Repertoriul jurisprudenței

HOTĂRÂREA CURȚII (Marea Cameră)

6 octombrie 2020 *

[Text rectificat prin Ordonanța din 16 noiembrie 2020]

Cuprins

* Limba de procedură: franceza.

„Trimitere preliminară – Prelucrarea datelor cu caracter personal în sectorul comunicațiilor electronice – Furnizori de servicii de comunicații electronice – Furnizori de servicii de stocare-hosting și furnizori de acces la internet – Stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare – Analiză automatizată a datelor – Acces în timp real la date – Protejarea securității naționale și combaterea terorismului – Combaterea infracționalității – Directiva 2002/58/CE – Domeniu de aplicare – Articolul 1 alineatul (3) și articolul 3 – Confidențialitatea comunicațiilor electronice – Protecție – Articolul 5 și articolul 15 alineatul (1) – Directiva 2000/31/CE – Domeniu de aplicare – Carta drepturilor fundamentale a Uniunii Europene – Articolele 4, 6-8 și 11 și articolul 52 alineatul (1) – Articolul 4 alineatul (2) TUE”

În cauzele conexate C-511/18, C-512/18 și C-520/18,

având ca obiect cereri de decizie preliminară formulate în temeiul articolului 267 TFUE de Conseil d'État (Consiliul de Stat, Franța), prin deciziile din 26 iulie 2018, primite de Curte la 3 august 2018 (C-511/18 și C-512/18), și de Cour constitutionnelle (Curtea Constituțională, Belgia), prin decizia din 19 iulie 2018, primită de Curte la 2 august 2018 (C-520/18), în procedurile

La Quadrature du Net (C-511/18 și C-512/18),

French Data Network (C-511/18 și C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 și C-512/18),

Igwan.net (C-511/18),

împotriva

Premier ministre (C-511/18 și C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 și C-512/18),

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18), cu participarea:

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18),

și

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

împotriva

Conseil des ministres,

cu participarea:

Child Focus (C-520/18),

CURTEA (Marea Cameră),

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

avocat general: domnul M. Campos Sánchez-Bordona,

grefier: doamna C. Strömholm, administratoare,

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

luând în considerare observațiile prezentate:

– pentru Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net și Center for Democracy and Technology, de A. Fitzjean Ò Cobhthaigh, avocat;

– pentru French Data Network, de Y. Padova, avocat;

– pentru Privacy International, de H. Roy, avocat;

– pentru Ordre des barreaux francophones et germanophone, de E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart și J.-F. Henrotte, avocats;

– pentru Académie Fiscale ASBL și UA, de J.-P. Riquet;

– pentru Liga voor Mensenrechten ASBL, de J. Vander Velpen, avocat;

– pentru Ligue des Droits de l'Homme ASBL, de R. Jespers și J. Fermon, avocats;

– pentru VZ, WY și XX, de D. Pattyn, avocat;

– pentru Child Focus, de N. Buisseret, K. De Meester și J. Van Cauter, avocats;

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

– pentru guvernul belgian, de J.-C. Halleux, P. Cottin și C. Pochet, în calitate de agenți, asistați de J. Vanpraet, Y. Peeters, S. Depré și E. de Lophem, avocats;

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

– pentru guvernul danez, inițial de J. Nymann-Lindegren, M. Wolff și P. Ngo, ulterior de J. Nymann-Lindegren și M. Wolff, în calitate de agenți;

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

– pentru guvernul estonian, de N. Grünberg și A. Kalbus, în calitate de agenți;

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

– pentru guvernul spaniol, inițial de L. Aguilera Ruiz și A. Rubio González, ulterior de L. Aguilera Ruiz, în calitate de agenți;

– pentru guvernul cipriot, de E. Neofytou, în calitate de agent;

– pentru guvernul leton, de V. Soņeca, în calitate de agent;

– pentru guvernul maghiar, inițial de M. Z. Fehér și Z. Wagner, ulterior de M. Z. Fehér, în calitate de agent;

– pentru guvernul neerlandez, de K. Bulterman și M. A. M. de Ree, în calitate de agenți;

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

– pentru guvernul suedez, inițial de H. Shev, H. Eklinder, C. Meyer-Seitz și A. Falk, ulterior de H. Shev, H. Eklinder, C. Meyer-Seitz și J. Lundberg, în calitate de agenți;

– pentru guvernul Regatului Unit, de S. Brandon, în calitate de agent, asistat de G. Facenna, QC, și C. Knight, barrister;

– [liniuță eliminată prin Ordonanța din 16 noiembrie 2020];

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

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

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

pronunță prezenta

Hotărâre

1 Cererile de decizie preliminară privesc interpretarea, pe de o parte, a articolului 15 alineatul (1) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO 2002, L 201, p. 37, Ediție specială, 13/vol. 36, p. 63), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 (JO 2009, L 337, p. 11) (denumită în continuare „Directiva 2002/58”), și, pe de altă parte, a articolelor 12-15 din Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (Directiva privind comerțul electronic) (JO 2000, L 178, p. 1, Ediție specială, 13/vol. 29, p. 257), citite în lumina articolelor 4, 6-8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”) și a articolului 4 alineatul (2) TUE.

2 Cererea în cauza C-511/18 a fost formulată în cadrul unor litigii între La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs și Igwan.net, pe de o parte, și Premier ministre (prim-ministrul, Franța), Garde des Sceaux, ministre de la Justice (păstrătorul sigiliilor, ministrul justiției, Franța), ministre de l'Intérieur (ministrul afacerilor interne, Franța) și ministre des Armées (ministrul forțelor armate, Franța), pe de altă parte, în legătură cu legalitatea décret nº 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de

renseignement (Decretul nr. 2015-1185 din 28 septembrie 2015 privind desemnarea serviciilor specializate de informații) (JORF din 29 septembrie 2015, textul 1 din 97, denumit în continuare „Decretul nr. 2015-1185”), a décret nº 2015-1211, du 1er octobre 2015, relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (Decretul nr. 2015-1211 din 1 octombrie 2015 privind contenciosul referitor la punerea în aplicare a tehnicilor de informare supuse autorizării și la fișierele legate de securitatea statului) (JORF din 2 octombrie 2015, textul 7 din 108, denumit în continuare „Decretul nr. 2015-1211”), a décret nº 2015-1639, du 11 décembre 2015, relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure (Decretul nr. 2015-1639 din 11 decembrie 2015 privind desemnarea altor servicii decât serviciile specializate de informații, autorizate să recurgă la tehnicile menționate în titlul V din cartea VIII din Codul privind securitatea internă) (JORF din 12 decembrie 2015, textul 28 din 127, denumit în continuare „Decretul nr. 2015-1639”), precum și a décret nº 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement (Decretul nr. 2016-67 din 29 ianuarie 2016 privind tehnicile de colectare a informațiilor) (JORF din 31 ianuarie 2016, textul 2 din 113, denumit în continuare „Decretul nr. 2016-67”).

3 Cererea în cauza C-512/18 a fost formulată în cadrul unor litigii între French Data Network, La Quadrature du Net și Fédération des fournisseurs d'accès à Internet associatifs, pe de o parte, și Premier ministre (prim-ministrul, Franța) și Garde des Sceaux, ministre de la Justice (păstrătorul sigiliilor, ministrul justiției, Franța), pe de altă parte, în legătură cu legalitatea articolului R. 10-13 din code des postes et des communications électroniques (Codul serviciilor poștale și al comunicațiilor electronice) (denumit în continuare „CPCE”) și a décret nº 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (Decretul nr. 2011-219 din 25 februarie 2011 privind stocarea și comunicarea datelor care permit identificarea oricărei persoane care a contribuit la crearea unui conținut oferit online) (JORF din 1 martie 2011, textul 32 din 170, denumit în continuare „Decretul nr. 2011-219”).

4 Cererea în cauza C-520/18 a fost formulată în cadrul unor litigii între Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY și XX, pe de o parte, și Conseil des ministres (Consiliul de Miniștri, Belgia), pe de altă parte, în legătură cu legalitatea loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (Legea din 29 mai 2016 privind colectarea și stocarea datelor în sectorul comunicațiilor electronice) (*Moniteur belge* din 18 iulie 2016, p. 44717, denumită în continuare „Legea din 29 mai 2016”).

Cadrul juridic

Dreptul Uniunii

Directiva 95/46

5 Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO 1995, L 281, p. 31, Ediție specială, 13/vol. 17, p. 10) a fost abrogată, cu efect de la 25 mai 2018, prin Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din

27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46 (JO 2016, L 119, p. 1). Articolul 3 alineatul (2) din Directiva 95/46 prevedea:

„Prezenta directivă nu se aplică prelucrării datelor cu caracter personal:

– puse în practică pentru exercitarea activităților din afara domeniului de aplicare al dreptului comunitar, cum ar fi cele prevăzute în titlurile V și VI din Tratatul privind Uniunea Europeană și, în orice caz, prelucrărilor care au ca obiect siguranța publică, apărarea, securitatea statului (inclusiv bunăstarea economică a statului atunci când aceste prelucrări sunt legate de probleme de securitate a statului) și activitățile statului în domeniul dreptului penal;

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

6 Articolul 22 din Directiva 95/46, care figurează în capitolul III din aceasta, intitulat „Acțiuni în justiție, răspundere și sancțiuni", avea următorul cuprins:

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

Directiva 97/66

7 Potrivit articolului 5 din Directiva 97/66/CE a Parlamentului European și a Consiliului din 15 decembrie 1997 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor (JO 1997, L 24, p. 1), intitulat „Confidențialitatea comunicațiilor":

„(1) Statele membre garantează, prin reglementări naționale, confidențialitatea comunicațiilor efectuate prin intermediul unei rețele publice de telecomunicații sau al unor servicii de telecomunicații accesibile publicului. În special, acestea interzic oricărei alte persoane decât utilizatorii, fără acordul utilizatorilor în cauză, să asculte, să intercepteze, să stocheze comunicațiile sau să le supună oricăror alte mijloace de interceptare sau supraveghere, cu excepția cazului în care aceste activități sunt autorizate în mod legal, în conformitate cu articolul 14 alineatul (1).

(2) Alineatul (1) nu împiedică înregistrarea autorizată prin lege a comunicațiilor, în cadrul procedurilor juridice comerciale în scopul furnizării dovezii unei tranzacții comerciale sau pentru alte comunicări comerciale." [traducere neoficială]

Directiva 2000/31

8 Considerentele (14) și (15) ale Directivei 2000/31 au următorul cuprins:

„(14) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este reglementată numai de Directiva [95/46] și de Directiva [97/66], care se aplică pe deplin serviciilor societății informaționale. Aceste directive stabilesc deja un cadru juridic comunitar în domeniul datelor cu caracter personal și, prin urmare, nu este necesar să se reglementeze această chestiune în prezenta directivă pentru a asigura buna funcționare a pieței interne, în special libera circulație a datelor cu caracter personal între statele membre. Punerea în aplicare a prezentei directive trebuie făcută respectând principiile referitoare la protecția datelor cu caracter personal, în special în ceea ce privește comunicările comerciale nesolicitate și răspunderea intermediarilor. Prezenta directivă nu poate împiedica folosirea anonimă a rețelelor deschise, așa cum este internetul.

(15) Confidențialitatea comunicărilor este garantată de articolul 5 din Directiva [97/66]. În conformitate cu această directivă, statele membre trebuie să interzică orice fel de interceptare sau supraveghere a comunicărilor de către altcineva decât expeditorii sau destinatarii, în afara cazului în care aceste activități sunt autorizate legal.”

9 Articolul 1 din Directiva 2000/31 are următorul cuprins:

„(1) Prezenta directivă își propune să contribuie la buna funcționare a pieței interne prin asigurarea liberei circulații a serviciilor societății informaționale între statele membre.

(2) Prezenta directivă apropie, în măsura necesară atingerii obiectivelor prevăzute la alineatul (1), anumite dispoziții de drept intern aplicabile serviciilor societății informaționale în ceea ce privește piața internă, stabilirea furnizorilor de servicii, comunicările comerciale, contractele încheiate prin mijloace electronice, răspunderea intermediarilor, codurile de conduită, soluționarea extrajudiciară a litigiilor, acțiunile în justiție și cooperarea între statele membre.

(3) Prezenta directivă completează dreptul comunitar aplicabil serviciilor societății informaționale fără a aduce atingere nivelului de protecție, în special în materie de sănătate publică și interese ale consumatorilor, stabilit prin instrumente comunitare și prin legislația internă care le pune în aplicare în măsura în care aceasta nu restrânge libera prestare a serviciilor societății informaționale.

[…]

(5) Prezenta directivă nu se aplică în:

[…]

(b) chestiunile referitoare la serviciile societății informaționale reglementate de Directivele [95/46] și [97/66];

[…]”

10 Articolul 2 din Directiva 2000/31 are următorul cuprins:

„În sensul prezentei directive, următorii termeni au înțelesurile de mai jos:

(a) «servicii ale societății informaționale»: servicii în sensul articolului 1 alineatul (2) din Directiva 98/34/CE [a Parlamentului European și a Consiliului din 22 iunie 1998 de stabilire a unei proceduri pentru furnizarea de informații în domeniul standardelor și reglementărilor tehnice (JO 1998, L 204, p. 37, Ediție specială, 13/vol. 23, p. 207)], astfel cum a fost modificată prin Directiva 98/48/CE [a Parlamentului European și a Consiliului din 20 iulie 1998 (JO 1998, L 217, p. 18, Ediție specială, 13/vol. 23, p. 282)];

[…]”

11 Articolul 15 din Directiva 2000/31 prevede:

„(1) Statele membre nu trebuie să impună furnizorilor obligația generală de supraveghere a informațiilor pe care le transmit sau le stochează atunci când furnizează serviciile prevăzute la articolele 12, 13 și 14 și nici obligația generală de a căuta în mod activ fapte sau circumstanțe din care să rezulte că activitățile sunt ilicite.

(2) Statele membre pot institui obligația furnizorilor de servicii ale societății informaționale de a informa prompt autoritățile publice competente despre presupuse activități ilicite pe care le-ar desfășura destinatarii serviciilor lor ori despre presupuse informații ilicite pe care aceștia le-ar furniza sau obligația de a comunica autorităților competente, la cererea acestora, informații care să permită identificarea destinatarilor serviciilor cu care au încheiat un acord de stocare-hosting."

Directiva 2002/21

12 Potrivit considerentului (10) al Directivei 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):

„Definiția «serviciului societății informaționale», prevăzută la articolul 1 din Directiva [98/34, astfel cum a fost modificată prin Directiva 98/48], se referă la o gamă largă de activități economice care au loc online. Majoritatea acestor activități nu intră sub incidența prezentei directive deoarece nu reprezintă activități integrale sau principale de transmisie de semnale prin rețele de comunicații electronice. Serviciile de telefonie vocală și de transmisie prin poșta electronică sunt reglementate de prezenta directivă. Aceeași întreprindere, de exemplu, un furnizor de servicii internet, poate oferi atât servicii de comunicații electronice, precum accesul la internet, cât și servicii care nu intră sub incidența prezentei directive, precum furnizarea de conținut din rețea."

13 Articolul 2 din Directiva 2002/21 prevede:

„În sensul prezentei directive:

[…]

(c) «serviciu de comunicații electronice» înseamnă serviciul furnizat de obicei contra cost și care constă în totalitate sau în principal în transmiterea de semnale prin rețele de comunicații electronice, inclusiv serviciile de telecomunicații și serviciile de transmisie prin rețele utilizate pentru radiodifuziune, dar nu și servicii care constau din furnizarea de conținuturi prin intermediul rețelelor și serviciilor de comunicații electronice [sau din exercitarea unei responsabilități editoriale asupra acestora]; nu include serviciile societății informaționale astfel cum sunt acestea definite la articolul 1 din Directiva [98/34] care nu constau în întregime sau în principal în transmiterea de semnale prin rețele de comunicații electronice;

[…]"

Directiva 2002/58

14 Considerentele (2), (6), (7), (11), (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 cartei.

[…]

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

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

[…]

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

[…]

(22) Interdicția stocării comunicațiilor și a datelor de transfer aferente de către alte persoane decât utilizatorul sau fără acordul acestuia nu înseamnă interzicerea oricărei stocări automate, intermediare sau tranzitorii a acestor informații, în cazul în care acest lucru se întâmplă cu unicul scop al efectuării transmisiei prin rețeaua de comunicații electronice și cu condiția ca informațiile să nu fie stocate pentru o perioadă mai lungă decât este necesar în vederea transmiterii sau în scopuri legate de gestionarea traficului și ca în timpul perioadei de stocare să fie garantată confidențialitatea datelor. […]

[…]

(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 online și numai pe o perioadă limitată de timp. Orice altă prelucrare a acestor date […] este permisă numai în cazul în care abonatul își dă acordul la aceasta după o informare corectă și completă din partea prestatorului de servicii publice de comunicații electronice cu privire la modul de prelucrare ulterioară a datelor pe care intenționează să o efectueze și la dreptul abonatului de a nu acorda sau de a-și retrage acordul pentru această prelucrare. Datele de transfer folosite pentru comercializarea serviciilor de comunicații […] trebuie de asemenea șterse sau trecute în anonimat […].

[…]

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

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

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

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

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

16 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].

Se aplică de asemenea următoarele definiții:

(a) «utilizator» înseamnă orice persoană fizică ce folosește un serviciu public de comunicații electronice, în scopuri profesionale sau personale, fără a fi în mod necesar abonat la serviciul respectiv;

(b) «date de transfer» înseamnă orice date prelucrate în scopul transmiterii comunicației printr-o rețea de comunicații electronice sau în vederea facturării;

(c) «date de localizare» înseamnă orice date prelucrate într-o rețea de comunicații electronice sau prin intermediul unui serviciu de comunicații electronice, care indică poziția geografică a echipamentului terminal al unui utilizator al unui serviciu de comunicații electronice destinat publicului;

(d) «comunicație» înseamnă orice informație trimisă sau transmisă între un număr finit de părți prin intermediul unui serviciu public de comunicații electronice. Această categorie nu include informațiile transmise în cadrul unui serviciu de radiodifuziune pentru public prin intermediul unei rețele de comunicații electronice, în măsura în care aceste informații nu pot fi relaționate cu un abonat sau cu un utilizator identificabil care primește informația;

[…]”

17 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.”

18 Potrivit articolului 5 din Directiva 2002/58, intitulat „Confidențialitatea comunicațiilor”:

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

[…]

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

19 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.

[…]”

20 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. […]”

21 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 [Uniunii], inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) al Tratatului privind Uniunea Europeană.

[…]

(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.

[…]”

Regulamentul 2016/679

22 Considerentul (10) al Regulamentului 2016/679 are următorul cuprins:

„Pentru a se asigura un nivel consecvent și ridicat de protecție a persoanelor fizice și pentru a se îndepărta obstacolele din calea circulației datelor cu caracter personal în cadrul Uniunii, nivelul protecției drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea unor astfel de date ar trebui să fie echivalent în toate statele membre. Aplicarea consecventă și omogenă a normelor în materie de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ar trebui să fie asigurată în întreaga Uniune. […]”

23 Articolul 2 din acest regulament prevede:

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

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

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

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

[…]

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

[…]

(4) Prezentul regulament nu aduce atingere aplicării Directivei [2000/31], în special normelor privind răspunderea furnizorilor de servicii intermediari, prevăzute la articolele 12-15 din directiva menționată."

24 Articolul 4 din regulamentul menționat prevede:

„În sensul prezentului regulament:

1. «date cu caracter personal» înseamnă orice informații privind o persoană fizică identificată sau identificabilă («persoana vizată»); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

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

[…]"

25 Articolul 5 din Regulamentul 2016/679 prevede:

„(1) Datele cu caracter personal sunt:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată («legalitate, echitate și transparență»);

(b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 alineatul (1) («limitări legate de scop»);

(c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate («reducerea la minimum a datelor»);

(d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere («exactitate»);

(e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate («limitări legate de stocare»);

(f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare («integritate și confidențialitate»).

[…]”

26 Articolul 6 din acest regulament are următorul cuprins:

„(1) Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

[…]

(c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

[…]

(3) Temeiul pentru prelucrarea menționată la alineatul (1) literele (c) și (e) trebuie să fie prevăzut în:

(a) dreptul Uniunii sau

(b) dreptul intern care se aplică operatorului.

Scopul prelucrării este stabilit pe baza respectivului temei juridic […]. Respectivul temei juridic poate conține dispoziții specifice privind adaptarea aplicării normelor prezentului regulament, printre altele: condițiile generale care reglementează legalitatea prelucrării de către operator; tipurile de date care fac obiectul prelucrării; persoanele vizate; entitățile cărora le pot fi divulgate datele și scopul pentru care respectivele date cu caracter personal pot fi divulgate; limitările legate de scop; perioadele de stocare și operațiunile și procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale și echitabile cum sunt cele pentru alte situații concrete de prelucrare astfel cum sunt prevăzute în capitolul IX. Dreptul Uniunii sau dreptul intern urmărește un obiectiv de interes public și este proporțional cu obiectivul legitim urmărit.

[…]”

27 Articolul 23 din regulamentul menționat prevede:

„(1) Dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la articolele 12-22 și 34, precum și la articolul 5 în măsura în care dispozițiile

acestuia corespund drepturilor și obligațiilor prevăzute la articolele 12-22, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura:

(a) securitatea națională;

(b) apărarea;

(c) securitatea publică;

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

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

(f) protejarea independenței judiciare și a procedurilor judiciare;

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

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

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

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

(2) În special, orice măsură legislativă menționată la alineatul (1) conține dispoziții specifice cel puțin, dacă este cazul, în ceea ce privește:

(a) scopurile prelucrării sau ale categoriilor de prelucrare;

(b) categoriile de date cu caracter personal;

(c) domeniul de aplicare al restricțiilor introduse;

(d) garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal;

(e) menționarea operatorului sau a categoriilor de operatori;

(f) perioadele de stocare și garanțiile aplicabile având în vedere natura, domeniul de aplicare și scopurile prelucrării sau ale categoriilor de prelucrare;

(g) riscurile pentru drepturile și libertățile persoanelor vizate și

(h) dreptul persoanelor vizate de a fi informate cu privire la restricție, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției.”

28 Potrivit articolului 79 alineatul (1) din regulamentul menționat:

„Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în temeiul articolului 77, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta prezentul regulament.”

29 Potrivit articolului 94 din Regulamentul 2016/679:

„(1) [Directiva] [95/46] se abrogă cu efect de la 25 mai 2018.

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

30 Articolul 95 din acest regulament prevede:

„Prezentul regulament nu impune obligații suplimentare pentru persoanele fizice sau juridice în ceea ce privește prelucrarea în legătură cu furnizarea de servicii de comunicații electronice destinate publicului în rețelele de comunicații publice din Uniune, cu privire la aspectele pentru care acestora le revin obligații specifice cu același obiectiv prevăzut în Directiva [2002/58].”

Dreptul francez

Codul privind securitatea internă

31 Cartea VIII din partea legislativă a Codului privind securitatea internă (denumit în continuare „CSI”) prevede, la articolele L. 801-1-L. 898-1, norme referitoare la interceptarea de informații.

32 L. 811-3 din CSI prevede:

„Serviciile specializate de informații pot recurge, numai în scopul exercitării atribuțiilor lor, la următoarele tehnici menționate în titlul V din prezenta carte pentru colectarea informațiilor referitoare la apărarea și la promovarea următoarelor interese fundamentale ale națiunii:

1. Independența națională, integritatea teritoriului și apărarea națională;

2. Interesele majore ale politicii externe, executarea angajamentelor europene și internaționale ale Franței și prevenirea oricărei forme de ingerință externă;

3. Interesele economice, industriale și științifice majore ale Franței;

4. Prevenirea terorismului;

5. Prevenirea:
   a) atingerilor aduse formei republicane a instituțiilor;
   b) acțiunilor prin care se urmărește menținerea sau reconstituirea de grupuri dizolvate în temeiul articolului L. 212-1;
   c) violențelor colective de natură să aducă o atingere gravă păcii publice;

6. Prevenirea criminalității și a delincvenței organizate;

7. Prevenirea proliferării armelor de distrugere în masă.”

33 Articolul L. 811-4 din CSI prevede:

„Un decret al Conseil d’État [(Consiliul de Stat)], adoptat în urma avizului Commission nationale de contrôle des techniques de renseignement [(Comisia Națională de Control al Tehnicilor de Informare)], desemnează serviciile, altele decât serviciile specializate de informații, care țin de miniștrii apărării, afacerilor interne și justiției, precum și de miniștrii economiei, bugetului sau vămilor, care pot fi autorizate să recurgă la tehnicile menționate în titlul V din prezenta carte în condițiile prevăzute în aceeași carte. Acesta precizează, pentru fiecare serviciu, scopurile menționate la articolul L. 811-3 și tehnicile care pot face obiectul unei autorizații.”

34 Articolul L. 821-1 primul paragraf din CSI are următorul cuprins:

„Punerea în aplicare pe teritoriul național a tehnicilor de colectare a informațiilor menționate în capitolele I-IV din titlul V din prezenta carte este supusă autorizării prealabile a prim-ministrului, emisă în urma avizului Comisiei Naționale de Control al Tehnicilor de Informare.”

35 Articolul L. 821-2 din CSI prevede:

„Autorizația menționată la articolul L. 821-1 se eliberează în urma unei cereri scrise și motivate a ministrului apărării, a ministrului afacerilor interne, a ministrului justiției sau a miniștrilor economiei, bugetului sau vămilor. Fiecare ministru poate delega această atribuție în mod individual numai colaboratorilor direcți abilitați în ceea ce privește secretele referitoare la apărarea națională.

Cererea precizează:

1. Tehnica sau tehnicile care trebuie puse în aplicare;

2. Serviciul pentru care este prezentată;

3. Scopul sau scopurile urmărite;

4. Motivul sau motivele măsurilor;

5. Durata de validitate a autorizației;

6. Persoana sau persoanele, locul sau locurile ori vehiculele vizate.

În scopul aplicării punctului 6, persoanele a căror identitate nu este cunoscută pot fi desemnate prin elementele lor de identificare sau prin calitatea lor, iar locurile sau vehiculele pot fi desemnate prin referire la persoanele care fac obiectul cererii.

[…]”

36 Potrivit articolului L. 821-3 primul paragraf din CSI:

„Cererea este comunicată președintelui sau, în lipsa acestuia, unuia dintre membrii Comisiei Naționale de Control al Tehnicilor de Informare dintre cei menționați la punctele 2 și 3 ale articolului L. 831-1, care emite un aviz pentru prim-ministru în termen de 24 de ore. În cazul în care cererea este examinată de completul restrâns sau de plenul comisiei, prim-ministrul este informat fără întârziere cu privire la aceasta, iar avizul este emis în termen de 72 de ore.”

37 Articolul L. 821-4 din CSI prevede:

„Autorizația de punere în aplicare a tehnicilor menționate în capitolele I-IV din titlul V din prezenta carte este eliberată de prim-ministru pentru o durată maximă de patru luni. […] Autorizația cuprinde motivele și mențiunile prevăzute la punctele 1-6 ale articolului L. 821-2. Orice autorizație poate fi reînnoită în aceleași condiții cu cele prevăzute în prezentul capitol.

În cazul în care autorizația este acordată în urma unui aviz nefavorabil al Comisiei Naționale de Control al Tehnicilor de Informare, aceasta indică motivele pentru care avizul respectiv nu a fost luat în considerare.

[…]”

38 Articolul L. 833-4 din CSI, care figurează în capitolul III din acest titlu, prevede:

„Din proprie inițiativă sau atunci când este sesizată cu o reclamație din partea oricărei persoane care dorește să verifice că nicio tehnică de informare nu este pusă în aplicare în mod nelegal în privința sa, comisia controlează tehnica sau tehnicile invocate pentru a verifica dacă acestea au fost sau sunt puse în aplicare cu respectarea prezentei cărți. Ea notifică autorului reclamației faptul că au fost efectuate verificările necesare, fără a confirma sau infirma punerea lor în aplicare.”

39 Articolul L. 841-1 primul și al doilea paragraf din CSI are următorul cuprins:

„Sub rezerva dispozițiilor speciale prevăzute la articolul L. 854-9 din prezentul cod, Conseil d’État [(Consiliul de Stat)] este competent să soluționeze, în condițiile prevăzute în capitolul III bis din titlul VII al cărții VII din Codul de procedură administrativă, cererile privind punerea în aplicare a tehnicilor de informare menționate în titlul V din prezenta carte.

Acesta poate fi sesizat de:

1. Orice persoană care dorește să verifice că nicio tehnică de informare nu este pusă în aplicare în mod nelegal în privința sa și care dovedește punerea în aplicare prealabilă a procedurii prevăzute la articolul L. 833-4;

2. Comisia Națională de Control al Tehnicilor de Informare, în condițiile prevăzute la articolul L. 833-8.”

40 Titlul V din cartea VIII din partea legislativă a CSI, referitor la „tehnicile de colectare de informații supuse autorizării”, cuprinde printre altele capitolul I, intitulat „Accesul administrativ la datele de conectare”, care conține articolele L. 851-1-L. 851-7 din CSI.

41 Articolul L. 851-1 din CSI prevede:

„În condițiile prevăzute în capitolul 1 din titlul II din prezenta carte, se poate autoriza colectarea, de la operatorii de comunicații electronice și de la persoanele menționate la articolul L. 34-1 din [CPCE], precum și de la persoanele menționate la articolul 6 alineatul I punctele 1 și 2 din loi nº 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique [(Legea nr. 2004-575 din 21 iunie 2004 privind încrederea în economia informațională) (JORF din 22 iunie 2004, p. 11168)], de informații sau documente prelucrate sau stocate prin rețelele lor sau prin serviciile lor de comunicații electronice, inclusiv de date tehnice referitoare la identificarea numerelor de abonament sau de conectare la serviciile de comunicații electronice, la inventarul numerelor de abonament sau de conectare ale unei persoane desemnate, la localizarea echipamentelor terminale utilizate, precum și la comunicațiile unui abonat privind lista numerelor apelate și apelante, durata și data comunicațiilor.

Prin derogare de la articolul L. 821-2, cererile scrise și motivate privind datele tehnice referitoare la identificarea numerelor de abonament sau de conectare la servicii de comunicații electronice sau la inventarul tuturor numerelor de abonament sau de conectare ale unei persoane desemnate sunt transmise direct Comisiei Naționale de Control al Tehnicilor de Informare de către agenții desemnați individual și abilitați ai serviciilor de informații menționate la articolele L. 811-2 și L. 811-4. Comisia își dă avizul în condițiile prevăzute la articolul L. 821-3.

Un serviciu al prim-ministrului este însărcinat cu colectarea informațiilor sau a documentelor de la operatorii și de la persoanele menționate la primul paragraf al prezentului articol. Comisia Națională de Control al Tehnicilor de Informare dispune de un acces permanent, complet, direct și imediat la informațiile sau la documentele colectate.

Modalitățile de aplicare a prezentului articol sunt stabilite prin decret al Conseil d'État [(Consiliul de Stat)], adoptat în urma avizului Commission nationale de l'informatique et des libertés [(Comisia Națională pentru Tehnologia Informației și Libertăți)] și al Comisiei Naționale de Control al Tehnicilor de Informare."

42 Articolul L. 851-2 din CSI prevede:

„I. – În condițiile prevăzute în capitolul I din titlul II din prezenta carte și exclusiv în scopul prevenirii terorismului, poate fi autorizată în mod individual colectarea în timp real, în rețelele operatorilor și ale persoanelor menționate la articolul L. 851-1, a informațiilor sau a documentelor menționate la același articol L. 851-1 referitoare la o persoană identificată în prealabil ca fiind susceptibilă să aibă legătură cu o amenințare. În cazul în care există motive întemeiate pentru a se crede că una sau mai multe persoane care aparțin anturajului persoanei vizate de autorizație pot furniza informații în legătură cu scopul care justifică autorizația, aceasta poate fi de asemenea acordată individual pentru fiecare dintre aceste persoane.

I bis. Numărul maxim de autorizații eliberate în temeiul prezentului articol în vigoare simultan este stabilit de prim-ministru, în urma avizului Comisiei Naționale de Control al Tehnicilor de Informare. Decizia de stabilire a acestui contingent și repartizarea sa între miniștrii menționați la primul paragraf al articolului L. 821-2, precum și numărul de autorizații de interceptare eliberate sunt comunicate comisiei.

[…]"

43 Articolul L. 851-3 din CSI prevede:

„I. – În condițiile prevăzute în capitolul I din titlul II din prezenta carte și exclusiv în scopul prevenirii terorismului, operatorii și persoanele menționate la articolul L. 851-1 pot fi obligate să efectueze în rețelele lor prelucrări automatizate destinate, în funcție de parametrii precizați în autorizație, să detecteze conexiuni care pot indica o amenințare teroristă.

Aceste prelucrări automatizate utilizează exclusiv informațiile sau documentele menționate la articolul L. 851-1, fără a colecta alte date decât cele care corespund parametrilor în care au fost concepute și fără a permite identificarea persoanelor la care se referă informațiile sau documentele.

Cu respectarea principiului proporționalității, autorizația acordată de prim-ministru precizează domeniul tehnic al punerii în aplicare a acestor prelucrări.

II. – Comisia Națională de Control al Tehnicilor de Informare emite un aviz cu privire la cererea de autorizare referitoare la prelucrările automatizate și la parametrii de detectare reținuți. Aceasta dispune de acces permanent, complet și direct la aceste prelucrări, precum și la informațiile și la datele colectate. Ea este informată cu privire la orice modificare adusă prelucrărilor și parametrilor și poate emite recomandări.

Prima autorizație de punere în aplicare a prelucrărilor automatizate prevăzută la alineatul I al prezentului articol este eliberată pentru o durată de două luni. Autorizația poate fi reînnoită în condițiile referitoare la durată prevăzute în capitolul I din titlul II din prezenta carte. Cererea de reînnoire cuprinde o listă cu elementele de identificare semnalate prin prelucrarea automatizată și o analiză a relevanței acestor semnalări.

III. – Condițiile prevăzute la articolul L. 871-6 sunt aplicabile operațiunilor materiale efectuate pentru această punere în aplicare de către operatorii și persoanele menționate la articolul L. 851-1.

IV. – Atunci când prelucrările menționate la alineatul I al prezentului articol detectează date care pot caracteriza existența unei amenințări cu caracter terorist, prim-ministrul sau una dintre persoanele delegate de acesta poate autoriza, în urma avizului Comisiei Naționale de Control al Tehnicilor de Informare dat în condițiile prevăzute în capitolul I din titlul II din prezenta carte, identificarea persoanei sau a persoanelor vizate și colectarea datelor referitoare la acestea. Datele respective sunt exploatate în termen de 60 de zile de la această colectare și sunt distruse la expirarea acestui termen, sub rezerva unor elemente serioase care confirmă existența unei amenințări teroriste din partea uneia sau a mai multe dintre persoanele vizate.

[…]”

44 Articolul L. 851-4 din CSI are următorul cuprins:

„În condițiile prevăzute în capitolul I din titlul II din prezenta carte, datele tehnice referitoare la localizarea echipamentelor terminale utilizate menționate la articolul L. 851-1 pot fi colectate la solicitarea rețelei și transmise în timp real de către operatori unui serviciu al prim-ministrului.”

45 Articolul L. 851-5 din CSI, care figurează în partea normativă a acestui cod, prevede:

„I. – Informațiile sau documentele menționate la articolul L. 851-1 sunt, cu excepția conținutului corespondenței schimbate sau al informațiilor consultate:

1. Cele enumerate la articolele R. 10-13 și R. 10-14 din [CPCE] și la articolul 1 din Decretul [nr. 2011-219];

2. Datele tehnice, altele decât cele menționate la punctul 1:

a) Care permit localizarea echipamentelor terminale;

b) Referitoare la accesul echipamentelor terminale la rețelele sau la serviciile de comunicații publice online;

c) Referitoare la efectuarea comunicațiilor electronice prin rețele;

d) Referitoare la identificarea și la autentificarea unui utilizator, a unei conexiuni, a unei rețele sau a unui serviciu de comunicații publice online;

e) Referitoare la caracteristicile echipamentelor terminale și la datele de configurare a software-ului lor.

II. – Numai informațiile și documentele menționate la alineatul I punctul 1 pot fi colectate în temeiul articolului L. 851-1. Această colectare are loc decalat.

Informațiile enumerate la alineatul I punctul 2 nu pot fi colectate decât în temeiul articolelor L. 851-2 și L. 851-3 în condițiile și cu limitele prevăzute de aceste articole și sub rezerva aplicării articolului L. 851-9.”

CPCE

46 Articolul L. 34-1 din CPCE prevede:

„I. – Prezentul articol se aplică prelucrării datelor cu caracter personal în contextul furnizării către public de servicii de comunicații electronice; în special, acesta se aplică rețelelor care permit accesul dispozitivelor de colectare a datelor și de identificare.

II. – Operatorii de comunicații electronice și în special persoanele a căror activitate constă în a oferi acces la serviciile de comunicații publice online trebuie să șteargă sau să anonimizeze toate datele de transfer, sub rezerva dispozițiilor alineatelor III, IV, V și VI.

Persoanele care furnizează publicului servicii de comunicații electronice stabilesc, în conformitate cu dispozițiile alineatului anterior, proceduri interne pentru soluționarea cererilor autorităților competente.

Persoanele care, în cadrul unei activități profesionale principale sau accesorii, oferă publicului o conexiune care permite o comunicare online prin intermediul accesului la rețea, inclusiv cu titlu gratuit, sunt obligate să respecte dispozițiile aplicabile operatorilor de comunicații electronice în conformitate cu prezentul articol.

III. – În vederea investigării, a constatării și a urmăririi penale a infracțiunilor sau a neîndeplinirii obligației definite la articolul L. 336-3 din code de la propriété intellectuelle [(Codul proprietății intelectuale)] sau în scopul prevenirii atacurilor asupra sistemelor de prelucrare automatizată a datelor prevăzute și pedepsite la articolele 323-1-323-3-1 din code pénal [(Codul penal)] și cu unicul scop de a permite, dacă este necesar, furnizarea către autoritatea judiciară sau către înalta autoritate menționată la articolul L. 331-12 din Codul proprietății intelectuale sau către autoritatea națională pentru securitatea sistemelor informative menționată la articolul L. 2321-1 din code de la défense [(Codul privind apărarea)], operațiunile care vizează eliminarea sau anonimizarea anumitor categorii de date tehnice pot fi amânate pentru o perioadă maximă de un an. Prin decret adoptat de Conseil d’État [(Consiliul de Stat)] în urma avizului Commission nationale de l’informatique et des libertés ([Comisia Națională pentru Tehnologia Informației și Libertăți)], se stabilesc, în limitele indicate la alineatul VI, categoriile de date respective și durata stocării acestora, în funcție de activitatea operatorilor și de natura comunicațiilor, precum și modalitățile de compensare, dacă este cazul, a costurilor suplimentare identificabile și specifice ale prestațiilor asigurate în acest temei, la cererea statului, de către operatori.

[…]

VI. – Datele stocate și prelucrate în condițiile stabilite la alineatele III, IV și V se referă exclusiv la identificarea persoanelor care utilizează serviciile furnizate de operatori, la caracteristicile tehnice ale comunicațiilor asigurate de aceștia din urmă și la localizarea echipamentelor terminale.

Datele respective nu se pot referi în niciun caz la conținutul corespondenței schimbate sau al informațiilor consultate, în orice formă, în cadrul acestor comunicații.

Stocarea și prelucrarea acestor date se efectuează în conformitate cu dispozițiile loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [(Legea nr. 78-17 din 6 ianuarie 1978 privind informatica, fișierele electronice și libertățile)].

Operatorii adoptă toate măsurile necesare pentru a împiedica o utilizare a datelor respective în alte scopuri decât cele prevăzute la prezentul articol."

47 Articolul R. 10-13 din CPCE are următorul cuprins:

„I. – În temeiul alineatului III al articolului L. 34-1, operatorii de comunicații electronice stochează, în scopul investigării, al constatării și al urmăririi penale a infracțiunilor:

a) informațiile care permit identificarea utilizatorului;

b) datele privind echipamentele terminale de comunicații utilizate;

c) caracteristicile tehnice, precum și data, ora și durata fiecărei comunicații;

d) datele referitoare la serviciile suplimentare solicitate sau utilizate și la furnizorii lor;

e) datele care permit identificarea destinatarului sau a destinatarilor comunicației.

II. – În cazul activităților de telefonie, operatorul stochează datele menționate la alineatul II și, în plus, pe cele care permit identificarea originii și a localizării comunicației.

III. – Perioada de stocare a datelor menționate la prezentul articol este de un an de la data înregistrării.

IV. – Costurile suplimentare identificabile și specifice suportate de operatorii cărora autoritățile judiciare le-au solicitat furnizarea de date din categoriile menționate la prezentul articol sunt compensate conform modalităților prevăzute la articolul R. 213-1 din Codul de procedură penală."

48 Articolul R. 10-14 din CPCE prevede:

„I. – În temeiul articolului L. 34-1 alineatul IV, operatorii de comunicații electronice sunt autorizați să stocheze, în scopul operațiunilor lor de facturare și de plată, datele cu caracter tehnic care permit identificarea utilizatorului, precum și a celor menționate la articolul R. 10-13 alineatul I literele b), c) și d).

II. – În cazul activităților de telefonie, operatorii pot stoca, pe lângă datele menționate la alineatul I, datele cu caracter tehnic referitoare la localizarea comunicației și la identificarea destinatarului sau a destinatarilor comunicației, precum și datele care permit facturarea.

III. – Datele menționate la alineatele I și II ale prezentului articol nu pot fi stocate decât în cazul în care sunt necesare pentru facturarea și pentru plata serviciilor furnizate. Stocarea lor trebuie să se limiteze la perioada strict necesară în acest scop, fără a depăși un an.

IV. – Pentru securitatea rețelelor și a instalațiilor, operatorii pot stoca, pentru o perioadă de cel mult trei luni:

a) datele care permit identificarea originii comunicației;

b) caracteristicile tehnice, precum și data, ora și durata fiecărei comunicații;

c) datele cu caracter tehnic care permit identificarea destinatarului sau a destinatarilor comunicației;

d) datele referitoare la serviciile suplimentare solicitate sau utilizate și la furnizorii lor.”

Legea nr. 2004-575 din 21 iunie 2004 privind încrederea în economia informațională

49 Articolul 6 din Legea nr. 2004-575 din 21 iunie 2004 privind încrederea în economia informațională (JORF din 22 iunie 2004, p. 11168, denumită în continuare „LCEN”) prevede:

„I. – 1. Persoanele a căror activitate constă în furnizarea accesului la servicii de comunicații publice online își informează abonații cu privire la existența unor mijloace tehnice care permit restrângerea accesului la anumite servicii sau selectarea acestora și le propun cel puțin unul dintre aceste mijloace.

[…]

2. Răspunderea civilă a persoanelor fizice sau juridice care asigură, inclusiv cu titlu gratuit, pentru punerea la dispoziția publicului prin servicii de comunicații publice online, stocarea de semnale, de texte, de imagini, de sunete sau de mesaje de orice natură furnizate de destinatarii acestor servicii nu poate fi angajată ca urmare a activităților sau a informațiilor stocate la cererea unui destinatar al acestor servicii dacă nu au avut cunoștință în mod efectiv de caracterul lor ilicit sau de fapte și împrejurări din care să rezulte acest caracter sau dacă, din momentul în care au avut cunoștință de acesta, au acționat cu promptitudine pentru a înlătura datele respective sau pentru a bloca accesul la ele.

[…]

II. – Persoanele menționate la alineatul I punctele 1 și 2 dețin și stochează datele de natură să permită identificarea oricărei persoane care a contribuit la crearea conținutului sau a unuia dintre conținuturile serviciilor pe care le furnizează.

Acestea furnizează persoanelor care editează un serviciu de comunicare publică online mijloace tehnice care le permit să îndeplinească condițiile de identificare prevăzute la alineatul III.

Autoritatea judiciară poate solicita furnizorilor menționați la alineatul I punctele 1 și 2 să comunice datele menționate la primul paragraf.

Dispozițiile articolelor 226-17, 226-21 și 226-22 din Codul penal se aplică prelucrării acestor date.

Printr-un decret al Conseil d’État [(Consiliul de Stat)], adoptat după obținerea avizului Comisiei Naționale pentru Tehnologia Informației și Libertăți, se definesc datele menționate la primul paragraf și se determină durata și modalitățile de stocare a acestora.

[…]”

Decretul nr. 2011-219

50 Capitolul I din Decretul nr. 2011-219, adoptat în temeiul articolului 6 alineatul II ultimul paragraf din LCEN, cuprinde articolele 1-4 din acest decret.

51 Articolul 1 din Decretul nr. 2011-219 prevede:

„Datele menționate la articolul 6 alineatul II din [LCEN], pe care persoanele sunt obligate să le stocheze în temeiul acestei dispoziții, sunt următoarele:

1. Pentru persoanele menționate la alineatul I punctul 1 al aceluiași articol și pentru fiecare conectare a abonaților lor:

a) identificatorul conexiunii;

b) identificatorul atribuit de aceste persoane abonatului;

c) identificatorul terminalului utilizat pentru conectare, atunci când au acces la acesta;

d) data și ora inițierii și a încheierii conexiunii;

e) caracteristicile liniei abonatului;

2. Pentru persoanele menționate la alineatul I punctul 2 al aceluiași articol și pentru fiecare operațiune de creare:

a) identificatorul conexiunii aflate la originea comunicației;

b) identificatorul atribuit de sistemul informațional conținutului care face obiectul operațiunii;

c) tipurile de protocoale utilizate pentru conectarea la serviciu și pentru transferul de conținuturi;

d) natura operațiunii;

e) data și ora operațiunii;

f) identificatorul utilizat de autorul operațiunii, atunci când acesta l-a furnizat;

3. Pentru persoanele menționate la alineatul I punctele 1 și 2 ale aceluiași articol, informațiile furnizate de un utilizator cu ocazia încheierii unui contract sau a creării unui cont:

a) la momentul creării contului, identificatorul acestei conexiuni;

b) numele și prenumele sau denumirea comercială;

c) adresele poștale asociate;

d) pseudonimele folosite;

e) adresele de e-mail sau de cont asociate;

f) numerele de telefon;

g) parola, precum și datele care permit verificarea sau modificarea acesteia, în ultima versiune actualizată;

4. Pentru persoanele menționate la alineatul I punctele 1 și 2 ale aceluiași articol, în cazul în care contractul încheiat sau contul creat implică plăți, următoarele informații referitoare la plată, pentru fiecare operațiune de plată:

a) tipul de plată utilizat;

b) referința plății;

c) suma;

d) data și ora tranzacției.

Datele menționate la punctele 3 și 4 nu trebuie stocate decât în măsura în care persoanele le colectează în mod obișnuit."

52 Articolul 2 din acest decret are următorul cuprins:

„Contribuția la crearea de conținut include operațiunile cu privire la:

a) crearea inițială a conținuturilor;

b) modificări ale conținuturilor și ale datelor aferente conținuturilor;

c) ștergerea conținuturilor."

53 Articolul 3 din decretul menționat prevede:

„Perioada de stocare a datelor menționate la articolul 1 este de un an:

a) în ceea ce privește datele menționate la punctele 1 și 2, începând din ziua creării conținuturilor pentru fiecare operațiune care contribuie la crearea unui conținut, astfel cum este definită la articolul 2;

b) în ceea ce privește datele menționate la punctul 3, începând din ziua rezilierii contractului sau a închiderii contului;

c) în ceea ce privește datele menționate la punctul 4, începând din ziua emiterii facturii sau a operațiunii de plată, pentru fiecare factură sau operațiune de plată."

Dreptul belgian

54 Legea din 29 mai 2016 a modificat printre altele loi du 13 juin 2005 relative aux communications électroniques (Legea din 13 iunie 2005 privind comunicațiile electronice) (*Moniteur belge* din 20 iunie 2005, p. 28070, denumită în continuare „Legea din 13 iunie 2005"), code d'instruction criminelle (Codul de procedură penală) și loi du 30 novembre 1998 organique des services de renseignement et de sécurité (Legea organică din 30 noiembrie 1998 privind serviciile de informații și de securitate) (*Moniteur belge* din 18 decembrie 1998, p. 40312, denumită în continuare „Legea din 30 noiembrie 1998").

55 Articolul 126 din Legea din 13 iunie 2005, în versiunea rezultată din Legea din 29 mai 2016, prevede:

„(1) Fără a aduce atingere loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel [Legea din 8 decembrie 1992 privind protecția vieții private în ceea ce privește prelucrarea datelor cu caracter personal], furnizorii de servicii publice de telefonie, inclusiv prin internet, de acces la internet, de mesagerie electronică prin internet, operatorii care furnizează rețele publice de comunicații electronice, precum și operatorii care furnizează unul dintre aceste servicii stochează datele prevăzute la alineatul (3), care sunt generate sau prelucrate de ei în cadrul furnizării serviciilor de comunicații în cauză.

Prezentul articol nu privește conținutul comunicațiilor.

Obligația de stocare a datelor menționate la alineatul (3) se aplică și în cazul apelurilor fără răspuns, în măsura în care aceste date, în cadrul furnizării serviciilor de comunicații în cauză:

1. în ceea ce privește datele de telefonie, sunt generate sau prelucrate de operatorii de servicii publice de comunicații electronice sau ai unei rețele publice de comunicații electronice sau

2. în ceea ce privește datele de internet, sunt înregistrate în jurnal electronic de acești furnizori.

(2) Numai următoarele autorități pot obține, pe baza unei simple cereri, de la furnizorii și de la operatorii menționați la alineatul (1) primul paragraf, date stocate în temeiul prezentului articol, în scopurile și în condițiile enumerate mai jos:

1. autoritățile judiciare, în vederea investigării, a instrucției și a urmăririi penale a infracțiunilor, pentru executarea măsurilor prevăzute la articolele 46a și 88a din Codul de procedură penală și în condițiile prevăzute la aceste articole;

2. serviciile de informații și de securitate, pentru a îndeplini misiuni de informare prin recurgerea la metodele de colectare a datelor prevăzute la articolele 16/2, 18/7 și 18/8 din Legea organică din 30 noiembrie 1998 privind serviciile de informații și de securitate și în condițiile stabilite prin această lege;

3. orice ofițer de poliție judiciară din cadrul [Institut belge des services postaux et des télécommunications (Institutul belgian al Serviciilor Poștale și al Telecomunicațiilor)] în vederea investigării, a instrucției și a urmăririi penale a infracțiunilor prevăzute la articolele 114 și 124 și la prezentul articol;

4. serviciile de urgență care oferă asistență la fața locului, atunci când, în urma unui apel de urgență, acestea nu obțin de la furnizorul sau de la operatorul respectiv datele de identificare a apelantului cu ajutorul bazei de date menționate la articolul 107 alineatul 2 al treilea paragraf sau obțin date incomplete sau incorecte. Numai datele de identificare a apelantului pot fi solicitate și în cel mult 24 de ore de la efectuarea apelului;

5. ofițerul de poliție judiciară al Unității pentru persoane dispărute a Poliției Federale, în cadrul misiunii sale de asistență pentru persoanele aflate în pericol, de căutare a persoanelor a căror dispariție este suspectă și atunci când există prezumții sau indicii temeinice că integritatea fizică a persoanei dispărute este în pericol iminent. Numai datele prevăzute la alineatul (3) primul și al doilea paragraf referitoare la persoana dispărută și stocate în cursul celor 48 de ore anterioare cererii de obținere a datelor pot fi solicitate operatorului sau furnizorului în cauză prin intermediul unui serviciu de poliție desemnat de Rege;

6. Serviciul de mediere pentru telecomunicații, în vederea identificării persoanei care a utilizat cu rea-credință o rețea sau un serviciu de comunicații electronice, în conformitate cu condițiile prevăzute la articolul 43a alineatul 3 punctul 7 din loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques [(Legea din 21 martie 1991 privind reforma anumitor întreprinderi publice economice)]. Numai datele de identificare pot fi solicitate.

Furnizorii și operatorii menționați la alineatul (1) primul paragraf acționează astfel încât datele prevăzute la alineatul (3) să fie accesibile în mod nelimitat din Belgia, iar aceste date și orice alte informații necesare privind aceste date să poată fi transmise fără întârziere și numai autorităților menționate la prezentul alineat.

Fără a aduce atingere altor dispoziții legale, furnizorii și operatorii menționați la alineatul (1) primul paragraf nu pot utiliza datele stocate în temeiul alineatului (3) în alte scopuri.

(3) Datele care vizează să identifice utilizatorul sau abonatul și mijloacele de comunicare, cu excluderea datelor prevăzute în mod specific la al doilea și la al treilea paragraf, sunt stocate timp de 12 luni de la data la care o comunicație este posibilă pentru ultima oară prin intermediul serviciului utilizat.

Datele referitoare la accesul și la conectarea echipamentului terminal la rețea și la serviciu, precum și la localizarea acestui echipament, inclusiv punctul terminal al rețelei, sunt stocate timp de 12 luni de la data comunicației.

Datele de comunicație, cu excluderea conținutului, inclusiv a originii și a destinației lor, sunt stocate timp de 12 luni de la data comunicației.

Regele stabilește, prin decret adoptat în cadrul Conseil des ministres [(Consiliul de Miniștri)], la propunerea ministrului justiției și a ministrului [competent în domeniul comunicațiilor electronice] și în urma avizului Comisiei pentru protecția vieții private și al Institutului, datele care trebuie stocate pe tipuri de categorii prevăzute la primul-al treilea paragraf, precum și cerințele pe care trebuie să le îndeplinească aceste date.

[…]”

Litigiile principale și întrebările preliminare

Cauza C-511/18

56 Prin cererile introductive formulate la 30 noiembrie 2015 și la 16 martie 2016, conexate în procedura principală, La Quadrature du Net, French Data Network și Fédération des fournisseurs d’accès à Internet associatifs, precum și Igwan.net au sesizat Conseil d’État (Consiliul de Stat, Franța) cu acțiuni având ca obiect anularea Decretelor nr. 2015-1185, 2015-1211, 2015-1639 și 2016-67, pentru motivul, printre altele, că acestea ar încălca Constituția franceză, Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale (denumită în continuare „CEDO”), precum și Directivele 2000/31 și 2002/58, interpretate în lumina articolelor 7, 8 și 47 din cartă.

57 În ceea ce privește în special motivele întemeiate pe nerespectarea Directivei 2000/31, instanța de trimitere arată că dispozițiile articolului L. 851-3 din CSI impun operatorilor de comunicații electronice și furnizorilor tehnici „să efectueze în rețelele lor prelucrări automatizate destinate, în funcție de parametrii stabiliți în autorizație, să detecteze conexiuni care pot indica o amenințare teroristă”. Această tehnică ar urmări să colecteze numai pentru o perioadă limitată, dintre toate datele

de conectare prelucrate de acești operatori și de acești furnizori, acele date care ar putea prezenta o legătură cu o asemenea infracțiune gravă. În aceste condiții, dispozițiile menționate, care nu ar impune o obligație generală de supraveghere activă, nu ar încălca articolul 15 din Directiva 2000/31.

58 În ceea ce privește motivele întemeiate pe încălcarea Directivei 2002/58, instanța de trimitere consideră că rezultă în special din dispozițiile acestei directive, precum și din Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, denumită în continuare „Hotărârea Tele2”, EU:C:2016:970), că dispozițiile naționale care impun obligații furnizorilor de servicii de comunicații electronice, precum stocarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare ale utilizatorilor și abonaților lor, în scopurile menționate la articolul 15 alineatul (1) din directiva menționată, printre care figurează protejarea securității naționale, a apărării și a siguranței publice, intră în domeniul de aplicare al aceleiași directive, întrucât aceste norme reglementează activitatea furnizorilor amintiți. Situația ar fi aceeași în ceea ce privește normele care reglementează accesul autorităților naționale la date, precum și utilizarea acestora.

59 Instanța de trimitere deduce de aici că intră în domeniul de aplicare al Directivei 2002/58 atât obligația de stocare care rezultă din articolul L. 851-1 din CSI, cât și accesul administrativ la datele menționate, inclusiv la cele în timp real, prevăzute la articolele L. 851-1, L. 851-2 și L. 851-4 din codul menționat. Potrivit acestei instanțe, situația este aceeași în ceea ce privește dispozițiile articolului L. 851-3 din același cod, care, deși nu impun operatorilor în cauză o obligație generală de stocare, le impun totuși să pună în aplicare în rețelele lor prelucrări automatizate destinate să detecteze conexiuni care pot indica o amenințare teroristă.

60 În schimb, această instanță consideră că nu intră în domeniul de aplicare al Directivei 2002/58 dispozițiile CSI vizate de cererile de anulare care privesc tehnicile de colectare a informațiilor aplicate în mod direct de stat, dar care nu reglementează activitățile furnizorilor de servicii de comunicații electronice prin impunerea unor obligații specifice în sarcina acestora. Prin urmare, nu se poate considera că dispozițiile respective pun în aplicare dreptul Uniunii, astfel încât motivele întemeiate pe nerespectarea de către acestea a Directivei 2002/58 nu ar putea fi invocate în mod util.

61 Astfel, pentru a soluționa litigiile privind legalitatea Decretelor nr. 2015-1185, 2015-1211, 2015-1639 și 2016-67 în raport cu Directiva 2002/58, în măsura în care acestea au fost adoptate pentru punerea în aplicare a articolelor L. 851-1-L. 851-4 din CSI, s-ar ridica trei probleme de interpretare a dreptului Uniunii.

62 În ceea ce privește interpretarea articolului 15 alineatul (1) din Directiva 2002/58, instanța de trimitere ridică, în primul rând, problema dacă o obligație de stocare generalizată și nediferențiată impusă furnizorilor de servicii de comunicații electronice în temeiul articolelor L. 851-1 și R. 851-5 din CSI trebuie să fie considerată, în special având în vedere garanțiile și controalele care însoțesc accesul administrativ la datele de conectare și utilizarea acestora, o ingerință justificată de dreptul la siguranță garantat la articolul 6 din cartă și de cerințele securității naționale, a cărei responsabilitate revine numai statelor membre, în temeiul articolului 4 TUE.

63 În ceea ce privește, în al doilea rând, celelalte obligații care pot fi impuse furnizorilor de servicii de comunicații electronice, instanța de trimitere arată că dispozițiile articolului L. 851-2 din CSI autorizează, exclusiv în scopul prevenirii terorismului, colectarea informațiilor sau a documentelor prevăzute la articolul L. 851-1 din acest cod de la aceleași persoane. Această colectare, care nu ar privi decât unul sau mai mulți indivizi identificați în prealabil ca fiind susceptibili să aibă legătură cu o amenințare teroristă, ar avea loc în timp real. Situația ar fi aceeași în ceea ce privește dispozițiile articolului L. 851-4 din codul menționat, care autorizează transmiterea în timp real de către operatori numai a datelor tehnice referitoare la localizarea echipamentelor terminale. Aceste tehnici ar reglementa, în funcție de scopuri și modalități diferite, accesul administrativ în timp real la datele stocate în temeiul CPCE și al LCEN, fără a impune însă furnizorilor în cauză o obligație de stocare

suplimentară față de ceea ce ar fi necesar pentru facturarea și furnizarea serviciilor lor. De asemenea, nici dispozițiile articolului L. 851-3 din CSI, care prevăd obligația furnizorilor de servicii de a efectua în rețelele lor o analiză automatizată a conexiunilor, nu ar implica o stocare generalizată și nediferențiată.

64 Or, pe de o parte, instanța de trimitere consideră că atât stocarea generalizată și nediferențiată, cât și accesul în timp real la datele de conectare prezintă, într-un context marcat de amenințări grave și persistente la adresa securității naționale, care țin în special de riscul terorist, o utilitate operațională fără echivalent. Astfel, stocarea generalizată și nediferențiată ar permite serviciilor de informații să aibă acces la datele referitoare la comunicații înainte de a fi identificate motivele pentru a se considera că persoana în cauză prezintă o amenințare pentru siguranța publică, pentru apărarea sau pentru siguranța statului. În plus, accesul în timp real la datele de conectare ar permite să se urmărească, cu o reactivitate puternică, comportamentele indivizilor care pot reprezenta o amenințare imediată pentru ordinea publică.

65 Pe de altă parte, tehnica prevăzută la articolul L. 851-3 din CSI ar permite să fie detectați, în temeiul unor criterii precis definite în acest scop, indivizii ale căror comportamente pot să indice, ținând seama de modurile lor de comunicare, o amenințare teroristă.

66 În al treilea rând, în ceea ce privește accesul autorităților competente la datele stocate, instanța de trimitere ridică problema dacă Directiva 2002/58, citită în lumina cartei, trebuie să fie interpretată în sensul că condiționează în toate cazurile legalitatea procedurilor de colectare a datelor de conectare de o cerință de informare a persoanelor vizate atunci când o asemenea informare nu mai poate compromite anchetele desfășurate de autoritățile competente sau dacă astfel de proceduri pot fi considerate legale ținând seama de ansamblul celorlalte garanții procedurale prevăzute de dreptul intern, atunci când acestea asigură efectivitatea dreptului la o cale de atac.

67 În ceea ce privește aceste alte garanții procedurale, instanța de trimitere precizează printre altele că orice persoană care dorește să verifice că nicio tehnică de informare nu este pusă în aplicare în mod nelegal în privința sa poate sesiza un complet specializat al Conseil d'État (Consiliul de Stat), căruia îi revine sarcina de a verifica, având în vedere elementele care îi sunt comunicate în afara procedurii contradictorii, dacă reclamantul a făcut obiectul unei tehnici și dacă aceasta a fost pusă în aplicare în conformitate cu cartea VIII din CSI. Competențele cu care ar fi învestit acest complet pentru a examina cererile ar garanta efectivitatea controlului jurisdicțional pe care îl exercită. Astfel, acesta ar fi competent să examineze cererile, să invoce din oficiu toate nelegalitățile pe care le constată și să oblige administrația să adopte toate măsurile utile pentru a remedia nelegalitățile constatate. În plus, Comisiei Naționale de Control al Tehnicilor de Informare i-ar reveni sarcina de a verifica dacă tehnicile de colectare de informații sunt puse în aplicare, pe teritoriul național, în conformitate cu cerințele care decurg din CSI. Astfel, împrejurarea că dispozițiile legislative în discuție în litigiul principal nu prevăd notificarea persoanelor vizate cu privire la măsurile de supraveghere al căror obiect l-au făcut nu ar constitui, în sine, o atingere excesivă adusă dreptului la respectarea vieții private.

68 În aceste condiții, Conseil d'État (Consiliul de Stat) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„1) Obligația de păstrare generalizată și nediferențiată, impusă furnizorilor în temeiul dispozițiilor permisive ale articolului 15 alineatul (1) din Directiva [2002/58], trebuie să fie considerată, într-un context marcat de amenințări grave și persistente la adresa siguranței naționale și în special de riscul terorismului, o ingerință justificată de dreptul la siguranță garantat la articolul 6 din [cartă] și de cerințele privind securitatea națională, care rămâne responsabilitatea exclusivă a statelor membre în temeiul articolului 4 [TUE]?

2) Directiva [2002/58], citită în lumina [cartei], trebuie interpretată în sensul că autorizează măsuri legislative, precum măsurile de colectare în timp real a datelor de transfer și a datelor de localizare ale unor persoane determinate, care, deși afectează drepturile și obligațiile furnizorilor unui serviciu de comunicații electronice, nu le impun totuși o obligație specifică de păstrare a datelor acestora?

3) Directiva [2002/58], citită în lumina [cartei], trebuie interpretată în sensul că condiționează în toate cazurile legalitatea procedurilor de colectare a datelor de conectare de o cerință de informare a persoanelor vizate atunci când o asemenea informare nu mai poate compromite anchetele desfășurate de autoritățile competente sau astfel de proceduri pot fi considerate legale ținând seama de ansamblul celorlalte garanții procedurale existente, din moment ce acestea din urmă asigură efectivitatea dreptului la o cale de atac?”

Cauza C-512/18

69 Prin cererea introductivă formulată la 1 septembrie 2015, French Data Network, La Quadrature du Net și Fédération des fournisseurs d’accès à Internet associatifs au sesizat Conseil d’État (Consiliul de Stat) cu o acțiune în anularea deciziei implicite de respingere născute din tăcerea păstrată de prim-ministru cu privire la cererea lor de abrogare a articolului R. 10-13 din CPCE, precum și a Decretului nr. 2011-219, pentru motivul, printre altele, că aceste texte ar încălca articolul 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7, 8 și 11 din cartă. Cererile de intervenție în procedura principală formulate de Privacy International, precum și de Center for Democracy and Technology au fost admise.

70 În ceea ce privește articolul R. 10-13 din CPCE și obligația de stocare generalizată și nediferențiată a datelor referitoare la comunicații care este prevăzută la acesta, instanța de trimitere, care exprimă considerații similare celor emise în cadrul cauzei C-511/18, arată că o asemenea stocare permite autorității judiciare accesul la datele referitoare la comunicațiile pe care le-a efectuat o persoană înainte de a fi suspectată de săvârșirea unei infracțiuni, astfel încât această stocare prezintă o utilitate fără echivalent pentru cercetarea, constatarea și urmărirea penală a infracțiunilor.

71 În ceea ce privește Decretul nr. 2011-219, instanța de trimitere consideră că articolul 6 alineatul II din LCEN, care impune o obligație de deținere și de stocare exclusiv a datelor referitoare la crearea de conținut, nu intră în domeniul de aplicare al Directivei 2002/58, întrucât acesta este limitat, în conformitate cu articolul 3 alineatul (1) din directiva menționată, la furnizarea de servicii publice de comunicații electronice în rețelele publice de comunicații din Uniune, ci în domeniul de aplicare al Directivei 2000/31.

72 Această instanță apreciază însă că din articolul 15 alineatele (1) și (2) din Directiva 2000/31 reiese că aceasta nu instituie o interdicție de principiu de stocare a datelor referitoare la crearea de conținut, de la care s-ar putea deroga numai prin excepție. Astfel, s-ar pune problema dacă articolele 12, 14 și 15 din directiva menționată, citite în lumina articolelor 6-8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie să fie interpretate în sensul că permit unui stat membru să instituie o reglementare națională precum articolul 6 alineatul II din LCEN, care impune persoanelor vizate să stocheze datele de natură să permită identificarea oricărei persoane care a contribuit la crearea conținutului sau a unuia dintre conținuturile serviciilor pe care le prestează, pentru ca autoritatea judiciară să poată solicita, dacă este cazul, comunicarea acestora, în vederea asigurării respectării normelor privind răspunderea civilă sau penală.

73 În aceste condiții, Conseil d'État (Consiliul de Stat) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„1) Obligația de păstrare generalizată și nediferențiată, impusă furnizorilor în temeiul dispozițiilor permisive ale articolului 15 alineatul (1) din Directiva [2002/58], trebuie să fie considerată, în special având în vedere garanțiile și controlul de care sunt însoțite ulterior colectarea și utilizarea acestor date de conectare, o ingerință justificată de dreptul la siguranță garantat la articolul 6 din [cartă] și de cerințele privind securitatea națională, care rămâne responsabilitatea exclusivă a statelor membre în temeiul articolului 4 [TUE]?

2) Dispozițiile Directivei [2000/31], citite în lumina articolelor 6, 7, 8 și 11, precum și a articolului 52 alineatul (1) din [cartă], trebuie interpretate în sensul că permit unui stat să instituie o reglementare națională care impune atât persoanelor a căror activitate constă în a oferi publicului online accesul la servicii de comunicații, cât și persoanelor fizice sau juridice care asigură, chiar cu titlu gratuit, pentru punerea la dispoziția publicului prin servicii de comunicații publice online, stocarea de semnale, de texte, de imagini, de sunete sau de mesaje de orice natură furnizate de destinatari ai acestor servicii, să păstreze datele de natură să permită identificarea oricărei persoane care a contribuit la crearea conținutului sau a unuia dintre conținuturile serviciilor pe care le prestează, pentru ca autoritatea judiciară să poată solicita, dacă este cazul, comunicarea acestora, în vederea asigurării respectării normelor privind răspunderea civilă sau penală?"

Cauza C-520/18

74 Prin cererile introductive formulate la 10 ianuarie, 16 ianuarie, 17 ianuarie și 18 ianuarie 2017, conexate în cadrul procedurii principale, Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL și UA, Liga voor Mensenrechten ASBL și Ligue des droits de l'Homme ASBL, precum și VZ, WY și XX au sesizat Cour constitutionnelle (Curtea Constituțională, Belgia) cu acțiuni având ca obiect anularea Legii din 29 mai 2016, pentru motivul că aceasta ar încălca articolele 10 și 11 din Constituția belgiană coroborate cu articolele 5, 6-11, 14, 15, 17 și 18 din CEDO, cu articolele 7, 8, 11 și 47, precum și cu articolul 52 alineatul (1) din cartă, articolul 17 din Pactul internațional cu privire la drepturile civile și politice, adoptat de Adunarea Generală a Organizației Națiunilor Unite la 16 decembrie 1966 și intrat în vigoare la 23 martie 1976, principiile generale ale securității juridice, proporționalității și autodeterminării în materie de informare, precum și articolul 5 alineatul (4) TUE.

75 În susținerea acțiunilor lor, reclamanții din litigiul principal arată în esență că nelegalitatea Legii din 29 mai 2016 rezultă în special din faptul că aceasta depășește limitele strictului necesar și nu prevede garanții de protecție suficiente. În special, nici dispozițiile sale privind stocarea datelor, nici cele care reglementează accesul autorităților la datele stocate nu ar îndeplini cerințele care decurg din 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), și din Hotărârea din 21 decembrie 2016, Tele2 (C-203/15 și C-698/15, EU:C:2016:970). Astfel, aceste dispoziții ar implica riscul stabilirii unor profiluri de personalitate, cu posibilele abuzuri rezultate din acestea din partea autorităților competente, și nici nu ar prevedea un nivel adecvat de securizare și de protecție a datelor stocate. În sfârșit, această lege ar acoperi persoane supuse secretului profesional, precum și persoane care au o obligație de confidențialitate și ar privi date de comunicații sensibile, cu caracter personal, fără a cuprinde garanții speciale în scopul protecției acestor din urmă date.

76 Instanța de trimitere arată că datele pe care trebuie să le stocheze furnizorii de servicii de telefonie, inclusiv prin internet, de acces la internet și de e-mail prin internet, precum și operatorii care furnizează rețele publice de comunicații electronice, în temeiul Legii din 29 mai 2016, sunt identice cu cele enumerate de 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), fără să fie prevăzută o distincție în ceea ce privește persoanele vizate sau în funcție de obiectivul urmărit. În această ultimă privință, instanța menționată precizează că obiectivul urmărit de legiuitor prin intermediul acestei legi este nu numai combaterea terorismului și a pornografiei infantile, ci și posibilitatea de a utiliza datele stocate într-o mare varietate de situații în cadrul anchetei penale. În plus, instanța de trimitere constată că din expunerea de motive a legii menționate reiese că legiuitorul național a considerat că era imposibil, în lumina obiectivului urmărit, să se instituie o obligație de stocare direcționată și diferențiată și a ales să asocieze obligației de stocare generală și nediferențiată garanții stricte, atât pe planul datelor stocate, cât și pe planul accesului la acestea, pentru a limita la minimum ingerința în dreptul la respectarea vieții private.

77 Instanța de trimitere adaugă că articolul 126 alineatul 2 punctele 1 și 2 din Legea din 13 iunie 2005, în versiunea rezultată din Legea din 29 mai 2016, prevede condițiile în care autoritățile judiciare și, respectiv, serviciile de informații și de securitate pot obține acces la datele stocate, astfel încât examinarea legalității acestei legi în raport cu cerințele dreptului Uniunii ar trebui să fie suspendată până când Curtea se pronunță în două proceduri preliminare aflate pe rolul său referitoare la un asemenea acces.

78 În sfârșit, instanța de trimitere arată că Legea din 29 mai 2016 urmărește să permită o urmărire penală eficientă și sancțiuni efective în cazul abuzurilor sexuale față de minori, precum și să facă posibilă identificarea autorului unei asemenea infracțiuni, chiar și atunci când sunt utilizate mijloace de comunicare electronică. În cadrul procedurii desfășurate în fața sa, ar fi fost atrasă atenția în această privință asupra obligațiilor pozitive care decurg din articolele 3 și 8 din CEDO. Aceste obligații ar putea decurge de asemenea din dispozițiile corespunzătoare ale cartei, care pot avea repercusiuni asupra interpretării articolului 15 alineatul (1) din Directiva 2002/58.

79 În aceste condiții, Cour constitutionnelle (Curtea Constituțională) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„1) Articolul 15 alineatul (1) din Directiva [2002/58] coroborat cu dreptul la siguranță, garantat de articolul 6 din [cartă], și cu dreptul la respectarea datelor cu caracter personal, astfel cum este garantat de articolele 7 și 8 și de articolul 52 alineatul (1) din [cartă], trebuie interpretat în sensul că se opune unei reglementări naționale precum cea în discuție, care prevede o obligație generală pentru operatorii și furnizorii de servicii de comunicații electronice de a păstra datele de transfer și de localizare în sensul Directivei [2002/58], generate sau prelucrate de ei în cadrul furnizării acestor servicii, reglementare națională care nu are ca obiect numai investigarea, detectarea și urmărirea penală a faptelor care țin de infracționalitatea gravă, ci și garantarea securității naționale, a apărării teritoriului și a securității publice, investigarea, detectarea și urmărirea penală a altor fapte decât cele care țin de infracționalitatea gravă sau prevenirea unei utilizări interzise a sistemelor de comunicații electronice ori realizarea unui alt obiectiv identificat la articolul 23 alineatul (1) din Regulamentul [2016/679] și care, în plus, este supusă unor garanții precizate de această reglementare pe planul păstrării datelor și al accesului la acestea?

2) Articolul 15 alineatul (1) din Directiva [2002/58] coroborat cu articolele 4, 7, 8 și 11 și cu articolul 52 alineatul (1) din [cartă] trebuie interpretat în sensul că se opune unei reglementări naționale precum cea în discuție, care prevede o obligație generală pentru operatorii și furnizorii de servicii de comunicații electronice de a păstra datele de transfer și de localizare în sensul Directivei [2002/58], generate sau prelucrate de ei în cadrul furnizării acestor servicii, în cazul în care această reglementare are ca obiect, printre altele, să aducă la îndeplinire obligațiile pozitive care revin autorității în temeiul articolelor 4 și [7] din cartă, care constau în instituirea unui cadru legal care să permită o urmărire penală efectivă și o reprimare efectivă a abuzului sexual asupra minorilor și care să permită efectiv identificarea autorului infracțiunii, chiar și atunci când sunt utilizate mijloace de comunicare electronică?

3) În cazul în care, în temeiul răspunsurilor date la prima sau la a doua întrebare preliminară, Cour constitutionnelle (Curtea Constituțională) ar ajunge la concluzia că legea atacată încalcă una sau mai multe dintre obligațiile care decurg din dispozițiile menționate în aceste întrebări, ar putea să mențină provizoriu efectele Legii din [29 mai 2016] pentru a evita o insecuritate juridică și pentru a permite ca datele colectate și păstrate anterior să mai poată fi utilizate în vederea obiectivelor prevăzute de lege?"

Cu privire la procedura în fața Curții

80 Prin Decizia președintelui Curții din 25 septembrie 2018, cauzele C-511/18 și C-512/18 au fost conexate pentru buna desfășurare a procedurii scrise și orale, precum și în vederea pronunțării hotărârii. Cauza C-520/18 a fost conexată cu aceste cauze prin Decizia președintelui Curții din 9 iulie 2020 în vederea pronunțării hotărârii.

Cu privire la întrebările preliminare

Cu privire la prima întrebare în cauzele C-511/18 și C-512/18, precum și cu privire la prima și la a doua întrebare în cauza C-520/18

81 Prin intermediul primei întrebări formulate în cauzele C-511/18 și C-512/18, precum și prin intermediul primei și al celei de a doua întrebări formulate în cauza C-520/18, care trebuie analizate împreună, instanțele de trimitere solicită în esență să se stabilească dacă articolul 15 alineatul (1) din Directiva 2002/58 trebuie să fie interpretat în sensul că se opune unei reglementări naționale care impune furnizorilor de servicii de comunicații electronice, în scopurile prevăzute la acest articol 15 alineatul (1), o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare.

Observații introductive

82 Din dosarele de care dispune Curtea reiese că reglementările în discuție în litigiul principal acoperă toate mijloacele de comunicare electronică și înglobează toți utilizatorii acestor mijloace, fără a face vreo diferențiere sau vreo excepție în această privință. În plus, datele a căror stocare este impusă furnizorilor de servicii de comunicații electronice prin aceste reglementări sunt în special cele care sunt necesare pentru a găsi sursa unei comunicații și destinația acesteia, pentru a determina data, ora, durata și tipul comunicației, pentru a identifica dispozitivul de comunicație utilizat, precum și pentru a localiza echipamentele terminale și comunicațiile, date printre care figurează în special numele și adresa utilizatorului, numerele de telefon ale apelantului și apelatului, precum și adresa IP pentru serviciile internet. În schimb, datele menționate nu acoperă conținutul comunicațiilor în cauză.

83 Astfel, datele care, în temeiul reglementărilor naționale în discuție în litigiul principal, trebuie să fie stocate timp de un an permit printre altele să se stabilească cine este persoana cu care a comunicat utilizatorul unui mijloc de comunicare electronică și prin ce mijloc a avut loc această comunicare, să se determine data, ora și durata comunicațiilor și a conexiunilor la internet, precum și locul de unde acestea au avut loc și să se cunoască localizarea echipamentelor terminale fără să fie transmisă în mod necesar o comunicare. În plus, acestea oferă posibilitatea de a se determina frecvența comunicărilor utilizatorului cu anumite persoane într-o anumită perioadă. În sfârșit, în ceea ce privește reglementarea națională în discuție în cauzele C-511/18 și C-512/18, se pare că aceasta, întrucât acoperă și datele referitoare la efectuarea comunicațiilor electronice prin rețele, permite de asemenea identificarea naturii informațiilor consultate online.

84 În ceea ce privește finalitățile urmărite, este necesar să se arate că reglementările în discuție în cauzele C-511/18 și C-512/18 vizează, printre alte scopuri, cercetarea, constatarea și urmărirea penală a infracțiunilor în general, independența națională, integritatea teritoriului și apărarea națională, interesele majore ale politicii externe, executarea angajamentelor europene și internaționale ale Franței, interesele economice, industriale și științifice majore ale Franței, precum și prevenirea terorismului, atingerile aduse formei republicane a instituțiilor și violențele colective de natură să aducă o atingere gravă păcii publice. În ceea ce privește reglementarea în discuție în cauza C-520/18, aceasta are drept obiective printre altele cercetarea, depistarea și urmărirea penală a infracțiunilor, precum și protejarea securității naționale, a apărării teritoriului și a siguranței publice.

85 Instanțele de trimitere ridică în special problema eventualelor efecte asupra interpretării articolului 15 alineatul (1) din Directiva 2002/58 ale dreptului la siguranță consacrat la articolul 6 din cartă. De asemenea, acestea ridică problema dacă ingerința în drepturile fundamentale consacrate la articolele 7 și 8 din cartă pe care o implică stocarea datelor prevăzută de reglementările în discuție în litigiul principal poate să fie considerată justificată având în vedere existența unor norme care restrâng accesul autorităților naționale la datele stocate. În plus, potrivit Conseil d'État (Consiliul de Stat), întrucât această problemă se ridică într-un context marcat de amenințări grave și persistente la adresa securității naționale, ea trebuie să fie apreciată și în raport cu articolul 4 alineatul (2) TUE. La rândul său, Cour constitutionnelle (Curtea Constituțională) subliniază că reglementarea națională în discuție în cauza C-520/18 pune de asemenea în aplicare obligații pozitive care decurg din articolele 4 și 7 din cartă, care constau în instituirea unui cadru legal care să permită reprimarea efectivă a abuzului sexual asupra minorilor.

86 Deși atât Conseil d'État (Consiliul de Stat), cât și Cour constitutionnelle (Curtea Constituțională) pornesc de la premisa potrivit căreia reglementările naționale în discuție în litigiul principal, care reglementează stocarea datelor de transfer și a datelor de localizare, precum și accesul autorităților naționale la aceste date în scopurile prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, precum protejarea securității naționale, intră în domeniul de aplicare al acestei directive, unele părți din litigiile principale și unele dintre statele membre care au prezentat observații scrise Curții exprimă o opinie diferită în această privință, în special în ceea ce privește interpretarea articolului 1 alineatul (3) din directiva menționată. Prin urmare, trebuie să se examineze mai întâi dacă reglementările menționate intră în domeniul de aplicare al acestei directive.

Cu privire la domeniul de aplicare al Directivei 2002/58

87 La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International și Center for Democracy and Technology susțin în esență, invocând în această privință jurisprudența Curții privind domeniul de aplicare al Directivei 2002/58, că atât stocarea datelor, cât și accesul la datele stocate intră în domeniul de aplicare menționat, indiferent dacă accesul respectiv are loc decalat sau în timp real. Astfel, întrucât obiectivul de protejare a securității naționale este menționat în mod expres la articolul 15 alineatul (1) din această directivă, urmărirea obiectivului respectiv nu ar determina inaplicabilitatea directivei menționate. Articolul 4 alineatul (2) TUE, avut în vedere de instanțele de trimitere, nu ar afecta această apreciere.

88 În ceea ce privește măsurile de informare pe care autoritățile franceze competente le aplică în mod direct, fără a reglementa activitatea furnizorilor de servicii de comunicații electronice prin impunerea unor obligații specifice, Center for Democracy and Technology arată că aceste măsuri intră în mod necesar în domeniul de aplicare al Directivei 2002/58 și în cel al cartei, întrucât constituie derogări de la principiul confidențialității garantat la articolul 5 din această directivă. Măsurile menționate ar trebui, așadar, să respecte cerințele care decurg din articolul 15 alineatul (1) din aceasta.

89 În schimb, guvernele francez, ceh și estonian, Irlanda, guvernele cipriot, maghiar, polonez, suedez și al Regatului Unit arată în esență că Directiva 2002/58 nu se aplică unor reglementări naționale precum cele în discuție în litigiul principal, întrucât acestea au ca finalitate protejarea securității naționale. Activitățile serviciilor de informații, în măsura în care țin de menținerea ordinii publice, precum și de apărarea securității interne și a integrității teritoriale, ar intra în sfera funcțiilor esențiale ale statelor membre și, prin urmare, ar fi de competența exclusivă a acestora din urmă, după cum ar demonstra printre altele articolul 4 alineatul (2) a treia teză TUE.

90 Aceste guverne, precum și Irlanda fac referire, în plus, la articolul 1 alineatul (3) din Directiva 2002/58, care ar exclude din domeniul de aplicare al acesteia, astfel cum prevedea deja articolul 3 alineatul (2) prima liniuță din Directiva 95/46, activitățile legate de siguranța publică, de apărare și de siguranța statului. Ele se întemeiază în această privință pe interpretarea acestei din urmă dispoziții care figurează în Hotărârea din 30 mai 2006, Parlamentul/Consiliul și Comisia (C-317/04 și C-318/04, EU:C:2006:346).

91 În această privință, trebuie arătat că, 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.

92 Articolul 1 alineatul (3) din directiva menționată exclude din domeniul de aplicare al acesteia „activitățile statului” în domeniile pe care le prevede, printre care se numără activitățile statului în domeniul penal, precum și cele legate de siguranța publică, de apărare și de siguranța statului, inclusiv de bunăstarea economică a statului, dacă activitățile respective sunt legate de chestiuni de siguranța statului. Activitățile astfel menționate cu titlu de exemplu sunt, în toate cazurile, activități proprii statelor sau autorităților statale, străine de domeniile de activitate ale particularilor (Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctul 32 și jurisprudența citată).

93 În plus, articolul 3 din Directiva 2002/58 prevede că această directivă se aplică prelucrării de date cu caracter personal legate de furnizarea de servicii de comunicații electronice destinate publicului prin intermediul rețelelor publice de comunicații din cadrul Uniunii, inclusiv al rețelelor publice de comunicații care presupun colectarea de date și dispozitive de identificare (denumite în continuare „servicii de comunicații electronice”). Prin urmare, trebuie considerat că directiva menționată reglementează activitățile furnizorilor de astfel de servicii (Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctul 33 și jurisprudența citată).

94 În acest cadru, articolul 15 alineatul (1) din Directiva 2002/58 permite statelor membre să adopte, cu respectarea condițiilor pe care le prevede, „măsuri legislative pentru a restrânge sfera de aplicare a drepturilor și obligațiilor prevăzute la articolul 5, articolul 6, articolul 8 alineatele (1), (2), (3) și (4) și articolul 9 din [această] directivă” (Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 71).

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

96 Având în vedere în special aceste considerații, Curtea a statuat că articolul 15 alineatul (1) din Directiva 2002/58 coroborat cu articolul 3 din aceasta trebuie să fie interpretat în sensul că intră în domeniul de aplicare al acestei directive nu numai o măsură legislativă care impune furnizorilor de servicii de comunicații electronice să stocheze datele de transfer și datele de localizare, ci și o măsură legislativă

care le impune să acorde autorităților naționale competente accesul la aceste date. Astfel, asemenea măsuri legislative implică în mod necesar o prelucrare de către acești furnizori a datelor respective și, întrucât guvernează activitățile acelorași furnizori, nu pot fi asimilate unor activități proprii statelor, prevăzute la articolul 1 alineatul (3) din directiva menționată (a se vedea în acest sens Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctele 35 și 37, precum și jurisprudența citată).

97 În plus, având în vedere considerațiile care figurează la punctul 95 din prezenta hotărâre și economia generală a Directivei 2002/58, o interpretare a acestei directive potrivit căreia măsurile legislative prevăzute la articolul 15 alineatul (1) din aceasta ar fi excluse din domeniul de aplicare al directivei menționate ca urmare a faptului că finalitățile la care trebuie să răspundă asemenea măsuri se pliază în esență pe finalitățile urmărite de activitățile menționate la articolul 1 alineatul (3) din aceeași directivă ar priva acest articol 15 alineatul (1) de orice efect util (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctele 72 și 73).

98 Noțiunea de „activități” care figurează la articolul 1 alineatul (3) din Directiva 2002/58 nu poate, așadar, astfel cum a arătat în esență domnul avocat general la punctul 75 din Concluziile sale prezentate în cauzele conexate La Quadrature du Net și alții (C-511/18 și C-512/18, EU:C:2020:6), să fie interpretată în sensul că acoperă măsurile legislative prevăzute la articolul 15 alineatul (1) din această directivă.

99 Dispozițiile articolului 4 alineatul (2) TUE, la care au făcut referire guvernele menționate la punctul 89 din prezenta hotărâre, nu pot infirma această concluzie. Astfel, potrivit jurisprudenței constante a Curții, deși este de competența statelor membre să își definească interesele esențiale de securitate și să adopte măsurile apte să asigure securitatea lor internă și externă, simplul fapt că o măsură națională a fost adoptată în vederea protejării securității naționale nu poate să determine inaplicabilitatea dreptului Uniunii și nici să absolve statele membre de necesitatea de a respecta acest drept [a se vedea în acest sens Hotărârea din 4 iunie 2013, ZZ, C-300/11, EU:C:2013:363, punctul 38, Hotărârea din 20 martie 2018, Comisia/Austria (Imprimerie de stat), C-187/16, EU:C:2018:194, punctele 75 și 76, precum și Hotărârea din 2 aprilie 2020, Comisia/Polonia, Ungaria și Republica Cehă (Mecanism temporar de transfer al solicitanților de protecție internațională), C-715/17, C-718/17 și C-719/17, EU:C:2020:257, punctele 143 și 170].

100 Este adevărat că, în Hotărârea din 30 mai 2006, Parlamentul/Consiliul și Comisia (C-317/04 și C-318/04, EU:C:2006:346, punctele 56-59), Curtea a statuat că transferul datelor cu caracter personal de către companii aeriene către autorități publice dintr-un stat terț în scopul prevenirii, precum și al combaterii terorismului și a altor infracțiuni grave nu intra, în temeiul articolului 3 alineatul (2) prima liniuță din Directiva 95/46, în domeniul de aplicare al acestei directive, întrucât acest transfer se înscria într-un cadru instituit de puterile publice, care privea securitatea publică.

101 Totuși, având în vedere considerațiile care figurează la punctele 93, 95 și 96 din prezenta hotărâre, această jurisprudență nu poate fi transpusă în ceea ce privește interpretarea articolului 1 alineatul (3) din Directiva 2002/58. Astfel, așa cum a arătat în esență domnul avocat general la punctele 70-72 din Concluziile sale prezentate în cauzele conexate La Quadrature du Net și alții (C-511/18 și C-512/18, EU:C:2020:6), articolul 3 alineatul (2) prima liniuță din Directiva 95/46, la care se raportează jurisprudența menționată, excludea din domeniul de aplicare al acestei din urmă directive, în general, „prelucrăril[e] care au ca obiect siguranța publică, apărarea, securitatea națională”, fără a efectua o distincție în funcție de autorul prelucrării de date în cauză. În schimb, în cadrul interpretării articolului 1 alineatul (3) din Directiva 2002/58, o asemenea distincție se dovedește necesară. Astfel, după cum reiese din cuprinsul punctelor 94-97 din prezenta hotărâre, toate prelucrările de date cu caracter personal efectuate de furnizorii de servicii de comunicații electronice intră în domeniul de aplicare al directivei menționate, inclusiv prelucrările care decurg din obligațiile care le sunt impuse de autoritățile publice, în timp ce aceste din urmă prelucrări puteau, eventual, să intre sub incidența

excepției prevăzute la articolul 3 alineatul (2) prima liniuță din Directiva 95/46, ținând seama de formularea mai largă a acestei dispoziții, care vizează toate prelucrările, indiferent de autorul lor, care au ca obiect siguranța publică, apărarea sau securitatea statului.

102 Pe de altă parte, trebuie arătat că Directiva 95/46, în discuție în cauza în care s-a pronunțat Hotărârea din 30 mai 2006, Parlamentul/Consiliul și Comisia (C-317/04 și C-318/04, EU:C:2006:346), a fost, în temeiul articolului 94 alineatul (1) din Regulamentul 2016/679, abrogată și înlocuită de acesta, cu efect de la 25 mai 2018. Or, deși regulamentul menționat precizează, la articolul 2 alineatul (2) litera (d), că acesta nu se aplică prelucrărilor efectuate „de către autoritățile competente” în scopul, printre altele, al prevenirii și depistării infracțiunilor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, din articolul 23 alineatul (1) literele (d) și (h) din același regulament reiese că prelucrările de date cu caracter personal efectuate de particulari în aceleași scopuri intră în domeniul de aplicare al acestuia. În consecință, interpretarea care precedă a articolului 1 alineatul (3), a articolului 3 și a articolului 15 alineatul (1) din Directiva 2002/58 este coerentă cu delimitarea domeniului de aplicare al Regulamentului 2016/679, pe care această directivă îl completează și îl precizează.

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

104 Din considerațiile care precedă rezultă că o reglementare națională care impune furnizorilor de servicii de comunicații electronice să stocheze date de transfer și date de localizare în scopul protejării securității naționale și al combaterii infracționalității, precum cele în discuție în litigiul principal, intră în domeniul de aplicare al Directivei 2002/58.

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

105 Trebuie amintit, cu titlu introductiv, că rezultă dintr-o jurisprudență constantă că, pentru a interpreta o dispoziție de drept al Uniunii, trebuie să se țină seama atât de termenii acesteia, cât și de contextul său și de obiectivele urmărite de reglementarea din care face parte, precum și să se ia în considerare printre altele geneza acestei reglementări (a se vedea în acest sens Hotărârea din 17 aprilie 2018, Egenberger, C-414/16, EU:C:2018:257, punctul 44).

106 Directiva 2002/58 are drept scop, astfel cum reiese printre altele din considerentele (6) și (7) ale acesteia, să protejeze utilizatorii serviciilor de comunicații electronice împotriva riscurilor pentru datele lor personale și pentru confidențialitatea comunicațiilor lor, care rezultă din tehnologiile noi și mai cu seamă din capacitatea în creștere de stocare automată și de prelucrare a datelor. În special, directiva menționată urmărește, astfel cum enunță considerentul (2) al acesteia, să asigure respectarea deplină a drepturilor menționate la articolele 7 și 8 din cartă. În această privință, din expunerea de motive a Propunerii 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”.

107 În acest scop, articolul 5 alineatul (1) din Directiva 2002/58 consacră principiul confidențialității atât a comunicațiilor electronice, cât și a datelor de transfer aferente acestora și instituie în special interdicția adresată, în principiu, oricăror alte persoane decât utilizatorii de a stoca, fără consimțământul acestora, comunicațiile și datele menționate.

108 În ceea ce privește în special prelucrarea și stocarea datelor de transfer de către furnizorii de servicii de comunicații electronice, din articolul 6, precum și din considerentele (22) și (26) ale Directivei 2002/58 reiese că o asemenea prelucrare nu este permisă decât în măsura și pe durata necesare comercializării serviciilor, facturării acestora și furnizării de servicii cu valoare adăugată. Odată expirată această durată, datele care au fost prelucrate și stocate trebuie să fie 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 nu pot fi prelucrate decât în anumite condiții și doar dacă au fost anonimizate sau există acordul utilizatorilor sau abonaților respectivi (Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 86 și jurisprudența citată).

109 Astfel, prin adoptarea acestei directive, legiuitorul Uniunii a concretizat drepturile consacrate la articolele 7 și 8 din cartă, așa încât utilizatorii mijloacelor de comunicații electronice sunt îndreptățiți să se aștepte ca, în principiu, comunicațiile lor și datele aferente acestora să rămână, în lipsa consimțământului lor, anonime și să nu poată face obiectul unei înregistrări.

110 Cu toate acestea, articolul 15 alineatul (1) din Directiva 2002/58 permite statelor membre să introducă excepții de la obligația de principiu, prevăzută la articolul 5 alineatul (1) din această directivă, de garantare a confidențialității datelor cu caracter personal, precum și de la obligațiile corespunzătoare, prevăzute în special la articolele 6 și 9 din directiva menționată, în cazul în care restrângerea lor constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice pentru a proteja securitatea națională, apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice. În acest scop, statele membre pot adopta, *inter alia*, măsuri legislative care să permită reținerea de date, pe perioadă limitată, pentru unul dintre aceste motive.

111 În aceste condiții, posibilitatea de a deroga de la drepturile și de la obligațiile prevăzute la articolele 5, 6 și 9 din Directiva 2002/58 nu poate să justifice ca derogarea de la obligația de principiu de a garanta confidențialitatea comunicațiilor electronice și a datelor aferente acestora și în special de la interdicția de a stoca aceste date, prevăzută la articolul 5 din directiva menționată, să devină regula (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctele 89 și 104).

112 În ceea ce privește obiectivele susceptibile să justifice o restrângere a drepturilor și a obligațiilor prevăzute printre altele la articolele 5, 6 și 9 din Directiva 2002/58, Curtea a statuat deja că enumerarea obiectivelor care figurează la articolul 15 alineatul (1) prima teză din această directivă prezintă un caracter exhaustiv, așa încât o măsură legislativă adoptată în temeiul acestei dispoziții trebuie să urmărească în mod efectiv și strict unul dintre aceste obiective (a se vedea în acest sens Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctul 52 și jurisprudența citată).

113 În plus, din articolul 15 alineatul (1) a treia teză din Directiva 2002/58 reiese că statele membre nu sunt autorizate să adopte măsuri legislative prin care se restrânge sfera de aplicare a drepturilor și obligațiilor prevăzute la articolele 5, 6 și 9 din această directivă decât cu respectarea principiilor generale ale dreptului Uniunii, printre care figurează principiul proporționalității, și a drepturilor fundamentale garantate de cartă. În această privință, Curtea a statuat deja că obligația impusă de un stat membru furnizorilor de servicii de comunicații electronice, printr-o reglementare națională, de a stoca datele de transfer în scopul de a le pune, dacă este cazul, la dispoziția autorităților naționale competente ridică probleme cu privire la respectarea nu numai a articolelor 7 și 8 din cartă, referitoare la protecția vieții private și, respectiv, la protecția datelor cu caracter personal, ci și a

articolului 11 din cartă, referitor la libertatea de exprimare (a se vedea în acest sens Hotărârea din 8 aprilie 2014, Digital Rights, C-293/12 și C-594/12, EU:C:2014:238, punctele 25 și 70, precum și Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctele 91 și 92, precum și jurisprudența citată).

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

115 Trebuie precizat, în această privință, că stocarea datelor de transfer și a datelor de localizare constituie, în sine, pe de o parte, o derogare de la interdicția prevăzută la articolul 5 alineatul (1) din Directiva 2002/58, impusă oricărei alte persoane decât utilizatorii, de a stoca aceste date și, pe de altă parte, o ingerință în drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal, consacrate la articolele 7 și 8 din cartă, fiind irelevant dacă informațiile vizate referitoare la viața privată prezintă sau nu un caracter sensibil sau dacă persoanele interesate au suferit sau nu eventuale inconveniente ca urmare a acestei ingerințe [a se vedea în acest sens Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctele 124 și 126, precum și jurisprudența citată; a se vedea prin analogie, în ceea ce privește articolul 8 din CEDO, Curtea EDO, 30 ianuarie 2020, Breyer împotriva Germaniei, CE:ECHR:2020:0130JUD005000112, § 81].

116 Este de asemenea irelevant dacă datele stocate sunt sau nu utilizate ulterior (a se vedea prin analogie, în ceea ce privește articolul 8 din CEDO, Curtea EDO, 16 februarie 2000, Amann împotriva Elveției, CE:ECHR:2000:0216JUD002779895, § 69, precum și 13 februarie 2020, Trjakovski și Chipovski împotriva Macedoniei de Nord, CE:ECHR:2020:0213JUD005320513, § 51), întrucât accesul la astfel de date constituie, indiferent de modul în care sunt utilizate ulterior, o ingerință distinctă în drepturile fundamentale prevăzute la punctul anterior [a se vedea în acest sens Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctele 124 și 126].

117 Această concluzie este cu atât mai justificată cu cât datele de transfer și datele de localizare pot revela informații cu privire la un număr important de aspecte ale vieții private a persoanelor în cauză, inclusiv informații sensibile, precum orientarea sexuală, opiniile politice, convingerile religioase, filozofice, sociale sau de altă natură, precum și starea de sănătate, în condițiile în care astfel de date beneficiază, pe de altă parte, de o protecție specială în dreptul Uniunii. Considerate în ansamblu, datele menționate pot permite deducerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost stocate, 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. În special, aceste date furnizează mijloacele de a stabili profilul persoanelor în cauză, informație la fel de sensibilă, din perspectiva dreptului la respectarea vieții private, ca și conținutul însuși al comunicațiilor (a se vedea în acest sens Hotărârea din 8 aprilie 2014, Digital Rights, C-293/12 și C-594/12, EU:C:2014:238, punctul 27, precum și Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 99).

118 Prin urmare, pe de o parte, stocarea datelor de transfer și a datelor de localizare în scopuri polițienești poate, în sine, să aducă atingere dreptului la respectarea comunicațiilor, consacrat la articolul 7 din cartă, și să aibă efecte disuasive asupra exercitării de către utilizatorii mijloacelor de comunicații electronice a libertății lor de exprimare, garantată la articolul 11 din aceasta (a se vedea în acest sens Hotărârea din 8 aprilie 2014, Digital Rights, C-293/12 și C-594/12, EU:C:2014:238, punctul 28, precum și Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 101). Or,

asemenea efecte disuasive pot afecta în special persoanele ale căror comunicații sunt supuse, potrivit normelor naționale, secretului profesional, precum și avertizorii ale căror activități sunt protejate prin Directiva (UE) 2019/1937 a Parlamentului European și a Consiliului din 23 octombrie 2019 privind protecția persoanelor care raportează încălcări ale dreptului Uniunii (JO 2019, L 305, p. 17). În plus, aceste efecte sunt cu atât mai grave cu cât numărul și varietatea datelor stocate sunt mai ridicate.

119 Pe de altă parte, ținând seama de cantitatea importantă de date de transfer și de date de localizare care pot fi stocate în mod continuu printr-o măsură de stocare generalizată și nediferențiată, precum și de caracterul sensibil al informațiilor pe care le pot furniza aceste date, simpla stocare a datelor menționate de către furnizorii de servicii de comunicații electronice presupune riscuri de abuz și de acces ilicit.

120 În aceste condiții, în măsura în care permite statelor membre să instituie derogările prevăzute la punctul 110 din prezenta hotărâre, articolul 15 alineatul (1) din Directiva 2002/58 reflectă împrejurarea că drepturile consacrate la articolele 7, 8 și 11 din cartă nu sunt prerogative absolute, ci trebuie să fie luate în considerare în raport cu funcția lor în societate (a se vedea în acest sens Hotărârea din 16 iulie 2020, Facebook Ireland și Schrems, C-311/18, EU:C:2020:559, punctul 172, precum și jurisprudența citată).

121 Astfel, după cum reiese din articolul 52 alineatul (1) din cartă, aceasta admite restrângeri ale exercitării acestor drepturi, cu condiția ca restrângerile respective să fie prevăzute de lege, să respecte substanța drepturilor menționate și, cu respectarea principiului proporționalității, să fie necesare și să răspundă efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

122 Astfel, interpretarea articolului 15 alineatul (1) din Directiva 2002/58 în lumina cartei impune să se țină seama și de importanța drepturilor consacrate la articolele 3, 4, 6 și 7 din cartă și de cea a obiectivelor de protejare a securității naționale și de combatere a infracționalității grave, contribuind la protecția drepturilor și libertăților celorlalți.

123 În această privință, articolul 6 din cartă, la care fac referire Conseil d'État (Consiliul de Stat) și Cour constitutionnelle (Curtea Constituțională), consacră dreptul oricărei persoane nu numai la libertate, ci și la siguranță și garantează drepturi care corespund celor garantate la articolul 5 din CEDO (a se vedea în acest sens Hotărârea din 15 februarie 2016, N., C-601/15 PPU, EU:C:2016:84, punctul 47, Hotărârea din 28 iulie 2016, JZ, C-294/16 PPU, EU:C:2016:610, punctul 48, precum și Hotărârea din 19 septembrie 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, punctul 42 și jurisprudența citată).

124 În plus, trebuie amintit că articolul 52 alineatul (3) din cartă este destinat să asigure coerența necesară între drepturile prevăzute de aceasta din urmă și drepturile corespunzătoare garantate de CEDO, fără a aduce atingere autonomiei dreptului Uniunii și al Curții de Justiție a Uniunii Europene. Prin urmare, trebuie să se țină seama de drepturile corespunzătoare din CEDO în vederea interpretării cartei, ca prag de protecție minimă [a se vedea în acest sens Hotărârea din 12 februarie 2019, TC, C-492/18 PPU, EU:C:2019:108, punctul 57, precum și Hotărârea din 21 mai 2019, Comisia/Ungaria (Uzufruct asupra unor terenuri agricole), C-235/17, EU:C:2019:432, punctul 72 și jurisprudența citată].

125 În ceea ce privește articolul 5 din CEDO, care consacră „dreptul la libertate" și „dreptul la siguranță", acesta urmărește, potrivit jurisprudenței Curții Europene a Drepturilor Omului, să protejeze individul împotriva oricărei privări de libertate arbitrare sau nejustificate (a se vedea în acest sens Curtea EDO, 18 martie 2008, Ladent împotriva Poloniei, CE:ECHR:2008:0318JUD001103603, § 45 și 46, 29 martie 2010, Medvedyev și alții împotriva Franței, CE:ECHR:2010:0329JUD000339403, § 76 și 77, precum și 13 decembrie 2012, El-Masri împotriva „The former Yugoslav Republic of Macedonia", CE:ECHR:2012:1213JUD003963009, § 239). Totuși, întrucât această dispoziție vizează o privare de

libertate săvârșită de o autoritate publică, articolul 6 din cartă nu poate fi interpretat în sensul că impune autorităților publice o obligație de a adopta măsuri specifice în vederea sancționării anumitor infracțiuni.

126 În schimb, în ceea ce privește în special combaterea efectivă a infracțiunilor ale căror victime sunt printre altele minorii și celelalte persoane vulnerabile, evocată de Cour constitutionnelle (Curtea Constituțională), trebuie subliniat că din articolul 7 din cartă pot rezulta obligații pozitive în sarcina autorităților publice în vederea adoptării unor măsuri juridice prin care se urmărește protejarea vieții private și de familie [a se vedea în acest sens Hotărârea din 18 iunie 2020, Comisia/Ungaria (Transparență asociativă), C-78/18, EU:C:2020:476, punctul 123 și jurisprudența citată a Curții Europene a Drepturilor Omului]. Asemenea obligații pot decurge de asemenea din articolul 7 menționat în ceea ce privește protecția domiciliului și a comunicațiilor, precum și din articolele 3 și 4 în ceea ce privește protecția integrității fizice și psihice a persoanelor, precum și interzicerea torturii și a tratamentelor inumane și degradante.

127 Or, în raport cu aceste diferite obligații pozitive, este necesar să se realizeze o conciliere a diverselor interese și drepturi în cauză.

128 Astfel, Curtea Europeană a Drepturilor Omului a statuat că obligațiile pozitive care decurg din articolele 3 și 8 din CEDO, ale căror garanții corespunzătoare figurează la articolele 4 și 7 din cartă, implică printre altele adoptarea unor dispoziții materiale și procedurale, precum și a unor măsuri de ordin practic care permit combaterea eficientă a infracțiunilor contra persoanei prin cercetări și urmăriri penale efective, această obligație fiind cu atât mai importantă atunci când este amenințată bunăstarea fizică și morală a unui copil. În aceste condiții, măsurile pe care trebuie să le adopte autoritățile competente trebuie să respecte pe deplin căile legale și celelalte garanții care sunt de natură să limiteze întinderea competențelor de cercetare penală, precum și celelalte libertăți și drepturi. În special, potrivit acestei instanțe, trebuie să se instituie un cadru legal care să permită concilierea diferitor interese și drepturi care trebuie protejate (Curtea EDO, 28 octombrie 1998, Osman împotriva Regatului Unit, CE:ECHR:1998:1028JUD002345294, § 115 și 116, 4 martie 2004, M.C. împotriva Bulgariei, CE:ECHR:2003:1204JUD003927298, § 151, 24 iunie 2004, Von Hannover împotriva Germaniei, CE:ECHR:2004:0624JUD005932000, § 57 și 58, precum și 2 decembrie 2008, K.U. împotriva Finlandei, CE:ECHR:2008:1202JUD 000287202, § 46, 48 și 49).

129 În ceea ce privește respectarea principiului proporționalității, articolul 15 alineatul (1) prima teză din Directiva 2002/58 prevede că statele membre pot adopta o măsură care să deroge de la principiul confidențialității comunicațiilor și a datelor de transfer aferente acestora în cazul în care o asemenea măsură se dovedește „necesară, corespunzătoare și proporțională în cadrul unei societăți democratice”, în lumina obiectivelor pe care le prevede această dispoziție. Considerentul (11) al acestei directive precizează că o măsură de această natură trebuie să fie „strict” proporțională cu scopul urmărit.

130 În această privință, trebuie amintit că protecția dreptului fundamental la respectarea vieții private impune, potrivit jurisprudenței constante a Curții, ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele strictului necesar. În plus, un obiectiv de interes general nu poate fi urmărit fără a se ține seama de faptul că acesta trebuie conciliat cu drepturile fundamentale avute în vedere de măsura respectivă, prin realizarea unei ponderări echilibrate între, pe de o parte, obiectivul interesului general și, pe de altă parte, drepturile în cauză [a se vedea în acest sens Hotărârea din 16 decembrie 2008, Satakunnan Markkinapörssi și Satamedia, C-73/07, EU:C:2008:727, punctul 56, Hotărârea din 9 noiembrie 2010, Volker und Markus Schecke și Eifert, C-92/09 și C-93/09, EU:C:2010:662, punctele 76, 77 și 86, precum și Hotărârea din 8 aprilie 2014, Digital Rights, C-293/12 și C-594/12, EU:C:2014:238, punctul 52; Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 140].

131 Mai precis, din jurisprudența Curții rezultă că posibilitatea statelor membre de a justifica o restrângere a drepturilor și a obligațiilor prevăzute printre altele la articolele 5, 6 și 9 din Directiva 2002/58 trebuie să fie apreciată măsurând gravitatea ingerinței pe care o implică o asemenea restrângere și verificând dacă importanța obiectivului de interes general urmărit prin restrângerea respectivă se raportează la această gravitate (a se vedea în acest sens Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctul 55 și jurisprudența citată).

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

133 Astfel, o reglementare care prevede o stocare a datelor cu caracter personal trebuie să răspundă întotdeauna unor criterii obiective, care să stabilească un raport între datele care trebuie stocate și obiectivul urmărit [a se vedea în acest sens Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 191 și jurisprudența citată, precum și Hotărârea din 3 octombrie 2019, A și alții, C-70/18, EU:C:2019:823, punctul 63].

– Cu privire la măsurile legislative care prevăd stocarea preventivă a datelor de transfer și a datelor de localizare în scopul protejării securității naționale

134 Trebuie arătat că obiectivul de protejare a securității naționale, evocat de instanțele de trimitere și de guvernele care au prezentat observații, nu a fost încă examinat în mod specific de Curte în hotărârile sale de interpretare a Directivei 2002/58.

135 În această privință, trebuie arătat de la bun început că articolul 4 alineatul (2) TUE prevede că securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru. Această responsabilitate corespunde interesului primordial de a proteja funcțiile esențiale ale statului și interesele fundamentale ale societății și include prevenirea și sancționarea activităților de natură să destabilizeze grav structurile constituționale, politice, economice sau sociale fundamentale ale unei țări și în special să amenințe în mod direct societatea, populația sau statul ca atare, cum ar fi printre altele activitățile de terorism.

136 Or, importanța obiectivului de protejare a securității naționale, interpretat în lumina articolului 4 alineatul (2) TUE, o depășește pe cea a celorlalte obiective prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, în special a obiectivelor de combatere a infracționalității în general, chiar grave, precum și de protejare a siguranței publice. Astfel, amenințările precum cele menționate la punctul precedent se disting, prin natura și prin gravitatea lor deosebită, de riscul general de apariție a unor tensiuni sau a unor tulburări, chiar grave, ale siguranței publice. Sub rezerva respectării celorlalte cerințe prevăzute la articolul 52 alineatul (1) din cartă, obiectivul de protejare a securității naționale poate justifica, așadar, măsuri care presupun ingerințe mai grave în drepturile fundamentale decât cele pe care le-ar putea justifica celelalte obiective.

137 Astfel, în situații precum cele descrise la punctele 135 și 136 din prezenta hotărâre, 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, în principiu, unei măsuri legislative care permite autorităților competente să impună furnizorilor de servicii de comunicații electronice să stocheze datele de transfer și datele de localizare ale tuturor utilizatorilor mijloacelor de comunicații electronice pentru o perioadă limitată, în măsura în care există împrejurări suficient de concrete care permit să se considere că statul membru în cauză se confruntă cu o amenințare gravă la adresa securității naționale, precum cea menționată la punctele 135 și 136 din prezenta hotărâre, care se dovedește a fi reală și actuală sau previzibilă. Chiar dacă o asemenea măsură vizează, în mod nediferențiat, toți utilizatorii de mijloace de comunicații electronice, fără ca aceștia să pară, la prima vedere, să prezinte un raport, în sensul jurisprudenței menționate la punctul 133 din prezenta hotărâre, cu o amenințare la adresa securității naționale a acestui stat membru, trebuie totuși să se considere că existența unei astfel de amenințări este de natură, prin ea însăși, să stabilească acest raport.

138 Obligația care prevede stocarea preventivă a datelor tuturor utilizatorilor mijloacelor de comunicații electronice trebuie însă să fie limitată în timp la strictul necesar. Deși nu poate fi exclus ca obligația impusă furnizorilor de servicii de comunicații electronice de a stoca datele să poată fi reînnoită ca urmare a menținerii unei astfel de amenințări, durata fiecărei obligații nu poate depăși un interval de timp previzibil. În plus, o asemenea stocare a datelor trebuie să fie supusă unor limitări și să fie încadrată de garanții stricte care să permită protejarea eficientă împotriva riscurilor de abuz a datelor cu caracter personal ale persoanelor în cauză. Astfel, această stocare nu poate avea caracter sistematic.

139 Având în vedere gravitatea ingerinței în drepturile fundamentale consacrate la articolele 7 și 8 din cartă care rezultă dintr-o asemenea măsură de stocare generalizată și nediferențiată a datelor, trebuie să se garanteze că recurgerea la aceasta este limitată efectiv la situațiile în care există o amenințare gravă la adresa securității naționale, precum cele menționate la punctele 135 și 136 din prezenta hotărâre. În acest scop, este esențial ca o decizie prin care furnizorii de servicii de comunicații electronice sunt obligați să procedeze la o astfel de stocare a datelor să poată face obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie are efect obligatoriu, prin care să se verifice existența uneia dintre aceste situații, precum și respectarea condițiilor și a garanțiilor care trebuie să fie prevăzute.

– Cu privire la măsurile legislative care prevăd stocarea preventivă a datelor de transfer și a datelor de localizare în vederea combaterii infracționalității și a protejării siguranței publice

140 În ceea ce privește obiectivul de prevenire, cercetare, depistare și urmărire penală a infracțiunilor, în conformitate cu principiul proporționalității, numai combaterea infracționalității grave și prevenirea amenințărilor grave la adresa siguranței publice sunt de natură să justifice ingerințe grave în drepturile fundamentale consacrate la articolele 7 și 8 din cartă, precum cele pe care le implică stocarea datelor de transfer și a datelor de localizare. Prin urmare, numai ingerințele în drepturile fundamentale menționate care nu au caracter grav pot fi justificate de obiectivul de prevenire, cercetare, depistare și urmărire penală a infracțiunilor în general [a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 102, precum și Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctele 56 și 57; Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 149].

141 O reglementare națională care prevede stocarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare în vederea combaterii infracționalității grave depășește 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 (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 107).

142 Astfel, ținând seama de caracterul sensibil al informațiilor pe care le pot furniza datele de transfer și datele de localizare, confidențialitatea acestora din urmă este esențială pentru dreptul la respectarea vieții private. Astfel și ținând seama, pe de o parte, de efectele disuasive asupra exercitării drepturilor fundamentale consacrate la articolele 7 și 11 din cartă, menționate la punctul 118 din prezenta hotărâre, pe care le poate cauza stocarea acestor date și, pe de altă parte, de gravitatea ingerinței pe care o implică o asemenea stocare, este important, într-o societate democratică, ca aceasta să fie, așa cum prevede sistemul instituit prin Directiva 2002/58, excepția, iar nu regula și ca datele respective să nu poată face obiectul unei stocări sistematice și continue. Această concluzie se impune chiar și în raport cu obiectivele de combatere a infracționalității grave și de prevenire a amenințărilor grave la adresa siguranței publice, precum și cu importanța care trebuie recunoscută acestora.

143 În plus, Curtea a subliniat că o reglementare care prevede stocarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare acoperă comunicațiile electronice ale cvasitotalității populației, fără să se facă nicio diferențiere, limitare sau excepție în funcție de obiectivul urmărit. Contrar cerinței amintite la punctul 133 din prezenta hotărâre, o asemenea reglementare 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 acest obiectiv de combatere a actelor de infracționalitate gravă și în special fără să fie prevăzută o legătură între datele a căror stocare este impusă și o amenințare la adresa siguranței publice (a se vedea în acest sens Hotărârea din 8 aprilie 2014, Digital Rights, C-293/12 și C-594/12, EU:C:2014:238, punctele 57 și 58, precum și Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 105).

144 În special, astfel cum a statuat deja Curtea, o asemenea reglementare nu este limitată la o stocare 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 stocarea datelor lor, la combaterea infracționalității (a se vedea în acest sens Hotărârea din 8 aprilie 2014, Digital Rights, C-293/12 și C-594/12, EU:C:2014:238, punctul 59, și Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 106).

145 Or, nici măcar obligațiile pozitive ale statelor membre care pot decurge, după caz, din articolele 3, 4 și 7 din cartă și care privesc, așa cum s-a arătat la punctele 126 și 128 din prezenta hotărâre, instituirea unor norme care să permită combaterea efectivă a infracțiunilor nu pot avea ca efect justificarea unor ingerințe atât de grave în drepturile fundamentale consacrate la articolele 7 și 8 din cartă precum cele pe care le presupune o reglementare care prevede stocarea datelor de transfer și a datelor de localizare ale cvasitotalității populației, fără ca datele persoanelor în cauză să fie susceptibile să prezinte o legătură, cel puțin indirectă, cu obiectivul urmărit.

146 În schimb, în conformitate cu cele menționate la punctele 142-144 din prezenta hotărâre și având în vedere concilierea necesară a drepturilor și a intereselor în discuție, obiectivele de combatere a infracționalității grave, de prevenire a unor atingeri grave aduse siguranței publice și, *a fortiori*, de protejare a securității naționale pot justifica, ținând seama de importanța lor, în raport cu obligațiile pozitive amintite la punctul anterior și la care a făcut referire printre altele Cour constitutionnelle (Curtea Constituțională), ingerința deosebit de gravă pe care o presupune o stocare direcționată a datelor de transfer și a datelor de localizare.

147 Astfel, după cum a statuat deja Curtea, 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, o stocare direcționată a datelor de transfer și a datelor de localizare în scopul combaterii infracționalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, precum și în scopul protejării securității naționale, cu condiția ca o asemenea stocare să fie, în ceea ce privește categoriile de date care trebuie stocate,

mijloacele de comunicare vizate, persoanele în cauză, precum și durata de stocare reținută, limitată la strictul necesar (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 108).

148 Referitor la delimitarea căreia trebuie să îi fie supusă o asemenea măsură de stocare a datelor, aceasta poate fi stabilită printre altele în funcție de categoriile de persoane în cauză, întrucât articolul 15 alineatul (1) din Directiva 2002/58 nu se opune unei reglementări întemeiate pe elemente obiective, care să permită să fie vizate persoane ale căror date de transfer și de localizare pot să prezinte 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 siguranța publică ori chiar un risc pentru securitatea națională (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 111).

149 În această privință, trebuie precizat că persoanele astfel vizate pot fi printre altele cele care au fost identificate în prealabil, în cadrul procedurilor naționale aplicabile și pe baza unor elemente obiective, ca reprezentând o amenințare la adresa siguranței publice sau a securității naționale a statului membru în cauză.

150 Delimitarea unei măsuri care prevede stocarea datelor de transfer și a datelor de localizare se poate întemeia de asemenea pe un criteriu geografic în cazul în care autoritățile naționale competente consideră, pe baza unor elemente obiective și nediscriminatorii, că există, într-una sau în mai multe zone geografice, o situație caracterizată printr-un risc ridicat privind pregătirea sau săvârșirea unor acte de infracționalitate gravă (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 111). Aceste zone pot fi printre altele locuri caracterizate de un număr ridicat de acte de infracționalitate gravă, locuri expuse în mod deosebit săvârșirii de acte de infracționalitate gravă, cum ar fi locurile sau infrastructurile frecventate în mod regulat de un număr foarte mare de persoane, sau locurile strategice, precum aeroporturile, gările sau zonele de taxare rutieră.

151 Pentru a se garanta că ingerința pe care o presupun măsurile de stocare direcționată descrise la punctele 147-150 din prezenta hotărâre este conformă cu principiul proporționalității, durata acestora nu o poate depăși pe cea care este strict necesară în raport cu obiectivul urmărit, precum și cu împrejurările care le justifică, fără a aduce atingere unei eventuale reînnoiri ca urmare a menținerii necesității de a se realiza o asemenea stocare.

– Cu privire la măsurile legislative care prevăd stocarea preventivă a adreselor IP și a datelor referitoare la identitatea civilă în vederea combaterii infracționalității și a protejării siguranței publice

152 Trebuie arătat că adresele IP, deși fac parte din datele de transfer, sunt generate fără a fi legate de o anumită comunicare și servesc în principal la identificarea, prin intermediul furnizorilor de servicii de comunicații electronice, a persoanei fizice proprietare a unui echipament terminal de la care se efectuează o comunicație prin intermediul internetului. Astfel, în materie de e-mail, precum și de telefonie prin internet, în măsura în care sunt stocate numai adresele IP ale sursei comunicației, iar nu cele ale destinatarului acesteia, adresele menționate nu dezvăluie, ca atare, nicio informație cu privire la terții care s-au aflat în contact cu persoana aflată la originea comunicației. Această categorie de date prezintă, așadar, un grad de sensibilitate mai redus decât celelalte date de transfer.

153 Totuși, întrucât adresele IP pot fi utilizate pentru a se realiza printre altele reconstituirea exhaustivă a parcursului de navigare al unui utilizator de internet și, prin urmare, a activității sale online, aceste date permit stabilirea profilului detaliat al acestuia din urmă. Astfel, stocarea și analiza adreselor IP menționate, pe care le necesită o asemenea reconstituire, constituie ingerințe grave în drepturile fundamentale ale utilizatorului de internet consacrate la articolele 7 și 8 din cartă, care pot avea efecte disuasive de tipul celor menționate la punctul 118 din prezenta hotărâre.

154 Or, în vederea concilierii necesare a drepturilor și a intereselor în cauză impuse de jurisprudența citată la punctul 130 din prezenta hotărâre, trebuie să se țină seama de faptul că, în cazul unei infracțiuni săvârșite online, adresa IP poate constitui singurul mijloc de investigare care să permită identificarea persoanei căreia îi era atribuită această adresă la momentul săvârșirii infracțiunii respective. La aceasta se adaugă faptul că stocarea adreselor IP de către furnizorii de servicii de comunicații electronice dincolo de durata atribuirii acestor date nu este, în principiu, necesară în scopul facturării serviciilor în discuție, astfel încât depistarea infracțiunilor săvârșite online se poate dovedi, din acest motiv, așa cum au indicat mai multe guverne în observațiile lor prezentate Curții, imposibilă dacă nu se recurge la o măsură legislativă în temeiul articolului 15 alineatul (1) din Directiva 2002/58. Această situație se poate regăsi printre altele, așa cum au arătat aceste guverne, în cazul infracțiunilor deosebit de grave în materia pornografiei infantile, precum achiziționarea, diseminarea, transmiterea sau punerea la dispoziție online de pornografie infantilă, în sensul articolului 2 litera (c) din Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO 2011, L 335, p. 1).

155 În aceste condiții, deși este adevărat că o măsură legislativă care prevede stocarea adreselor IP ale tuturor persoanelor fizice proprietare ale unui echipament terminal de la care se poate realiza accesul la internet ar viza persoane care nu prezintă, la prima vedere, o legătură, în sensul jurisprudenței citate la punctul 133 din prezenta hotărâre, cu obiectivele urmărite și că utilizatorii de internet dispun, în conformitate cu ceea ce s-a constatat la punctul 109 din prezenta hotărâre, de dreptul de a se aștepta, în temeiul articolelor 7 și 8 din cartă, ca identitatea lor să nu fie, în principiu, dezvăluită, o măsură legislativă care prevede stocarea generalizată și nediferențiată numai a adreselor IP atribuite sursei unei conexiuni nu este, în principiu, contrară articolului 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, cu condiția ca această posibilitate să fie supusă respectării stricte a condițiilor materiale și procedurale care trebuie să guverneze utilizarea acestor date.

156 Având în vedere caracterul grav al ingerinței în drepturile fundamentale consacrate la articolele 7 și 8 din cartă pe care o presupune această stocare, numai combaterea infracționalității grave și prevenirea amenințărilor grave la adresa siguranței publice sunt de natură, la fel ca protejarea securității naționale, să justifice această ingerință. În plus, durata de stocare nu o poate depăși pe cea strict necesară în raport cu obiectivul urmărit. În sfârșit, o măsură de această natură trebuie să prevadă condiții și garanții stricte în ceea ce privește exploatarea acestor date, în special printr-o reconstituire, în privința comunicațiilor și a activităților efectuate online de persoanele vizate.

157 În ceea ce privește, în sfârșit, datele referitoare la identitatea civilă a utilizatorilor mijloacelor de comunicații electronice, aceste date nu permit, în sine, să se cunoască data, ora, durata și destinatarii comunicațiilor efectuate și nici locurile în care au avut loc aceste comunicații sau frecvența acestora cu anumite persoane într-o perioadă determinată, astfel încât ele nu furnizează, cu excepția datelor de contact ale acestora, precum adresele lor, nicio informație cu privire la comunicațiile respective și, în consecință, cu privire la viața lor privată. Astfel, ingerința pe care o presupune o stocare a acestor date nu poate, în principiu, să fie calificată drept gravă (a se vedea în acest sens Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctele 59 și 60).

158 Rezultă de aici că, în conformitate cu cele expuse la punctul 140 din prezenta hotărâre, măsurile legislative care vizează prelucrarea acestor date ca atare, în special stocarea lor și accesul la acestea, numai în scopul identificării utilizatorului în cauză și fără ca datele menționate să poată fi asociate unor informații referitoare la comunicațiile efectuate, pot fi justificate de obiectivul de prevenire, cercetare, depistare și urmărire penală a infracțiunilor în general, la care face referire articolul 15 alineatul (1) prima teză din Directiva 2002/58 (a se vedea în acest sens Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctul 62).

159 În aceste condiții, având în vedere concilierea necesară a drepturilor și a intereselor în cauză și pentru motivele care figurează la punctele 131 și 158 din prezenta hotărâre, trebuie să se considere că, chiar în lipsa unei legături între toți utilizatorii mijloacelor de comunicații electronice și obiectivele urmărite, 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 unei măsuri legislative care impune, fără un termen specific, furnizorilor de servicii de comunicații electronice stocarea datelor referitoare la identitatea civilă a tuturor utilizatorilor mijloacelor de comunicații electronice în scopul prevenirii, cercetării, depistării și urmăririi penale a infracțiunilor, precum și al protejării siguranței publice, fără să fie necesar ca infracțiunile sau amenințările la adresa siguranței publice sau atingerile aduse acesteia să fie grave.

– Cu privire la măsurile legislative care prevăd conservarea rapidă a datelor de transfer și a datelor de localizare în scopul combaterii infracționalității grave

160 În ceea ce privește datele de transfer și datele de localizare prelucrate și stocate de furnizorii de servicii de comunicații electronice pe baza articolelor 5, 6 și 9 din Directiva 2002/58 sau a măsurilor legislative adoptate în temeiul articolului 15 alineatul (1) din aceasta, astfel cum sunt descrise la punctele 134-159 din prezenta hotărâre, este necesar să se arate că datele respective trebuie să fie, în principiu, după caz, șterse sau anonimizate la expirarea termenelor legale în cadrul cărora trebuie să aibă loc, în conformitate cu dispozițiile naționale de transpunere a acestei directive, prelucrarea și stocarea lor.

161 Cu toate acestea, pe durata prelucrării și a stocării menționate pot apărea situații în care intervine necesitatea stocării datelor respective dincolo de aceste termene, în scopul elucidării unor infracțiuni grave sau a unor atingeri aduse securității naționale, atât în situația în care aceste infracțiuni sau atingeri au putut fi deja constatate, cât și în situația în care existența lor poate fi suspectată în mod rezonabil în urma unei examinări obiective a tuturor împrejurărilor pertinente.

162 În această privință, trebuie arătat că Convenția Consiliului Europei privind criminalitatea informatică din 23 noiembrie 2001 (Seria Tratatelor Europene – nr. 185), care a fost semnată de cele 27 de state membre și ratificată de 25 dintre acestea și al cărei obiectiv este de a facilita combaterea infracțiunilor săvârșite prin intermediul rețelelor informatice, prevede, la articolul 14, că părțile contractante adoptă, în scopul desfășurării anchetelor sau procedurilor penale specifice, anumite măsuri cu privire la datele de transfer deja stocate, precum conservarea rapidă a acestor date. În special, articolul 16 alineatul (1) din această convenție prevede că părțile contractante adoptă măsurile legislative care se dovedesc necesare pentru a permite autorităților lor competente să ordone sau să impună într-un alt mod conservarea rapidă a datelor de transfer stocate prin intermediul unui sistem informatic, cu precădere atunci când există motive de a crede că aceste date sunt susceptibile de pierdere sau de modificare.

163 Într-o situație precum cea prevăzută la punctul 161 din prezenta hotărâre, statele membre pot, având în vedere concilierea necesară a drepturilor și a intereselor în cauză menționată la punctul 130 din prezenta hotărâre, să prevadă, printr-o legislație adoptată în temeiul articolului 15 alineatul (1) din Directiva 2002/58, posibilitatea, prin intermediul unei decizii a autorității competente supuse unui control jurisdicțional efectiv, de a impune furnizorilor de servicii de comunicații electronice să realizeze, pentru o perioadă determinată, conservarea rapidă a datelor de transfer și a datelor de localizare de care dispun.

164 În măsura în care scopul unei asemenea conservări rapide nu mai corespunde celor pentru care datele au fost colectate și stocate inițial și în măsura în care orice prelucrare de date trebuie să răspundă, în temeiul articolului 8 alineatul (2) din cartă, unor scopuri determinate, statele membre trebuie să precizeze în legislația lor scopul în care poate avea loc conservarea rapidă a datelor. Având în vedere caracterul grav al ingerinței în drepturile fundamentale consacrate la articolele 7 și 8 din cartă pe care o poate presupune o asemenea stocare, numai combaterea infracționalității grave și, *a fortiori*, protejarea securității naționale sunt de natură să justifice această ingerință. În plus, pentru a se

garanta că ingerința pe care o presupune o măsură de acest tip este limitată la strictul necesar, trebuie, pe de o parte, ca obligația de stocare să privească numai datele de trafic și datele de localizare care pot contribui la elucidarea infracțiunii grave sau a atingerii aduse securității naționale în cauză. Pe de altă parte, durata de stocare a datelor trebuie să fie limitată la strictul necesar, aceasta putând fi totuși prelungită atunci când împrejurările și obiectivul urmărit prin măsura menționată justifică acest lucru.

165 În această privință, trebuie precizat că o asemenea conservare rapidă nu trebuie să fie limitată la datele persoanelor suspectate în mod concret de săvârșirea unei infracțiuni sau a unei atingeri aduse securității naționale. Cu respectarea cadrului stabilit prin articolul 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă și ținând seama de considerațiile care figurează la punctul 133 din prezenta hotărâre, o astfel de măsură poate, potrivit alegerii legiuitorului și cu respectarea limitelor strictului necesar, să fie extinsă la datele de transfer și la datele de localizare aferente altor persoane decât cele care sunt suspectate de planificarea sau de săvârșirea unei infracțiuni grave sau a unei atingeri aduse securității naționale, în măsura în care aceste date pot contribui, pe baza unor elemente obiective și nediscriminatorii, la elucidarea unei asemenea infracțiuni sau a unei asemenea atingeri aduse securității naționale, precum datele victimei acesteia, ale anturajului său social sau profesional ori chiar ale unor anumite zone geografice, precum locurile săvârșirii și pregătirii infracțiunii ori atingerii aduse securității naționale în discuție. În plus, accesul autorităților competente la datele astfel stocate trebuie să aibă loc cu respectarea condițiilor care rezultă din jurisprudența de interpretare a Directivei 2002/58 (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctele 118-121 și jurisprudența citată).

166 Mai trebuie adăugat că, după cum reiese în special din cuprinsul punctelor 115 și 133 din prezenta hotărâre, accesul la datele de transfer și la datele de localizare stocate de furnizori în temeiul unei măsuri adoptate în conformitate cu articolul 15 alineatul (1) din Directiva 2002/58 nu poate fi justificat, în principiu, decât prin obiectivul de interes general pentru care această stocare a fost impusă furnizorilor respectivi. Rezultă în special că accesul la astfel de date în scopul urmăririi penale și al sancționării unei infracțiuni ordinare nu poate fi în niciun caz acordat atunci când stocarea acestora a fost justificată de obiectivul de combatere a infracționalității grave sau, *a fortiori*, de protejare a securității naționale. În schimb, în conformitate cu principiul proporționalității, astfel cum a fost precizat la punctul 131 din prezenta hotărâre, accesul la datele stocate în vederea combaterii infracționalității grave poate fi justificat, în măsura în care sunt respectate condițiile materiale și procedurale aferente unui asemenea acces menționate la punctul anterior, de obiectivul de protejare a securității naționale.

167 În această privință, statele membre pot prevedea în legislația lor că accesul la datele de transfer și la datele de localizare poate avea loc, cu respectarea acelorași condiții materiale și procedurale, în scopul combaterii infracționalității grave sau al protejării securității naționale atunci când datele menționate sunt stocate de un furnizor într-o manieră conformă cu articolele 5, 6 și 9 sau chiar cu articolul 15 alineatul (1) din Directiva 2002/58.

168 Având în vedere ansamblul considerațiilor care precedă, este necesar să se răspundă la prima întrebare formulată în cauzele C-511/18 și C-512/18, precum și la prima și a doua întrebare formulate în cauza C-520/18 că articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie să fie interpretat în sensul că se opune unor măsuri legislative care prevăd, în scopurile prevăzute la acest articol 15 alineatul (1), cu titlu preventiv, o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare. În schimb, articolul 15 alineatul (1) menționat, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, nu se opune unor măsuri legislative

– care permit, în scopul protejării securității naționale, impunerea unei obligații furnizorilor de servicii de comunicații electronice de a efectua o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare, în situații în care statul membru în cauză se confruntă cu o

amenințare gravă la adresa securității naționale, care se dovedește reală și actuală sau previzibilă, în condițiile în care decizia care prevede această obligație poate face obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie are efect obligatoriu, prin care se urmărește să se verifice existența uneia dintre aceste situații, precum și respectarea condițiilor și a garanțiilor care trebuie să fie prevăzute, iar obligația menționată nu poate fi impusă decât pentru o perioadă limitată în timp la strictul necesar, dar care poate fi reînnoită în cazul menținerii acestei amenințări;

– care prevăd, în scopul protejării securității naționale, al combaterii infracționalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o stocare direcționată a datelor de transfer și a datelor de localizare care să fie delimitată, pe baza unor elemente obiective și nediscriminatorii, în funcție de categoriile de persoane vizate sau prin intermediul unui criteriu geografic, pentru o perioadă limitată în timp la strictul necesar, dar care poate fi reînnoită;

– care prevăd, în scopul protejării securității naționale, al combaterii infracționalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o stocare generalizată și nediferențiată a adreselor IP atribuite sursei unei conexiuni, pentru o perioadă limitată în timp la strictul necesar;

– care prevăd, în scopul protejării securității naționale, al combaterii infracționalității și al protejării siguranței publice, o stocare generalizată și nediferențiată a datelor referitoare la identitatea civilă a utilizatorilor de mijloace de comunicații electronice și

– care permit, în scopul combaterii infracționalității grave și, *a fortiori*, al protejării securității naționale, impunerea unei obligații furnizorilor de servicii de comunicații electronice, prin intermediul unei decizii a autorității competente, supuse unui control jurisdicțional efectiv, de a realiza, pentru o perioadă determinată, conservarea rapidă a datelor de transfer și a datelor de localizare de care dispun acești furnizori de servicii,

din moment ce aceste măsuri garantează, prin norme clare și precise, că stocarea datelor în discuție este condiționată de respectarea condițiilor materiale și procedurale aferente acestora și că persoanele în cauză dispun de garanții efective împotriva riscurilor de abuz.

Cu privire la a doua și la a treia întrebare în cauza C-511/18

169 Prin intermediul celei de a doua și al celei de a treia întrebări formulate în cauza C-511/18, instanța de trimitere solicită în esență să se stabilească dacă articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie să fie interpretat în sensul că se opune unei reglementări naționale care impune furnizorilor de servicii de comunicații electronice punerea în aplicare în rețelele lor a unor măsuri care permit, pe de o parte, analiza automatizată, precum și colectarea în timp real a datelor de transfer și a datelor de localizare și, pe de altă parte, colectarea în timp real a datelor tehnice referitoare la localizarea echipamentelor terminale utilizate, fără a fi prevăzută informarea persoanelor vizate de aceste prelucrări și de aceste colectări.

170 Instanța de trimitere precizează că tehnicile de colectare de informații prevăzute la articolele L. 851-2-L. 851-4 din CSI nu implică, pentru furnizorii de servicii de comunicații electronice, o obligație specifică de stocare a datelor de transfer și a datelor de localizare. În ceea ce privește în special analiza automatizată prevăzută la articolul L. 851-3 din CSI, această instanță arată că prelucrarea respectivă are ca obiect detectarea, în funcție de criterii definite în acest scop, a conexiunilor care pot indica o amenințare teroristă. În ceea ce privește colectarea în timp real prevăzută la articolul L. 851-2 din CSI, instanța menționată constată că aceasta nu privește decât una sau mai multe persoane identificate în prealabil ca putând avea legătură cu o amenințare teroristă. Potrivit aceleiași instanțe, aceste două tehnici nu pot fi puse în aplicare decât în vederea prevenirii terorismului și privesc datele prevăzute la articolele L. 851-1 și R. 851-5 din CSI.

171 Cu titlu introductiv, trebuie precizat că împrejurarea că, potrivit articolului L. 851-3 din CSI, analiza automatizată prevăzută de acesta nu permite, ca atare, identificarea utilizatorilor ale căror date sunt supuse acestei analize nu se opune calificării unor astfel de date drept „date cu caracter personal”. Astfel, din moment ce procedura prevăzută la alineatul IV al aceleiași dispoziții permite, într-o etapă ulterioară, identificarea persoanei sau a persoanelor vizate de datele a căror analiză automatizată a indicat că puteau caracteriza existența unei amenințări teroriste, toate persoanele ale căror date fac obiectul unei analize automatizate rămân identificabile pornind de la aceste date. Or, potrivit definiției datelor cu caracter personal cuprinse la articolul 4 punctul 1 din Regulamentul 2016/679, constituie astfel de date informațiile referitoare printre altele la o persoană identificabilă.

Cu privire la analiza automatizată a datelor de transfer și a datelor de localizare

172 Din articolul L. 851-3 din CSI reiese că analiza automatizată prevăzută de acesta corespunde în esență unei filtrări a tuturor datelor de transfer și de localizare stocate de furnizorii de servicii de comunicații electronice, efectuată de aceștia din urmă la cererea autorităților naționale competente și în temeiul parametrilor pe care le-au stabilit acestea. Rezultă că toate datele utilizatorilor mijloacelor de comunicații electronice sunt verificate dacă corespund acestor parametri. Prin urmare, trebuie să se considere că o asemenea analiză automatizată implică, pentru furnizorii de servicii de comunicații electronice în cauză, realizarea, pe seama autorității competente, a unei prelucrări generalizate și nediferențiate sub forma unei utilizări cu ajutorul unui mijloc automatizat, în sensul articolului 4 punctul 2 din Regulamentul 2016/679, care acoperă ansamblul datelor de transfer și al datelor de localizare ale tuturor utilizatorilor de mijloace de comunicații electronice. Această prelucrare este independentă de colectarea ulterioară a datelor aferente persoanelor identificate în urma analizei automatizate, colectare care este autorizată în temeiul articolului L. 851-3 alineatul IV din CSI.

173 Or, o reglementare națională care autorizează o asemenea analiză automatizată a datelor de transfer și a datelor de localizare derogă de la obligația de principiu, prevăzută la articolul 5 din Directiva 2002/58, de asigurare a confidențialității comunicațiilor electronice și a datelor aferente acestora. O astfel de reglementare constituie de asemenea o ingerință în drepturile fundamentale consacrate la articolele 7 și 8 din cartă, indiferent de utilizarea ulterioară a acestor date. În sfârșit, reglementarea menționată poate, conform jurisprudenței citate la punctul 118 din prezenta hotărâre, să genereze efecte disuasive asupra exercitării libertății de exprimare consacrate la articolul 11 din cartă.

174 În plus, ingerința care rezultă dintr-o analiză automatizată a datelor de transfer și a datelor de localizare, precum cea în discuție în litigiul principal, se dovedește deosebit de gravă din moment ce acoperă în mod generalizat și nediferențiat datele persoanelor care utilizează mijloacele de comunicații electronice. Această constatare se impune cu atât mai mult atunci când, astfel cum reiese din reglementarea națională în discuție în litigiul principal, datele care fac obiectul analizei automatizate pot indica natura informațiilor consultate online. În plus, o asemenea analiză automatizată se aplică în mod global tuturor persoanelor care utilizează mijloace de comunicații electronice și, prin urmare, și celor pentru care nu există niciun indiciu de natură să sugereze că comportamentul lor ar putea avea o legătură, chiar indirectă sau îndepărtată, cu activități de terorism.

175 În ceea ce privește justificarea unei asemenea ingerințe, trebuie precizat că cerința, prevăzută la articolul 52 alineatul (1) din cartă, potrivit căreia orice restrângere a exercitării drepturilor fundamentale trebuie să fie prevăzută de lege presupune ca temeiul juridic care permite această ingerință să definească el însuși întinderea restrângerii exercitării dreptului vizat (a se vedea în acest sens Hotărârea din 16 iulie 2020, Facebook Ireland și Schrems, C-311/18, EU:C:2020:559, punctul 175, precum și jurisprudența citată).

176 În plus, pentru a îndeplini cerința proporționalității, amintită la punctele 130 și 131 din prezenta hotărâre, potrivit căreia derogările de la protecția datelor cu caracter personal și restrângerile acesteia trebuie să fie efectuate în limitele strictului necesar, o reglementare națională care guvernează accesul

autorităților competente la date de transfer și la date de localizare stocate trebuie să respecte cerințele rezultate din jurisprudența citată la punctul 132 din prezenta hotărâre. În special, o asemenea reglementare nu se poate limita la a impune ca accesul autorităților la date să corespundă finalității urmărite de această reglementare, ci trebuie să prevadă și condițiile materiale și procedurale care guvernează această utilizare [a se vedea prin analogie Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 192 și jurisprudența citată].

177 În această privință, trebuie amintit că ingerința deosebit de gravă pe care o implică stocarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare, avută în vedere de considerațiile care figurează la punctele 134-139 din prezenta hotărâre, precum și ingerința deosebit de gravă pe care o constituie analiza lor automatizată nu pot îndeplini cerința proporționalității decât în situațiile în care un stat membru se confruntă cu o amenințare gravă la adresa securității naționale, care se dovedește reală și actuală sau previzibilă, și cu condiția ca durata acestei păstrări să fie limitată la strictul necesar.

178 În situații precum cele avute în vedere la punctul anterior, punerea în aplicare a unei analize automatizate a datelor de transfer și a datelor de localizare ale tuturor utilizatorilor de mijloace de comunicații electronice, pentru o perioadă strict limitată, poate fi considerată justificată în raport cu cerințele care decurg din 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.

179 În aceste condiții, pentru a se garanta că recurgerea la o astfel de măsură se limitează efectiv la ceea ce este strict necesar pentru protejarea securității naționale și, mai specific, pentru prevenirea terorismului, este esențial, în conformitate cu cele constatate la punctul 139 din prezenta hotărâre, ca decizia prin care este autorizată analiza automatizată să poată face obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie are efect obligatoriu, prin care să se verifice existența unei situații care justifică măsura menționată, precum și respectarea condițiilor și a garanțiilor care trebuie să fie prevăzute.

180 În această privință, trebuie precizat că modelele și criteriile prestabilite pe care se întemeiază acest tip de prelucrare a datelor trebuie să fie, pe de o parte, specifice și fiabile, pentru a permite să se ajungă la rezultate care identifică indivizi cu privire la care ar putea exista o suspiciune rezonabilă de participare la infracțiuni de terorism și, pe de altă parte, nediscriminatorii [a se vedea în acest sens Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 172].

181 În plus, trebuie amintit că orice analiză automatizată efectuată în funcție de modele și de criterii întemeiate pe postulatul potrivit căruia originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice, apartenența sindicală, starea de sănătate sau viața sexuală ale unei persoane ar putea, prin ele însele și independent de comportamentul individual al acestei persoane, să fie relevante din perspectiva prevenirii terorismului ar încălca drepturile garantate la articolele 7 și 8 din cartă coroborate cu articolul 21 din aceasta. Astfel, modelele și criteriile prestabilite în vederea unei analize automatizate prin care se urmărește prevenirea activităților de terorism care prezintă o amenințare gravă la adresa securității naționale nu se pot întemeia numai pe aceste date sensibile [a se vedea în acest sens Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 165].

182 Pe de altă parte, întrucât analizele automatizate ale datelor de transfer și ale datelor de localizare presupun în mod necesar o anumită marjă de eroare, orice rezultat pozitiv obținut în urma unei prelucrări automatizate trebuie să fie supus unei reexaminări individuale prin mijloace neautomatizate înainte de adoptarea unei măsuri individuale care să producă efecte negative în privința persoanelor în cauză, precum colectarea ulterioară a datelor de transfer și a datelor de localizare în timp real, o asemenea măsură neputând, astfel, să se întemeieze în mod decisiv numai pe rezultatul unei prelucrări automatizate. De asemenea, pentru a garanta în practică că modelele și criteriile prestabilite, utilizarea dată acestora, precum și bazele de date utilizate nu prezintă un caracter discriminatoriu și sunt limitate la strictul necesar în raport cu obiectivul de prevenire a activităților de terorism care prezintă o

amenințare gravă la adresa securității naționale, fiabilitatea și actualitatea acestor modele și a acestor criterii prestabilite, precum și a bazelor de date utilizate trebuie să facă obiectul unei reexaminări periodice [a se vedea în acest sens Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctele 173 și 174].

Cu privire la colectarea în timp real a datelor de transfer și a datelor de localizare

183 În ceea ce privește colectarea în timp real a datelor de transfer și a datelor de localizare prevăzută la articolul L. 851-2 din CSI, trebuie arătat că aceasta poate fi autorizată în mod individual în ceea ce privește „o persoană identificată în prealabil ca fiind susceptibilă să aibă legătură cu o amenințare [teroristă]”. De asemenea, potrivit acestei dispoziții, „în cazul în care există motive întemeiate pentru a se crede că una sau mai multe persoane care aparțin anturajului persoanei vizate de autorizație pot furniza informații în legătură cu scopul care justifică autorizația, aceasta poate fi de asemenea acordată individual pentru fiecare dintre aceste persoane”.

184 Datele care fac obiectul unei măsuri de această natură permit autorităților naționale competente să supravegheze, pe perioada autorizării, în mod continuu și în timp real, interlocutorii cu care comunică persoanele în cauză, mijloacele pe care acestea le utilizează, durata comunicațiilor pe care le transmit, precum și locurile lor de ședere și deplasările lor. De asemenea, ele par susceptibile să indice natura informațiilor consultate online. Considerate în ansamblu, aceste date permit, astfel cum reiese din cuprinsul punctului 117 din prezenta hotărâre, deducerea unor concluzii foarte precise privind viața privată a persoanelor în cauză și furnizează mijloacele de stabilire a profilului acestora, o asemenea informație fiind la fel de sensibilă, din perspectiva dreptului la respectarea vieții private, ca și conținutul însuși al comunicațiilor.

185 În ceea ce privește colectarea de date în timp real prevăzută la articolul L. 851-4 din CSI, această dispoziție autorizează colectarea datelor tehnice referitoare la localizarea echipamentelor terminale și transmiterea în timp real către un serviciu al prim-ministrului. Rezultă că astfel de date permit serviciului competent, în orice moment pe durata autorizării, să localizeze, în mod continuu și în timp real, echipamentele terminale utilizate, precum telefoanele mobile.

186 Or, o reglementare națională care autorizează astfel de colectări în timp real derogă, asemenea celei care autorizează analiza automatizată a datelor, de la obligația de principiu, prevăzută la articolul 5 din Directiva 2002/58, de asigurare a confidențialității comunicațiilor electronice și a datelor aferente acestora. Prin urmare, aceasta constituie de asemenea o ingerință în drepturile fundamentale consacrate la articolele 7 și 8 din cartă și poate să genereze efecte disuasive asupra exercitării libertății de exprimare garantate la articolul 11 din cartă.

187 Trebuie subliniat că ingerința pe care o presupune colectarea în timp real a datelor care permit localizarea unui echipament terminal este deosebit de gravă, din moment ce aceste date furnizează autorităților naționale competente mijlocul unei monitorizări precise și permanente a deplasărilor utilizatorilor de telefoane mobile. Întrucât aceste date trebuie, astfel, să fie considerate deosebit de sensibile, trebuie să se facă distincție între accesul în timp real al autorităților competente la asemenea date și un acces decalat la acestea, primul fiind mai intruziv, întrucât permite o supraveghere aproape perfectă a utilizatorilor respectivi (a se vedea prin analogie, în ceea ce privește articolul 8 din CEDO, Curtea EDO, 8 februarie 2018, Ben Faiza împotriva Franței, CE:ECHR:2018:0208JUD003144612, § 74). În plus, intensitatea acestei ingerințe este agravată atunci când colectarea în timp real se extinde și la datele de transfer ale persoanelor în cauză.

188 Deși obiectivul de prevenire a terorismului pe care îl urmărește reglementarea națională în discuție în litigiul principal poate, având în vedere importanța sa, să justifice ingerința pe care o presupune colectarea în timp real a datelor de transfer și a datelor de localizare, o astfel de măsură nu poate fi pusă în aplicare, ținând seama de caracterul său deosebit de intruziv, decât în privința persoanelor cu

privire la care există un motiv valabil de a se suspecta că sunt implicate într-un mod sau altul în activități de terorism. În ceea ce privește datele persoanelor care nu intră în această categorie, ele pot face numai obiectul unui acces decalat, acesta neputând avea loc, în conformitate cu jurisprudența Curții, decât în situații speciale, precum cele în care sunt în discuție activități de terorism, și 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 terorismului (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 119 și jurisprudența citată).

189 În plus, o decizie prin care este autorizată colectarea în timp real a datelor de transfer și a datelor de localizare trebuie să se întemeieze pe criterii obiective prevăzute de legislația națională. În special, această legislație trebuie să definească, în conformitate cu jurisprudența citată la punctul 176 din prezenta hotărâre, împrejurările și condițiile în care poate fi autorizată o asemenea colectare și să prevadă că, astfel cum s-a precizat la punctul anterior, pot fi vizate numai persoanele care au legătură cu obiectivul de prevenire a terorismului. În plus, o decizie prin care este autorizată colectarea în timp real a datelor de transfer și a datelor de localizare trebuie să se întemeieze pe criterii obiective și nediscriminatorii prevăzute de legislația națională. În scopul de a garanta, în practică, respectarea acestor condiții, este esențial ca punerea în aplicare a măsurii prin care este autorizată colectarea în timp real să fie supusă unui control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă, a cărei decizie are efect obligatoriu, această instanță sau această entitate trebuind în special să se asigure că o astfel de colectare în timp real nu este autorizată decât în limita a ceea ce este strict necesar (a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 120). În caz de urgență justificată corespunzător, controlul trebuie să aibă loc în termen scurt.

Cu privire la informarea persoanelor ale căror date au fost colectate sau analizate

190 Se impune ca autoritățile naționale competente care colectează în timp real datele de transfer și datele de localizare să informeze persoanele în cauză cu privire la aceasta, în cadrul procedurilor naționale aplicabile, în măsura și din momentul în care această comunicare nu poate compromite misiunile care revin acestor autorități. Astfel, această informare este, de fapt, necesară pentru a permite persoanelor respective să își exercite drepturile rezultate din articolele 7 și 8 din cartă de a solicita accesul la datele lor cu caracter personal care fac obiectul acestor măsuri și, dacă este cazul, rectificarea sau ștergerea acestora, precum și să introducă, în conformitate cu articolul 47 primul paragraf din cartă, o cale de atac efectivă în fața unei instanțe judecătorești, un asemenea drept fiind, de altfel, garantat în mod explicit la articolul 15 alineatul (2) din Directiva 2002/58 coroborat cu articolul 79 alineatul (1) din Regulamentul 2016/679 [a se vedea în acest sens Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctul 121 și jurisprudența citată, precum și Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctele 219 și 220].

191 În ceea ce privește informarea necesară în contextul unei analize automatizate a datelor de transfer și a datelor de localizare, autoritatea națională competentă este obligată să publice informații de natură generală referitoare la această analiză, fără a trebui să efectueze o informare individuală a persoanelor în cauză. În schimb, în ipoteza în care datele corespund parametrilor precizați în măsura prin care se autorizează analiza automatizată, iar această autoritate identifică persoana în cauză pentru a analiza mai detaliat datele care o privesc, este necesară informarea individuală a acestei persoane. Totuși, o astfel de informare nu trebuie să intervină decât în măsura și din momentul în care ea nu poate compromite misiunile care revin autorității menționate [a se vedea prin analogie Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctele 222-224].

192 Având în vedere ansamblul considerațiilor care precedă, este necesar să se răspundă la a doua și la a treia întrebare formulate în cauza C-511/18 că articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie să fie interpretat în sensul că nu se opune unei reglementări naționale care impune furnizorilor de servicii de

comunicații electronice să recurgă, pe de o parte, la analiza automatizată, precum și la colectarea în timp real printre altele a datelor de transfer și a datelor de localizare și, pe de altă parte, la colectarea în timp real a datelor tehnice referitoare la localizarea echipamentelor terminale utilizate, atunci când

– recurgerea la analiza automatizată se limitează la situațiile în care un stat membru se confruntă cu o amenințare gravă la adresa securității naționale, care se dovedește reală și actuală sau previzibilă, în condițiile în care recurgerea la această analiză poate face obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie are efect obligatoriu, prin care se urmărește să se verifice existența unei situații care justifică măsura menționată, precum și respectarea condițiilor și a garanțiilor care trebuie să fie prevăzute, iar

– recurgerea la colectarea în timp real a datelor de transfer și a datelor de localizare este limitată la persoanele în privința cărora există un motiv valabil pentru a suspecta că sunt implicate într-un mod sau altul în activități de terorism și este supusă unui control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă, a cărei decizie are efect obligatoriu, pentru a se asigura că o astfel de colectare în timp real nu este autorizată decât în limita a ceea ce este strict necesar. În caz de urgență justificată corespunzător, controlul trebuie să aibă loc în termen scurt.

Cu privire la a doua întrebare în cauza C-512/18

193 Prin intermediul celei de a doua întrebări formulate în cauza C-512/18, instanța de trimitere solicită în esență să se stabilească dacă dispozițiile Directivei 2000/31, citite în lumina articolelor 6-8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie să fie interpretate în sensul că se opun unei reglementări naționale care impune furnizorilor de acces la servicii de comunicații publice online și furnizorilor de servicii de stocare-hosting stocarea generalizată și nediferențiată printre altele a datelor cu caracter personal aferente acestor servicii.

194 Deși consideră că astfel de servicii intră în domeniul de aplicare al Directivei 2000/31, iar nu în cel al Directivei 2002/58, instanța de trimitere apreciază că articolul 15 alineatele (1) și (2) din Directiva 2000/31 coroborat cu articolele 12 și 14 din aceasta nu instituie, în sine, o interdicție de principiu de stocare a datelor referitoare la crearea de conținut, de la care s-ar putea deroga numai în mod excepțional. Instanța menționată ridică însă problema dacă această apreciere trebuie să fie reținută, ținând seama de necesitatea respectării drepturilor fundamentale consacrate la articolele 6-8 și 11 din cartă.

195 În plus, instanța de trimitere precizează că întrebarea sa privește obligația de stocare prevăzută la articolul 6 din LCEN coroborat cu Decretul nr. 2011-219. Datele pe care trebuie să le stocheze în acest temei furnizorii de servicii în cauză includ printre altele datele privind identitatea civilă a persoanelor care au utilizat aceste servicii, precum numele, prenumele, adresele lor poștale asociate, adresele lor de e-mail sau de cont asociate, parolele lor și, în cazul în care contractul încheiat sau contul creat implică plăți, tipul de plată utilizat, referința plății, suma, precum și data și ora tranzacției.

196 De asemenea, datele vizate de obligația de stocare acoperă elementele de identificare a abonaților, a conexiunilor și a echipamentelor terminale utilizate, identificatorii atribuiți conținuturilor, datele și orele inițierii și ale încheierii conexiunilor și ale operațiunilor, precum și tipurile de protocoale utilizate pentru conectarea la serviciu și pentru transferul conținuturilor. Accesul la aceste date, a căror durată de stocare se ridică la un an, poate fi solicitat în cadrul procedurilor penale și civile, în vederea asigurării respectării normelor privind răspunderea civilă sau penală, precum și în cadrul măsurilor de colectare de informații cărora li se aplică articolul L. 851-1 din CSI.

197 În această privință, trebuie arătat că, potrivit articolului 1 alineatul (2) din Directiva 2000/31, ea apropie anumite dispoziții de drept intern aplicabile serviciilor societății informaționale menționate la articolul 2 litera (a) din aceasta.

198 Astfel de servicii le includ, desigur, pe cele care sunt prestate la distanță prin intermediul echipamentului electronic de prelucrare și de stocare a datelor, la cererea individuală a destinatarului serviciilor și, în mod obișnuit, în schimbul unei remunerații, cum ar fi serviciile de acces la internet sau la o rețea de comunicații, precum și serviciile de stocare-hosting (a se vedea în acest sens Hotărârea din 24 noiembrie 2011, Scarlet Extended, C-70/10, EU:C:2011:771, punctul 40, Hotărârea din 16 februarie 2012, SABAM, C-360/10, EU:C:2012:85, punctul 34, Hotărârea din 15 septembrie 2016, Mc Fadden, C-484/14, EU:C:2016:689, punctul 55, precum și Hotărârea din 7 august 2018, SNB-REACT, C-521/17, EU:C:2018:639, punctul 42 și jurisprudența citată).

199 Totuși, articolul 1 alineatul (5) din Directiva 2000/31 prevede că aceasta nu se aplică în chestiunile referitoare la serviciile societății informaționale reglementate de Directivele 95/46 și 97/66. În această privință, din considerentele (14) și (15) ale Directivei 2000/31 reiese că protecția confidențialității comunicațiilor, precum și a persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal în cadrul serviciilor societății informaționale este reglementată numai de Directivele 95/46 și 97/66, aceasta din urmă interzicând, la articolul 5, în scopul protejării confidențialității comunicațiilor, orice formă de interceptare sau de supraveghere a comunicațiilor.

200 Astfel, aspectele legate de protecția confidențialității comunicațiilor și a datelor cu caracter personal trebuie să fie apreciate în lumina Directivei 2002/58 și a Regulamentului 2016/679, întrucât acestea au înlocuit Directiva 97/66 și, respectiv, Directiva 95/46, cu precizarea că protecția pe care urmărește să o asigure Directiva 2000/31 nu poate, în orice caz, să aducă atingere cerințelor care rezultă din Directiva 2002/58 și din Regulamentul 2016/679 (a se vedea în acest sens Hotărârea din 29 ianuarie 2008, Promusicae, C-275/06, EU:C:2008:54, punctul 57).

201 Obligația impusă de reglementarea națională menționată la punctul 195 din prezenta hotărâre furnizorilor de acces la servicii de comunicații publice online și furnizorilor de servicii de stocare-hosting de a stoca date cu caracter personal aferente acestor servicii trebuie, așadar, astfel cum a arătat în esență domnul avocat general la punctul 141 din Concluziile sale prezentate în cauzele conexate La Quadrature du Net și alții (C-511/18 și C-512/18, EU:C:2020:6), să fie apreciată în lumina Directivei 2002/58 sau a Regulamentului 2016/679.

202 Astfel, după cum furnizarea serviciilor care intră sub incidența reglementării naționale respective intră sau nu în domeniul de aplicare al Directivei 2002/58, ea va fi reglementată fie de această din urmă directivă, în special de articolul 15 alineatul (1) din aceasta, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, fie de Regulamentul 2016/679, în special de articolul 23 alineatul (1) din regulamentul menționat, interpretat în lumina acelorași dispoziții ale cartei.

203 În speță, nu se poate exclude, astfel cum a arătat Comisia Europeană în observațiile sale scrise, că unele dintre serviciile cărora li se aplică reglementarea națională menționată la punctul 195 din prezenta hotărâre constituie servicii de comunicații electronice în sensul Directivei 2002/58, aspect a cărui verificare revine instanței de trimitere.

204 În această privință, trebuie arătat că Directiva 2002/58 acoperă serviciile de comunicații electronice care îndeplinesc condițiile prevăzute la articolul 2 litera (c) din Directiva 2002/21, la care face trimitere articolul 2 din Directiva 2002/58 și care definește serviciul de comunicații electronice ca fiind „serviciul furnizat de obicei contra cost și care constă în totalitate sau în principal în transmiterea de semnale prin rețele de comunicații electronice, inclusiv serviciile de telecomunicații și serviciile de transmisie prin rețele utilizate pentru radiodifuziune”. În ceea ce privește serviciile societății informaționale, astfel cum sunt avute în vedere la punctele 197 și 198 din prezenta hotărâre și prevăzute de Directiva

2000/31, acestea constituie servicii de comunicații electronice în condițiile în care acestea constau în totalitate sau în principal în transmiterea de semnale prin rețelele de comunicații electronice (a se vedea în acest sens Hotărârea din 5 iunie 2019, Skype Communications, C-142/18, EU:C:2019:460, punctele 47 și 48).

205 Astfel, serviciile de acces la internet, care par să intre sub incidența reglementării naționale menționate la punctul 195 din prezenta hotărâre, constituie, așa cum confirmă considerentul (10) al Directivei 2002/21, servicii de comunicații electronice în sensul acestei directive (a se vedea în acest sens Hotărârea din 5 iunie 2019, Skype Communications, C-142/18, EU:C:2019:460, punctul 37). Aceasta este și situația serviciilor de poștă electronică pe internet, care nu pare exclus să intre de asemenea sub incidența reglementării naționale respective, din moment ce, pe plan tehnic, ele presupun în totalitate sau în principal transmiterea de semnale pe rețele de comunicații electronice (a se vedea în acest sens Hotărârea din 13 iunie 2019, Google, C-193/18, EU:C:2019:498, punctele 35 și 38).

206 În ceea ce privește cerințele care decurg din 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, trebuie să se facă trimitere la toate constatările și aprecierile efectuate în cadrul răspunsului dat la prima întrebare formulată în cauzele C-511/18 și C-512/18, precum și la prima și la a doua întrebare formulate în cauza C-520/18.

207 În privința cerințelor care decurg din Regulamentul 2016/679, trebuie amintit că acesta urmărește în special, astfel cum reiese din considerentul (10) al acestuia, să asigure un nivel ridicat de protecție a persoanelor fizice în cadrul Uniunii și, în acest scop, să asigure aplicarea consecventă și omogenă a normelor în materie de protecție a drepturilor și libertăților fundamentale ale acestor persoane în ceea ce privește prelucrarea datelor cu caracter personal în întreaga Uniune (a se vedea în acest sens Hotărârea din 16 iulie 2020, Facebook Ireland și Schrems, C-311/18, EU:C:2020:559, punctul 101).

208 În acest scop, orice prelucrare a datelor cu caracter personal trebuie, sub rezerva derogărilor admise la articolul 23 din Regulamentul 2016/679, să respecte principiile care reglementează prelucrările datelor cu caracter personal, precum și drepturile persoanei în cauză prevăzute în capitolele II și, respectiv, III din acest regulament. În special, orice prelucrare a datelor cu caracter personal trebuie, pe de o parte, să fie conformă cu principiile enunțate la articolul 5 din regulamentul menționat și, pe de altă parte, să îndeplinească condițiile de legalitate enumerate la articolul 6 din același regulament (a se vedea prin analogie, în ceea ce privește Directiva 95/46, Hotărârea din 30 mai 2013, Worten, C-342/12, EU:C:2013:355, punctul 33 și jurisprudența citată).

209 În ceea ce privește, mai precis, articolul 23 alineatul (1) din Regulamentul 2016/679, trebuie arătat că acesta, asemenea celor prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, permite statelor membre să restricționeze, în raport cu scopurile pe care le menționează și prin intermediul unor măsuri legislative, domeniul de aplicare al obligațiilor și al drepturilor prevăzute de acesta „atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura” scopul urmărit. Orice măsură legislativă adoptată în acest temei trebuie în special să respecte cerințele specifice stabilite la articolul 23 alineatul (2) din regulamentul menționat.

210 Astfel, articolul 23 alineatele (1) și (2) din Regulamentul 2016/679 nu poate fi interpretat în sensul că poate conferi statelor membre puterea de a aduce atingere respectării vieții private, cu încălcarea articolului 7 din cartă, precum și celorlalte garanții prevăzute de aceasta (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 91). În special, precum în cazul articolului 15 alineatul (1) din Directiva 2002/58, puterea pe care articolul 23 alineatul (1) din Regulamentul 2016/679 o conferă statelor membre nu poate fi exercitată decât cu respectarea cerinței proporționalității, potrivit căreia derogările de la protecția datelor cu caracter personal și limitările

acestora trebuie să fie efectuate în limitele strictului necesar (a se vedea prin analogie, în ceea ce privește Directiva 95/46, Hotărârea din 7 noiembrie 2013, IPI, C-473/12, EU:C:2013:715, punctul 39 și jurisprudența citată).

211 În consecință, constatările și aprecierile efectuate în cadrul răspunsului dat la prima întrebare formulată în cauzele C-511/18 și C-512/18, precum și la prima și la a doua întrebare formulate în cauza C-520/18 se aplică *mutatis mutandis* în privința articolului 23 din Regulamentul 2016/679.

212 Având în vedere considerațiile care precedă, este necesar să se răspundă la a doua întrebare formulată în cauza C-512/18 că Directiva 2000/31 trebuie să fie interpretată în sensul că nu se aplică în materie de protecție a confidențialității comunicațiilor și a persoanelor fizice în raport cu prelucrarea datelor cu caracter personal în cadrul serviciilor societății informaționale, această protecție fiind, după caz, reglementată de Directiva 2002/58 sau de Regulamentul 2016/679. Articolul 23 alineatul (1) din Regulamentul 2016/679, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie să fie interpretat în sensul că se opune unei reglementări naționale care impune furnizorilor de acces la servicii de comunicații publice online și furnizorilor de servicii de stocare-hosting stocarea generalizată și nediferențiată printre altele a datelor cu caracter personal aferente acestor servicii.

Cu privire la a treia întrebare în cauza C-520/18

213 Prin intermediul celei de a treia întrebări formulate în cauza C-520/18, instanța de trimitere solicită în esență să se stabilească dacă o instanță națională poate aplica o dispoziție a dreptului său național care îi permite să limiteze în timp efectele unei declarații de nelegalitate pe care trebuie să o facă, în temeiul acestui drept, în privința unei legislații naționale care impune furnizorilor de servicii de comunicații electronice, în vederea, printre altele, a urmăririi obiectivelor de protejare a securității naționale și de combatere a infracționalității, o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare, ca urmare a caracterului incompatibil al acesteia cu 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.

214 Principiul supremației dreptului Uniunii consacră prevalența dreptului Uniunii asupra dreptului statelor membre Acest principiu impune, prin urmare, tuturor entităților statelor membre să dea efect deplin diferitor norme ale Uniunii, întrucât dreptul statelor membre nu poate afecta efectul recunoscut acestor diferite norme pe teritoriul statelor menționate [Hotărârea din 15 iulie 1964, Costa, 6/64, EU:C:1964:66, p. 1159 și 1160, precum și Hotărârea din 19 noiembrie 2019, A. K. și alții (Independența camerei disciplinare a Curții Supreme), C-585/18, C-624/18 și C-625/18, EU:C:2019:982, punctele 157 și 158 și jurisprudența citată].

215 În temeiul principiului supremației, în cazul în care nu poate să procedeze la o interpretare a reglementării naționale care să fie conformă cu cerințele dreptului Uniunii, instanța națională însărcinată cu aplicarea, în cadrul competenței proprii, a dispozițiilor dreptului Uniunii are obligația de a asigura efectul deplin al acestora, lăsând, la nevoie, neaplicată, din oficiu, orice dispoziție contrară a legislației naționale, chiar ulterioară, fără să solicite și fără să aștepte eliminarea prealabilă a acesteia pe cale legislativă sau prin orice alt procedeu constituțional [Hotărârea din 22 iunie 2010, Melki și Abdeli, C-188/10 și C-189/10, EU:C:2010:363, punctul 43 și jurisprudența citată, Hotărârea din 24 iunie 2019, Popławski, C-573/17, EU:C:2019:530, punctul 58, precum și Hotărârea din 19 noiembrie 2019, A. K. și alții (Independența camerei disciplinare a Curții Supreme), C-585/18, C-624/18 și C-625/18, EU:C:2019:982, punctul 160].

216 Numai Curtea poate, cu titlu excepțional și pentru considerații imperative de securitate juridică, să acorde o suspendare provizorie a efectului de înlăturare avut de o normă din dreptul Uniunii asupra dreptului național contrar acesteia. O asemenea limitare în timp a efectelor interpretării acestui drept de către Curte nu poate fi acordată decât în însăși hotărârea care se pronunță asupra interpretării

solicitate [a se vedea în acest sens Hotărârea din 23 octombrie 2012, Nelson și alții, C-581/10 și C-629/10, EU:C:2012:657, punctele 89 și 91, Hotărârea din 23 aprilie 2020, Herst, C-401/18, EU:C:2020:295, punctele 56 și 57, precum și Hotărârea din 25 iunie 2020, A și alții (Turbine eoliene la Aalter și la Nevele), C-24/19, EU:C:2020:503, punctul 84 și jurisprudența citată].

217 S-ar aduce atingere supremației și aplicării uniforme a dreptului Uniunii dacă instanțele naționale ar avea puterea de a conferi dispozițiilor naționale supremație în raport cu dreptul Uniunii față de care aceste dispoziții sunt contrare, chiar și numai cu titlu provizoriu (a se vedea în acest sens Hotărârea din 29 iulie 2019, Inter-Environnement Wallonie și Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, punctul 177, precum și jurisprudența citată).

218 Cu toate acestea, Curtea a statuat, într-o cauză în care era în discuție legalitatea unor măsuri adoptate cu încălcarea obligației prevăzute de dreptul Uniunii de a efectua o evaluare prealabilă a efectelor unui proiect asupra mediului și asupra unui sit protejat, că o instanță națională poate, dacă dreptul intern permite aceasta, să mențină în mod excepțional efectele unor astfel de măsuri atunci când această menținere este justificată de considerații imperative legate de necesitatea de a înlătura o amenințare reală și gravă de întrerupere a aprovizionării cu energie electrică a statului membru în cauză căreia nu i se poate face față prin alte mijloace și alternative, în special în cadrul pieței interne, menținerea respectivă neputând acoperi decât perioada strict necesară pentru remedierea nelegalității menționate (a se vedea în acest sens Hotărârea din 29 iulie 2019, Inter-Environnement Wallonie și Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, punctele 175, 176, 179 și 181).

219 Or, spre deosebire de omisiunea unei obligații procedurale precum evaluarea prealabilă a efectelor unui proiect în domeniul specific al protecției mediului, o încălcare a articolului 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, nu poate face obiectul unei regularizări pe calea unei proceduri comparabile cu cea menționată la punctul anterior. Astfel, menținerea efectelor unei legislații naționale precum cea în discuție în litigiul principal ar însemna că această legislație continuă să impună furnizorilor de servicii de comunicații electronice obligații care sunt contrare dreptului Uniunii și care implică ingerințe grave în drepturile fundamentale ale persoanelor ale căror date au fost stocate.

220 Prin urmare, instanța de trimitere nu poate aplica o dispoziție a dreptului său național care îi permite să limiteze în timp efectele unei declarații de nelegalitate pe care trebuie să o facă, în temeiul acestui drept, în privința legislației naționale în discuție în litigiul principal.

221 În aceste condiții, în observațiile prezentate Curții, VZ, WY și XX arată că a treia întrebare ridică, în mod implicit, dar necesar, problema dacă dreptul Uniunii se opune unei exploatări, în cadrul unei proceduri penale, a informațiilor și a elementelor de probă care au fost obținute printr-o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare incompatibilă cu acest drept.

222 În această privință și pentru a da un răspuns util instanței de trimitere, trebuie amintit că, în stadiul actual al dreptului Uniunii, revine, în principiu, numai dreptului național sarcina de a stabili normele referitoare la admisibilitatea și la aprecierea, în cadrul unei proceduri penale inițiate împotriva unor persoane suspectate de acte de infracționalitate gravă, a informațiilor și a elementelor de probă care au fost obținute printr-o asemenea stocare a datelor contrară dreptului Uniunii.

223 Astfel, rezultă dintr-o jurisprudență constantă că, în lipsa unor norme ale Uniunii în materie, revine ordinii juridice interne a fiecărui stat membru, în temeiul principiului autonomiei procedurale, atribuția de a stabili modalitățile procedurale aplicabile acțiunilor în justiție destinate să asigure protecția drepturilor conferite justițiabililor de dreptul Uniunii, cu condiția însă ca acestea să nu fie mai puțin favorabile decât cele aplicabile unor situații similare supuse dreptului intern (principiul echivalenței) și de a nu face imposibilă în practică sau excesiv de dificilă exercitarea drepturilor conferite de dreptul Uniunii (principiul efectivității) (a se vedea în acest sens Hotărârea din

6 octombrie 2015, Târșia, C-69/14, EU:C:2015:662, punctele 26 și 27, Hotărârea din 24 octombrie 2018, XC și alții, C-234/17, EU:C:2018:853, punctele 21 și 22, precum și jurisprudența citată, și Hotărârea din 19 decembrie 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, punctul 33).

224 În ceea ce privește principiul echivalenței, instanței naționale sesizate cu o procedură penală întemeiată pe informații sau pe elemente de probă obținute cu încălcarea cerințelor rezultate din Directiva 2002/58 îi revine sarcina de a verifica dacă dreptul național care guvernează această procedură prevede norme mai puțin favorabile în ceea ce privește admisibilitatea și exploatarea unor astfel de informații și a unor astfel de elemente de probă decât cele care reglementează informațiile și elementele de probă obținute cu încălcarea dreptului intern.

225 În ceea ce privește principiul efectivității, trebuie arătat că normele naționale referitoare la admisibilitatea și la exploatarea informațiilor și a elementelor de probă au ca obiectiv, în temeiul alegerilor efectuate de dreptul național, să evite ca informațiile și elementele de probă care au fost obținute în mod nelegal să prejudicieze în mod nejustificat o persoană suspectată de săvârșirea unor infracțiuni. Or, potrivit dreptului național, acest obiectiv poate fi atins nu numai printr-o interdicție de a exploata astfel de informații și astfel de elemente de probă, ci și prin norme și practici naționale care reglementează aprecierea și ponderarea informațiilor și a elementelor de probă sau chiar prin luarea în considerare a caracterului lor nelegal în cadrul stabilirii pedepsei.

226 În aceste condiții, reiese din jurisprudența Curții că necesitatea de a exclude informațiile și elementele de probă obținute cu încălcarea prevederilor dreptului Uniunii trebuie să fie apreciată printre altele în raport cu riscul pe care îl presupune admisibilitatea unor astfel de informații și elemente de probă pentru respectarea principiului contradictorialității și, prin urmare, a dreptului la un proces echitabil (a se vedea în acest sens Hotărârea din 10 aprilie 2003, Steffensen, C-276/01, EU:C:2003:228, punctele 76 și 77). Or, o instanță care consideră că o parte nu este în măsură să prezinte în mod eficient observații cu privire la un mijloc de probă care provine dintr-un domeniu care nu este cunoscut de judecători și care poate influența în mod preponderent aprecierea faptelor trebuie să constate o încălcare a dreptului la un proces echitabil și să excludă acest mijloc de probă pentru a evita o asemenea încălcare (a se vedea în acest sens Hotărârea din 10 aprilie 2003, Steffensen, C-276/01, EU:C:2003:228, punctele 78 și 79).

227 Prin urmare, principiul efectivității impune instanței penale naționale să înlăture informațiile și elementele de probă care au fost obținute prin intermediul unei stocări generalizate și nediferențiate a datelor de transfer și a datelor de localizare, incompatibilă cu dreptul Uniunii, în cadrul unei proceduri penale inițiate împotriva unor persoane suspectate de săvârșirea unor infracțiuni, în cazul în care persoanele respective nu sunt în măsură să prezinte în mod eficient observații cu privire la aceste informații și elemente de probă, care provin dintr-un domeniu care nu este cunoscut de judecători și care pot influența în mod preponderent aprecierea faptelor.

228 Având în vedere considerațiile care precedă, este necesar să se răspundă la cea de a treia întrebare formulată în cauza C-520/18 că o instanță națională nu poate aplica o dispoziție a dreptului său național care îi permite să limiteze în timp efectele unei declarații de nelegalitate pe care trebuie să o facă, în temeiul acestui drept, în privința unei legislații naționale care impune furnizorilor de servicii de comunicații electronice, în vederea, printre altele, a protejării securității naționale și a combaterii infracționalității, o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare, incompatibilă cu 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. Acest articol 15 alineatul (1), interpretat în lumina principiului efectivității, impune instanței penale naționale să înlăture informațiile și elementele de probă care au fost obținute printr-o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare, incompatibilă cu dreptul Uniunii, în cadrul unei proceduri penale inițiate împotriva unor persoane suspectate de săvârșirea unor infracțiuni, în cazul în care persoanele

respective nu sunt în măsură să prezinte în mod eficient observații cu privire la aceste informații și elemente de probă, care provin dintr-un domeniu care nu este cunoscut de judecători și care pot influența în mod preponderent aprecierea faptelor.

Cu privire la cheltuielile de judecată

229 Întrucât, în privința părților din litigiile principale, 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:

1) **Articolul 15 alineatul (1) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene, trebuie să fie interpretat în sensul că se opune unor măsuri legislative care prevăd, în scopurile prevăzute la acest articol 15 alineatul (1), cu titlu preventiv, o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare. În schimb, articolul 15 alineatul (1) din Directiva 2002/58, astfel cum a fost modificată prin Directiva 2009/136, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale, nu se opune unor măsuri legislative**

   – **care permit, în scopul protejării securității naționale, impunerea unei obligații furnizorilor de servicii de comunicații electronice de a efectua o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare, în situații în care statul membru în cauză se confruntă cu o amenințare gravă la adresa securității naționale, care se dovedește reală și actuală sau previzibilă, în condițiile în care decizia care prevede această obligație poate face obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie are efect obligatoriu, prin care se urmărește să se verifice existența uneia dintre aceste situații, precum și respectarea condițiilor și a garanțiilor care trebuie să fie prevăzute, iar obligația menționată nu poate fi impusă decât pentru o perioadă limitată în timp la strictul necesar, dar care poate fi reînnoită în cazul menținerii acestei amenințări;**

   – **care prevăd, în scopul protejării securității naționale, al combaterii infracționalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o stocare direcționată a datelor de transfer și a datelor de localizare care să fie delimitată, pe baza unor elemente obiective și nediscriminatorii, în funcție de categoriile de persoane vizate sau prin intermediul unui criteriu geografic, pentru o perioadă limitată în timp la strictul necesar, dar care poate fi reînnoită;**

   – **care prevăd, în scopul protejării securității naționale, al combaterii infracționalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o stocare generalizată și nediferențiată a adreselor IP atribuite sursei unei conexiuni, pentru o perioadă limitată în timp la strictul necesar;**

   – **care prevăd, în scopul protejării securității naționale, al combaterii infracționalității și al protejării siguranței publice, o stocare generalizată și nediferențiată a datelor referitoare la identitatea civilă a utilizatorilor de mijloace de comunicații electronice și**

– **care permit, în scopul combaterii infracționalității grave și, *a fortiori*, al protejării securității naționale, impunerea unei obligații furnizorilor de servicii de comunicații electronice, prin intermediul unei decizii a autorității competente, supuse unui control jurisdicțional efectiv, de a realiza, pentru o perioadă determinată, conservarea rapidă a datelor de transfer și a datelor de localizare de care dispun acești furnizori de servicii,**

din moment ce aceste măsuri garantează, prin norme clare și precise, că stocarea datelor în discuție este condiționată de respectarea condițiilor materiale și procedurale aferente acestora și că persoanele în cauză dispun de garanții efective împotriva riscurilor de abuz.

2) **Articolul 15 alineatul (1) din Directiva 2002/58, astfel cum a fost modificată prin Directiva 2009/136, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale, trebuie să fie interpretat în sensul că nu se opune unei reglementări naționale care impune furnizorilor de servicii de comunicații electronice să recurgă, pe de o parte, la analiza automatizată, precum și la colectarea în timp real printre altele a datelor de transfer și a datelor de localizare și, pe de altă parte, la colectarea în timp real a datelor tehnice referitoare la localizarea echipamentelor terminale utilizate, atunci când**

– **recurgerea la analiza automatizată se limitează la situațiile în care un stat membru se confruntă cu o amenințare gravă la adresa securității naționale, care se dovedește reală și actuală sau previzibilă, în condițiile în care recurgerea la această analiză poate face obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie are efect obligatoriu, prin care se urmărește să se verifice existența unei situații care justifică măsura menționată, precum și respectarea condițiilor și a garanțiilor care trebuie să fie prevăzute, iar**

– **recurgerea la colectarea în timp real a datelor de transfer și a datelor de localizare este limitată la persoanele în privința cărora există un motiv valabil pentru a suspecta că sunt implicate într-un mod sau altul în activități de terorism și este supusă unui control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă, a cărei decizie are efect obligatoriu, pentru a se asigura că o astfel de colectare în timp real nu este autorizată decât în limita a ceea ce este strict necesar. În caz de urgență justificată corespunzător, controlul trebuie să aibă loc în termen scurt.**

3) **Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (Directiva privind comerțul electronic) trebuie să fie interpretată în sensul că nu se aplică în materie de protecție a confidențialității comunicațiilor și a persoanelor fizice în raport cu prelucrarea datelor cu caracter personal în cadrul serviciilor societății informaționale, această protecție fiind, după caz, reglementată de Directiva 2002/58, astfel cum a fost modificată prin Directiva 2009/136, sau de Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46. Articolul 23 alineatul (1) din Regulamentul 2016/679, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale, trebuie să fie interpretat în sensul că se opune unei reglementări naționale care impune furnizorilor de acces la servicii de comunicații publice online și furnizorilor de servicii de stocare-hosting stocarea generalizată și nediferențiată printre altele a datelor cu caracter personal aferente acestor servicii.**

4) **O instanță națională nu poate aplica o dispoziție a dreptului său național care îi permite să limiteze în timp efectele unei declarații de nelegalitate pe care trebuie să o facă, în temeiul acestui drept, în privința unei legislații naționale care impune furnizorilor de servicii de**

comunicații electronice, în vederea, printre altele, a protejării securității naționale și a combaterii infracționalității, o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare, incompatibilă cu articolul 15 alineatul (1) din Directiva 2002/58, astfel cum a fost modificată prin Directiva 2009/136, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale. Acest articol 15 alineatul (1), citit în lumina principiului efectivității, impune instanței penale naționale să înlăture informațiile și elementele de probă care au fost obținute printr-o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare, incompatibilă cu dreptul Uniunii, în cadrul unei proceduri penale inițiate împotriva unor persoane suspectate de săvârșirea unor infracțiuni, în cazul în care persoanele respective nu sunt în măsură să prezinte în mod eficient observații cu privire la aceste informații și elemente de probă, care provin dintr-un domeniu care nu este cunoscut de judecători și care pot influența în mod preponderent aprecierea faptelor.

Semnături