(hidden)

HOTĂRÂREA CURȚII (Marea Cameră)

21 decembrie 2016(*)

„Trimitere preliminară – Comunicații electronice – Prelucrarea datelor cu caracter personal – Confidențialitatea comunicațiilor electronice – Protecție – Directiva 2002/58/CE – Articolele 5, 6 și 9, precum și articolul 15 alineatul (1) – Carta drepturilor fundamentale a Uniunii Europene – Articolele 7, 8 și 11, precum și articolul 52 alineatul (1) – Legislaţie naţională – Furnizori de servicii de comunicații electronice – Obligație de păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare – Autorități naționale – Acces la date – Lipsa controlului prealabil de către o instanță sau o autoritate administrativă independentă – Compatibilitate cu dreptul Uniunii”

În cauzele conexate C-203/15 și C-698/15,

având ca obiect cereri de decizie preliminară formulate în temeiul articolului 267 TFUE de Kammarrätten i Stockholm (Curtea de Apel Administrativă din Stockholm, Suedia) și Court of Appeal (England & Wales) (Civil Division) [Curtea de Apel (Anglia și Țara Galilor) (secția civilă), Regatul Unit], prin deciziile din 29 aprilie 2015 și, respectiv, din 9 decembrie 2015, primite de Curte la 4 mai 2015 și la 28 decembrie 2015, în procedurile

Tele2 Sverige AB (C-203/15)

împotriva

Post- och telestyrelsen,

și

Secretary of State for the Home Department (C-698/15)

împotriva

Tom Watson,

Peter Brice,

Geoffrey Lewis,

cu participarea:

Open Rights Group,

Privacy International,

The Law Society of England and Wales,

CURTEA (Marea Cameră),

compusă din domnul K. Lenaerts, președinte, domnul A. Tizzano, vicepreședinte, doamna R. Silva de Lapuerta, domnii T. von Danwitz (raportor), J. L. da Cruz Vilaça, E. Juhász și M. Vilaras, președinți de cameră, și domnii A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen și C. Lycourgos, judecători,

avocat general: H. Saugmandsgaard Øe,

grefier: C. Strömholm, administrator,

având în vedere decizia președintelui Curții din 1 februarie 2016 de judecare a cauzei C-698/15 potrivit procedurii accelerate prevăzute la articolul 105 alineatul (1) din Regulamentul de procedură al Curții,

având în vedere procedura scrisă și în urma ședinței din 12 aprilie 2016,

luând în considerare observațiile prezentate:

– pentru Tele2 Sverige AB, de M. Johansson și de N. Torgerzon, advokater, precum și de E. Lagerlöf și de S. Backman;

– pentru Watson, de J. Welch și de E. Norton, solicitors, de I. Steele, advocate, de B. Jaffey, barrister, precum și de D. Rose, QC;

– pentru Brice și Lewis, de A. Suterwalla și de R. de Mello, barristers, de R. Drabble, QC, precum și de S. Luke, solicitor;

– pentru Open Rights Group și Privacy International, de D. Carey, solicitor, precum și de R. Mehta și de J. Simor, barristers;

– pentru The Law Society of England and Wales, de T. Hickman, barrister, precum și de N. Turner;

– pentru guvernul suedez, de A. Falk, de C. Meyer-Seitz, de U. Persson, de N. Otte Widgren și de L. Swedenborg, în calitate de agenți;

– pentru guvernul Regatului Unit, de S. Brandon, de L. Christie și de V. Kaye, în calitate de agenți, asistați de D. Beard, de G. Facenna și de J. Eadie, QC, precum și de S. Ford, barrister;

– pentru guvernul belgian, de J.-C. Halleux, de S. Vanrie și de C. Pochet, în calitate de agenți;

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

– pentru guvernul danez, de C. Thorning și de M. Wolff, în calitate de agenți;

– pentru guvernul german, de T. Henze, de M. Hellmann și de J. Kemper, în calitate de agenți, asistați de M. Kottmann și de U. Karpenstein, Rechtsanwalte;

– pentru guvernul eston, de K. Kraavi-Käerdi, în calitate de agent;

– pentru Irlanda, de E. Creedon, de L. Williams și de A. Joyce, în calitate de agenți, asistați de D. Fennelly, BL;

– pentru guvernul spaniol, de A. Rubio González, în calitate de agent;

– pentru guvernul francez, de G. de Bergues, de D. Colas, de F.-X. Bréchot și de C. David, în calitate de agenți;

– pentru guvernul cipriot, de K. Kleanthous, în calitate de agent;

– pentru guvernul maghiar, de M. Fehér și de G. Koós, în calitate de agenți;

– pentru guvernul neerlandez, de M. Bulterman, de M. Gijzen și de J. Langer, în calitate de agenți;

– pentru guvernul polonez, de B. Majczyna, în calitate de agent;

– pentru guvernul finlandez, de J. Heliskoski, în calitate de agent;

– pentru Comisia Europeană, de H. Krämer, de K. Simonsson, de H. Kranenborg, de D. Nardi, de P. Costa de Oliveira și de J. Vondung, în calitate de agenți,

după ascultarea concluziilor avocatului general în ședința din 19 iulie 2016,

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 publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO 2002, L 201, p. 37, Ediție specială, 13/vol. 36, p. 63), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 (JO 2009, L 337, p. 11, rectificare în JO 2013, L 241, p. 9) (denumită în continuare „Directiva 2002/58”), lecturat în lumina articolelor 7 și 8, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”).

2 Aceste cereri au fost formulate în cadrul a două litigii între, în cel dintâi, Tele2 Sverige AB, pe de o parte, și Post- och telestyrelsen (Autoritatea Suedeză de Reglementare a Poștei și Telecomunicațiilor, denumită în continuare „PTS”), pe de altă parte, în legătură cu o somație emisă de aceasta din urmă și adresată Tele2 Sverige de a păstra datele referitoare la trafic și datele de localizare a abonaților și a utilizatorilor înregistrați ai acesteia (cauza C-203/15), iar în cel de al doilea, între domnii Tom Watson, Peter Brice și Geoffrey Lewis, pe de o parte, și Secretary of State for the Home Department (ministrul de interne, Regatul Unit al Marii Britanii și Irlandei de Nord), pe de altă parte, în legătură cu conformitatea cu dreptul Uniunii a articolului 1 din Data Retention and Investigatory Powers Act 2014 (Legea din 2014 privind păstrarea datelor și competențele de investigare, denumită în continuare „DRIPA”) (cauza C-698/15).

Cadrul juridic

Dreptul Uniunii

Directiva 2002/58

3 Considerentele (2), (6), (7), (11), (21), (22), (26) și (30) ale Directivei 2002/58 au următorul cuprins:

„(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 ale [acesteia].

[...]

(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 prelucrarea a datelor referitoare la abonați și utilizatori.

[...]

(11) La fel ca 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)], 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 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, 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

[...]

(21) Trebuie luate măsuri pentru a evita accesul neautorizat la comunicații pentru a proteja confidențialitatea acestora, atât în privința conținutului, cât și a datelor referitoare la comunicații în sine realizate prin rețelele de comunicații publice sau prin servicii publice de comunicații electronice. Legislația internă a unora dintre statele membre interzice doar accesul neautorizat intenționat la comunicații.

(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. [...]

[...]

(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 pe o perioadă limitată de timp. Orice altă prelucrare a acestor date pe care prestatorul de servicii publice de comunicații electronice ar dori să o efectueze [...] 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. [...]

[...]

(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. [...]"

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

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

(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 de instituire a Comunității Europene, cum sunt cele menționate la titlurile V și VI al Tratatului privind Uniunea Europeană, și în orice caz activităților legate de siguranța publică, de apărare, de siguranța statului (inclusiv de bunăstarea economică a acestuia, dacă activitățile respective sunt legate de chestiuni de siguranța statului) și activităților statului în domeniul legii penale."

5 Potrivit articolului 2 din Directiva 2002/58, 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 un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice (Directivă-cadru) [(JO 2002, L 108, p. 33, Ediție specială, 13/vol. 35, p. 195)].

Se aplică de asemenea următoarele definiții:

[...]

(b) «date de transfer» înseamnă orice date prelucrare 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;

[...]”

6 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”

7 Articolul 4 din această directivă, intitulat „Securitatea prelucrării datelor”, are următorul cuprins:

„(1) Prestatorul unui serviciu public de comunicații electronice trebuie să ia măsurile tehnice și organizaționale corespunzătoare pentru protejarea securității serviciilor sale, dacă este necesar împreună cu furnizorul rețelei de comunicații electronice, în privința securității rețelei. Având în vedere noutatea și costurile punerii lor în aplicare, aceste măsuri trebuie să asigure un nivel de securitate corespunzător riscurilor.

(1a) Fără a aduce atingere Directivei [95/46], măsurile menționate la alineatul (1) realizează cel puțin următoarele:

– garantează că datele cu caracter personal pot fi accesate exclusiv de personalul autorizat și în scopuri autorizate din punct de vedere juridic;

– protejează datele cu caracter personal stocate sau transmise împotriva distrugerii accidentale sau ilicite, împotriva pierderii sau deteriorării accidentale și împotriva stocării, prelucrării, accesării sau divulgării ilicite și

– asigură punerea în aplicare a unei politici de securitate în ceea ce privește prelucrarea datelor cu caracter personal.

[...]”

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, 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.”

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:

„(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 comunitare, inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) al Tratatului privind Uniunea Europeană.

[...]

(1b) Furnizorii stabilesc proceduri interne pentru a răspunde solicitărilor de accesare a datelor cu caracter personal ale utilizatorilor pe baza dispozițiilor naționale adoptate în conformitate cu alineatul (1). La cerere, aceștia oferă autorității naționale competente informații despre procedurile respective, numărul de solicitări primite, justificarea legală invocată și răspunsul acestora.

(2) Dispozițiile capitolului III cu privire la măsuri judiciare, responsabilitate și sancțiuni din Directiva [95/46] se aplică în privința dispozițiilor de drept intern adoptate în conformitate cu prezenta directivă și cu privire la drepturile individuale ce decurg din prezenta directivă.

[...]"

Directiva 95/46

12 Articolul 22 din Directiva 95/46, care figurează în capitolul III din aceasta, are următorul cuprins:

„Fără să aducă atingere oricărei căi administrative de atac care poate fi prevăzută, inter alia, în fața autorității de supraveghere menționată la articolul 28, anterior sesizării autorității judecătorești, statele membre prevăd dreptul oricărei persoane la o cale atac în justiție în caz de încălcare a drepturilor garantate prin dreptul intern aplicabil prelucrării în cauză."

Directiva 2006/24/CE

13 Articolul 1 din 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), intitulat „Obiectul și domeniul de aplicare", prevedea la alineatul (2):

„Prezenta directivă se aplică datelor de trafic și localizare, atât pentru entități juridice, cât și pentru persoane fizice, precum și datelor necesare pentru identificarea abonatului sau a utilizatorului înregistrat. Nu se aplică pentru conținutul comunicațiilor electronice, inclusiv informațiile consultate prin utilizarea unei rețele de comunicații electronice."

14 Potrivit articolului 3 din această directivă, intitulat „Obligația de păstrare a datelor":

„(1) Prin derogare de la articolele 5, 6 și 9 din Directiva [2002/58], statele membre adoptă măsuri pentru a se asigura că datele menționate la articolul 5 din prezenta directivă sunt păstrate în conformitate cu dispozițiile acesteia, în măsura în care acele date sunt generate sau prelucrate de către furnizorii de comunicații electronice accesibile publicului sau de rețele publice de comunicații, de competența acestora, în procesul de furnizare a serviciilor de comunicații respective.

(2) Obligația de a păstra datele prevăzute la alineatul (1) include păstrarea datelor specificate la articolul 5 referitoare la încercări nereușite de apeluri telefonice, în cazul în care aceste date sunt generate sau prelucrate și păstrate (în ceea ce privește datele de telefonie), sau înregistrate în jurnal electronic (în ceea ce privește datele de Internet) de către furnizorii de servicii de comunicații electronice accesibile publicului sau de rețele publice de comunicații în cadrul competenței statului membru respectiv, în procesul de furnizare a serviciilor de comunicații în cauză. Prezenta directivă nu impune păstrarea datelor referitoare la apelurile care nu se conectează."

Dreptul suedez

15 Din decizia de trimitere în cauza C-203/15 reiese că, pentru a transpune Directiva 2006/24 în dreptul național, legiuitorul suedez a modificat lagen (2003:389) om elektronisk kommunikation [Legea (2003:389) privind comunicațiile electronice, denumită în continuare „LEK”] și förordningen (2003:396) om elektronisk kommunikation [Regulamentul (2003:396) privind comunicațiile electronice]. Atât unul, cât și celălalt text, în versiunea aplicabilă litigiului principal, conțin norme privind păstrarea datelor referitoare la comunicațiile electronice, precum și la accesul autorităților naționale la aceste date.

16 Accesul la respectivele date este, în plus, reglementat de lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet [Legea (2012:278) privind colectarea datelor referitoare la comunicațiile electronice în activitățile de investigare desfășurate de autoritățile represive, denumită în continuare „Legea 2012:278”], precum și de rättegångsbalken (Codul de procedură judiciară, denumit în continuare „RB”).

Cu privire la obligația de păstrare a datelor referitoare la comunicațiile electronice

17 Potrivit indicațiilor instanței de trimitere în cauza C-203/15, dispozițiile articolului 16a din capitolul 6 din LEK coroborate cu articolul 1 din capitolul 2 din această lege prevăd o obligație pentru furnizorii de servicii de comunicații electronice de a păstra datele a căror păstrare era prevăzută de Directiva 2006/24. Este vorba despre datele referitoare la abonamentele și la toate comunicațiile electronice necesare pentru a detecta și a identifica sursa și destinația unei comunicații, pentru a stabili data, ora, durata și tipul acesteia, pentru a identifica echipamentele de comunicații utilizate, precum și pentru a localiza echipamentele de comunicații mobile utilizate la începutul și la sfârșitul comunicației. Obligația de păstrare a datelor vizează datele generate sau prelucrate în cadrul unui serviciu de telefonie, al unui serviciu de telefonie care utilizează o conexiune mobilă, al unui sistem de mesagerie electronică, al unui serviciu de acces la internet, precum și al unui serviciu de furnizare a posibilității de acces la internet (mod de conectare). Această obligație include și datele referitoare la comunicațiile nereușite. Aceasta nu privește însă conținutul comunicațiilor.

18 Articolele 38-43 din Regulamentul (2003:396) privind comunicațiile electronice precizează categoriile de date care trebuie păstrate. În ceea ce privește serviciile de telefonie, trebuie păstrate în special datele privind apelurile și numerele apelate, precum și datele și orele urmărite de început și de sfârșit ale comunicației. În ceea ce privește serviciile de telefonie care utilizează o conexiune mobilă, sunt impuse obligații suplimentare precum, de exemplu, păstrarea datelor de localizare privind începutul și sfârșitul comunicației. În ceea ce privește serviciile de telefonie care utilizează un pachet IP, pe lângă datele menționate mai sus, trebuie păstrate în special datele referitoare la adresele IP ale apelantului și ale apelatului. În ceea ce privește sistemele de mesagerie electronică, trebuie păstrate în special datele referitoare la numele emitenților și ale destinatarilor, adresele IP sau orice altă adresă de mesagerie. În ceea ce privește serviciile de acces la internet, trebuie păstrate, de exemplu, datele referitoare la adresele IP ale utilizatorilor, precum și datele și orele urmărite de conectare și de deconectare de la serviciul de acces la internet.

Cu privire la durata de păstrare a datelor

19 Conform articolului 16 d din capitolul 6 din LEK, datele la care se face referire la articolul 16 a din acest capitol trebuie să fie păstrate de furnizorii serviciilor de comunicații electronice pentru o perioadă de șase luni, calculată de la data finalizării comunicării. Acestea trebuie apoi să fie șterse imediat, cu excepția cazului în care articolul 16 d al doilea paragraf din capitolul 6 din LEK prevede altfel.

Cu privire la accesul la datele păstrate

20 Accesul la datele păstrate de autoritățile naționale este reglementat de dispozițiile Legii 2012:278, ale LEK și ale RB.

– Legea 2012:278

21 În cadrul activităților de informare, poliția națională, Säkerhetspolisen (poliția însărcinată cu securitatea, Suedia) și Tullverket (Administrația Vamală, Suedia) pot, în temeiul articolului 1 din Legea 2012:278, în condițiile prevăzute de această lege și fără știrea furnizorului unei rețele electronice de comunicații sau al unui serviciu de comunicații electronice autorizat în temeiul LEK, să colecteze date referitoare la mesajele transmise într-o rețea de comunicații electronice, la echipamentele de comunicații electronice prezente într-o anumită zonă geografică, precum și la zona sau zonele geografice în care se situează sau se situa un echipament de comunicare electronică.

22 Conform articolelor 2 și 3 din Legea 2012:278, datele pot fi colectate, în principiu, dacă împrejurările sunt de așa natură încât măsura prezintă o importanță deosebită pentru prevenirea, evitarea sau detectarea unor fapte penale care includ una sau mai multe infracțiuni pentru care pedeapsa este de cel puțin doi ani de închisoare sau una dintre faptele enumerate la articolul 3 din legea menționată care includ infracțiunile sancționate cu o pedeapsă cu închisoarea mai mică de doi ani. Motivele care impun această măsură trebuie să prevaleze asupra considerațiilor privind atingerea sau prejudiciul pe care aceasta le implică pentru cel care face obiectul ei sau pentru un interes care i se opune. Conform articolului 5 din Legea 2012:278, durata măsurii nu poate depăși o lună.

23 Decizia de a lua o astfel de măsură revine șefului autorității relevante sau oricărei persoane delegate în acest scop. Aceasta nu este supusă controlului prealabil al unei autorități judiciare sau al unei autorități administrative independente.

24 În temeiul articolului 6 din Legea 2012:278, Säkerhets och integritetsskyddsnämnden (Comisia pentru Securitate și Protecția Integrității, Suedia) trebuie să fie informată despre orice decizie privind colectarea de date. Conform articolului 1 din lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet [Legea (2007:980) privind supravegherea anumitor activități represive], această autoritate supraveghează aplicarea legii de către autoritățile cărora le revine această responsabilitate.

– LEK

25 În temeiul articolului 22 primul paragraf punctul 2 din capitolul 6 din LEK, orice furnizor de servicii de comunicații electronice trebuie să comunice datele referitoare la un abonament la cererea organului de urmărire penală, a poliției naționale, a poliției însărcinate cu securitatea sau a oricărei alte autorități căreia îi revine responsabilitatea combaterii criminalității, dacă aceste date au legătură cu o suspiciune privind o infracțiune. Potrivit indicațiilor instanței de trimitere în cauza C-203/15, nu este necesar să fie vorba despre o infracțiune gravă.

– RB

26 RB reglementează comunicarea datelor păstrate către autoritățile naționale în cadrul unor anchete preliminare. Conform articolului 19 din capitolul 27 din RB, „monitorizarea comunicațiilor electronice” fără știrea unui terț este în principiu autorizată în cadrul unor anchete preliminare care privesc, printre altele, infracțiuni sancționate cu o pedeapsă cu închisoarea de minim șase luni. Prin „monitorizarea comunicațiilor electronice” trebuie să se înțeleagă, conform articolului 19 din capitolul 27 din RB, obținerea de date fără știrea unui terț în ceea ce privește un mesaj transmis printr-o rețea de comunicare electronică, echipamentele de comunicare electronică prezente sau care au fost prezente într-o anumită zonă geografică, precum și zona sau zonele geografice în care un anumit echipament de comunicare electronică este sau a fost prezent.

27 Potrivit indicațiilor instanței de trimitere în cauza C-203/15, informații cu privire la conținutul unui mesaj nu pot fi obținute pe baza articolului 19 din capitolul 27 din RB. În principiu, monitorizarea comunicațiilor electronice poate fi dispusă, în temeiul articolului 20 din capitolul 27 din RB, numai în prezența unor indicii plauzibile care permit să se suspecteze că o persoană este autorul unei infracțiuni și că

măsura prezintă o importanță deosebită pentru necesitățile anchetei, aceasta din urmă trebuind să vizeze în plus o infracțiune sancționată cu pedeapsa închisorii de până la doi ani sau tentativa, pregătirea sau asocierea în vederea comiterii unei asemenea infracțiuni. Conform articolului 21 din capitolul 27 din RB, parchetul trebuie, cu excepția unor cazuri de urgență, să solicite instanței competente autorizația de a proceda la monitorizarea comunicațiilor electronice.

Cu privire la securitatea și protecția datelor păstrate

28 Potrivit articolului 3 a din capitolul 6 din LEK, furnizorii de servicii de comunicații electronice care au obligația de a păstra datele trebuie să ia măsurile tehnice și organizatorice adecvate pentru a asigura protejarea datelor cu ocazia prelucrării acestora. Potrivit indicațiilor instanței de trimitere în cauza C-203/15, dreptul suedez nu prevede însă dispoziții cu privire la locul păstrării datelor.

Dreptul Regatului Unit

DRIPA

29 Articolul 1 din DRIPA, intitulat „Competențe privind păstrarea datelor relevante referitoare la comunicațiile care fac obiectul garanțiilor", prevede:

„(1) [Ministrul de interne] poate, printr-un act (denumit în continuare „act de păstrare") să solicite unui operator de telecomunicații publice să păstreze date relevante privind comunicațiile în cazul în care consideră că solicitarea este necesară și proporțională în raport cu unul sau mai multe dintre scopurile prevăzute la articolul 22 alineatul (2) literele (a)-(h) din Regulation of Investigatory Powers Act 2000 [Legea din 2000 de reglementare a competențelor de investigare] (scopuri pentru care pot fi obținute datele privind comunicațiile).

(2) Un act de păstrare poate:

(a) să privească un anumit operator sau orice categorie de operatori,

(b) să impună păstrarea tuturor datelor sau a oricărei categorii de date,

(c) să specifice perioada sau perioadele pentru care urmează să fie păstrate datele,

(d) să conțină cerințe sau restricții suplimentare în legătură cu păstrarea datelor,

(e) să prevadă diverse dispoziții în scopuri diverse,

(f) să vizeze date care există sau care nu există la momentul emiterii sau al intrării în vigoare a actului.

(3) [Ministrul de interne] poate, prin regulament, să prevadă dispoziții suplimentare referitoare la păstrarea datelor relevante privind comunicațiile.

(4) Aceste dispoziții pot să includă în special prevederi referitoare la:

(a) cerințele anterioare adoptării actului de păstrare,

(b) perioada maximă pentru care urmează să fie păstreze datele în temeiul unui act de păstrare,

(c) conținutul, adoptarea, intrarea în vigoare, examinarea, modificarea sau revocarea unui act de păstrare,

(d) integritatea, securitatea sau protecția, accesarea sau divulgarea ori distrugerea datelor păstrate în temeiul prezentului articol,

(e) aplicarea cerințelor sau restricțiilor relevante ori controlul respectării acestora,

(f) un ghid de practici referitoare la cerințele sau restricțiile relevante sau la competențele relevante,

(g) rambursarea de către [ministrul de interne] (cu sau fără stabilirea unor condiții) a cheltuielilor suportate de operatorii de telecomunicații publice, efectuate ca urmare a respectării cerințelor sau restricțiilor relevante,

(h) încetarea efectelor [Data Retention (EC Directive) Regulations 2009 (Regulamentului din 2009 privind păstrarea datelor în sensul Directivei CE)] și tranziția la păstrarea datelor în temeiul prezentului articol.

(5) Perioada maximă prevăzută potrivit alineatului (4) litera (b) nu trebuie să depășească 12 luni începând cu ziua care este stabilită în raport cu datele în cauză prin regulamentul vizat la alineatul (3).

[...]"

30 Articolul 2 din DRIPA definește „datele relevante privind comunicațiile" ca însemnând „date privind comunicațiile de tipul celor menționate în anexa la Regulamentul din 2009 privind păstrarea datelor în sensul Directivei CE, în măsura în care astfel de date sunt generate sau prelucrate în Regatul Unit de către operatori de telecomunicații publice în cadrul procesului de furnizare a serviciilor de telecomunicații respective".

RIPA

31 Articolul 21 din Legea din 2000 privind stabilirea competențelor de investigare (denumită în continuare „RIPA"), care figurează în capitolul II din această lege și este intitulat „Obținerea și divulgarea datelor privind comunicațiile", precizează la alineatul (4):

„În acest capitol, «datele privind comunicațiile» au oricare dintre următoarele semnificații:

(a) orice date de trafic cuprinse într-o comunicație sau anexate acesteia (fie de către expeditor, fie în alt mod) în vederea prestării oricărui serviciu poștal sau al funcționării oricărui sistem de telecomunicații prin intermediul căruia datele sunt transmise sau pot fi transmise;

(b) orice informații care nu includ nimic din conținutul unei comunicații [cu excepția oricăror informații care intră sub incidența 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, a oricărei părți a unui sistem de telecomunicații;

(c) orice informații, care nu intră sub incidența literelor (a) sau (b), care sunt deținute sau obținute în legătură cu persoanele beneficiare ale serviciului de către o persoană care furnizează un serviciu poștal sau de telecomunicații."

32 Potrivit indicațiilor conținute în decizia de trimitere în cauza C-698/15, aceste date includ „datele de localizare a unui utilizator", dar nu și pe cele privind conținutul unei comunicații.

33 În ceea ce privește accesul la datele păstrate, articolul 22 din RIPA prevede:

„(1) Acest articol se aplică în cazul în care persoana responsabilă în temeiul acestui capitol consideră că, pentru motivele prevăzute la alineatul (2) al prezentului articol, este necesar să obțină orice dată de comunicare.

(2) Pentru motive care intră sub incidența prezentului alineat este necesar să se obțină date cu privire la comunicări dacă ele sunt necesare:

(a) în interesul siguranței naționale;

(b) în vederea prevenirii sau detectării infracțiunilor sau în vederea prevenirii tulburărilor ordinii publice;

(c) în interesul bunăstării economice din Regatul Unit:

(d) în interesul securității publice;

(e) în vederea protecției sănătății publice:

(f) în vederea evaluării sau colectării oricăror impozite, taxe, cotizații sau a altor impuneri, contribuții sau taxe datorate administrației publice;

(g) în vederea prevenirii, în caz de urgență, a morții sau rănirii sau a oricăror prejudicii aduse sănătății fizice sau mentale a unei persoane sau în vederea diminuării oricăror daune sau prejudicii aduse sănătății fizice sau mentale a unei persoane;

(h) în orice alt scop [care nu intră sub incidența literelor (a)-(g)] precizat într-o somație emisă de [ministrul de interne].

(4) Sub rezerva alineatului (5), persoana responsabilă poate, atunci când apreciază că un operator de telecomunicații sau un operator poștal se află sau s-ar putea afla în posesia unor date ori ar putea fi capabil să obțină date, să solicite printr-o cerere operatorului de telecomunicații sau operatorului poștal ca acest operator:

(a) să obțină datele, dacă nu le deține deja, și

(b) să divulge, în orice situație, toate datele care se află în posesia sa sau pe care le-a obținut ulterior.

(5) Persoana responsabilă nu trebuie să acorde o autorizație în conformitate cu alineatul (3) sau să facă o cerere în temeiul alineatului (4), cu excepția cazului în care apreciază că obținerea datelor în discuție care rezultă dintr-un comportament autorizat sau impus în temeiul unei autorizații sau al unei cereri este proporțională cu scopul urmărit prin obținerea datelor.”

34 Conform articolului 65 din RIPA, se pot formula plângeri la Investigatory Powers Tribunal (Tribunalul pentru Litigii referitoare la Competențele de Investigare, Regatul Unit) dacă există motive pentru a considera că datele au fost colectate în mod necorespunzător.

Data Retention Regulations 2014

35 Data Retention Regulations 2014 (Regulamentul din 2014 privind păstrarea datelor), adoptat în temeiul DRIPA, este împărțit în trei părți, a doua dintre ele incluzând articolele 2-14 din acest regulament. Articolul 4, intitulat „Cereri în materie de păstrare”, prevede:

„(1) Cererile în materie de păstrare trebuie să precizeze:

(a) operatorul public de telecomunicații (sau descrierea operatorilor) căruia i se adresează,

(b) datele privind comunicațiile pertinente care trebuie păstrate,

(c) perioada sau perioadele pentru care urmează să fie păstrate datele,

(d) orice altă cerință sau restricție în legătură cu păstrarea datelor.

(2) Printr-o cerere în materie de păstrare nu se poate solicita ca o dată să fie păstrată mai mult de 12 luni începând cu:

(a) în cazul datelor de transfer sau al datelor privind utilizarea serviciului, ziua comunicației în cauză și

(b) în cazul datelor referitoare la abonați, ziua în care persoana în cauză încheie serviciul de comunicații în cauză sau ziua în care datele sunt modificate (dacă aceasta este anterioară)

[...]”

36 Potrivit articolului 7 din acest regulament, intitulat „Integritatea și securitatea datelor”:

„(1) Un operator public de telecomunicații care păstrează date în temeiul articolului 1 din [DRIPA] trebuie:

(a) să se asigure că datele beneficiază de aceeași integritate și de cel puțin același nivel de securitate și de protecție precum datele din sistemele din care provin;

(b) să se asigure, prin măsuri tehnice și organizatorice adecvate, că numai personalul special autorizat poate avea acces la date și

(c) să protejeze datele, prin măsuri tehnice și organizatorice adecvate, împotriva distrugerii ilicite, a pierderilor sau a deteriorărilor cu caracter accidental ori împotriva păstrării, a prelucrării, a accesului sau a divulgărilor ilicite ori neautorizate.

(2) Un operator public de telecomunicații care păstrează date privind comunicațiile în temeiul articolului 1 din [DRIPA] trebuie să distrugă datele dacă păstrarea datelor nu mai este autorizată de acest articol și nu este autorizată în alt mod prin lege.

(3) Cerința prevăzută la alineatul (2) de a distruge datele este o cerință care constă în ștergerea datelor astfel încât accesul la aceste date să devină imposibil.

(4) Este suficient ca operatorul să adopte dispoziții pentru ca ștergerea datelor să intervină lunar sau la intervale mai scurte potrivit posibilităților practice ale operatorului.”

37 Articolul 8 din regulamentul menționat, intitulat „Divulgarea datelor păstrate”, prevede:

„(1) Un operator public de telecomunicații trebuie să instituie sisteme de securitate adecvate (care includ măsuri tehnice și organizatorice) care să determine accesul la datele privind comunicațiile păstrate în temeiul articolului 1 din [DRIPA] pentru a preveni orice divulgare care nu intră sub incidența articolului 1 alineatul (6) litera (a) din [DRIPA].

(2) Un operator public de telecomunicații care păstrează date în temeiul articolului 1 din [DRIPA] trebuie să păstreze datele astfel încât să le poată transmite, fără vreo întârziere nejustificată, ca răspuns la cereri."

38 Articolul 9 din același regulament, intitulat „Controlul comisarului pentru informații", prevede:

„Comisarul pentru informații trebuie să controleze respectarea cerințelor sau a restricțiilor prevăzute în această parte, în legătură cu integritatea, securitatea și distrugerea datelor păstrate în temeiul articolului 1 din [DRIPA]."

Codul de practici

39 Acquisition and Disclosure of Communications Data Code of Practice (Codul de bune practici privind colectarea și divulgarea datelor privind comunicațiile, denumit în continuare „codul de practici") conține, la punctele 2.5-2.9 și 2.36-2.45, orientări cu privire la necesitatea și la proporționalitatea obținerii datelor privind comunicații. Potrivit explicațiilor instanței de trimitere în cauza C-698/15, trebuie să se acorde, în conformitate cu punctele 3.72-3.77 din acest cod, o atenție deosebită necesității și proporționalității în cazul în care datele solicitate privind comunicațiile se raportează la o persoană care este membru al unei profesii care beneficiază de informații protejate prin secretul profesional sau confidențiale în alt mod.

40 În temeiul punctelor 3.78-3.84 din codul menționat, o ordonanță judecătorească este necesară în cazul specific al unei cereri de obținere de date privind comunicațiile care este formulată în scopul de a identifica sursa folosită de un jurnalist. Potrivit punctelor 3.85-3.87 din același cod, se impune o aprobare judecătorească în cazul unei cereri de acces formulate de autoritățile locale. Nicio autorizație judiciară sau emisă de o entitate independentă nu este, în schimb, necesară pentru a accesa datele privind comunicațiile protejate de un secret profesional legal sau datele referitoare la medici, la membri ai Parlamentului sau la preoți.

41 Punctul 7.1 din codul de practici prevede că datele privind comunicațiile dobândite sau obținute în temeiul dispozițiilor din RIPA, precum și toate extrasele, sintezele și copiile acestora trebuie să fie prelucrate și păstrate în siguranță. În plus, trebuie respectate cerințele care figurează în Data Protection Act (Legea privind protecția datelor).

42 În conformitate cu punctul 7.18 din codul de practici, în cazul în care o autoritate publică din Regatul Unit are în vedere posibila divulgare către autorități străine a unor date privind comunicațiile, aceasta trebuie printre altele să examineze dacă respectivele date vor fi protejate în mod adecvat. Din cuprinsul punctului 7.22 din acest cod reiese însă că un transfer al datelor către țări terțe poate avea loc atunci când acest transfer este necesar din motive legate de un interes public important, chiar și atunci când țara terță nu asigură un nivel de protecție adecvat. Potrivit indicațiilor instanței de trimitere în cauza C-698/15, ministrul de interne poate emite un certificat de securitate națională care scutește anumite date de la respectarea dispozițiilor prevăzute de legislație.

43 La punctul 8.1 din codul menționat se amintește că RIPA a instituit Interception of Communications Commissioner (comisarul pentru interceptarea comunicațiilor, Regatul Unit), al cărui rol este, printre altele, de a supraveghea în mod independent exercitarea și punerea în aplicare a competențelor și a obligațiilor prevăzute în capitolul II din partea I din RIPA. Astfel cum reiese din cuprinsul punctului 8.3 din același cod, acest comisar este autorizat, atunci când poate „dovedi că un individ a fost lezat printr-o încălcare

intenționată sau prin imprudență”, să îl informeze pe acest individ că este suspectat de o utilizare nelegală a competențelor.

Litigiile principale și întrebările preliminare

Cauza C-203/15

44 La 9 aprilie 2014, Tele2 Sverige, furnizor de servicii de comunicații electronice cu sediul în Suedia, a notificat PTS că, în urma invalidării Directivei 2006/24 prin Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții (C-293/12 și C-594/12, denumită în continuare „Hotărârea Digital Rights”, EU:C:2014:238), aceasta va înceta, începând cu 14 aprilie 2014, să păstreze datele privind comunicațiile electronice, vizate de LEK, și că va proceda la ștergerea datelor păstrate până la acea dată.

45 La 15 aprilie 2014, Rikspolisstyrelsen (Direcția Generală a Poliției Naționale, Suedia) a sesizat PTS cu o plângere pentru faptul că Tele2 Sverige încetase să îi comunice datele în cauză.

46 La 29 aprilie 2014, justitieminister (ministrul justiției, Suedia) a desemnat un raportor special care să analizeze reglementarea suedeză în cauză în lumina Hotărârii Digital Rights. În raportul din 13 iunie 2014, intitulat „Datalagring, EU-rätt och svensk rätten, n° Ds 2014:23” (Păstrarea datelor, dreptul Uniunii și dreptul suedez, denumit în continuare „raportul din 2014”), raportorul special a concluzionat că reglementarea națională privind păstrarea datelor, astfel cum este prevăzută la articolele 16 a-16 f din LEK, nu este contrară nici dreptului Uniunii, nici Convenției europene pentru apărarea drepturilor omului și a libertăților fundamentale, semnată la Roma la 4 noiembrie 1950 (denumită în continuare „CEDO”). Raportorul special a subliniat că Hotărârea Digital Rights nu poate fi interpretată în sensul că ar fi cenzurat principiul însuși al unei păstrări generalizate și nediferențiate a datelor. Din punctul său de vedere, Hotărârea Digital Rights nu trebuie interpretată nici în sensul că Curtea ar fi stabilit în aceasta o serie de criterii care trebuiau să fie îndeplinite toate pentru ca o reglementare să poată fi considerată proporțională. Pentru a stabili conformitatea reglementării suedeze cu dreptul Uniunii ar trebui să fie apreciate toate împrejurările, precum amploarea păstrării datelor în lumina dispozițiilor privind accesul la date, durata păstrării lor, protecția lor, precum și securitatea acestora.

47 Pe acest temei, PTS a informat societatea Tele2 Sverige, la 19 iunie 2014, că aceasta nu își îndeplinește obligațiile prevăzute de reglementarea națională prin faptul că nu păstrează datele vizate de LEK timp de șase luni în vederea combaterii infracționalității. Prin somația din 27 iunie 2014, PTS i-a dispus ulterior să procedeze, cel târziu la 25 iulie 2014, la păstrarea acelor date.

48 Întrucât a considerat că raportul din 2014 se întemeiază pe o interpretare eronată a Hotărârii Digital Rights și că obligația de păstrare a datelor este contrară drepturilor fundamentale garantate de cartă, Tele2 Sverige a introdus o acțiune la Förvaltningsrätten i Stockholm (Tribunalul Administrativ din Stockholm, Suedia) împotriva somației din 27 iunie 2014. Dat fiind că această instanță a respins acțiunea prin hotărârea din 13 octombrie 2014, Tele2 Sverige a declarat apel împotriva acestei hotărâri la instanța de trimitere.

49 Potrivit instanței de trimitere, compatibilitatea reglementării suedeze cu dreptul Uniunii trebuie apreciată în lumina articolului 15 alineatul (1) din Directiva 2002/58. Astfel, în condițiile în care această directivă ar prevedea principiul potrivit căruia datele de transfer și datele de localizare trebuie să fie șterse sau anonimizate atunci când nu mai sunt necesare pentru transmiterea unei comunicații, articolul 15 alineatul (1) din directiva menționată ar introduce o derogare de la acest principiu întrucât ar permite statelor membre, atunci când acest lucru este justificat de unul dintre motivele pe care le prevede, să limiteze această obligație de ștergere sau de anonimizare ori chiar să prevadă păstrarea unor date. Astfel, dreptul Uniunii ar permite, în anumite situații, păstrarea datelor privind comunicațiile electronice.

50 Instanța de trimitere se întreabă totuși dacă o obligație generalizată și nediferențiată de păstrare a datelor privind comunicațiile electronice, precum cea în discuție în litigiul principal, este compatibilă, ținând seama de Hotărârea Digital Rights, cu articolul 15 alineatul (1) din Directiva 2002/58, interpretat în

lumina articolelor 7 și 8, precum și a articolului 52 alineatul (1) din cartă. Având în vedere părerile divergente ale părților în această privință, Curtea ar trebui să se pronunțe în mod univoc cu privire la aspectul dacă, astfel cum consideră Tele2 Sverige, păstrarea generalizată și nediferențiată a datelor privind comunicațiile electronice este prin ea însăși incompatibilă cu articolele 7 și 8, precum și cu articolul 52 alineatul (1) din cartă, sau dacă, astfel cum ar reieși din raportul din 2014, compatibilitatea unei asemenea păstrări de date trebuie apreciată în lumina dispozițiilor privind accesul la date, protecția și securitatea lor, precum și durata păstrării lor.

51 În aceste condiții instanța de trimitere a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„1) O obligație generală de păstrare a datelor de transfer care include toate persoanele, toate mijloacele de comunicații electronice și toate datele de transfer fără niciun fel de distincții, limitări sau excepții, în vederea combaterii criminalității […], este compatibilă cu articolul 15 alineatul (1) din Directiva 2002/58, ținând seama de articolele 7 și 8, precum și de articolul 52 alineatul (1) din cartă?

2) În cazul unui răspuns negativ la prima întrebare, se poate permite totuși păstrarea atunci când:

a) modul de acces al autorităților naționale la datele păstrate este stabilit astfel cum se arată la punctele 19-36 [din cererea de decizie preliminară] și

b) cerințele de securitate sunt reglementate astfel cum se arată la punctele 38-43 [din cererea de decizie preliminară] și

c) toate datele relevante trebuie să fie păstrate pentru o perioadă de șase luni, calculată de la data la care s-a terminat comunicația, iar ulterior să fie șterse astfel cum se arată la punctul 37 [din cererea de decizie preliminară]?”

Cauza C-698/15

52 Domnii Watson, Brice și Lewis au formulat fiecare, la High Court of Justice (England & Wales), Queens’ Bench Division (Divisional Court) [Înalta Curte de Justiție (Anglia și Țara Galilor), secția Queens’ Bench (camera de apel), Regatul Unit], o acțiune având ca obiect controlul legalității articolului 1 din DRIPA, invocând în special incompatibilitatea acestui articol cu articolele 7 și 8 din cartă, precum și cu articolul 8 din CEDO.

53 Prin Hotărârea din 17 iulie 2015, High Court of Justice (England & Wales), Queens’ Bench Division (Divisional Court) [Înalta Curte de Justiție (Anglia și Țara Galilor), secția Queens’ Bench (camera de apel)] a constatat că Hotărârea Digital Rights stabilește „cerințe imperative ale dreptului Uniunii” aplicabile reglementărilor statelor membre în materie de păstrare a datelor privind comunicațiile, precum și accesului la astfel de date. Potrivit instanței menționate, întrucât Curtea a considerat, în această hotărâre, că Directiva 2006/24 este incompatibilă cu principiul proporționalității, nici o reglementare națională cu un conținut identic cu cel al acestei directive nu ar putea fi compatibilă cu acest principiu. Din logica ce stă la baza Hotărârii Digital Rightsar reieși că o legislație care instituie un regim generalizat de păstrare a datelor privind comunicații încalcă drepturile garantate la articolele 7 și 8 din cartă, cu excepția cazului în care această legislație este completată de un regim privind accesul la date, definit de dreptul național, care prevede garanții suficiente pentru protecția acestor drepturi. Astfel, articolul 1 din DRIPA nu ar fi compatibil cu articolele 7 și 8 din cartă întrucât nu ar institui norme clare și precise cu privire la acces și la utilizarea datelor păstrate și nu ar condiționa accesul la aceste date de un control prealabil efectuat de o instanță sau de o entitate administrativă independentă.

54 Ministrul de interne a atacat cu apel această hotărâre la Court of Appeal (England & Wales) (Civil Division) [Curtea de Apel (Anglia și Țara Galilor) (secția civilă), Regatul Unit].

55 Această instanță arată că articolul 1 alineatul (1) din DRIPA îl abilitează pe ministrul de interne să adopte, în lipsa oricărei autorizații prealabile a unei instanțe sau a unei entități administrative independente, un regim general care să impună operatorilor de telecomunicații publice să păstreze toate datele care privesc orice serviciu poștal sau orice serviciu de telecomunicații pe o durată maximă de 12 luni în măsura în care apreciază că o astfel de cerință este necesară și proporțională pentru a atinge scopurile prevăzute de reglementarea din Regatul Unit. Chiar dacă aceste date nu cuprind conținutul unei comunicații, ele ar putea avea un caracter deosebit de intruziv în viața privată a utilizatorilor de servicii de telecomunicații.

56 În decizia de trimitere și în hotărârea din 20 noiembrie 2015, pronunțată în cadrul procedurii de apel și prin care instanța de trimitere a decis să adreseze Curții prezenta cerere de decizie preliminară, aceasta consideră că normele naționale privind păstrarea datelor intră în mod necesar sub incidența articolului 15 alineatul (1) din Directiva 2002/58 și trebuie, așadar, să respecte cerințele care decurg din cartă. Cu toate acestea, conform articolului 1 alineatul (3) din directiva menționată, legiuitorul Uniunii nu ar fi armonizat normele privind accesul la datele păstrate.

57 În ceea ce privește incidența Hotărârii Digital Rights asupra problemelor ridicate în litigiul principal, instanța de trimitere arată că, în cauza care a determinat pronunțarea acestei hotărâri, Curtea fusese sesizată cu privire la validitatea Directivei 2006/24, iar nu cu privire la cea a reglementării naționale. Având în vedere în special raportul strâns care există între păstrarea datelor și accesul la respectivele date, ar fi fost indispensabil ca această directivă să fie însoțită de o serie de garanții și ca Hotărârea Digital Rights să analizeze, cu ocazia examinării legalității regimului de păstrare a datelor prevăzut de directiva menționată, normele privind accesul la aceste date. Prin urmare, Curtea nu ar fi urmărit să stabilească, în această hotărâre, cerințe imperative care să se aplice reglementărilor naționale privind accesul la datele care nu pun în aplicare dreptul Uniunii. În plus, raționamentul Curții ar fi fost strâns legat de obiectivul urmărit de aceeași directivă. Cu toate acestea, o reglementarea națională ar trebui apreciată în lumina obiectivelor urmărite de aceasta și a contextului său.

58 În ceea ce privește necesitatea de a sesiza Curtea cu o trimitere preliminară, instanța de trimitere scoate în evidență faptul că, la data adoptării deciziei de trimitere, șase instanțe din alte state membre, dintre care cinci de ultim grad de jurisdicție, anulaseră legislații naționale întemeindu-se pe Hotărârea Digital Rights. Răspunsul la întrebările ridicate nu ar fi, așadar, evident, în condițiile în care acesta ar fi necesar pentru judecarea cauzelor cu care respectiva instanță este sesizată.

59 În aceste condiții, Court of Appeal (England & Wales) (Civil Division) [Curtea de Apel (Anglia și Țara Galilor) (Secția civilă)] a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„1) Hotărârea Digital Rights (inclusiv în special punctele 60-62 din aceasta) stabilește cerințe imperative ale dreptului Uniunii aplicabile regimului național al unui stat membru care reglementează accesul la datele păstrate în conformitate cu legislația națională, în vederea respectării articolelor 7 și 8 din cartă?

2) Hotărârea Digital Rights extinde domeniul de aplicare al articolelor 7 și/sau 8 din cartă dincolo de cel al articolului 8 din CEDO, astfel cum este stabilit în jurisprudența Curții Europene a Drepturilor Omului?”

Cu privire la procedura în fața Curții

60 Prin Ordonanța din 1februarie 2016, Davis și alții (C-698/15, nepublicată, EU:C:2016:70), președintele Curții a decis să admită cererea Court of Appeal (England & Wales) (Civil Division) [Curtea de Apel (Anglia și Țara Galilor) (Secția civilă)] prin care s-a solicitat judecarea cauzei C-698/15 potrivit procedurii accelerate prevăzute la articolul 105 alineatul (1) din Regulamentul de procedură al Curții.

61 Prin decizia președintelui Curții din 10 martie 2016, cauzele C-203/15 și C-698/15 au fost conexate pentru buna desfășurare a procedurii orale și în vederea pronunțării hotărârii.

Cu privire la întrebările preliminare

Cu privire la prima întrebare în cauza C-203/15

62 Prin intermediul primei întrebări în cauza C-203/15, Kammarrätten i Stockholm (Curtea de Apel Administrativă din Stockholm) solicită, în esență, să se stabilească dacă articolul 15 alineatul (1) din Directiva 2002/58, lecturat în lumina articolelor 7 și 8, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că se opune unei reglementări naționale precum cea în discuție în litigiul principal care prevede, în scopul combaterii infracționalității, o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare a tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică.

63 Această întrebare își are originea în special în faptul că Directiva 2006/24, pe care reglementarea națională în discuție în litigiul principal a transpus-o, a fost declarată invalidă prin Hotărârea Digital Rights, dar părțile nu sunt de acord în ceea ce privește sfera de aplicare a acestei hotărâri și incidența sa asupra respectivei reglementări, care guvernează păstrarea datelor de transfer și a datelor de localizare, precum și accesul autorităților naționale la aceste date.

64 Trebuie să se analizeze în prealabil dacă o reglementare națională precum cea în discuție în litigiul principal intră în domeniul de aplicare al dreptului Uniunii.

Cu privire la domeniul de aplicare al Directivei 2002/58

65 Statele membre care au prezentat observații scrise Curții au exprimat păreri divergente în ceea ce privește aspectul dacă și în ce măsură reglementările naționale privind păstrarea datelor de transfer și a datelor de localizare, precum și accesul autorităților naționale la aceste date, în scopul combaterii infracționalității, intră în domeniul de aplicare al Directivei 2002/58. Astfel, în timp ce, printre altele, guvernele belgian, danez, german, estonian și Irlanda, precum și guvernul neerlandez au exprimat opinia că se impune un răspuns afirmativ la o astfel de întrebare, guvernul ceh a propus să se răspundă în sens negativ la întrebarea menționată, remarcând că aceste reglementări au ca obiectiv unic combaterea infracționalității. În ceea ce privește guvernul Regatului Unit, acesta arată că intră în domeniul de aplicare al directivei amintite numai reglementările privind păstrarea datelor, iar nu și cele privind accesul autorităților naționale competente în materie de represiune la aceste date.

66 În ceea ce privește, în sfârșit, Comisia, deși aceasta a susținut, în observațiile scrise prezentate Curții în cauza C-203/15, că reglementarea națională în discuție în litigiul principal intră în domeniul de aplicare al Directivei 2002/58, ea a arătat, în observațiile scrise în cauza C-698/15, că numai normele naționale privind păstrarea datelor, iar nu și cele privind accesul autorităților naționale la aceste date intră în domeniul de aplicare al directivei menționate. Aceste din urmă norme ar trebui totuși, în opinia sa, să fie luate în considerare pentru a evalua dacă o reglementare națională care guvernează păstrarea datelor de către furnizorii de servicii de comunicații electronice constituie o ingerință proporțională în drepturile fundamentale garantate la articolele 7 și 8 din cartă.

67 În această privință, trebuie să se arate că întinderea domeniului de aplicare al Directivei 2002/58 trebuie apreciată ținând seama în special de economia generală a acesteia din urmă.

68 Potrivit articolului 1 alineatul (1) din Directiva 2002/58, aceasta 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.

69 Articolul 1 alineatul (3) din această directivă exclude din domeniul de aplicare al acesteia „activitățile statului” în domeniile care sunt vizate la acest alineat, și anume în special 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 [a se vedea prin analogie, în ceea ce privește articolul 3 alineatul (2) prima liniuță din Directiva 95/46, Hotărârea din 6 noiembrie 2003, Lindqvist, C-101/01, EU:C:2003:596, punctul 43, precum și Hotărârea din 16 decembrie 2008, Satakunnan Markkinapörssi și Satamedia, C-73/07, EU:C:2008:727, punctul 41].

70 În ceea ce privește articolul 3 din Directiva 2002/58, acesta 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.

71 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". Articolul 15 alineatul (1) a doua teză din directiva menționată identifică, ca exemplu de măsuri care pot fi adoptate astfel de statele membre, măsuri „care să permită reținerea de date".

72 Desigur, măsurile legislative prevăzute la articolul 15 alineatul (1) din Directiva 2002/58 se raportează la activități proprii statelor sau autorităților statale, străine de domeniile de activitate ale particularilor (a se vedea în acest sens Hotărârea din 29 ianuarie 2008, Promusicae, C-275/06, EU:C:2008:54, punctul 51). În plus, finalitățile la care trebuie să răspundă, în temeiul acestei dispoziții, asemenea măsuri, în speță protecția securității naționale, a apărării și a siguranței publice, precum și punerea în aplicare a prevenirii, a investigării, a detectării și a urmăririi penale a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice, se pliază în esență pe finalitățile urmărite de activitățile menționate la articolul 1 alineatul (3) din această directivă.

73 Cu toate acestea, având în vedere economia generală a Directivei 2002/58, elementele menționate la punctul anterior din prezenta hotărâre nu permit să se concluzioneze că măsurile legislative prevăzute la articolul 15 alineatul (1) din Directiva 2002/58 ar fi excluse din domeniul de aplicare al acestei directive, în caz contrar această dispoziție fiind privată de orice efect util. Astfel, dispoziția menționată presupune în mod necesar ca măsurile naționale prevăzute la acest articol, precum cele privind păstrarea unor date în scopul combaterii infracționalității, intră în domeniul de aplicare al aceleiași directive, din moment ce aceasta din urmă permite în mod expres statelor membre să le adopte numai cu respectarea condițiilor pe care le prevede.

74 În plus, măsurile legislative care sunt prevăzute la articolul 15 alineatul (1) din Directiva 2002/58 guvernează, în scopurile menționate la această dispoziție, activitatea furnizorilor de servicii de comunicații electronice. Prin urmare, acest articol 15 alineatul (1) coroborat cu articolul 3 din directiva respectivă trebuie interpretat în sensul că astfel de măsuri legislative intră în domeniul de aplicare al aceleiași directive.

75 Intră în special în acest domeniu de aplicare o măsură legislativă, precum cea în discuție în litigiul principal, care impune acestor furnizori să păstreze datele de transfer și datele de localizare, întrucât o astfel de activitate implică în mod necesar o prelucrare, de către aceștia, a unor date cu caracter personal.

76 Intră de asemenea în respectivul domeniu de aplicare o măsură legislativă privind, precum în cauza principală, accesul autorităților naționale la datele păstrate de furnizorii de servicii de comunicații electronice.

77 Astfel, protecția confidențialității comunicațiilor electronice și a datelor de transfer aferente acestora, garantată la articolul 5 alineatul (1) din Directiva 2002/58, se aplică măsurilor adoptate de orice alte persoane decât utilizatorii, indiferent dacă este vorba despre persoane sau entități private ori despre entități

statale. Astfel cum se confirmă în considerentul (21) al directivei menționate, aceasta urmărește să evite „accesul” neautorizat la comunicații, inclusiv la „datel[e] referitoare la comunicații”, pentru a proteja confidențialitatea comunicațiilor electronice.

78 În aceste condiții, o măsură legislativă prin care un stat membru impune, în temeiul articolului 15 alineatul (1) din Directiva 2002/58, furnizorilor de servicii de comunicații electronice, în scopurile menționate de această dispoziție, să acorde autorităților naționale, în condițiile prevăzute de o astfel de măsură, accesul la datele păstrate de respectivii furnizori, privește prelucrări a unor date cu caracter personal de către aceștia din urmă, prelucrări care intră în domeniul de aplicare al directivei menționate.

79 În plus, din moment ce păstrarea unor date intervine numai pentru ca datele, dacă este cazul, să devină accesibile autorităților naționale competente, o reglementare națională care prevede păstrarea datelor implică, în principiu, în mod necesar existența unor dispoziții privind accesul autorităților naționale competente la datele păstrate de furnizorii unor servicii de comunicații electronice.

80 Această interpretare este confirmată de articolul 15 alineatul (1b) din Directiva 2002/58, potrivit căruia furnizorii stabilesc proceduri interne pentru a răspunde solicitărilor de accesare a datelor cu caracter personal ale utilizatorilor pe baza dispozițiilor naționale adoptate în conformitate cu articolul 15 alineatul (1) din această directivă.

81 Din considerațiile de mai sus rezultă că o reglementare națională, precum cea în discuție în litigiul principal în cauzele C-203/15 și C-698/15, intră în domeniu de aplicare al Directivei 2002/58.

Cu privire la interpretarea articolului 15 alineatul (1) din Directiva 2002/58 în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă

82 Trebuie să se arate că, potrivit articolului 1 alineatul (2) din Directiva 2002/58, dispozițiile acesteia „precizează și completează” Directiva 95/46. Astfel cum se enunță în considerentul (2) al Directivei 2002/58, aceasta urmărește să asigure în special 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 se află la originea 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”.

83 În acest scop, Directiva 2002/58 conține dispoziții specifice menite, astfel cum reiese în special din cuprinsul considerentelor (6) și (7) ale acesteia, să îi protejeze pe utilizatorii serviciilor împotriva riscurilor pentru datele lor personale și pentru confidențialitatea comunicațiilor lor care rezultă din tehnologii noi și din capacitatea în creștere de stocare automată și de prelucrare a datelor.

84 În special, articolul 5 alineatul (1) din această directivă prevede că 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 lor internă.

85 Principiul confidențialității comunicațiilor instituit de Directiva 2002/58 implică printre altele, astfel cum reiese din articolul 5 alineatul (1) a doua teză din aceasta, o interdicție pentru, în principiu, orice alte persoane decât utilizatorii de a stoca, fără acordul acestora, datele de transfer aferente comunicațiilor electronice. Sunt exceptate numai persoanele autorizate în mod legal în conformitate cu articolul 15 alineatul (1) din directivă și stocarea tehnică necesară pentru transmisia comunicației (a se vedea în acest sens Hotărârea din 29 ianuarie 2008, Promusicae, C-275/06, EU:C:2008:54, punctul 47).

86 Prin urmare, după cum se confirmă în considerentele (22) și (26) ale Directivei 2002/58, prelucrarea și stocarea datelor de transfer sunt permise, potrivit articolului 6 din această directivă, numai în măsura și pe durata de timp necesare comercializării acestora sau furnizării unor servicii suplimentare (a se vedea în acest sens Hotărârea din 29 ianuarie 2008, Promusicae, C-275/06, EU:C:2008:54, punctele 47 și 48). În ceea ce privește, în special, facturarea serviciilor, o astfel de prelucrare este permisă numai până la sfârșitul perioadei în care factura poate fi contestată în mod legal sau plata poate fi urmărită. Odată expirată această perioadă, datele care au fost prelucrate și stocate trebuie șterse sau anonimizate. În ceea ce privește datele de localizare altele decât datele de transfer, articolul 9 alineatul (1) din această directivă prevede că aceste date pot fi prelucrate numai în anumite condiții și doar dacă au fost anonimizate sau există acordul utilizatorilor sau abonaților respectivi.

87 Sfera de aplicare a dispozițiilor articolelor 5 și 6 și ale articolului 9 alineatul (1) din Directiva 2002/58, care urmăresc să asigure confidențialitatea comunicațiilor și a datelor de transfer și să minimizeze riscurile de abuz, trebuie apreciată în plus în lumina considerentului (30) al acestei directive, potrivit căruia „[s]istemele de furnizare de servicii și rețele de comunicații electronice trebuie astfel construite încât să limiteze cantitatea de date personale necesare la un minimum strict”.

88 Desigur, articolul 15 alineatul (1) din Directiva 2002/58 permite statelor membre să introducă excepții de la obligația de principiu, prevăzută la articolul 5 alineatul (1) din această directivă, de garantare a confidențialității datelor cu caracter personal, precum și de la obligațiile corespunzătoare, menționate în special la articolele 6 și 9 din directiva respectivă (a se vedea în acest sens Hotărârea din 29 ianuarie 2008, Promusicae, C-275/06, EU:C:2008:54, punctul 50).

89 Cu toate acestea, în măsura în care articolul 15 alineatul (1) din Directiva 2002/58 permite statelor membre să restrângă sfera de aplicare a obligației de principiu de a asigura confidențialitatea comunicațiilor și a datelor de transfer aferente acestora, acesta este, conform jurisprudenței constante a Curții, de strictă interpretare (a se vedea prin analogie Hotărârea din 22 noiembrie 2012, Probst, C-119/12, EU:C:2012:748, punctul 23). O asemenea dispoziție nu poate, așadar, să justifice ca derogarea de la această obligație de principiu și, în special, de la interdicția de a stoca aceste date, prevăzută la articolul 5 din directiva menționată, să devină regula, fără a vida semnificativ această din urmă dispoziție de conținutul său.

90 Trebuie să se arate în această privință că articolul 15 alineatul (1) prima teză din Directiva 2002/58 prevede că măsurile legislative pe care le vizează și care derogă de la principiul confidențialității comunicațiilor și a datelor de transfer aferente acestora trebuie să aibă obiectivul de a „proteja securitatea națională (de exemplu siguranța statului), apărarea, siguranța publică sau [de a asigura] prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice”, sau trebuie să urmărească unul dintre obiectivele vizate la articolul 13 alineatul (1) din Directiva 95/46, la care face trimitere articolul 15 alineatul (1) prima teză din Directiva 2002/58 (a se vedea în acest sens Hotărârea din 29 ianuarie 2008, Promusicae, C-275/06, EU:C:2008:54, punctul 53). O asemenea enumerare a unor obiective are caracter exhaustiv, astfel cum reiese din articolul 15 alineatul (1) a doua teză din această din urmă directivă, potrivit căruia măsurile legislative trebuie să fie justificate de „motivele arătate” la articolul 15 alineatul (1) prima teză din directiva menționată. Prin urmare, statele membre nu pot adopta astfel de măsuri în alte scopuri decât cele enumerate la această din urmă dispoziție.

91 În plus, articolul 15 alineatul (1) a treia teză din Directiva 2002/58 prevede că „[t]oate măsurile menționate [la articolul 15 alineatul (1) din această directivă] trebuie să fie conforme cu principiile generale ale legislației [Uniunii], inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) [UE]”, printre care figurează principiile generale și drepturile fundamentale care sunt în prezent garantate de cartă. Articolul 15 alineatul (1) din Directiva 2002/58 trebuie să fie interpretat, așadar, în lumina drepturilor fundamentale garantate de cartă (a se vedea prin analogie, în ceea ce privește Directiva 95/46, Hotărârea din 20 mai 2003, Österreichischer Rundfunk și alții, C-465/00, C-138/01 și C-139/01, EU:C:2003:294, punctul 68, Hotărârea din 13 mai 2014, Google Spain și Google, C-131/12, EU:C:2014:317, punctul 68, precum și Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 38).

92 În această privință, trebuie subliniat că obligația stabilită în sarcina furnizorilor de servicii de comunicații electronice, printr-o reglementare națională precum cea în discuție în litigiul principal, 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, care sunt menționate în mod expres în întrebările preliminare, ci și cu privire la respectarea libertății de exprimare garantate la articolul 11 din cartă (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctele 25 și 70).

93 Prin urmare, cu ocazia interpretării articolului 15 alineatul (1) din Directiva 2002/58 trebuie luate în considerare atât importanța dreptului la respectarea vieții private, garantat la articolul 7 din cartă, cât și cea a dreptului la protecția datelor cu caracter personal, garantat la articolul 8 din aceasta, astfel cum reiese din jurisprudența Curții (a se vedea în acest sens Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 39 și jurisprudența citată). Acest lucru este valabil și în ceea ce privește libertatea de expresie, având în vedere importanța deosebită pe care o prezintă această libertate în orice societate democratică. Acest drept fundamental, garantat la articolul 11 din cartă, constituie 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 12 iunie 2003, Schmidberger, C-112/00, EU:C:2003:333, punctul 79, și Hotărârea din 6 septembrie 2011, Patriciello, C-163/10, EU:C:2011:543, punctul 31).

94 În această privință, trebuie amintit că, potrivit articolului 52 alineatul (1) din cartă, orice restrângere a exercițiului drepturilor și libertăților consacrate prin aceasta trebuie să fie prevăzută de lege și să respecte substanța acestor drepturi. Prin respectarea principiului proporționalității, pot fi impuse restrângeri exercitării acestor drepturi și acestor libertăți numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți (Hotărârea din 15 februarie 2016, N., C-601/15 PPU, EU:C:2016:84, punctul 50).

95 În această ultimă privință, articolul 15 alineatul (1) prima teză din Directiva 2002/58 prevede că statele membre pot adopta o măsură care să deroge de la principiul confidențialității comunicațiilor și a datelor de transfer aferente acestor în cazul în care ea se dovedește „necesară, corespunzătoare și proporțională în cadrul unei societăți democratice”, în lumina obiectivelor pe care le prevede această dispoziție. În ceea ce privește considerentul (11) al directivei menționate, acesta precizează că o măsură de această natură trebuie să fie „strict” proporțională cu scopul urmărit. În ceea ce privește, în special, păstrarea unor date, articolul 15 alineatul (1) a doua teză din directiva respectivă impune ca aceasta să aibă loc numai „pe perioadă limitată” și „[atunci când se justifică]” prin unul dintre obiectivele menționate la articolul 15 alineatul (1) prima teză din aceeași directivă.

96 Respectarea principiului proporționalității decurge și din jurisprudența constantă a Curții potrivit căreia protecția dreptului fundamental la respectarea vieții private la nivelul Uniunii impune ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele strictului necesar (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, punctul 77, Hotărârea Digital Rights, punctul 52, precum și Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 92).

97 În ceea ce privește aspectul dacă o reglementare națională, precum cea în discuție în cauza C-203/15, îndeplinește aceste condiții, trebuie să se arate că aceasta prevede o păstrare generalizată și nediferențiată a ansamblului datelor de transfer și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică și că îi obligă pe furnizorii de servicii de comunicații electronice să păstreze aceste date în mod sistematic și continuu, fără nicio excepție. După cum reiese din decizia de trimitere, categoriile de date vizate de această reglementare corespund, în esență, celor a căror conservare era prevăzută de Directiva 2006/24.

98 Datele pe care trebuie să le păstreze astfel furnizorii de servicii de comunicații electronice permit să se găsească și să se identifice sursa unei comunicații și destinația acesteia, să se determine data, ora, durata și tipul unei comunicații, dispozitivele de comunicații ale utilizatorilor, precum și să localizeze dispozitivele de comunicații mobile. Printre aceste date figurează, *inter alia*, numele și adresa abonatului sau a utilizatorului înregistrat, numărul de telefon al apelantului și numărul apelat, precum și o adresă IP pentru serviciile internet. Aceste date permit în special stabilirea persoanei cu care a comunicat un abonat sau un utilizator înregistrat și prin ce mijloace, precum și stabilirea duratei comunicației și a locului de unde a fost inițiată aceasta. În plus, acestea permit să se cunoască frecvența comunicațiilor abonatului sau ale utilizatorului înregistrat cu anumite persoane într-o perioadă determinată (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 26).

99 Considerate în ansamblu, aceste date 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 ședere permanente sau temporare, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 27). În special, aceste date furnizează mijloacele de a stabili, astfel cum a subliniat avocatul general la punctele 253, 254 și 257-259 din concluzii, profilul persoanelor în cauză, informație la fel de sensibilă, din perspectiva dreptului la respectarea vieții private, ca și conținutul însuși al comunicațiilor.

100 Ingerința pe care o implică o astfel de reglementare în drepturile fundamentale consacrate la articolele 7 și 8 din cartă se dovedește a fi de o mare amploare și trebuie considerată deosebit de gravă. Împrejurarea că păstrarea datelor este efectuată fără ca utilizatorii serviciilor de comunicații electronice să fie informați cu privire la aceasta este susceptibilă să genereze în mintea persoanelor vizate sentimentul că viața lor privată face obiectul unei supravegheri constante (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 37).

101 Chiar dacă o astfel de reglementare nu permite păstrarea conținutului unei comunicații și, prin urmare, nu este de natură să aducă atingere conținutului esențial al respectivelor drepturi (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 39), păstrarea datelor de transfer și a datelor de localizare ar putea avea totuși o incidență asupra utilizării mijloacelor de comunicații electronice și, în consecință, asupra exercitării de către utilizatori a acestor mijloace ale libertății lor de exprimare, garantată la articolul 11 din cartă (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 28).

102 Având în vedere gravitatea ingerinței în drepturile fundamentale în cauză pe care o constituie o reglementare națională care prevede, în scopul combaterii infracționalității, păstrarea datelor de transfer și a datelor de localizare, numai combaterea infracționalității grave poate justifica o asemenea măsură (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 60).

103 În plus, deși eficacitatea combaterii infracționalității grave, în special combaterea crimei organizate și a terorismului, poate să depindă în mare măsură de utilizarea tehnicilor moderne de investigație, un astfel de obiectiv de interes general, oricât de fundamental ar fi, nu poate, în sine, să justifice ca o reglementare națională care prevede păstrarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare să fie considerată necesară în scopul acestei combateri (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 51).

104 În această privință, trebuie să se arate, pe de o parte, că o astfel de reglementare are ca efect, având în vedere caracteristicile sale descrise la punctul 97 din prezenta hotărâre, că păstrarea datelor de transfer și a datelor de localizare este regula, în timp ce sistemul instituit de Directiva 2002/58 impune ca această conservare a datelor să fie excepția.

105 Pe de altă parte, o reglementare națională precum cea în discuție în litigiul principal, care acoperă în mod generalizat toți abonații și utilizatorii înregistrați și privește toate mijloacele de comunicare

electronică, precum și toate datele de transfer, nu prevede nicio diferențiere, limitare sau excepție în funcție de obiectivul urmărit. Aceasta privește în mod global ansamblul persoanelor care utilizează servicii de comunicații electronice, fără ca aceste persoane să se regăsească, fie și în mod indirect, într-o situație susceptibilă să declanșeze începerea urmăririi penale. 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 infracțiuni grave. În plus, aceasta nu prevede nicio excepție, astfel încât ea se aplică chiar și acelor persoane ale căror comunicații sunt supuse, potrivit normelor dreptului național, secretului profesional (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctele 57 și 58).

106 O astfel de reglementare nu impune nicio relație între datele a căror păstrare este prevăzută și o amenințare pentru securitatea publică. În special, aceasta nu este limitată la o păstrare care privește fie datele aferente unei perioade și/sau unei zone geografice și/sau unui cerc de persoane care pot fi implicate într-un fel sau altul într-o infracțiune gravă, fie persoane care, din alte motive, ar putea să contribuie, prin păstrarea datelor lor, la combaterea infracționalității (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 59).

107 O reglementare națională precum cea în discuție în litigiul principal depășește, așadar, limitele strictului necesar și nu poate fi considerată justificată, într-o societate democratică, astfel cum se prevede la 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.

108 În schimb, 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 ca un stat membru să adopte o reglementare care să permită, cu titlu preventiv, păstrarea direcționată a datelor de transfer și a datelor de localizare, în scopul combaterii infracționalității grave, cu condiția ca păstrarea datelor să fie, în ceea ce privește categoriile de date care trebuie păstrate, mijloacele de comunicare vizate, persoanele în cauză, precum și durata de păstrare reținută, limitată la strictul necesar.

109 Pentru a îndeplini cerințele menționate la punctul anterior din prezenta hotărâre, această reglementare națională trebuie, în primul rând, să prevadă norme clare și precise care să reglementeze conținutul și aplicarea unei astfel de măsuri de păstrare a datelor și să impună un minimum de cerințe, astfel încât persoanele ale căror date au fost păstrate să dispună de garanții suficiente care să le permită să protejeze în mod eficient datele lor cu caracter personal împotriva riscurilor de abuz. Aceasta trebuie în special să indice în ce împrejurări și în ce condiții o măsură de păstrare a datelor poate fi luată, cu titlu preventiv, garantând astfel că o asemenea măsură este limitată la strictul necesar (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 54 și jurisprudența citată).

110 În al doilea rând, în ceea ce privește condițiile materiale pe care trebuie să le îndeplinească reglementarea națională care permite, în cadrul combaterii infracționalității, păstrarea cu titlu preventiv a datelor de transfer și a datelor de localizare, pentru a garanta că aceasta este limitată la strictul necesar, trebuie să se arate că, deși aceste condiții pot varia în funcție de măsurile adoptate pentru prevenirea, investigarea, detectarea și urmărirea penală a infracțiunilor grave, păstrarea datelor trebuie să răspundă întotdeauna unor criterii obiective, care să stabilească un raport între datele care trebuie păstrate și obiectivul urmărit. În special, astfel de condiții trebuie să se dovedească, în practică, de natură să delimiteze în mod efectiv amploarea măsurii și, în consecință, publicul în cauză.

111 Referitor la delimitarea unei asemenea măsuri în ceea ce privește publicul și situațiile potențial vizate, reglementarea națională trebuie să se întemeieze pe elemente obiective care să permită să fie vizat un public ale cărui date pot prezenta o legătură, cel puțin indirectă, cu acte de infracționalitate gravă, să contribuie într-un mod sau altul la combaterea infracționalității grave sau să prevină un risc grav pentru securitatea publică. O astfel de delimitare poate fi asigurată prin intermediul unui criteriu geografic în cazul în care autoritățile naționale competente consideră pe baza unor elemente obiective, că există, într-una sau în mai multe zone geografice, un risc ridicat privind pregătirea sau comiterea unor asemenea acte.

112 Având în vedere toate considerațiile care precedă, trebuie să se răspundă la prima întrebare în cauza C-203/15 că articolul 15 alineatul (1) din Directiva 2002/58, lecturat 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 infracționalității, o păstrare generalizată și nediferențiată a ansamblului datelor de transfer și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică.

Cu privire la a doua întrebare în cauza C-203/15 și prima întrebare în cauza C-698/15

113 Este necesar să se arate cu titlu introductiv că Kammarrätten i Stockholm (Curtea de Apel Administrativă din Stockholm) a adresat a doua întrebare în cauza C-203/15 numai în ipoteza unui răspuns negativ la prima întrebare din cauza respectivă. Totuși, această a doua întrebare este independentă de caracterul generalizat sau direcționat al unei păstrări a datelor, în sensul avut în vedere la punctele 108-111 din prezenta hotărâre. Prin urmare, trebuie să se răspundă împreună la a doua întrebare în cauza C-203/15 și la prima întrebare în cauza C-698/15, care este adresată independent de întinderea obligației de păstrare a unor date care ar fi impusă furnizorilor de servicii de comunicații electronice.

114 Prin intermediul celei de a doua întrebări în cauza C-203/15 și al primei întrebări în cauza C-698/15, instanțele de trimitere solicită în esență să se stabilească dacă articolul 15 alineatul (1) din Directiva 2002/58, lecturat 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 reglementează protecția și securitatea datelor de transfer și a datelor de localizare, în special accesul autorităților naționale competente la datele păstrate, fără a limita acest acces numai la scopul combaterii infracționalității grave, fără a supune respectivul acces unui control prealabil al unei instanțe sau al unei autorități administrative independente, și fără a impune ca datele în cauză să fie păstrate pe teritoriul Uniunii.

115 În ceea ce privește obiectivele care pot justifica o reglementare națională care derogă de la principiul confidențialității comunicațiilor electronice, trebuie amintit că, întrucât, astfel cum s-a constatat la punctele 90 și 102 din prezenta hotărâre, enumerarea obiectivelor care figurează la articolul 15 alineatul (1) prima teză din Directiva 2002/58 prezintă un caracter exhaustiv, accesul la datele păstrate trebuie să urmărească în mod efectiv și strict unul dintre aceste obiective. În plus, din moment ce obiectivul urmărit de această reglementare trebuie să se raporteze la gravitatea ingerinței în drepturile fundamentale pe care o determină acest acces, rezultă că, în materie de prevenție, cercetare, detectare și urmărire penală a infracțiunilor, numai combaterea infracționalității grave poate justifica un astfel de acces la datele păstrate.

116 În ceea ce privește respectarea principiului proporționalității, o reglementare națională care guvernează condițiile în care furnizorii de servicii de comunicații electronice trebuie să acorde autorităților naționale competente accesul la datele păstrate trebuie să asigure, în conformitate cu cele constatate la punctele 95 și 96 din prezenta hotărâre, că un astfel de acces are loc numai în limitele strictului necesar.

117 În plus, întrucât măsurile legislative menționate la articolul 15 alineatul (1) din Directiva 2002/58 trebuie, conform considerentului (11) al acestei directive, să fie „însoțite de precauțiile corespunzătoare”, o asemenea măsură trebuie, după cum rezultă din jurisprudența citată la punctul 109 din prezenta hotărâre, să prevadă norme clare și precise care să indice în ce împrejurări și în ce condiții furnizorii de servicii de comunicații electronice trebuie să acorde autorităților naționale competente accesul la date. De asemenea, o măsură de această natură trebuie să fie obligatorie din punct de vedere juridic în dreptul intern.

118 Pentru a garanta că accesul autorităților naționale competente la datele păstrate este limitat la strictul necesar, revine, desigur, dreptului național sarcina de a stabili condițiile în care furnizorii de servicii de comunicații electronice trebuie să acorde un astfel de acces. Cu toate acestea, reglementarea națională în cauză nu se poate limita la a impune ca accesul să urmărească unul dintre obiectivele menționate la articolul 15 alineatul (1) din Directiva 2002/58, chiar dacă acesta constă în combaterea infracționalității grave. Astfel, o asemenea reglementare națională trebuie să prevadă și condițiile materiale și procedurale

care guvernează accesul autorităților naționale competente la datele păstrate (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 61).

119 Prin urmare, întrucât un acces general la toate datele păstrate, independent de orice legătură, chiar indirectă, cu scopul urmărit nu poate fi considerat limitat la strictul necesar, reglementarea națională în cauză 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 abonaților sau ale utilizatorilor înregistrați. În această privință, accesul nu poate fi acordat, în principiu, în raport cu obiectivul de combatere a infracționalității, decât la datele persoanelor bănuite că ar pregăti, că ar săvârși sau că ar fi săvârșit o infracțiune gravă ori că ar fi implicate în orice mod într-o astfel de infracțiune (a se vedea prin analogie Curtea Europeană a Drepturilor Omului, 4 decembrie 2015, Zakharov împotriva Rusiei, CE:ECHR:2015:1204JUD004714306, § 260). Cu toate acestea, în situații speciale, precum cele în care interese vitale privind securitatea națională, apărarea sau securitatea publică sunt amenințate prin activități teroriste, ar putea de asemenea să fie permis accesul la datele altor persoane în cazul în care există elemente obiective care permit să se considere că aceste date ar putea aduce, într-un caz concret, o contribuție efectivă la combaterea unor asemenea activități.

120 În scopul de a garanta, în practică, deplina respectare a acestor condiții, este esențial ca accesul autorităților naționale competente la datele păstrate să fie, în principiu, cu excepția unor situații de urgență justificate corespunzător, condiționat de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă, și ca decizia acestei instanțe sau a acestei entități să intervină în urma unei cereri motivate formulate de autoritățile respective, printre altele în cadrul unor proceduri de prevenire, de detectare sau de urmărire penală (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 62; a se vedea de asemenea, prin analogie, în ceea ce privește articolul 8 din CEDO, Curtea Europeană a Drepturilor Omului, 12 ianuarie 2016, Szabó și Vissy împotriva Ungariei, CE:ECHR:2016:0112JUD003713814, §§ 77 și 80).

121 De asemenea, se impune ca autoritățile naționale competente cărora le-a fost acordat accesul la datele păstrate să informeze persoanele în cauză, în cadrul procedurilor naționale aplicabile, din momentul în care această comunicare nu poate compromite anchetele desfășurate de autoritățile respective. Astfel, această informație este, de fapt, necesară pentru a le permite să își exercite printre altele dreptul de a introduce acțiunea, prevăzut expres la articolul 15 alineatul (2) din Directiva 2002/58 coroborat cu articolul 22 din Directiva 95/46, în cazul încălcării drepturilor lor (a se vedea prin analogie Hotărârea din 7 mai 2009, Rijkeboer, C-553/07, EU:C:2009:293, punctul 52, precum și Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 95).

122 În ceea ce privește normele referitoare la securitatea și la protecția datelor păstrate de furnizorii de servicii de comunicații electronice, trebuie să se constate că articolul 15 alineatul (1) din Directiva 2002/58 nu permite statelor membre să deroge de la articolul 4 alineatul (1) și nici de la articolul 4 alineatul (1a) din aceasta. Aceste din urmă dispoziții impun ca respectivii furnizori să adopte măsurile de ordin tehnic și organizatoric adecvate care să permită să se asigure o protecție eficientă a datelor păstrate împotriva riscurilor de abuz, precum și împotriva oricărui acces ilicit la aceste date. Ținând seama de cantitatea datelor păstrate, de caracterul sensibil al respectivelor date, precum și de riscul de acces ilicit la acestea, furnizorii de servicii de comunicații electronice trebuie, în scopul de a asigura deplina integritate și confidențialitate a datelor menționate, să garanteze un nivel deosebit de ridicat de protecție și de securitate prin măsuri tehnice și organizatorice adecvate. În special, reglementarea națională trebuie să prevadă păstrarea pe teritoriul Uniunii, precum și distrugerea iremediabilă a datelor la finalul duratei de păstrare a acestora (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctele 66-68).

123 În orice caz, statele membre trebuie să garanteze controlul, de către o autoritate independentă, al respectării nivelului de protecție garantat de dreptul Uniunii în materie de protecție a persoanelor fizice față de prelucrarea datelor cu caracter personal, dat fiind că un astfel de control este impus în mod expres la articolul 8 alineatul (3) din cartă și constituie, conform jurisprudenței constante a Curții, un element esențial al respectării protecției persoanelor în ceea ce privește prelucrarea datelor cu caracter personal. În caz

contrar, persoanele ale căror date cu caracter personal au fost păstrate ar fi private de dreptul, garantat la articolul 8 alineatele (1) și (3) din cartă, de a sesiza autoritățile naționale de supraveghere cu o cerere în vederea protejării drepturilor lor fundamentale (a se vedea în acest sens Hotărârea Digital Rights, punctul 68, precum și Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctele 41 și 58).

124 Revine instanțelor de trimitere sarcina de a verifica dacă și în ce măsură reglementările naționale în discuție în litigiul principal respectă cerințele care decurg din cuprinsul articolului 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolele 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, astfel cum au fost clarificate la punctele 115-123 din prezenta hotărâre, în ceea ce privește atât accesul autorităților naționale competente la datele conservate, cât și protecția și nivelul de securitate al acestor date.

125 Având în vedere toate considerațiile care precedă, trebuie să se răspundă la a doua întrebare în cauza C-203/15 și la prima întrebare în cauza C-698/15 că articolul 15 alineatul (1) din Directiva 2002/58, lecturat în lumina articolele 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că se opune unei reglementări naționale care guvernează protecția și securitatea datelor de transfer și a datelor de localizare și, în special, accesul autorităților naționale competente la datele păstrate, fără a limita acest acces, în cadrul combaterii infracționalității, numai la combaterea infracționalității grave, fără a supune respectivul acces unui control prealabil din partea unei instanțe sau a unei autorități administrative independente, și fără a impune ca datele în cauză să fie păstrate pe teritoriul Uniunii.

Cu privire la a doua întrebare în cauza C-698/15

126 Prin intermediul celei de a doua întrebări în cauza C-698/15, Court of Appeal (England & Wales) (Civil Division) [Curtea de Apel (Anglia și Țara Galilor) (Secția civilă)] solicită în esență să se stabilească dacă, în Hotărârea Digital Rights, Curtea a interpretat articolele 7 și/sau 8 din cartă într-un sens care îl depășește pe cel conferit la articolul 8 din CEDO de Curtea Europeană a Drepturilor Omului.

127 Cu titlu introductiv, trebuie amintit că deși, astfel cum confirmă articolul 6 alineatul (3) TUE, drepturile fundamentale recunoscute de CEDO constituie principii generale ale dreptului Uniunii, convenția menționată nu constituie, atât timp cât Uniunea nu a aderat la ea, un instrument juridic integrat formal în ordinea juridică a Uniunii (a se vedea în acest sens Hotărârea din 15 februarie 2016, N., C-601/15 PPU, EU:C:2016:84, punctul 45 și jurisprudența citată).

128 Astfel, interpretarea Directivei 2002/58, în discuție în speță, trebuie să se realizeze numai din perspectiva drepturilor fundamentale garantate de cartă (a se vedea în acest sens Hotărârea din 15 februarie 2016, N., C-601/15 PPU, EU:C:2016:84, punctul 46 și jurisprudența citată).

129 În plus, trebuie amintit că explicațiile aferente articolului 52 din cartă arată că articolul 52 alineatul (3) din aceasta este destinat să asigure coerența necesară între cartă și CEDO, „fără a aduce atingere autonomiei dreptului Uniunii și Curții de Justiție a Uniunii Europene” (Hotărârea din 15 februarie 2016, N., C-601/15 PPU, EU:C:2016:84, punctul 47). În special, astfel cum prevede în mod expres articolul 52 alineatul (3) a doua teză din cartă, articolul 52 alineatul (3) prima teză din aceasta nu împiedică dreptul Uniunii să acorde o protecție mai largă decât CEDO. La acest lucru se adaugă, în sfârșit, faptul că articolul 8 din cartă privește un drept fundamental distinct de cel consacrat la articolul 7 din aceasta și care nu are echivalent în CEDO.

130 Or, potrivit unei jurisprudențe constante a Curții, justificarea unei cereri de decizie preliminară nu o constituie formularea de opinii consultative cu privire la chestiuni generale sau ipotetice, ci necesitatea inerentă soluționării efective a unui litigiu privind dreptul Uniunii (a se vedea în acest sens Hotărârea din 24 aprilie 2012, Kamberaj, C-571/10, EU:C:2012:233, punctul 41, Hotărârea din 26 februarie 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, punctul 42, precum și Hotărârea din 27 februarie 2014, Pohotovosť, C-470/12, EU:C:2014:101, punctul 29).

131 În speță, având în vedere considerațiile care figurează în special la punctele 128 și 129 din prezenta hotărâre, aspectul dacă protecția conferită la articolele 7 și 8 din cartă o depășește pe cea garantată la articolul 8 din CEDO nu este de natură să aibă o influență asupra interpretării Directivei 2002/58, lecturată în lumina cartei, care este în discuție în litigiul principal, în cauza C-698/15.

132 Astfel, nu rezultă că un răspuns la a doua întrebare în cauza C-698/15 poate aduce elemente de interpretare a dreptului Uniunii care să fie necesare pentru soluționarea, în lumina acestui drept, a litigiului respectiv.

133 În consecință, a doua întrebare în cauza C-698/15 este inadmisibilă.

Cu privire la cheltuielile de judecată

134 Întrucât, în privința părților din litigiul principal, procedura are caracterul unui incident survenit la instanțele de trimitere, este de competența acestora 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, lecturat în lumina articolelor 7 și 8, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene, trebuie interpretat în sensul că se opune unei reglementări naționale care prevede, în scopul combaterii infracționalității, o păstrare generalizată și nediferențiată a ansamblului datelor de transfer și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică.Articolul 15 alineatul (1) din Directiva 2002/58, astfel cum a fost modificată prin Directiva 2009/136/CE, lecturat în lumina articolelor 7 și 8, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale, trebuie interpretat în sensul că se opune unei reglementări naționale care guvernează protecția și securitatea datelor de transfer și a datelor de localizare, în special accesul autorităților naționale competente la datele păstrate, fără a limitaacest acces, în cadrul combaterii infracționalității, numai la combaterea infracționalității grave, fără a supune respectivul acces unui control prealabil din partea unei instanțe sau a unei autorități administrative independente, și fără a impune ca datele în cauză să fie păstrate pe teritoriul Uniunii.A doua întrebare adresată de Court of Appeal (England & Wales) (Civil Division) [Curtea de Apel (Anglia și Țara Galilor) (Secția civilă), Regatul Unit] este inadmisibilă.**

---

* Limbile de procedură: suedeza și engleza.

(hidden)