerea de motive la Propunerea de directivă a Parlamentului European și a Consiliului privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice [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”.

54 În acest scop, articolul 5 alineatul (1) din Directiva 2002/58 prevede că „[s]tatele 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”. Aceeași dispoziție subliniază de asemenea că „[statele membre] interzic astfel în special ascultarea, interceptarea, 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)”, și precizează că „[acest] alineat nu interzice stocarea tehnică necesară pentru transmisia comunicației care nu aduce atingere principiului confidențialității.”

55 Astfel, articolul 5 alineatul (1) consacră principiul confidențialității atât a comunicațiilor electronice, cât și a datelor de transfer aferente acestora și implică în special interdicția, în principiu, pentru orice altă persoană decât utilizatorii, de a stoca, fără consimțământul lor, aceste comunicații și aceste date. Având în vedere caracterul general al modului său de redactare, dispoziția menționată privește în mod necesar orice operațiune care permite terților să ia cunoștință de comunicațiile și de datele aferente acestora în alte scopuri decât transmiterea unei comunicații.

56 Interdicția de a intercepta comunicațiile și datele aferente, care figurează la articolul 5 alineatul (1) din Directiva 2002/58, include, așadar, orice formă de punere la dispoziție de către furnizorii de servicii de comunicații electronice a datelor de transfer și a datelor de localizare autorităților publice, precum agenții de securitate și de informații, dar și păstrarea datelor respective de către aceste autorități, indiferent de modul în care acestea sunt ulterior utilizate.

57 Astfel, prin adoptarea directivei menționate, legiuitorul Uniunii a concretizat drepturile consacrate la articolele 7 și 8 din cartă, astfel încât utilizatorii mijloacelor de comunicații electronice sunt îndreptățiți să se aștepte, în principiu, ca, în lipsa consimțământului lor, comunicațiile lor și datele aferente să rămână anonime și să nu poată face obiectul unei înregistrări (Hotărârea din 6 octombrie 2020, La Quadature du Net și alții, C-511/18, C-512/18 și C-520/18, punctul 109).

58 Cu toate acestea, articolul 15 alineatul (1) din Directiva 2002/58 permite statelor membre să introducă excepții de la obligația de principiu, prevăzută la articolul 5 alineatul (1) din această directivă, de a asigura confidențialitatea datelor cu caracter personal, precum și de la obligațiile corespunzătoare, menționate în special la articolele 6 și 9 din directiva menționată, atunci când o asemenea limitare constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice pentru a proteja securitatea națională, apărarea și siguranța publică sau pentru a asigura prevenirea, cercetarea, depistarea și urmărirea infracțiunilor sau a utilizărilor neautorizate ale sistemului de

comunicații electronice. În acest scop, statele membre pot adopta, între altele, măsuri legislative care prevăd păstrarea de date pentru o perioadă limitată, în cazul în care acest lucru este justificat de unul dintre motivele amintite.

59 Astfel, posibilitatea de a deroga de la drepturile și obligațiile prevăzute la articolele 5, 6 și 9 din Directiva 2002/58 nu poate să justifice transformarea în regulă a derogării de la obligația de principiu de a asigura confidențialitatea comunicațiilor electronice și a datelor aferente acestora și în special de la interdicția de a stoca aceste date, prevăzută în mod explicit la articolul 5 din directiva menționată (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctele 89 și 104, precum și Hotărârea din 6 octombrie 2020, La Quadrature du Net și alții, C-511/18, C-512/18 și C-520/18, punctul 111).

60 În plus, din articolul 15 alineatul (1) a treia teză din Directiva 2002/58 reiese că statele membre nu sunt autorizate să adopte măsuri legislative pentru a restrânge sfera de aplicare a drepturilor și obligațiilor prevăzute la articolele 5, 6 și 9 din această directivă decât cu respectarea principiilor generale ale dreptului Uniunii, printre care figurează principiul proporționalității, și cu respectarea drepturilor fundamentale garantate de cartă. În această privință, Curtea a statuat deja că obligația impusă de un stat membru furnizorilor de servicii de comunicații electronice, printr-o reglementare națională, 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 referitoare la protecția vieții private și la protecția datelor cu caracter personal, ci și a articolului 11 din cartă referitor la libertatea de exprimare (a se vedea în acest sens Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctele 25 și 70, precum și Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctele 91 și 92, precum și jurisprudența citată).

61 Aceleași probleme se ridică și pentru alte tipuri de prelucrări de date, precum transmiterea lor către alte persoane decât utilizatorii sau accesul la aceste date în vederea utilizării lor [a se vedea prin analogie Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctele 122 și 123, precum și jurisprudența citată].

62 Astfel, interpretarea articolului 15 alineatul (1) din Directiva 2002/58 trebuie să țină seama atât de importanța dreptului la respectarea vieții private, garantat la articolul 7 din cartă, cât și de importanța dreptului la protecția datelor cu caracter personal, garantat la articolul 8 din aceasta, astfel cum reiese din jurisprudența Curții, precum și de libertatea de exprimare, acest drept fundamental, garantat la articolul 11 din cartă, constituind unul dintre fundamentele esențiale al unei societăți democratice și pluraliste, care reflectă valorile pe care, conform articolului 2 TUE, se întemeiază Uniunea (a se vedea în acest sens Hotărârea din 6 martie 2001, Connolly/Comisia, C-274/99 P, EU:C:2001:127, punctul 39, și Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 93 și jurisprudența citată).

63 Cu toate acestea, drepturile consacrate la articolele 7, 8 și 11 din cartă nu sunt prerogative absolute, ci trebuie să fie luate în considerare în raport cu funcția lor în societate (a se vedea în acest sens Hotărârea din 16 iulie 2020, Facebook Ireland și Schrems, C-311/18, EU:C:2020:559, punctul 172, precum și jurisprudența citată).

64 Astfel, după cum reiese din articolul 52 alineatul (1) din cartă, aceasta admite restrângeri ale exercițiului acestor drepturi, în măsura în care aceste restrângeri sunt prevăzute de lege, respectă substanța drepturilor respective și, prin respectarea principiului proporționalității, sunt necesare și răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

65 Trebuie adăugat că cerința ca orice restrângere a exercitării drepturilor fundamentale să fie prevăzută de lege presupune ca temeiul juridic care permite ingerința în aceste drepturi să definească el însuși întinderea restrângerii exercitării dreptului vizat (Hotărârea din 16 iulie 2020, Facebook Ireland și Schrems, C-311/18, EU:C:2020:559, punctul 175, precum și jurisprudența citată).

66 În ceea ce privește respectarea principiului proporționalității, articolul 15 alineatul (1) prima teză din Directiva 2002/58 prevede că statele membre pot adopta o măsură care derogă de la principiul confidențialității comunicațiilor și datelor de transfer aferente în cazul în care o asemenea măsură este „necesară, corespunzătoare și proporțională în cadrul unei societăți democratice”, în raport cu obiectivele enunțate de dispoziția menționată. Considerentul (11) al acestei directive precizează 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 ține seama de faptul că acesta trebuie să fie compatibil cu drepturile fundamentale vizate de măsură, prin realizarea unui just echilibru între obiectivul și interesele și drepturile în cauză [a se vedea în acest sens Hotărârea din 16 decembrie 2008, Satakunnan Markkinapörssi și Satamedia, C-73/07, EU:C:2008:727, punctul 56, Hotărârea din 9 noiembrie 2010, Volker und Markus Schecke și Eifert, C-92/09 și C-93/09, EU:C:2010:662, punctele 76, 77 și 86, precum și Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctul 52; Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 140].

68 Pentru a respecta cerința proporționalității, o reglementare trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime astfel încât persoanele ale căror date cu caracter personal sunt vizate să dispună de garanții suficiente care să permită protejarea în mod eficient a acestor date împotriva riscurilor de abuz. Această reglementare trebuie să fie obligatorie din punct de vedere juridic în dreptul intern și în special să indice în ce împrejurări și în ce condiții o măsură care prevede prelucrarea unor asemenea date poate fi luată, garantând în acest mod că o ingerință este limitată la strictul necesar. Necesitatea de a dispune de astfel de garanții este cu atât mai importantă atunci când datele cu caracter personal sunt supuse unei prelucrări automatizate, în special în cazul în care există un risc important privind un acces ilicit la aceste date. Aceste considerații sunt aplicabile în special atunci când în discuție este protecția categoriei speciale de date cu caracter personal pe care o reprezintă datele sensibile [a se vedea în acest sens Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctele 54 și 55, Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 117, precum și Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 141].

69 În ceea ce privește aspectul dacă o reglementare națională precum cea în discuție în litigiul principal îndeplinește cerințele 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, trebuie arătat că transmiterea datelor de transfer și a datelor de localizare altor persoane decât utilizatorii, precum agențiile de securitate și de informații, derogă de la principiul confidențialității. Din moment ce această operațiune este efectuată, precum în speță, în mod generalizat și nediferențiat, ea are ca efect să transforme derogarea de la obligația de principiu de a asigura confidențialitatea datelor într-o regulă, în timp ce sistemul instituit de Directiva 2002/58 impune ca o asemenea derogare să rămână o excepție.

70 În plus, potrivit jurisprudenței constante a Curții, transmiterea datelor de transfer și a datelor de localizare unui terț constituie o ingerință în drepturile fundamentale consacrate la articolele 7 și 8 din cartă, indiferent de utilizarea ulterioară a acestor date. În această privință, este irelevant dacă informațiile vizate referitoare la viața privată prezintă sau nu caracter sensibil sau dacă persoanele interesate au suferit sau nu eventuale inconveniente ca urmare a acestei ingerințe [a se vedea în acest

sens Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctele 124 și 126, precum și jurisprudența citată, și Hotărârea din 6 octombrie 2020, La Quadrature du Net și alții, C-511/18, C-512/18 și C-520/18, punctele 115 și 116].

71 Ingerința pe care o implică transmiterea datelor de transfer și a datelor de localizare pentru agențiile de securitate și de informații în dreptul consacrat la articolul 7 din cartă trebuie considerată deosebit de gravă, ținând seama în special de caracterul sensibil al informațiilor pe care le pot furniza aceste date și în special de posibilitatea de a stabili pe baza acestora profilul persoanelor în cauză, o asemenea informație fiind la fel de sensibilă ca și conținutul însuși al comunicațiilor. În plus, aceasta este susceptibilă să genereze în mintea persoanelor vizate sentimentul că viața lor privată face obiectul unei supravegheri constante (a se vedea prin analogie Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctele 27 și 37, precum și Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctele 99 și 100).

72 Trebuie de asemenea arătat că o transmitere a datelor de transfer și a datelor de localizare către autorități publice în scopuri de securitate este susceptibilă, prin ea însăși, să aducă atingere dreptului la respectarea comunicațiilor, consacrat la articolul 7 din cartă, și să aibă efecte disuasive asupra exercitării de către utilizatorii mijloacelor de comunicații electronice a libertății lor de exprimare, garantată la articolul 11 din cartă. Astfel de efecte disuasive pot afecta în special persoanele ale căror comunicări sunt supuse, potrivit normelor naționale, secretului profesional, precum și avertizorii ale căror activități sunt protejate de Directiva (UE) 2019/1937 a Parlamentului European și a Consiliului din 23 octombrie 2019 privind protecția persoanelor care raportează încălcări ale dreptului Uniunii (JO 2019, L 305, p. 17). În plus, aceste efecte sunt cu atât mai grave, cu cât numărul și varietatea datelor păstrate sunt mai ridicate (a se vedea în acest sens Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctul 28, Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 101, precum și Hotărârea din 6 octombrie 2020, La Quadrature du Net și alții, C-511/18, C-512/18 și C-520/18, punctul 118).

73 În sfârșit, ținând seama de cantitatea importantă a datelor de transfer și a datelor de localizare care pot fi păstrate în mod continuu printr-o măsură de păstrare generalizată, 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.

74 În ceea ce privește obiectivele care pot justifica asemenea ingerințe, în special obiectivul apărării securității naționale în discuție în litigiul principal, trebuie arătat de la bun început că articolul 4 alineatul (2) TUE prevede că securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru. Această responsabilitate corespunde interesului primordial de a proteja funcțiile esențiale ale statului și interesele fundamentale ale societății și include prevenirea și sancționarea activităților de natură să destabilizeze grav structurile constituționale, politice, economice sau sociale fundamentale ale unei țări, în special să amenințe direct societatea, populația sau statul ca atare, cum ar fi, printre altele, activitățile de terorism (Hotărârea din 6 octombrie 2020, La Quadrature du Net și alții, C-511/18, C-512/18 și C-520/18, punctul 135).

75 Or, importanța obiectivului apărării securității naționale, interpretat în lumina articolului 4 alineatul (2) TUE, o depășește pe cea a celorlalte obiective prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, în special obiective de combatere a infracționalității în general, chiar gravă, precum și de protejare a siguranței publice. Astfel, amenințări precum cele menționate la punctul precedent se disting, prin natura și prin gravitatea lor deosebită, de riscul general de apariție a unor tensiuni sau tulburări, chiar grave, ale siguranței publice. Sub rezerva respectării celorlalte cerințe prevăzute la articolul 52 alineatul (1) din cartă, obiectivul apărării securității naționale poate justifica, așadar, măsuri care presupun ingerințe în drepturile fundamentale mai grave decât cele pe care le-ar putea justifica aceste alte obiective (Hotărârea din 6 octombrie 2020, La Quadrature du Net și alții, C-511/18, C-512/18 și C-520/18, punctul 136).

76 Cu toate acestea, pentru a îndeplini cerința proporționalității amintită la punctul 67 din prezenta hotărâre, potrivit căreia derogările de la protecția datelor cu caracter personal și limitările acesteia trebuie să fie efectuate în limitele strictului necesar, o reglementare națională care conține o ingerință în drepturile fundamentale consacrate la articolele 7 și 8 din cartă trebuie să respecte cerințele care rezultă din jurisprudența citată la punctele 65, 67 și 68 din prezenta hotărâre.

77 În special, în ceea ce privește accesul unei autorități la date cu caracter personal, o reglementare nu se poate limita la a impune ca accesul autorităților la date să corespundă finalității urmărite de această reglementare, ci trebuie să prevadă și condițiile materiale și procedurale care guvernează această utilizare [a se vedea prin analogie Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 192 și jurisprudența citată].

78 Prin urmare, întrucât un acces general la toate datele păstrate, în lipsa oricărei legături, chiar indirectă, cu scopul urmărit, nu poate fi considerat limitat la strictul necesar, o reglementare națională care guvernează accesul la datele de transfer și la datele de localizare trebuie să se întemeieze pe criterii obiective pentru a defini împrejurările și condițiile în care trebuie să se acorde autorităților naționale competente accesul la datele în cauză (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 119 și jurisprudența citată).

79 Aceste cerințe se aplică *a fortiori* unei măsuri legislative precum cea în discuție în litigiul principal, pe baza căreia autoritatea națională competentă poate impune furnizorilor de servicii de comunicații electronice să transmită în mod generalizat și nediferențiat datele de transfer și datele de localizare agențiilor de securitate și de informații. Astfel, o asemenea transmitere are ca efect punerea acestor date la dispoziția autorităților publice [a se vedea prin analogie Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 212].

80 Întrucât transmiterea datelor de transfer și a datelor de localizare are loc în mod generalizat și nediferențiat, aceasta privește în mod global ansamblul persoanelor care utilizează servicii de comunicații electronice. Ea se aplică, așadar, chiar și acelor persoane în privința cărora nu există niciun indiciu de natură să sugereze că comportamentul lor poate avea o legătură, chiar indirectă sau îndepărtată, cu obiectivul apărării securității naționale și mai ales fără să se stabilească o relație între datele a căror transmitere este prevăzută și o amenințare pentru securitatea națională (a se vedea în acest sens Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctele 57 și 58, precum și Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 105). Având în vedere faptul că transmiterea unor astfel de date autorităților publice echivalează, în conformitate cu cele constatate la punctul 79 din prezenta hotărâre, cu un acces, trebuie să se considere că o reglementare care permite o transmitere generalizată și nediferențiată a datelor către autoritățile publice conduce la un acces general.

81 Rezultă că o reglementare națională care impune furnizorilor de servicii de comunicații electronice să transmită în mod generalizat și nediferențiat datele de transfer și datele de localizare agențiilor de securitate și de informații depășește limitele strictului necesar și nu poate fi considerată justificată într-o societate democratică, astfel cum impune articolul 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolului 4 alineatul (2) TUE, precum și a articolelor 7, 8 și 11 și a articolului 52 alineatul (1) din cartă.

82 Având în vedere toate considerațiile care precedă, este necesar să se răspundă la a doua întrebare că articolul 15 alineatul (1) din Directiva 2002/58, prin raportare la articolul 4 alineatul (2) TUE, precum și la articolele 7, 8 și 11 și la articolul 52 alineatul (1) din cartă, trebuie interpretat în sensul că se opune unei reglementări naționale care permite unei autorități statale să impună, în scopul apărării securității naționale, ca furnizorii de servicii de comunicații electronice să transmită în mod generalizat și nediferențiat date de transfer și date de localizare agențiilor de securitate și de informații.

Cu privire la cheltuielile de judecată

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

Pentru aceste motive, Curtea (Marea Cameră) declară:

1) **Articolul 1 alineatul (3), articolul 3 și 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, prin raportare la articolul 4 alineatul (2) TUE, trebuie interpretate în sensul că o reglementare națională care permite unei autorități statale să impună furnizorilor de servicii de comunicații electronice să transmită agențiilor de securitate și de informații date de transfer și date de localizare în scopul apărării securității naționale intră în domeniul de aplicare al acestei directive.**

2) **Articolul 15 alineatul (1) din Directiva 2002/58, astfel cum a fost modificată prin Directiva 2009/136, prin raportare la articolul 4 alineatul (2) TUE, precum și la articolele 7, 8 și 11 și la articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene, trebuie interpretat în sensul că se opune unei reglementări naționale care permite unei autorități statale să impună, în scopul apărării securității naționale, furnizorilor de servicii de comunicații electronice să transmită în mod generalizat și nediferențiat date de transfer și date de localizare agențiilor de securitate și de informații.**

Semnături