Cauza C-793/19

Rezumatul cererii de decizie preliminară întocmit în temeiul articolului 98 alineatul (1) din Regulamentul de procedură al Curții de Justiție

Data depunerii:

29 octombrie 2019

Instanța de trimitere:

Bundesverwaltungsgericht (Curtea Administrativă Federală, Germania)

Data deciziei de trimitere:

25 septembrie 2019

Reclamantă și intimată în recurs:

Pârâtă și recurentă în recurs:

Bundesrepublik Deutschland (Republica Federală Germania)

Obiectul procedurii principale

Acțiune în constatarea inexistenței obligației SpaceNet de a stoca datele de transfer de telecomunicații menționate la articolul 113b alineatul (3) din TKG ale clienților cărora aceasta le furnizează acces la internet.

Obiectul și temeiul juridic al trimiterii preliminare

Interpretarea dreptului Uniunii şi, în special, a articolului 15 alineatul (1) din Directiva 2002/58, precum și a Hotărârii Tele2 Sverige și Watson și alții; articolul 267 TFUE.

Întrebarea preliminară

Articolul 15 din Directiva 2002/58/CE, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene, pe de o parte, și a articolului 6 din Carta drepturilor fundamentale a Uniunii Europene, precum și a articolului 4 din Tratatul privind Uniunea Europeană, pe de altă parte, trebuie interpretat în sensul că se opune unei reglementări naționale care impune prestatorilor de servicii publice de comunicații electronice să păstreze datele de transfer și de localizare ale utilizatorilor finali ai acestor servicii atunci când

– această obligație nu presupune existența unui motiv specific din punct de vedere geografic, temporal sau teritorial,

– obiectul obligației de stocare în cazul furnizării de servicii telefonice publice – inclusiv transmiterea de mesaje scurte, multimedia sau similare, precum și apelurile pierdute sau care au rămas fără răspuns – este reprezentat de următoarele date:

  – numărul de telefon sau alt identificator al liniei apelante și al liniei apelate, precum și în cazul redirecționărilor sau al transferurilor altei părți interesate,

  – data și ora de început și de sfârșit a conexiunii sau – în cazul transmiterii unui mesaj scurt, multimedia sau similar – momentul trimiterii și al primirii mesajului cu indicarea fusului orar respectiv,

  – indicații privind serviciul utilizat dacă în cadrul serviciului telefonic pot fi utilizate servicii diferite,

  – în plus, în cazul serviciilor de telefonie mobilă,

    – identificatorul internațional al abonatului mobil pentru linia apelantă și pentru linia apelată,

    – identificatorul internațional al terminalului de pe care se inițiază apelul și al celui apelat,

    – data și ora primei activări a serviciului cu indicarea fusului orar respectiv, dacă serviciile au fost plătite în avans,

    – denumirile celulelor care au fost utilizate de linia apelantă și de linia apelată la începutul conexiunii,

  – în cazul serviciilor telefonice prin internet, inclusiv adresele de protocol internet ale liniei apelante și ale liniei apelate și identificatorii de utilizator,

- în cadrul furnizării de servicii publice de acces la internet, obiectul obligației de stocare este reprezentat de următoarele date:
  - adresa de protocol internet alocată abonatului pentru utilizarea internetului,
  - un identificator clar al liniei prin intermediul căreia se utilizează internetul, precum și un identificator alocat utilizatorului,
  - data și ora de început și de sfârșit a utilizării internetului prin intermediul adresei de protocol internet alocate, cu indicarea fusului orar respectiv,
  - în cazul utilizării mobile, denumirea celulei utilizate la începutul conexiunii la internet,
- următoarele date nu pot fi stocate:
  - conținutul comunicației,
  - date privind site-urile internet accesate,
  - date ale serviciilor de poștă electronică,
  - datele de bază ale apelurilor către sau provenite de la anumite linii aparținând persoanelor, autorităților și organizațiilor din domeniul social sau religios,
- durata de păstrare pentru datele de localizare, și anume denumirea celulei utilizate, este de patru săptămâni, iar pentru celelalte date, durata păstrare este de zece săptămâni,
- este garantată o protecție eficientă a datelor păstrate împotriva riscurilor de abuz, precum și a accesului neautorizat și
- datele păstrate pot fi utilizate numai în scopul urmăririi unor fapte penale deosebit de grave și al prevenirii unui pericol concret pentru integritatea corporală, pentru viața sau pentru libertatea unei persoane ori pentru existența federației sau a unui land, cu excepția adresei de protocol internet alocate unui abonat pentru utilizarea internetului, a cărei utilizare este autorizată în cadrul accesului la informații privind datele stocate în vederea urmăririi oricăror fapte penale, prevenirii unui pericol pentru siguranța publică și ordinea publică, precum și pentru îndeplinirea sarcinilor serviciilor de informații?

Dispozițiile de drept al Uniunii invocate

Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”), articolele 6, 7, 8, 11 și 52

Tratatul privind Uniunea Europeană (TUE), articolele 4 și 6

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 (denumită în continuare „Directiva 2002/58”), articolele 5, 6, 8, 9, în special articolul 15, considerentul (11)

Dispozițiile naționale invocate

Telekommunikationsgesetz [Legea privind telecomunicațiile (denumită în continuare „TKG”)], articolul 113a alineatul (1) prima teză („Persoana obligată”), articolul 113b („Obligații privind stocarea datelor de transfer”), articolul 113c („Utilizarea datelor”), articolul 113d („Garantarea securității datelor”), articolul 113e [„Înregistrarea” (de către persoana obligată a accesului la datele stocate)], articolul 113f [„Catalog de cerințe” (în legătură cu dispozițiile tehnice și alte măsuri)], articolul 99 alineatul (2) („Facturarea detaliată”, punctele excluse de la identificare în cadrul facturărilor detaliate)

Strafprozessordnung [Codul de procedură penală (denumit în continuare „StPO”)], articolul 100g alineatul (2) („Colectarea datelor de transfer” potrivit articolului 113b din TKG)

Jurisprudența Curții de Justiție citată

Hotărârea Curții de Justiție a Uniunii Europene din 21 decembrie 2016, Tele2 Sverige și Watson și alții, C-203/15 și C-698/15, EU:C:2016:970 (denumită în continuare „Hotărârea Tele2 Sverige și Watson și alții”)

Hotărârea din 8 aprilie 2014, Digital Rights Ireland și Seitlinger și alții, C-293/12 și C-594/12, EU:C:2014:238 (denumită în continuare „Hotărârea Digital Rights Ireland și alții”)

Avizul 1/15 din 26 iulie 2017, EU:C:2017:592

De asemenea: Hotărârea din 29 iulie 2019, Funke Medien (C-469/17, EU:C:2019:623), Hotărârea din 9 martie 1978, Simmenthal (106/77, EU:C:1978:49), Hotărârea din 3 mai 2005, Berlusconi și alții (C-387/02, C-391/02 și C-403/02, EU:C:2005:270), Hotărârea din 22 iunie 2010, Melki și Abdeli (C-

188/10 și C-189/10, EU:C:2010:363), Hotărârea din 18 septembrie 2014, Vueling Airlines (C-487/12, EU:C: 2014:2232).

Prezentare succintă a situației de fapt și a procedurii

1 Reclamanta, SpaceNet AG (denumită în continuare „reclamanta” sau „SpaceNet”) furnizează servicii publice de acces la internet. Aceasta contestă obligația stabilită în sarcina sa prin articolul 113a alineatul (1) coroborat cu articolul 113b din TKG, astfel cum a fost modificată prin Legea din 10 decembrie 2015, de a păstra datele de transfer de telecomunicații ale clienților ei începând de la 1 iulie 2017.

2 În primă instanță, Verwaltungsgericht [Tribunalul Administrativ] a constatat că SpaceNet nu este obligată să stocheze datele de transfer de telecomunicații menționate la articolul 113b alineatul (3) din TKG ale clienților săi cărora aceasta le furnizează acces la internet. Pârâta, Bundesrepublik Deutschland (denumită în continuare „pârâta”), a formulat recurs împotriva hotărârii pronunțate de Verwaltungsgericht.

3 Recursul poate fi admis numai dacă obligația prevăzută de dispozițiile TKG menționate, impusă furnizorilor de servicii publice de telecomunicații (denumiți în continuare „furnizori de telecomunicații”) privind păstrarea datelor de transfer de telecomunicații nu încalcă dreptul Uniunii.

4 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten [legea de stabilire a unei obligații de stocare și a unui termen maxim pentru stocarea datelor de transfer din 10 decembrie 2015 (denumită în continuare „Legea din 10 decembrie 2015”)] a instituit un nou regim privind această obligație a furnizorilor de telecomunicații de a stoca anumite date de transfer pentru o perioadă limitată.

5 Noua reglementare era necesară după ce printr-o hotărâre din anul 2010, Bundesverfassungsgericht [Curtea Constituțională Federală] declarase nevalide dispozițiile anterioare care reglementau păstrarea datelor, ca urmare a unei încălcări a drepturilor fundamentale și, de asemenea, după ce Directiva 2006/24 pentru a cărei transpunere fuseseră adoptate dispozițiile anterioare în cauză, a fost declarată nevalidă în anul 2014, prin Hotărârea Digital Rights Ireland și alții. Legea din 10 decembrie 2015 este menită să completeze lacunele în legătură cu urmărirea penală și cu prevenirea riscurilor, respectând totodată prevederile de drept constituțional și de drept al Uniunii care decurg din deciziile menționate.

6 Pentru a răspunde la întrebarea preliminară dacă obligația de stocare impusă prin articolul 113a alineatul (1) coroborat cu articolul 113b din TKG încalcă dreptul Uniunii, este necesară interpretarea de către Curte a Directivei 2002/58, în special, o precizare privind modul în care trebuie înțeleasă Hotărârea Tele2 Sverige și Watson și alții.

Prezentare succintă a motivării trimiterii preliminare

7 Obligația de stocare a datelor de transfer de telecomunicații prevăzută la articolul 113a alineatul (1) prima teză coroborat cu articolul 113b din TKG restrânge drepturile prevăzute la articolul 5 alineatul (1), la articolul 6 alineatul (1) și la articolul 9 alineatul (1) din Directiva 2002/58.

8 Aceasta constituie o ingerință în confidențialitatea comunicațiilor electronice, astfel cum este aceasta protejată la articolul 5 alineatul (1) prima teză din directivă și este contrară principiului potrivit căruia, în principiu, oricăror altor persoane decât utilizatorii le este interzisă stocarea, fără acordul utilizatorilor, a datelor de transfer aferente comunicațiilor electronice.

9 De asemenea, aceasta nu respectă prevederea articolului 6 din directivă potrivit căreia prelucrarea și stocarea datelor de transfer sunt permise numai în măsura și pe durata necesare comercializării serviciilor sau furnizării unor servicii suplimentare.

10 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, articolul 9 alineatul (1) prima teză din Directiva 2002/58 prevede că 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. Reglementarea legislativă derogă și de la această prevedere în măsura în care, potrivit articolului 113b alineatul (1) punctul 2 coroborat cu alineatul (4) din TKG, este necesară și stocarea datelor de localizare menționate de acesta.

11 Restrângerea drepturilor prevăzute la articolul 5 alineatul (1), la articolul 6 alineatul (1) și la articolul 9 alineatul (1) din Directiva 2002/58/CE nu este justificată decât dacă dispoziția prevăzută la 113a alineatul (1) prima teză coroborat cu articolul 113b din TKG poate fi întemeiată pe articolul 15 alineatul (1) din Directiva 2002/58.

12 Potrivit acestei din urmă dispoziții, statele membre pot adopta măsuri legislative pentru a restrânge sfera de aplicare a drepturilor și obligațiilor prevăzute la articolul 5, articolul 6, articolul 8 alineatele (1), (2), (3) și (4) și articolul 9 ale prezentei directive, în cazul în care restrângerea lor constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice pentru a proteja securitatea națională (de exemplu, siguranța statului), apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice, în conformitate cu articolul 13 alineatul (1) al Directivei 95/46. În acest scop, statele membre pot adopta, *inter alia*, măsuri legislative care să permită reținerea de date, pe perioadă limitată, pentru motivele arătate anterior în acest alineat. Toate măsurile menționate în acest alineat trebuie să fie conforme cu principiile generale

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

13 În Hotărârea Tele2 Sverige și Watson și alții, în special la punctul 82 și următoarele și la punctul 108 și următoarele, Curtea a declarat că admisibilitatea unei reglementări naționale privind păstrarea datelor în temeiul articolului 15 alineatul (1) din Directiva 2002/58 presupune existența unui motiv suficient. Acest lucru înseamnă că sunt vizate numai persoanele care oferă un indiciu care să sugereze o legătură cu infracțiuni grave, că o delimitare are loc în ceea ce privește regiunea, perioada, precum și mijloacele de comunicare relevante în această privință și că vor fi colectate numai datele care sunt indispensabile pentru instrumentarea infracțiunilor menționate.

14 Opinia pârâtei potrivit căreia însăși utilizarea serviciilor de acces la internet sau de telefonie ar trebui să fie considerată un motiv suficient pentru stocare, este în mod vădit în contradicție cu aceasta. Ipoteza exprimată în Hotărârea Tele2 Sverige și Watson și alții privind o încălcare generală a dreptului Uniunii în cazul oricărei păstrări fără motiv a datelor nu este pusă în discuție nici prin menționarea de către pârâtă a Avizului Curții din 26 iulie 2017 referitor la acordul dintre Canada și Uniunea Europeană privind transferul datelor din registrul cu numele pasagerilor aerieni. Chiar dacă în cadrul sublinierii caracterului necesar al ingerințelor în drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal, Curtea a arătat că datele PNR sunt transmise Canadei, indiferent dacă există indicii obiective care să permită concluzia că pasagerii aerieni prezintă un pericol pentru siguranța publică în Canada, în acest caz nu este vorba însă despre o păstrare fără motiv a datelor, întrucât stocarea și transmiterea sunt legate de controalele la frontieră la care, în conformitate cu prevederile legislației canadiene în vigoare, sunt supuși toți pasagerii aerieni care doresc să călătorească în și din Canada. Motivul păstrării nu mai există în cazul plecării pasagerilor aerieni. Prin urmare, păstrarea după această dată presupune – ca motiv nou – existența unor indicii obiective care să sugereze că pasagerii aerieni respectivi ar putea prezenta un risc în legătură cu combaterea terorismului și a altor infracțiuni transnaționale grave.

15 În cazul în care jurisprudența Curții trebuie interpretată în sensul că o păstrare fără motiv a datelor nu este în niciun caz compatibilă cu dreptul Uniunii, recursul pârâtei formulat împotriva hotărârii atacate pronunțată de Verwaltungsgericht nu poate fi admis, întrucât, asemenea dispozițiilor suedeze și britanice privind păstrarea datelor care au făcut obiectul Hotărârii Tele2 Sverige și Watson și alții, articolul 113a alineatul (1) prima teză coroborat cu articolul 113b din TKG nu impune existența unui motiv pentru stocare – dincolo de simpla utilizare a serviciilor de acces la internet sau a serviciilor de telefonie – și nici a unei legături între datele stocate și o faptă penală sau un pericol pentru siguranța publică. Dimpotrivă, este vorba despre o dispoziție care impune stocarea fără motiv, generalizată și nediferențiată din punct de vedere personal, temporal și geografic a unei părți semnificative a tuturor datelor de transfer de telecomunicații relevante.

16 În pofida considerațiilor din Hotărârea Tele2 Sverige și Watson și alții, instanța de trimitere nu exclude însă ca obligația prevăzută la articolul 113a alineatul (1) prima teză coroborat cu articolul 113b din TKG privind păstrarea fără motiv a datelor de transfer de telecomunicații să poată fi întemeiată pe articolul 15 alineatul (1) din Directiva 2002/58, pentru următoarele motive:

17 În primul rând, reglementarea prevăzută de dispozițiile din TKG în discuție nu impune stocarea tuturor datelor de transfer de telecomunicații ale tuturor abonaților și utilizatorilor înregistrați în legătură cu toate mijloacele de comunicare electronică. Din domeniul de aplicare al obligației de stocare nu este exclus numai conținutul comunicațiilor, ci sunt excluse și datele privind site-urile internet accesate, datele serviciilor de e-mail, precum și datele de bază ale apelurilor către sau provenite de la anumite linii din domeniul social sau religios [a se vedea articolul 113b alineatele (5) și (6) din TKG]. În cazul în care, din domeniul de aplicare al obligației sunt excluse anumite mijloace de comunicare sau categorii de date, acest lucru nu poate înlătura riscul de elaborare a unui profil complet al persoanelor în cauză, dar, cel puțin, poate reduce în mod semnificativ acest risc.

18 În al doilea rând, instanța de trimitere consideră că o diferență și mai importantă între dispozițiile TKG în discuție în speță și regimul anterior prevăzut de Directiva 2006/24 sau de dispozițiile suedeze și britanice care se întemeiază pe acesta – în discuție în Hotărârea Tele2 Sverige și Watson și alții – constă în faptul că perioada de păstrare cuprinsă între șase luni și doi ani (a se vedea articolul 6 din Directiva 2006/24) a fost scurtată în mod considerabil, potrivit articolului 113b alineatul (1) din TKG, la patru, respectiv la zece săptămâni.

19 Riscul de elaborare a unui profil complet al persoanelor în cauză trebuie să fie considerat cu atât mai scăzut, cu cât perioadele de stocare a datelor de transfer sunt mai reduse. Cu cât perioada de stocare este mai redusă, cu atât mai lacunar este, în mod inevitabil, profilul de personalitate și cu atât mai scăzută este intensitatea ingerinței în drepturile fundamentale.

20 În al treilea rând, dispozițiile TKG în discuție în speță fac obiectul unor restricții stricte în ceea ce privește protecția datelor stocate și accesul la aceste date. Pe de o parte, prevederile articolului 113d și următoarele din TKG garantează o protecție eficientă a datelor păstrate împotriva riscului de abuz, precum și a accesului neautorizat. Pe de altă parte, datele păstrate în temeiul articolului 113c alineatul (1) din TKG nu pot fi utilizate decât în scopul urmăririi unor fapte penale deosebit de grave și al prevenirii unui pericol concret pentru integritatea corporală, pentru viața sau pentru libertatea unei persoane ori pentru existența federației sau a unui land.

21 Potrivit articolului 100g alineatul (2) din StPO, colectarea datelor de transfer în scopul urmării penale presupune existența suspiciunii de săvârșire a unor fapte penale deosebit de grave prevăzute în mod limitativ de lege, fapta să fie deosebit de gravă inclusiv în speță, cercetarea situației de fapt sau stabilirea locului de

ședere al persoanei în cauză să fie îngreunată considerabil sau imposibilă în alt mod, iar colectarea datelor să fie proporțională cu importanța cauzei. În temeiul articolului 100g alineatul (4) din StPO, sunt inadmisibile colectarea sau utilizarea datelor de transfer ale persoanelor care dețin secrete profesionale menționate la articolul 53 alineatul (1) prima teză punctele 1-5 din StPO, printre care se numără, de exemplu, avocații, medicii sau jurnaliștii. În plus, articolul 101a alineatul (1) din StPO prevede existența unei hotărâri judecătorești pentru colectarea datelor de transfer prevăzute la articolul 100g din StPO.

22 Desigur, aceste dispoziții restrictive privind accesul nu sunt aplicabile în cazul adresei de protocol internet alocată abonatului pentru utilizarea internetului. Astfel, potrivit articolului 113c alineatul (1) punctul 3 din TKG, aceasta poate fi utilizată, de asemenea, în cadrul accesului la informații privind datele stocate în vederea urmăririi faptelor penale, prevenirii pericolelor pentru siguranța publică și ordinea publică, precum și pentru îndeplinirea sarcinilor serviciilor de informații. Cu toate acestea, este necesar să se considere că accesul la informațiile referitoare la titularul conectat la internet printr-o adresă de protocol internet deja cunoscută nu autorizează elaborarea profilurilor de personalitate și de deplasare.

23 Chiar dacă ar fi primită argumentația SpaceNet și s-ar presupune că sunt utilizate tot mai mult proceduri tehnice în cazul cărora o adresă de protocol internet nu mai poate fi atribuită unei anumite linii de telecomunicații, ci doar unui grup mai mare de linii și, prin urmare, accesul la informații privind datele stocate a evoluat într-o măsură de amploare, intensitatea ingerinței unui astfel de acces la informații privind datele stocate rămâne net inferioară inclusiv celei aferente solicitării și utilizării datelor de transfer de telecomunicații.

24 În al patrulea rând, în favoarea ipotezei că obligația prevăzută la articolul 113a alineatul (1) prima teză coroborat cu articolul 113b din TKG privind păstrarea fără motiv a datelor de transfer de telecomunicații se poate întemeia pe articolul 15 alineatul (1) din Directiva 2002/58, pledează inclusiv faptul că legiuitorul național s-a conformat obligațiilor de acțiune care decurg pentru statele membre din dreptul la siguranță garantat de articolul 6 din cartă. În Hotărârea Digital Rights Ireland și alții, Curtea a menționat în mod expres articolul 6 din cartă, indicând în acest context că combaterea terorismului internațional pentru menținerea păcii și a securității internaționale constituie un obiectiv de interes general al Uniunii și că același lucru este valabil în ceea ce privește combaterea criminalității grave în scopul garantării siguranței publice.

25 În acest context, instanța de trimitere are îndoieli cu privire la aspectul dacă jurisprudența anterioară a Curții trebuie interpretată în sensul că o păstrare fără motiv a datelor nu se poate întemeia pe articolul 15 alineatul (1) din Directiva 2002/58 nici în configurația concertă – astfel cum s-a regăsit în Directiva 2006/24 și în dispozițiile suedeze și britanice întemeiate pe aceasta – și nici în general. Astfel, conceptul fundamental al păstrării datelor nu trebuie adus în conformitate cu cerința Curții, formulată fără rezerve, potrivit căreia datele care urmează a fi stocate trebuie diferențiate în funcție de persoane, perioade și zone geografice.

26 Împotriva ipotezei conform căreia păstrarea fără motiv a datelor de transfer ar fi incompatibilă *per se* cu carta, militează, din punctul de vedere al instanței de trimitere, și necesitatea creării unui echilibru între obligația statelor membre de a asigura siguranța persoanelor care se află pe teritoriul acestora, pe de o parte, și respectarea drepturilor fundamentale consacrate la articolele 7 și 8 din cartă, pe de altă parte.

27 Prin urmare, instanța de trimitere nu poate deduce în mod clar din jurisprudența Curții că legiuitorul național nu ar mai avea posibilitatea de a institui o păstrare fără motiv a datelor – eventual, completată prin dispoziții stricte privind accesul – pe baza unei comparații globale, pentru a lua în considerare riscurile potențiale specifice corelate cu noile mijloace de telecomunicații.

28 În al cincilea rând, instanța de trimitere arată că, în cazul în care o păstrare fără motiv a datelor nu s-ar putea întemeia, în general, pe articolul 15 alineatul (1) din Directiva 2002/58 și, prin urmare, nu prezintă importanță dispozițiile specifice privind mijloacele de comunicare vizate, categoriile de date care trebuie păstrate, perioada de păstrare, condițiile de acces la datele păstrate și protecția împotriva riscurilor de abuz, ar fi limitată în mod considerabil marja de manevră lăsată legiuitorului național într-un domeniu al urmăririi penale și al siguranței publice care, potrivit articolului 4 alineatul (2) a treia teză TUE rămân în orice caz, în principiu, responsabilitatea exclusivă a fiecărui stat membru.

29 În sfârșit, în al șaselea rând, aspectul dacă considerațiile Curții din Hotărârea Tele2 Sverige și Watson și alții trebuie interpretate în sensul unei interdicții adresate statelor membre de a întemeia instituirea unei obligații privind păstrarea fără motiv a datelor de transfer de telecomunicații pe articolul 15 alineatul (1) din Directiva 2002/58, nu este considerat de către instanța de trimitere ca fiind clarificat, inclusiv în contextul jurisprudenței recente a Curții Europene a Drepturilor Omului (denumită în continuare „CEDO”).

30 Recent, într-o hotărâre din 19 iunie 2018, CEDO a statuat că legislația suedeză privind supravegherea de masă a traficului transfrontalier de date este în conformitate cu articolul 8 din Convenția Europeană pentru Protecția Drepturilor Omului și a Libertăților Fundamentale (denumită în continuare „CEDO”). Având în vedere amenințările cu care se confruntă în prezent statele, printre care se numără terorismul global și alte infracțiuni grave cum ar fi traficul de droguri, traficul de persoane, exploatarea sexuală a copiilor și criminalitatea informatică, precum și progresele tehnologice care înlesnesc nedescoperirea pe internet a teroriștilor și a infractorilor și caracterul imprevizibil al căilor de transmitere a datelor electronice, decizia de a institui un sistem de supraveghere de masă pentru a identifica amenințările necunoscute până în prezent la adresa securității naționale ar intra în sfera puterii de apreciere a statului (CEDO, Hotărârea din 19 iunie 2018 – nr. 35252/08 [ECLI: CE:ECHR:2018:0619JUD003525208], Centrum för Rättvisa împotriva Suediei – punctul 112). În măsura în care Curtea Europeană a Drepturilor Omului face trimitere la caracterul imprevizibil al căilor de transmitere a datelor, precum și la progresele tehnologice care înlesnesc

nedescoperirea teroriștilor și a infractorilor pe internet, aceasta subliniază mai mult decât Curtea de Justiție a Uniunii Europene riscurile potențiale specifice corelate cu noile mijloace de telecomunicații.

31 Instanța de trimitere face referire la considerentul (11) al Directivei 2002/58 și la articolul 52 alineatul (3) din cartă din care reiese că ar trebui să se asigure coerența necesară între drepturile prevăzute de aceasta și drepturile corespunzătoare garantate de CEDO, fără a aduce atingere autonomiei dreptului Uniunii și Curții de Justiție a Uniunii Europene.

32 În încheiere, instanța de trimitere evocă alte proceduri preliminare pendinte care privesc o interpretare a Hotărârii Tele2 Sverige și Watson și alții, și anume, privind aspectul dacă din aceasta trebuie să se deducă o interdicție generală privind păstrarea fără motiv a datelor care nu poate fi depășită nici în ceea ce privește importanța pericolelor care trebuie combătute pentru siguranța publică, nici în cadrul unei „compensări” prin dispoziții restrictive privind accesul și cerințe ridicate de securitate.

33 În acest sens, sunt menționate cererea de decizie preliminară formulată de Investigatory Powers Tribunal – London (Regatul Unit) (C-623/17), cererea de decizie preliminară formulată de Conseil d'État (Franța) (C-511/18 și C-512/18) și cererea de decizie preliminară formulată de Curtea Constituțională din Belgia (C-520/18).