CONCLUZIILE AVOCATULUI GENERAL
DOMNUL CAMPOS SÁNCHEZ-BORDONA
prezentate la 15 ianuarie 2020[1]

Cauzele conexate C-511/18 și C-512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (C-511/18)
împotriva
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

[cerere de decizie preliminară formulată de Conseil d'État (Consiliul de stat, acționând în calitate de Curte Supremă de Contencios Administrativ, Franța)]

„Întrebare preliminară – Prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice – Protecția securității naționale și combaterea terorismului – Directiva 2002/58/CE – Domeniu de aplicare – Articolul 1 alineatul (3) – Articolul 15 alineatul (3) – Articolul 4 alineatul (2) TUE – Carta Drepturilor Fundamentale a Uniunii Europene – Articolele 6, 7, 8, 11 și 47 și articolul 52 alineatul (1) – Păstrare generalizată și nediferențiată a datelor de conectare și a datelor care permit identificarea creatorilor de conținut – Colectarea datelor de transfer și de localizare – Acces la date"

1. În ultimii ani, Curtea a menținut o linie jurisprudențială constantă cu privire la păstrarea și la accesarea datelor cu caracter personal, dintre care reprezintă repere majore:

– Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții[2], în care aceasta a declarat nevaliditatea Directivei 2006/24/CE[3], deoarece permite o ingerință disproporționată în drepturile consacrate la articolele 7 și 8 din Carta Drepturilor Fundamentale a Uniunii Europene (denumită în continuare „carta");

– Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții[4], în care aceasta a interpretat articolul 15 alineatul (1) din Directiva 2002/58/CE[5];

1 Limba originală: spaniola.

2 Cauzele C-293/12 și C-594/12, în continuare „Hotărârea Digital Rights", EU:C:2014:238.

3 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).

4 Cauzele C-203/15 și C-698/15, în continuare „Hotărârea Tele2 Sverige și Watson", EU:C:2016:970.

5 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).

– Hotărârea din 2 octombrie 2018, Ministerio Fiscal[6], în care aceasta a confirmat interpretarea aceleiași dispoziții din Directiva 2002/58.

2. Hotărârile respective (în special a doua) preocupă autoritățile din anumite state membre, deoarece, în opinia lor, le privează de un instrument pe care îl consideră indispensabil pentru protecția securității naționale și pentru combaterea criminalității și a terorismului. Prin urmare, o parte dintre aceste state membre solicită revocarea sau nuanțarea jurisprudenței respective.

3. Anumite instanțe din statele membre au subliniat această preocupare în patru trimiteri preliminare[7], în privința cărora prezentăm concluzii la aceeași dată.

4. În cele patru cauze se ridică în primul rând problema aplicării Directivei 2002/58 la activitățile legate de securitatea națională și de combaterea terorismului. Dacă directiva respectivă ar fi aplicabilă în acest context, ar trebui să se stabilească în continuare în ce măsură li se permite statelor membre să restrângă dreptul la respectarea vieții private protejat de aceasta. În ultimul rând, va trebui să se analizeze măsura în care diversele legislații naționale (engleză[8], belgiană[9] și franceză[10]) în această materie respectă dreptul Uniunii, astfel cum a fost interpretat de Curte.

I. Cadrul normativ

A. Dreptul Uniunii

1. Directiva 2002/58

5. În temeiul articolului 1 („Sfera de aplicare și scopul”):

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

[…]

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

6 Cauza C-207/16, denumită în continuare „Hotărârea Ministerio Fiscal”, EU:C:2018:788.

7 În afar de acestea două (cauzele C-511/18 și C-512/18), a se vedea Hotărârea C-623/17, Privacy International, și Hotărârea C-520/18, Ordre des barreaux francophones et germanophone și alții.

8 Hotărârea Privacy International, C-623/17.

9 Hotărârea Ordre des barreaux francophones et germanophone și alții, C-520/18.

10 Hotărârea La Quadrature du Net și alții, C-511/18 și C-512/18.

6. Articolul 3 („Serviciile vizate”) subliniază:

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

7. Articolul 5 alineatul (1) („Confidențialitatea comunicațiilor”) prevede:

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

8. Articolul 6 („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.”

9. Articolul 15 („Aplicarea anumitor dispoziții ale Directivei 95/46/CE”[11]) alineatul (1) arată:

„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/CE. 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.”

11 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).

2. Directiva 2000/31/CE[12]

10. Articolul 14 prevede:

„(1) Statele membre veghează ca atunci când un serviciu al societății informaționale constă în stocarea informațiilor furnizate de un destinatar al serviciului, furnizorul acelui serviciu să nu fie responsabil pentru informațiile stocate la cererea unui destinatar al serviciului, cu condiția ca:

[…]

(3) Prezentul articol nu afectează posibilitatea ca o instanță judecătorească sau o autoritate administrativă să impună furnizorului de servicii, în conformitate cu cadrul legislativ din statele membre, să pună capăt unei încălcări sau să o prevină și nici nu afectează posibilitatea ca statele membre să instituie proceduri de reglementare a eliminării informațiilor sau blocării accesului la acestea.”

11. Conform articolului 15:

„(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.”

3. Regulamentul (UE) 2016/679[13]

12. În conformitate cu articolul 2 („Domeniul de aplicare material”):

„(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;

(c) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice;

12 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).

13 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/CE (Regulamentul general privind protecția datelor) (JO 2016, L 119, p. 1).

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

[…]”

13. În temeiul alineatului (1) al articolului 23 („Restricții”):

„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.”

14. Articolul 95 („Relația cu Directiva 2002/58/CE”) 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/CE.”

B. Dreptul național

1. Code de la sécurité intérieure (Codul privind securitatea internă)

15. În conformitate cu articolul L. 851-1:

„În condițiile prevăzute în capitolul 1 din titlul II al prezentei cărți, se poate autoriza colectarea de la operatorii de comunicații electronice și de la persoanele menționate la articolul L. 34-1 din code des postes et des communications électroniques [(Codul serviciilor poștale și al comunicațiilor electronice)], 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)], de informații sau de documente prelucrate sau păstrate prin rețelele lor sau prin serviciile de comunicații electronice, inclusiv de date tehnice referitoare la identificarea numerelor de abonament sau de conectare la serviciile de comunicații electronice, la inventarul tuturor 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 […]".

16. Articolele L. 851-2 și L. 851-4 reglementează, în funcție de diversele scopuri și modalități, accesul administrativ în timp real la datele de conectare astfel păstrate.

17. Articolul L. 851-2 autorizează, exclusiv în scopul prevenirii terorismului, colectarea informațiilor sau a documentelor menționate la articolul L. 851-1 de la aceleași persoane. Această colectare, care privește numai una sau mai multe persoane identificate în prealabil ca fiind susceptibile să aibă legătură cu o amenințare teroristă, are loc în timp real. În mod analog, articolul L. 851-4 din același cod autorizează transmiterea în timp real de către operatori numai a datelor tehnice referitoare la localizarea echipamentelor terminale [14].

18. În temeiul articolului L. 851-3, operatorii de comunicații electronice și prestatorii de servicii tehnice pot fi obligați „să efectueze în rețelele lor prelucrări automatizate de date destinate, în funcție de parametrii stabiliți în autorizație, să detecteze conexiuni care pot indica o amenințare teroristă" [15].

19. Articolul L. 851-5 prevede că, în anumite condiții, „se poate autoriza utilizarea unui dispozitiv tehnic care permite localizarea în timp real a unei persoane, a unui vehicul sau a unui obiect".

20. În conformitate cu articolul L. 851-6 alineatul I, este posibilă, în anumite condiții, „colectarea […] directă, prin intermediul unui aparat sau al unui dispozitiv tehnic menționat la articolul 226-3 alineatul (1) din code pénal [(Codul penal)], datele tehnice de conectare care permit identificarea unui echipament terminal sau a numărului de abonat al utilizatorului său, precum și datele privind localizarea echipamentelor terminale utilizate".

14 Potrivit instanței de trimitere, aceste tehnici nu creează pentru prestatorii de servicii o obligație de păstrare suplimentară față de cea impusă pentru facturarea și pentru comercializarea serviciilor lor, precum și pentru prestarea de servicii cu valoare adăugată.

15 În opinia instanței de trimitere, tehnica respectivă, care nu implică o păstrare generalizată și nediferențiată de date, urmărește numai colectarea, pentru o perioadă limitată, dintre toate datele de conectare prelucrate de persoanele respective, a celor care ar putea avea legătură cu o infracțiune gravă de această natură.

2. Codul serviciilor poștale și al comunicațiilor electronice

21. În conformitate cu articolul L. 34-1, în versiunea aplicabilă situației de fapt:

„I. Prezentul articol se aplică prelucrării datelor cu caracter personal în contextul furnizării de servicii publice 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.

Furnizorii de servicii de comunicații electronice publice stabilesc, în conformitate cu dispozițiile alineatului anterior, proceduri interne pentru soluționarea cererilor autorităților competente.

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

III. În scopul investigării, al verificării și al urmăririi penale a infracțiunilor sau al executării obligației definite la articolul L. 336-3 din code de la propriété intellectuelle [(Codul privind proprietatea intelectuală)] sau în scopul prevenirii atacurilor asupra sistemelor de prelucrare automatizată a datelor prevăzute și pedepsite la articolele 323-1-323-3-1 din 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 privind proprietatea intelectuală sau către autoritatea națională pentru securitatea sistemelor informative menționată la articolul L. 2321-1 din cod 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 decretul 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 păstrării 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 garantate cu titlul respectiv, la cererea statului, de către operatori.

[…]

VI. Datele păstrate și prelucrate în condițiile stabilite la alineatele III, IV și V se referă exclusiv la identificarea utilizatorilor serviciilor furnizate de operatori, la caracteristicile tehnice ale comunicațiilor furnizate de aceștia din urmă și la locația 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.

Păstrarea și prelucrarea datelor se efectuează în conformitate cu dispozițiile Legii 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."

22. În temeiul articolului R. 10-13 alineatul I, operatorii trebuie să păstreze, în scopul investigării, al constatării și al urmăririi penale a infracțiunilor, următoarele date:

„a) informațiile care permit identificarea utilizatorului;

b) datele privind echipamentele terminale de comunicații utilizate;

c) caracteristicile tehnice, precum 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."

23. În conformitate cu alineatul II al aceleiași dispoziții, în cazul activităților de telefonie, operatorul trebuie să păstreze de asemenea datele care permit identificarea originii și localizarea comunicației.

24. În conformitate cu alineatul III al aceluiași articol, datele menționate trebuie păstrate timp de un an de la data înregistrării lor.

3. Loi n.º 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)

25. Articolul 6 alineatul II primul paragraf prevede că persoanele a căror activitate constă în furnizarea accesului la serviciile de comunicații publice online și persoanele 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 „au obligația să stocheze și să păstreze datele astfel încât să permită identificarea oricărei persoane care a contribuit la crearea conținutului sau a unuia dintre conținuturile serviciilor pe care le prestează".

26. Alineatul II al treilea paragraf al dispoziției respective subliniază că autoritatea judiciară poate solicita acestor persoane să comunice datele menționate la primul paragraf.

27. Conform alineatului II ultimul paragraf, prin decretul adoptat de Conseil d'État (Consiliul de Stat), „se definesc datele menționate la primul paragraf și se determină durata și modalitățile de păstrare a acestora" [16].

16 Definiția s-a stabilit prin décret n.º 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 păstrarea datelor care permit identificarea oricărei persoane care a contribuit la crearea unui conținut oferit online). Din acest decret, se remarcă: a) articolul 1 alineatul 1, conform căruia cei care oferă acces la serviciile de comunicații publice online trebuie să păstreze următoarele date: identificatorul conexiunii, identificatorul atribuit abonatului, identificatorul terminalului utilizat pentru conectare, data și ora inițierii și a încheierii conexiunii, caracteristicile liniei abonatului; b) conform articolului 1 alineatul 2, persoanele 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 destinatari ai acestor servicii, au obligația să păstreze, pentru fiecare operațiune, următoarele date: identificatorul conexiunii din care provine comunicația, identificatorul atribuit conținutului care face obiectul operațiunii, tipurile de protocoale utilizate pentru conectarea la serviciu și pentru transferul de conținuturi, natura operațiunii, data și ora operațiunii, identificatorul utilizat de autorul operațiunii și c) în sfârșit, articolul 1 alineatul 3 prevede că persoanele menționate la cele două alineate anterioare trebuie să păstreze următoarele informații furnizate de un utilizator cu ocazia încheierii unui contract sau a creării unui cont: identificatorul conexiunii folosite la momentul creării contului; numele, prenumele sau denumirea comercială; adrese poștale asociate, pseudonimele folosite, adresele de e-mail sau cele asociate contului, numerele de telefon, parola actualizată și datele pentru verificarea sau modificarea ei.

II. Situația de fapt și întrebările preliminare

A. Cauza C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net și Fédération des fournisseurs d'accès à internet associatifs (denumite în continuare „reclamantele") au solicitat Conseil d'État (Consiliul de Stat) anularea mai multor decrete de punere în aplicare a anumitor dispoziții din Codul privind securitatea internă [17].

29. Reclamantele susțineau în esență că atât decretele atacate, cât și dispozițiile respective din Codul privind securitatea internă încălcau dreptul la respectarea vieții private, la protecția datelor cu caracter personal și la o cale de atac efectivă, consacrate la articolele 7, 8 și, respectiv, 47 din cartă.

30. În acest context, Conseil d'État (Consiliul de stat) adresează Curții următoarele întrebări:

„1) Obligația de păstrare generalizată și nediferențiată, impusă furnizorilor de servicii în temeiul dispozițiilor permisive ale articolului 15 alineatul (1) din Directiva 2002/58/CE […], 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?"

B. Cauza C-512/18

31. Reclamantele din litigiul care stă la baza cauzei C-511/18, cu excepția Igwan.net, au solicitat de asemenea Conseil d'État (Consiliul de Stat) anularea deciziei de respingere (prin tăcerea administrației) a cererii lor privind derogarea de la articolul R. 10-13 din code des postes et des communications électroniques (Codul serviciilor poștale și al comunicațiilor electronice) și de la Decretul nr. 2011-219 din 25 februarie 2011.

17 Decretele atacate erau următoarele: a) décret n.º 2015-1885 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); b) décret n.º 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre 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); c) décret n.º 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 libre VIII 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 VII din Codul privind securitatea internă) și d) décret n.º 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).

32. În opinia reclamantelor respective, normele atacate impun o obligație de păstrare a datelor de transfer, de localizare și de conectare care, ca urmare a caracterului lor general, implică o atingere adusă dreptului la respectarea vieții private și de familie, la protecția datelor cu caracter personal și la libertatea de exprimare, consacrate la articolele 7, 8 și 11 din cartă, cu încălcarea articolului 15 alineatul (1) din Directiva 2002/58.

33. În cadrul acestei proceduri, Conseil d'État (Consiliul de Stat) a formulat următoarele întrebări preliminare:

„1) Obligația de păstrare generalizată și nediferențiată, impusă furnizorilor de servicii în temeiul dispozițiilor permisive ale articolului 15 alineatul (1) din Directiva 2002/58/CE […] 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/CE […], 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?"

III. Procedura în fața Curții și pozițiile părților

34. Întrebările preliminare au fost înregistrate la grefa Curții la 3 august 2018.

35. Au formulat observații scrise La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, French Data Network, guvernele german, belgian, britanic, ceh, cipriot danez, spaniol, estonian, francez, maghiar, irlandez, polonez și suedez, precum și Comisia.

36. La 9 septembrie 2019 a avut loc o ședință publică care s-a desfășurat în comun cu cele în cauzele C-623/17, Privacy International, și C-520/18, Ordre des barreaux francophones et germanophone și alții, la care au participat părțile din cele patru proceduri preliminare, guvernele menționate anterior și guvernele Țărilor de Jos și Norvegiei, precum și Comisia și Autoritatea Europeană pentru Protecția Datelor.

IV. Analiză

37. Întrebările adresate de Conseil d'État (Consiliul de Stat) pot fi grupate în trei:

– în primul rând, întrebarea privind compatibilitatea cu dreptul Uniunii a unei reglementări naționale care impune furnizorilor de servicii de comunicații electronice obligația de păstrare generalizată și nediferențiată a datelor de conectare (prima întrebare adresată în cauza C-511/18 și în cauza C-512/18) și, în special, a datelor care permit identificarea creatorilor de conținuturi oferite de furnizorii respectivi (a doua întrebare adresată în cauza C-512/18);

– în al doilea rând, întrebarea privind aspectul dacă legalitatea procedurilor de colectare a datelor de conectare este condiționată, în orice caz, de obligația de informare a persoanelor vizate, atunci când nu se compromit anchetele desfășurate (a treia întrebare din cauza C-511/18);

– în al treilea rând, întrebarea privind aspectul dacă colectarea în timp real a datelor de transfer și de localizare, fără obligația de a le păstra, este compatibilă – și în ce condiții – cu Directiva 2002/58 (a doua întrebare din cauza C-511/18).

38. În definitiv, trebuie să se determine compatibilitatea cu dreptul Uniunii a unei reglementări naționale care impune furnizorilor de servicii de comunicații electronice două tipuri de obligații: a) pe de o parte, *colectarea* anumitor date, dar nu și păstrarea lor; și b) pe de altă parte, *păstrarea* datelor de conectare și a celor care permit identificarea creatorilor conținuturilor serviciilor prestate de furnizorii respectivi.

39. Cu caracter preliminar, trebuie să se clarifice dacă, tocmai ca urmare a contextului [18] în care s-a adoptat reglementarea națională respectivă (și anume, în împrejurări în care se poate compromite securitatea națională), este aplicabilă Directiva 2002/58.

A. Cu privire la aplicabilitatea Directivei 2002/58

40. Instanța de trimitere pleacă de la premisa că reglementarea în litigiu intră în domeniul de aplicare al Directivei 2002/58. Astfel reiese, în opinia sa, din jurisprudența stabilită prin Hotărârea Tele2 Sverige și Watson, care a fost confirmată prin Hotărârea Ministerio Fiscal.

41. Dimpotrivă, anumite guverne care au intervenit în procedură arată că reglementarea în litigiu nu este inclusă în domeniul de aplicare respectiv. În susținerea poziției lor, acestea invocă, printre alte argumente, Hotărârea din 30 mai 2006, Parlamentul/Consiliul și Comisia [19].

42. Împărtășim opinia Conseil d'État (Consiliul de Stat), potrivit căreia Hotărârea Tele 2 Sverige și Watson a soluționat această parte a diferendului, confirmând că Directiva 2002/58 se aplică în principiu atunci când furnizorii de servicii electronice sunt obligați prin lege să păstreze datele abonaților lor și să permită accesul autorităților publice la ele. Această teză nu este afectată de faptul că obligațiile sunt impuse furnizorilor pentru motive de securitate națională.

43. Trebuie menționat, încă de acum, că, în cazul în care ar exista vreo neconcordanță între Hotărârea Tele 2 Sverige și Watson și cele anterioare, aceasta ar trebui să prevaleze, întrucât este ulterioară și a fost confirmată prin Hotărârea Ministerio Fiscal. Cu toate acestea, considerăm că nu există nicio neconcordanță, astfel cum vom încerca să explicăm.

1. Hotărârea Parlamentul/Consiliul și Comisia

44. Cauzele soluționate prin Hotărârea Parlamentul/Consiliul și Comisia se refereau la:

– Acordul dintre Comunitatea Europeană și Statele Unite ale Americii cu privire la prelucrarea și la transferul datelor PNR [Passenger Name Records (datele din registrul pasagerilor)] din registrul cu numele pasagerilor de către transportatorii aerieni către autoritățile americane [20];

18 „Un context marcat de amenințări grave și persistente la adresa siguranței naționale, și în special de riscul terorismului", astfel cum se arată în prima întrebare din cauza C-511/18.

19 Cauzele C-317/04 și C-318/04, denumită în continuare „Hotărârea Parlamentul/Consiliul și Comisia", EU:C:2006:346.

20 Decizia 2004/496/CE a Consiliului din 17 mai 2004 privind încheierea unui acord între Comunitatea Europeană și Statele Unite ale Americii cu privire la prelucrarea și la transferul datelor PNR de către transportatorii aerieni către Biroul vamal și de protecție la frontieră din cadrul Ministerului pentru Securitate Internă american (JO 2004, L 183, p. 83, rectificare în JO 2005, L 255, p. 168) (cauza C-317/04).

– caracterul adecvat al protecției datelor cu caracter personal din registrul cu numele pasagerilor transmise autorităților respective [21].

45. Curtea a concluzionat că transferul datelor respective reprezenta o prelucrare care avea drept scop protecția securității publice și activitățile statului în materie penală. Conform articolului 3 alineatul (2) prima liniuță din Directiva 95/46, cele două decizii în litigiu nu intrau în domeniul de aplicare al acestei directive.

46. Datele erau inițial colectate de companiile aeriene în cadrul unei activități – vânzarea de bilete – incluse în domeniul de aplicare al dreptului Uniunii. Cu toate acestea, prelucrarea lor, astfel cum prevedea decizia în litigiu, „nu este necesară pentru realizarea unei prestări de servicii, ci pentru protecția securității publice și în scopuri represive” [22].

47. Curtea a adoptat astfel o abordare teleologică, luând în considerare scopul urmărit prin prelucrarea datelor cu caracter personal: în cazul în care, prin aceasta, se urmărea protecția securității publice, ar trebui considerat exclus din domeniul de aplicare al Directivei 95/46. Cu toate acestea, scopul respectiv nu era singurul criteriu determinant [23], astfel încât în hotărârea respectivă s-a subliniat că prelucrarea în cauză „este inclusă într-un cadru creat de autoritățile publice și are scopul de a proteja securitatea publică” [24].

48. Hotărârea Parlamentul/Consiliul și Comisia permite, așadar, aprecierea diferenței dintre clauza de excludere și clauzele de restricționare sau de limitare din Directiva 95/46 (similare celor din Directiva 2002/58). Totuși, este adevărat că ambele directive se referă la obiective de interes general similare, ceea ce generează confuzii cu privire la domeniul lor de aplicare, astfel cum sublinia la momentul respectiv avocatul general Bot [25].

49. Este posibil ca această confuzie să stea la baza poziției adoptate de statele membre care susțin că Directiva 2002/58 nu este aplicabilă în acest context. În opinia lor, interesul privind securitatea națională este protejat numai prin excluderea prevăzută la articolul 1 alineatul (3) din Directiva 2002/58. Este însă cert că limitările autorizate de articolul 15 alineatul (1) din directiva menționată – printre care figurează cea privind securitatea națională – urmăresc același obiectiv. Această din urmă dispoziție ar fi inutilă dacă Directiva 2002/58 ar fi inaplicabilă în orice situație în care se invocă securitatea națională.

21 Decizia 2004/535/CE a Comisiei din 14 mai 2004 privind protecția adecvată a datelor cu caracter personal din registrele cu numele pasagerilor transferate către Biroul vamal și de protecție la frontieră al Statelor Unite (JO 2004, L 235, p. 11) (cauza C-318/04).

22 Hotărârea Parlamentul/Consiliul și Comisia, punctul 57. La punctul 58 se subliniază că „faptul că anumite date cu caracter personal sunt colectate de operatori privați în scopuri comerciale și că aceștia sunt cei care organizează transferul lor către o țară terță” nu înseamnă că acest transfer nu reprezintă una dinte situațiile care nu face parte din domeniul de aplicare al Directivei 95/46 enumerate la articolul 3 alineatul 2 a doua liniuță din această directivă, deoarece transferul respectiv „se înscrie într-un cadru instituit de autoritățile publice și care vizează protecția siguranței publice”.

23 Astfel cum a subliniat ulterior regretatul avocat general Bot în Concluziile prezentate în cauza Irlanda/Parlamentul și Consiliul (C-301/06, EU:C:2008:558). Acesta a afirmat că Hotărârea Parlamentul/Consiliul și Comisia „nu poate însemna […] că numai examinarea finalității urmărite de prelucrarea datelor cu caracter personal este relevantă pentru a include sau a exclude o astfel de prelucrare din domeniului de aplicare al sistemului de protecție a datelor instituit prin Directiva 95/46. Trebuie de asemenea să se verifice în cadrul cărui tip de activități este efectuată prelucrarea datelor. Numai în cazul în care o astfel de prelucrare este efectuată în vederea exercitării activităților specifice statului sau autorităților statului și care nu au legătură cu domeniile de activitate ale particularilor, aceasta este exclusă din sistemul comunitar de protecție a datelor cu caracter personal instituit prin Directiva 95/46, în conformitate cu articolul 3 alineatul (2) prima liniuță din această directivă.” (punctul 122).

24 Hotărârea Parlamentul/Consiliul și Comisia, punctul 58. Obiectivul principal al acordului era de a impune pasagerilor companiilor aeriene care prestează servicii de transport de pasageri între Uniunea Europeană și Statele Unite ale Americii să ofere autorităților nord-americane acces electronic la datele PNR din registrul cu numele pasagerilor existente în sistemele informatice de control al rezervărilor și al plecărilor. Acesta instaura, așadar, o formă de cooperare internațională între Uniunea Europeană și Statele Unite ale Americii pentru combaterea terorismului și a altor infracțiuni grave, încercând să concilieze acest obiectiv cu cel de protecție a datelor cu caracter personal ale pasagerilor. În acest context, obligația impusă companiilor nu era foarte diferită de un schimb direct de date între autoritățile publice.

25 Concluziile avocatului general Bot prezentate în cauza Irlanda/Parlamentul și Consiliul (C-301/06, EU:C:2008:558, punctul 127).

2. Hotărârea Tele2 Sverige și Watson

50. În Hotărârea Tele2 Sverige și Watson s-a analizat compatibilitatea cu dreptul Uniunii a anumitor regimuri naționale care impuneau furnizorilor de servicii publice de comunicații electronice o obligație generală de păstrare a datelor privind comunicațiile respective. Prin urmare, situația de fapt era identică în esență cu cea din prezentele trimiteri preliminare.

51. În contextul unei noi sesizări cu privire la aplicabilitatea dreptului Uniunii – de data aceasta, în temeiul Directivei 2002/58 – Curtea a subliniat în primul rând că „întinderea domeniului de aplicare al Directivei 2002/58 trebuie apreciată având în vedere în special economia generală a acesteia” [26].

52. În această privință, Curtea a subliniat că „[d]esigur, măsurile legislative prevăzute la articolul 15 alineatul (1) din Directiva 2002/58 se raportează la activități proprii statelor sau autorităților statale, străine de domeniile de activitate ale particularilor […]. În plus, finalitățile la care trebuie să răspundă, în temeiul acestei dispoziții, asemenea măsuri, în speță protecția securității naționale, […] se pliază în esență pe finalitățile urmărite de activitățile menționate la articolul 1 alineatul (3) din această directivă” [27].

53. Prin urmare, finalitatea măsurilor care, în conformitate cu articolul 15 alineatul (1) din Directiva 2002/58, pot fi adoptate de statele membre pentru a restrânge dreptul la respectarea vieții private coincide (din această perspectivă) cu cea care justifică exceptarea anumitor activități ale statului de la regimul prevăzut de directivă, în conformitate cu articolul 1 alineatul (3) din aceasta.

54. Cu toate acestea, Curtea a considerat că, „având în vedere economia generală a Directivei 2002/58”, împrejurarea respectivă nu permitea „să se concluzioneze că măsurile legislative prevăzute la articolul 15 alineatul (1) din Directiva 2002/58 ar fi excluse din domeniul de aplicare al acestei directive, în caz contrar această dispoziție fiind privată de orice efect util. Astfel, dispoziția menționată presupune în mod necesar că măsurile naționale prevăzute la acest articol […] intră în domeniul de aplicare al aceleiași directive, din moment ce aceasta din urmă permite în mod expres statelor membre să le adopte numai cu respectarea condițiilor pe care le prevede” [28].

55. La cele de mai sus li se adaugă faptul că limitările autorizate de articolul 15 alineatul (1) din Directiva 2002/58, „guvernează, în scopurile menționate la această dispoziție, activitatea furnizorilor de servicii de comunicații electronice”. Prin urmare, acest articol coroborat cu articolul 3 din directiva respectivă „trebuie interpretat în sensul că astfel de măsuri legislative intră în domeniul de aplicare al aceleiași directive” [29].

56. În consecință, Curtea a susținut că intră în domeniul de aplicare al Directivei 2002/58 atât o măsură legislativă care obligă furnizorii „să păstreze datele de transfer și datele de localizare, întrucât o astfel de activitate implică în mod necesar o prelucrare de către aceștia a unor date cu caracter personal” [30], cât și o măsură care reglementează accesul autorităților la datele păstrate de furnizorii respectivi [31].

57. Interpretarea Directivei 2002/58 adoptată de Curte în Hotărârea Tele2 Sverige și Watson este reiterată în Hotărârea Ministerio Fiscal.

26 Hotărârea Tele2 Sverige și Watson, punctul 67.

27 *Ibidem*, punctul 72.

28 *Ibidem*, punctul 73.

29 *Ibidem*, punctul 74.

30 *Ibidem*, punctul 75.

31 *Ibidem*, punctul 76.

58. S-ar putea susține că Hotărârea Tele2 Sverige și Watson reprezintă o schimbare de abordare mai mult sau mai puțin implicită cu privire la jurisprudența stabilită prin Hotărârea Parlamentul/Consiliul și Comisia? Aceasta este, de exemplu, teza susținută de guvernul Irlandei, potrivit căruia numai această din urmă hotărâre ar fi compatibilă cu temeiul juridic al Directivei 2002/58 și ar respecta articolul 4 alineatul (2) TUE [32].

59. La rândul său, guvernul francez consideră că această incompatibilitate ar putea fi evitată dacă se consideră că jurisprudența stabilită prin Hotărârea Tele2 Sverige și Watson face referire la activități ale statelor membre în materia dreptului penal, în timp ce jurisprudența stabilită prin Hotărârea Parlamentul/Consiliul și Comisia se referă la siguranța statului și la apărare. Astfel, jurisprudența stabilită prin Hotărârea Tele2 Sverige și Watson nu ar fi aplicabilă în prezenta cauză, în care ar trebuie să se ia considerare soluția adoptată în Hotărârea Parlamentul/Consiliul și Comisia [33].

60. Astfel cum am subliniat, considerăm că se poate găsi o modalitate de integrare a celor două hotărâri, diferită de cea propusă de guvernul francez. Nu suntem de acord cu aceasta din urmă, deoarece, în opinia noastră, considerațiile din Hotărârea Tele2 Sverige și Watson, care se referă în mod explicit la combaterea terorismului [34], pot fi aplicate în privința oricărei alte amenințări la adresa securității naționale (printre care figurează și terorismul).

3. Posibilitatea unei interpretări supletive a Hotărârii Parlamentul/Consiliul și Comisia și a Hotărârii Tele2 Sverige și Watson

61. În opinia noastră, în Hotărârile Tele2 Sverige și Watson și Ministerio Fiscal, Curtea a luat în considerare scopul clauzelor de excludere și de restricționare, precum și relația sistematică dintre cele două tipuri de clauze.

62. Curtea a statuat în Hotărârea Parlamentul/Consiliul și Comisia că prelucrarea datelor nu intră în domeniul de aplicare al Directivei 95/46 ca urmare a faptului că, astfel cum am menționat anterior, în contextul cooperării dintre Uniunea Europeană și Statele Unite ale Americii, într-un cadru tipic internațional, dimensiunea națională a activității trebuia să prevaleze în raport cu faptul că prelucrarea respectivă avea de asemenea o dimensiune comercială sau privată. Una dintre chestiunile dezbătute în cauza respectivă a fost chiar temeiul juridic adecvat al deciziei în litigiu.

63. Pe de altă parte, în ceea ce privește măsurile naționale analizate în Hotărârile Tele2 Sverige și Watson și Ministerio Fiscal, Curtea a adus în prim-plan domeniul de aplicare intern al prelucrării datelor: cadrul normativ în care aceasta a fost efectuată era exclusiv național, lipsind, așadar, dimensiunea externă care caracteriza obiectul Hotărârii Parlamentul/Consiliul și Comisia.

64. Importanța diferită a dimensiunilor internațională și internă (comercială și privată) ale prelucrării datelor a avut drept consecință faptul că, în primul caz, clauza de excludere prevăzută de dreptul Uniunii a avut întâietate ca urmare a caracterului său mai adecvat pentru protecția interesului general privind securitatea națională. În al doilea rând, dimpotrivă, acest interes ar putea fi protejat mai eficient prin intermediul clauzei de limitare prevăzute la articolul 15 alineatul (1) din Directiva 2002/58.

65. Ar mai trebui analizată o altă divergență legată de contextul normativ diferit: fiecare dintre hotărârile respective s-a concentrat pe interpretarea a două dispoziții care, dincolo de aparența lor, nu sunt identice.

32 Punctele 15 și 16 din observațiile scrise ale guvernului irlandez.

33 Punctele 34-50 din observațiile scrise ale guvernului francez.

34 Hotărârea Tele2 Sverige și Watson, punctele 103 și 119.

66. Astfel, Hotărârea Parlamentul/Consiliul și Comisia avea ca obiect interpretarea articolului 3 alineatul (2) din Directiva 95/46, în timp ce Hotărârea Tele2 Sverige și Watson, pe cea a articolului 1 alineatul (3) din Directiva 2002/58. Citite cu atenție, aceste articole relevă diferențe suficiente pentru a confirma soluțiile date de Curte în cele două cauze.

67. În conformitate cu articolul 3 alineatul (2) din Directiva 95/46, „[p]rezenta directivă *nu se aplică prelucrării datelor cu caracter personal* […] puse în practică pentru exercitarea activităților din afara domeniului de aplicare al dreptului comunitar […] și, în orice caz, *prelucrărilor* care au ca obiect siguranța publică, apărarea, securitatea națională (inclusiv bunăstarea economică a statului atunci când aceste *prelucrări* sunt legate de probleme de securitate a statului) și activitățile statului în domeniul dreptului penal”[35].

68. La rând său, articolul 1 alineatul (3) din Directiva 2002/58 prevede că aceasta „*nu se aplică activităților* care nu sunt cuprinse în domeniul de aplicare al Tratatului de instituire a Comunității Europene […], 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”[36].

69. În timp ce articolul 3 alineatul (2) din Directiva 95/46 exclude *prelucrarea datelor* care are drept scop – în sensul prezentei cauze – siguranța statului, articolul 1 alineatul (3) din Directiva 2002/58 exclude prelucrarea respectivă în ceea ce privește *activitățile* prin care se urmărește – tot în sensul prezentei cauze – protecția securității naționale.

70. Diferența nu este nesemnificativă. Directiva 95/46 nu includea în domeniul său de aplicare o activitate („prelucrarea datelor cu caracter personal”) care poate fi realizată de oricine. Din cadrul acestei activități erau exceptate în special prelucrările care aveau ca obiect, printre altele, siguranța statului. În schimb, natura persoanei care efectua prelucrarea datelor cu caracter personal era irelevantă. Abordarea adoptată pentru identificarea acțiunilor excluse era, așadar, teleologică sau axată pe scop și nu efectua nicio distincție între persoane din perspectiva subiectului activ.

71. Astfel, se consideră că, în cauza Parlamentul/Consiliul și Comisia, Curtea a avut în vedere în principal scopul urmărit prin prelucrarea datelor. Nu era relevant „faptul că datele […] sunt colectate de operatori privați în scopuri comerciale și că aceștia sunt cei care organizează transferul lor către un stat terț”, ci faptul că „acest transfer intră într-un domeniu creat de autoritățile publice, care are drept scop protecția securității publice”[37].

72. În schimb, „activitățile al căror scop îl constituie securitatea națională”, din afara domeniului de aplicare al Directivei 2002/58 analizat în cauza Tele2 Sverige și Watson, nu pot fi atribuite oricui, ci numai statului însuși. În plus, acestea nu includ funcții normative sau de reglementare, ci exclusiv actele materiale ale autorităților publice.

73. Astfel, *activitățile* enumerate la articolul 1 alineatul (3) din Directiva 2002/58 „se raportează la activități proprii statelor sau autorităților statale, străine de domeniile de activitate ale particularilor”[38]. Or, aceste „activități” nu pot fi de natură normativă. În caz contrar, toate dispozițiile adoptate de statele membre în legătură cu prelucrarea datelor cu caracter personal ar fi excluse din domeniul de aplicare al Directivei 2002/58, cu excepția cazului în care ar urmări să se justifice ca fiind necesare pentru a garanta siguranța statului.

35 Sublinierea noastră.

36 Sublinierea noastră.

37 Hotărârea Parlamentul/Consiliul și Comisia, punctul 58.

38 Hotărârea Ministerio Fiscal, punctul 32. A se vedea în același sens Hotărârea Teje2 Sverige și Watson, punctul 72.

74. Pe de o parte, aceasta ar presupune o pierdere importantă a eficacității directivei respective, deoarece simpla invocare a unei noțiuni juridice atât de vagi precum cea de „securitate națională” ar fi suficientă pentru a lăsa fără aplicabilitate față de statele membre garanțiile instituite de legiuitorul Uniunii pentru a proteja datele cu caracter personal ale cetățenilor. Protecția respectivă nu poate fi aplicată fără sprijinul statelor membre, aceasta fiind garantată pentru cetățeni inclusiv în raport cu autoritățile publice naționale.

75. Pe de altă parte, o interpretare a noțiunii „activități ale statului”, care le-ar include pe cele constând în promulgarea normelor și a dispozițiilor juridice, ar lipsi de sens articolul 15 din Directiva 2002/58 care oferă statelor membre competența – pentru motive legate de protecția, printre altele, a securității naționale – de a adopta „măsuri legale” cu scopul de a limita domeniul de aplicare al anumitor drepturi și obligații prevăzute de directiva respectivă [39].

76. Astfel cum a subliniat Curtea în Hotărârea Tele2 Sverige și Watson, „întinderea domeniului de aplicare al Directivei 2002/58 trebuie apreciată ținând seama în special de economia generală a acesteia din urmă” [40]. Din această perspectivă, interpretarea articolului 1 alineatul (3) și a articolului 15 alineatul (1) din Directiva 2002/58, care le conferă sens fără să își piardă eficacitatea, este cea care identifică, în prima dintre dispoziții, o excludere materială referitoare la *activitățile* desfășurate de statele membre în domeniul securității naționale (și echivalente) și, în a doua, o autorizare pentru a adopta *măsuri legale* (cu alte cuvinte, norme general obligatorii) care, în vederea protecției securității naționale, se referă la activități ale indivizilor aflați sub *imperium*-ul statelor membre și restrâng drepturile consacrate de Directiva 2002/58.

4. Excluderea securității naționale din domeniul de aplicare al Directivei 2002/58

77. Securitatea națională (sau expresia sinonimă a acesteia, „siguranța statului”) este prezentată din două perspective în Directiva 2002/58. Pe de o parte, aceasta constituie un motiv de excludere (din domeniul de aplicare al directivei respective) a tuturor activităților statelor membre, care „o au ca obiect” în mod special. Pe de altă parte, aceasta este invocată drept motiv de *limitare*, care trebuie reglementat prin lege, a drepturilor și a obligațiilor prevăzute de Directiva 2002/58, cu alte cuvinte a activităților de natură privată sau comercială, din afara domeniului activităților regaliene [41].

78. La ce activități se referă articolul 1 alineatul (3) din Directiva 2002/58? În opinia noastră, Conseil d’État (Consiliul de Stat) însuși oferă un exemplu bun atunci când menționează articolele L. 851-5 și L. 851-6 din Codul privind securitatea internă, făcând referire la „tehnicile de colectare a informațiilor care sunt aplicate în mod direct de către stat, dar care nu reglementează activitățile furnizorilor de servicii de comunicații electronice prin impunerea unor obligații specifice în sarcina acestora” [42].

39 Astfel, ar fi dificil de susținut că articolul 15 alineatul (1) din Directiva 2002/58 permite limitarea drepturilor și a obligațiilor pe care le prevede într-un domeniu care, precum cel al securității naționale, nu ar intra în principiu în domeniul său de aplicare, conform articolului 1 alineatul (3) din directiva respectivă. Astfel cum a statuat Curtea în Hotărârea Tele2 Sverige și Watson, punctul 73, articolul 15 alineatul (1) din Directiva 2002/58 „presupune în mod necesar ca măsurile naționale prevăzute la acest articol […] intră în domeniul de aplicare al aceleiași directive, din moment ce aceasta din urmă permite în mod expres statelor membre să le adopte numai cu respectarea condițiilor pe care le prevede”.

40 Hotărârea Tele2 Sverige și Watson, punctul 67.

41 Astfel cum sublinia, în mod incidental, avocatul general Saugmandsgaard Øe în Concluziile prezentate în cauza Ministerio Fiscal (C-207/16, EU:C:2018:300, punctul 47), „trebuie să nu existe o confuzie între, pe de o parte, datele cu caracter personal prelucrate *în mod direct* în cadrul activităților – de natură regaliană – […] ale unui prestator de servicii de comunicații electronice care sunt utilizate *ulterior* de autoritățile competente ale statului”.

42 Punctele 18 și 21 din decizia de trimitere pronunțată în cauza C-511/18.

79. Considerăm că aceasta este cheia pentru a stabili domeniul de aplicare al excluderii prevăzute la articolul 1 alineatul (3) din Directiva 2002/58. Nu sunt supuse regimului acesteia *activitățile* prin care se urmărește apărarea securității naționale, efectuate de autoritățile publice în mod independent, fără colaborarea particularilor, și, prin urmare, fără ca acestora să li se impună obligații privind gestionarea activităților comerciale.

80. Trebuie însă ca lista cu activitățile autorităților publice excluse din regimul general al prelucrării datelor cu caracter personal să fie interpretată în mod restrictiv. Concret, noțiunea de „securitate națională”, care se află sub responsabilitatea exclusivă a fiecărui stat membru în conformitate cu articolul 4 alineatul (2) TUE, nu poate fi extinsă la alte sectoare, mai mult sau mai puțin apropiate, ale vieții publice.

81. Având în vedere că în aceste trimiteri preliminare sunt implicați particulari (cu alte cuvinte, persoane care prestează pentru utilizatori serviciile de comunicații electronice) și că nu este vorba despre simpla intervenție a autorităților statale, nu va fi necesar să insistăm asupra stabilirii domeniului de aplicare al securității naționale *stricto sensu*.

82. Cu toate acestea, considerăm că poate fi utilizat în scop orientativ criteriul stabilit în Decizia-cadru 2006/960/JAI [43], care, la articolul 2 litera (a), efectuează o distincție între serviciile de securitate în sens amplu – care includ „o poliție națională, o vamă națională sau orice altă autoritate care este autorizată prin legislația națională să depisteze, să prevină și să cerceteze infracțiunile sau activitățile infracționale, să își exercite autoritatea și să ia măsuri coercitive în cadrul unor astfel de activități” – pe de o parte, și „agențiile sau unitățile specializate pe probleme de siguranță națională”, pe de altă parte [44].

83. În cuprinsul considerentului (11) al Directivei 2002/58 se arată că aceasta, „[l]a fel ca Directiva 95/46/CE […], nu se referă la chestiuni de protecție a drepturilor și libertăților fundamentale legate de activități care nu sunt reglementate de [dreptul Uniunii]”. Prin urmare, Directiva 2002/58 „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, […] în vederea protejării […] siguranței statului”.

84. Există, astfel, o continuitate între Directiva 95/46 și Directiva 2002/58 în ceea ce privește competențele statelor membre în materia securității naționale. Niciuna dintre cele două nu are ca obiect protecția drepturilor fundamentale în acest domeniu specific, în care activitățile statelor membre nu sunt „reglementate de dreptul [Uniunii]”.

85. „Echilibrul” la care se referă considerentul [(21) al Directivei 2002/58] rezultă din necesitatea de a respecta competențele statelor membre în materia securității naționale, atunci când acestea le exercită *în mod direct și prin mijloace proprii*. Dimpotrivă, atunci când, chiar și pentru aceleași motive de securitate națională, este necesară participarea particularilor, cărora li se impun anumite obligații, această circumstanță determină intrarea într-un domeniu (dreptul la protecția vieții private pe care trebuie să îl respecte particularii respectivi) reglementat de dreptul Uniunii.

86. Atât Directiva 95/46, cât și Directiva 2002/58 încearcă să atingă acest echilibru autorizând limitarea drepturilor particularilor în temeiul măsurilor normative adoptate de statele membre în temeiul articolului 13 alineatul (1) și, respectiv, al articolului 15 alineatul (1) din acestea. Nu există nicio diferență în această privință între cele două directive.

43 Decizia-cadru 2006/960/JAI a Consiliului din 18 decembrie 2016 privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre ale Uniunii Europene (JO 2006, L 386, p. 89, Ediție specială, 19/vol. 09, p. 96).

44 În același sens, articolul 1 alineatul (4) din Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (JO 2008, L 350, p. 60) prevedea că aceasta „nu aduce atingere intereselor naționale fundamentale în materie de securitate și nici activităților specifice ale serviciilor de informații în domeniul siguranței naționale”.

87. În ceea ce privește Regulamentul 2016/679, care instituie un (nou) cadru general pentru protecția datelor cu caracter personal, articolul 2 alineatul (2) din acesta elimină aplicarea sa în privința „prelucrării datelor cu caracter personal" atunci când statele membre „desfășoară activități care intră sub incidența capitolului 2 al titlului V din Tratatul UE".

88. Astfel cum, în Directiva 95/46, prelucrarea datelor cu caracter personal era calificată în funcție de scopul său, făcându-se abstracție de cel care o efectuează, în Regulamentul 2016/679 prelucrările excluse sunt identificate atât în funcție de scopul, cât și de autorii lor: sunt excluse prelucrările realizate de statele membre în contextul exercitării unei activități care nu intră în domeniul de aplicare al dreptului Uniunii [articolul 2 alineatul (2) literele (a) și (b)] și cele efectuate de autorități *în scopul prevenirii infracțiunilor și al protecției* împotriva amenințărilor la adresa siguranței publice [45].

89. Identificarea acestor activități ale autorităților publice trebuie să fie în mod obligatoriu restrictivă, deoarece, în caz contrar, aceasta lipsește de efecte dreptul Uniunii în materia protecției vieții private. Regulamentul 2016/679 prevede la articolul 23 – în conformitate cu articolul 15 alineatul (1) din Directiva 2002/58 – restricționarea, *printr-o măsură legislativă*, a domeniului de aplicare al drepturilor și al obligațiilor prevăzute de acesta, atunci când o astfel de restricție constituie o măsură necesară pentru a asigura, printre alte obiective, securitatea națională, apărarea sau siguranța publică. Astfel cum am menționat, dacă protejarea acestor obiective ar fi suficientă pentru a determina excluderea din domeniul de aplicare al Regulamentului 2016/679, ar fi inutil să se invoce securitatea națională drept motiv justificativ al restricționării, printr-o anumită măsură legislativă, a drepturilor garantate de regulamentul respectiv.

90. La fel ca în cazul Directivei 2002/58, nu ar fi logic ca măsurile legislative prevăzute la articolul 23 din Regulamentul 2016/679 (care, astfel cum am menționat, autorizează limitările naționale privind dreptul la respectarea vieții private a cetățenilor pentru motive legate de siguranța statului) să intre în domeniul său de aplicare și, în același timp, acesta să devină inaplicabil, pur și simplu, în vederea garantării siguranței statului, ceea ce ar implica nerecunoașterea oricărui drept subiectiv.

B. Confirmarea jurisprudenței stabilite prin Hotărârea Tele2 Sverige și Watson și posibilitățile de dezvoltare a acesteia

91. În concluziile noastre prezentate în cauza C-520/18, am efectuat o analiză detaliată [46] a jurisprudenței Curții în această materie, în urma căreia am propus confirmarea sa, sugerând în același timp o interpretare pentru stabilirea conținutului ei.

92. Facem trimitere la analiza respectivă, pe care considerăm că nu este necesar să o transcriem, din simple considerente de economie de text. Considerațiile pe care le vom prezenta în continuare cu privire la întrebările preliminare adresate de Conseil d'Etat (Consiliul de Stat) trebuie înțelese, așadar, luând drept premisă secțiunile corespunzătoare din Concluziile prezentate în cauza C-520/18.

45 Regulamentul 2016/679 exclude, astfel, prelucrarea datelor efectuată de statele membre în contextul exercitării unei activități care nu intră în domeniul de aplicare al dreptului Uniunii, precum și pe cea efectuată de autorități *în vederea protecției* securității publice.

46 Punctele 27-68.

C. Răspunsul la întrebările preliminare

1. Cu privire la obligația de păstrare a datelor (prima întrebare preliminară adresată în cauzele C-511/18 și C-512/18 și a doua întrebare preliminară adresată în cauza C-512/18)

93. În ceea ce privește obligația de păstrare a datelor impusă furnizorilor de servicii de comunicații electronice, instanța de trimitere solicită să se stabilească, în concret:

– dacă obligația respectivă, impusă în temeiul articolului 15 alineatul (1) din Directiva 2002/58, constituie o ingerință justificată de „dreptul la siguranță” garantat la articolul 6 din cartă și de cerințele privind securitatea națională (prima întrebare adresată în cauzele C-511/18 și C-512/18, precum și a treia întrebare din cauza C-511/18);

– dacă Directiva 2000/31 autorizează păstrarea datelor care pot permite identificarea celor care au contribuit la crearea conținuturilor accesibile publicului online (a doua întrebare adresată în cauza C-512/18).

a) Considerație introductivă

94. Conseil d'État face referire la drepturile fundamentale consacrate la articolul 7 (respectarea vieții private și de familie), la articolul 8 (protecția datelor cu caracter personal) și la articolul 11 (libertatea de expresie și de informare) din cartă. Acestea sunt, astfel, drepturile cărora, potrivit Curții, li s-ar putea aduce atingere prin impunerea obligației de păstrare a datelor de transfer de către autoritățile naționale în sarcina furnizorilor de comunicații electronice [47].

95. Instanța de trimitere face referire de asemenea la dreptul la siguranță protejat la articolul 6 din cartă. Aceasta invocă dreptul respectiv ca factor care ar putea justifica impunerea acelei obligații, mai degrabă decât ca drept afectat.

96. Împărtășim opinia Comisiei potrivit căreia invocarea articolului 6 în acești termeni se poate dovedi ambiguă. Asemenea Comisiei, considerăm că dispoziția nu trebuie interpretată în sensul că este aptă „să impună Uniunii o obligație pozitivă de a adopta măsuri care au ca scop protejarea persoanelor împotriva actelor criminale” [48].

97. Siguranța garantată la articolul respectiv din cartă nu se identifică cu securitatea publică. Sau, altfel spus, dreptul la siguranță are legătură cu securitatea națională la fel ca orice alt drept fundamental, în măsura în care securitatea publică reprezintă o condiție indispensabilă pentru exercitarea drepturilor și a libertăților fundamentale.

98. Astfel cum amintește Comisia, articolul 6 din cartă corespunde articolului 5 din Convenția Europeană a Drepturilor Omului (denumită în continuare „convenția”), conform explicațiilor care o însoțesc. Din interpretarea articolului 5 din convenție rezultă că „siguranța” protejată de acesta este exclusiv cea personală, considerată drept garanție a dreptului la libertate fizică împotriva arestării sau a deținerii arbitrare. În definitiv, siguranța că nimeni nu poate fi privat de libertatea sa, cu excepția cazurilor, în condițiile și în conformitate cu procedurile prevăzute de lege.

47 A se vedea în acest sens Hotărârea Tele2 Sverige și Watson, punctul 92, care citează, prin analogie, Hotărârea Digital Rights, punctele 25 și 70.
48 Punctul 37 din observațiile Comisiei.

99. Prin urmare, este vorba despre *siguranța personală*, referitoare la condițiile în care poate fi restrânsă libertatea fizică a persoanelor [49], iar nu despre *securitatea publică* inerentă existenței statului, care, într-o societate dezvoltată, constituie o condiție indispensabilă pentru concilierea exercitării puterilor publice cu exercitarea drepturilor individuale.

100. Cu toate acestea, anumite guverne solicită ca dreptul la siguranță să fie avut în vedere mai degrabă în cel de al doilea sens. În realitate, Curtea nu a ignorat acest drept, ci, dimpotrivă, a făcut referire la el în hotărârile [50] și în avizele sale [51]. Aceasta nu a contestat niciodată importanța obiectivelor de interes general de protecție a securității naționale și a ordinii publice [52], de combatere a terorismului internațional pentru menținerea păcii și a securității internaționale și de combatere a criminalității grave pentru garantarea siguranței publice [53], pe care le-a calificat în mod corect ca fiind „primordiale” [54]. Astfel cum Curtea a subliniat la momentul respectiv, „protecția securității publice contribuie de asemenea la protecția drepturilor și a libertăților celorlalți” [55].

101. S-ar putea profita de oportunitatea pe care o oferă prezentele trimiteri preliminare pentru a propune într-un mod mai clar concilierea dreptului la siguranță, pe de o parte, cu dreptul la respectarea vieții private și cu dreptul la protecția datelor personale, pe de altă parte. Astfel, s-ar evita criticile privind favorizarea acestora din urmă în detrimentul primului.

102. În opinia noastră, la acest echilibru fac referire considerentul (11) al Directivei 2002/58 și articolul 15 alineatul (1) din aceasta, atunci când menționează condițiile privind necesitatea și caracterul proporțional al măsurilor *într-o societate democratică*. Astfel cum am menționat, dreptul la siguranță este inerent existenței înseși și supraviețuirii unei democrații, ceea ce justifică faptul că este luat în considerare pe deplin în contextul aprecierii caracterului proporțional respectiv. Cu alte cuvinte, dacă protejarea principiului confidențialității datelor este primordială într-o societate democratică, nu trebuie să se subestimeze nici importanța securității acesteia.

103. Prin urmare, trebuie să se aibă în vedere contextul amenințărilor grave și persistente la adresa securității naționale și, în special, riscul terorismului în acord cu cele statuate în ultima frază a punctului 119 din Hotărârea Tele2 Sverige și Watson. Un sistem național poate răspunde în mod proporțional amenințărilor cu care se confruntă, indiferent de natura și de gravitatea lor, fără a fi obligatoriu ca răspunsul respectiv să fie identic cu cel al altor state membre.

104. În sfârșit, trebuie să adăugăm că reflecțiile anterioare nu împiedică, în situații realmente *excepționale*, caracterizate printr-o amenințare iminentă sau printr-un risc extraordinar care justifică declararea oficială a situației de urgență într-un stat membru, legislația națională să prevadă, pentru o perioadă limitată, posibilitatea de a impune o obligație de păstrare a datelor atât de amplă și de generală cât se consideră necesar [56].

105. În consecință, prima întrebare din cele două trimiteri preliminare ar trebui reformulată, astfel încât aceasta să se refere mai degrabă la posibilitatea de a justifica ingerința în motivele privind securitatea națională. Îndoiala ar viza, așadar, aspectul dacă obligația impusă operatorilor de servicii de comunicații electronice este compatibilă cu articolul 15 alineatul (1) din Directiva 2002/58.

49 Conform interpretării efectuate de CEDO. A se vedea în special Hotărârea din 5 iulie 2016, Buzadji împotriva Republicii Moldova, ECHR:2016:0705JUD002375507, în care se statuează, la § 84, că scopul principal al dreptului consacrat la articolul 5 din convenție este de a preveni privarea arbitrară și nejustificată de o libertate individuală.

50 Hotărârea Digital Rights, punctul 42.

51 Avizul nr. 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017 (denumit în continuare „Avizul nr. 1/15”, EU:C:2017:592, punctul 149 și jurisprudența citată).

52 Hotărârea de 15 februarie 2016, N. (C-601/15 PPU, EU:C:2016:84, punctul 53).

53 Hotărârea Digital Rights, punctul 42 și jurisprudența citată.

54 *Ibidem*, punctul 51.

55 Avizul nr. 1/15, punctul 149.

56 A se vedea punctele 105-107 din Concluziile noastre prezentate în cauza C-520/18.

b) Analiză

1) Caracterizarea normelor naționale, astfel cum sunt prezentate în cele două trimiteri preliminare, în lumina jurisprudenței Curții

106. Conform deciziei de trimitere, reglementarea în discuție în procedurile principale impune obligația de păstrare a datelor cu caracter personal în sarcina:

– operatorilor de comunicații electronice și, în special, a celor care oferă acces la serviciile de comunicații publice online; și

– persoanelor fizice sau juridice care asigură, inclusiv cu titlu gratuit, pentru punerea la dispoziție online, stocarea de semnale, de texte, de sunete, de imagini, sau de mesaje de orice natură furnizate de destinatari ai acestor servicii [57].

107. Operatorii trebuie să păstreze informațiile care permit identificarea utilizatorului, datele referitoare la echipamentele terminale utilizate, caracteristicile tehnice, data, ora și durata fiecărui apel, datele privind serviciile suplimentare solicitate sau utilizate și furnizorii acestora, precum și datele care permit identificarea destinatarului comunicației și, în cazul activităților de telefonie, originea și localizarea comunicației timp de un an de la data înregistrării lor [58].

108. Fiind vorba, în special, despre serviciile de acces la internet și despre serviciile de stocare, reglementarea națională pare să impună obligația de păstrare a adreselor IP [59], a parolelor și, în cazul în care s-a încheiat un contract sau s-a deschis un cont de plată, a tipului de plată efectuată, precum și a referinței sale, a sumei, a datei și a orei tranzacției [60].

109. Această obligație de păstrare a datelor este impusă în scopul investigării, al constatării și al urmăririi penale a infracțiunilor [61]. Cu alte cuvinte, spre deosebire – astfel cum vom arăta – de cazul obligației de *colectare* a datelor de transfer și de localizare, obligația de *păstrare a acestora* nu are drept unic scop combaterea terorismului [62].

110. În ceea ce privește condițiile de *acces* la datele păstrate, din informațiile furnizate în dosar rezultă că acestea fie sunt stabilite pentru regimul comun (intervenția autorității judiciare), fie accesul respectiv este limitat la agenții desemnați și mandatați în mod individual în temeiul unei autorizații emise de prim-ministru pe baza avizului neobligatoriu al unei autorități administrative independente [63].

57 Astfel cum rezultă din articolul L. 851-1 din Codul securității interne, care face trimitere la articolul L. 34-1 din Codul serviciilor poștale și al comunicațiilor electronice și la articolul 6 din Legea nr. 2004-575 privind încrederea în cadrul economiei informaționale.

58 Astfel cum prevede articolul R. 10-13 din Codul serviciilor poștale și al comunicațiilor electronice.

59 Revine instanței de trimitere sarcina de a verifica acest aspect, care a făcut obiectul unor dezacorduri în cadrul ședinței.

60 Articolul 1 din Decretul nr. 2011-219.

61 Articolul R. 10-13 din Codul serviciilor poștale și al comunicațiilor electronice.

62 Atât La Quadrature du Net, cât și Fédération des founisseurs d'accès à Internet associatifs subliniază importanța scopurilor pe care le îndeplinește păstrarea, marja de apreciere discreționară atribuită autorităților, lipsa criteriilor obiective privind definiția sa și relevanța conferită unor tipuri de infracțiuni care nu pot fi calificate drept grave.

63 Commission nationale de contrôle des techniques de renseignement (Comisia națională pentru controlul tehnicilor informative). A se vedea în acest sens punctele 145-148 din observațiile guvernului francez.

111. Este ușor de observat că, astfel cum a subliniat Comisia [64], datele a căror păstrare este impusă de normele naționale corespund în esență cu cele examinate de Curte în Hotărârile Digital Rights și Tele2 Sverige și Watson [65]. La fel ca în cauzele respective, aceste date fac obiectul unei „obligații de păstrare generalizate și nediferențiate", astfel cum subliniază cu toată sinceritatea Conseil d'État (Consiliul de Stat) la începutul întrebărilor preliminare.

112. Dacă acest lucru se confirmă – ceea ce, în definitiv, trebuie să analizeze instanța de trimitere –, nu ne rămâne decât să concluzionăm că reglementarea în discuție implică o „ingerință [...] în drepturile fundamentale consacrate la articolele 7 și 8 din cartă [care] se dovedește a fi de o mare amploare și trebuie considerată deosebit de gravă" [66].

113. Niciuna dintre părțile care s-au înfățișat nu a contestat faptul că o reglementare cu aceste caracteristici implică o ingerință în drepturile respective. Nu este necesar să ne concentrăm acum asupra acestui aspect, nici măcar pentru a aminti că atingerea adusă acestor drepturi afectează în mod inevitabil fundamentele unei societăți care urmărește să respecte, printre alte valori, viața privată a indivizilor consacrată de cartă.

114. Aplicarea jurisprudenței stabilite prin Hotărârea Tele2 Sverige și Watson și confirmate prin Hotărârea Ministerio Fiscal ar determina în mod firesc să se susțină că o reglementare precum cea în discuție în prezenta cauză „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" [67].

115. Astfel, la fel ca reglementarea națională analizată în Hotărârea Tele2 Sverige și Watson, cea în discuție în prezenta cauză „acoperă în mod generalizat toți abonații și utilizatorii înregistrați și privește toate mijloacele de comunicare electronică, precum și toate datele de transfer [și] nu prevede nicio diferențiere, limitare sau excepție în funcție de obiectivul urmărit" [68]. În consecință, ea „se aplică, așadar, chiar și acelor persoane în privința cărora nu există niciun indiciu de natură să sugereze că comportamentul lor poate avea o legătură, chiar indirectă sau îndepărtată, cu infracțiuni grave", fără să prevadă vreo excepție, „astfel încât ea se aplică chiar și acelor persoane ale căror comunicații sunt supuse, potrivit normelor dreptului național, secretului profesional" [69].

116. De asemenea, reglementarea în litigiu „nu impune nicio relație între datele a căror păstrare este prevăzută și o amenințare pentru securitatea publică. În special, aceasta nu este limitată la o păstrare care privește fie datele aferente unei perioade și/sau unei zone geografice și/sau unui cerc de persoane care pot fi implicate într-un fel sau altul într-o infracțiune gravă, fie persoane care, din alte motive, ar putea să contribuie, prin păstrarea datelor lor, la combaterea infracționalității" [70].

117. Din cele ce precedă rezultă că reglementarea respectivă „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" [71].

64 Punctul 60 din observațiile scrise ale Comisiei.

65 În realitate, este vorba și despre alte date, deoarece, în cazul serviciilor de acces la internet, pare să se prevadă de asemenea păstrarea adresei IP sau a parolelor.

66 Hotărârea Tele2 Sverige și Watson, punctul 100.

67 *Ibidem*, punctul 107.

68 *Ibidem*, punctul 105.

69 *Loc. ult. cit.*

70 Hotărârea Tele2 Sverige și Watson, punctul 106.

71 *Ibidem*, punctul 107.

118. Considerațiile de mai sus au fost suficiente pentru Curte ca să concluzioneze că normele naționale corelative nu erau compatibile cu articolul 15 alineatul (1) din Directiva 2002/58, în măsura în care prevedeau, „în scopul combaterii infracționalității, o păstrare generalizată și nediferențiată a ansamblului datelor de transfer și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică” [72].

119. Problema care se ridică în acest punct se referă la aspectul dacă jurisprudența Curții în materia păstrării datelor cu caracter personal poate fi, dacă nu reformată, cel puțin nuanțată, atunci când scopul pe care îl îndeplinește păstrarea „generalizată și nediferențiată” constă în combaterea terorismului. Prima întrebare adresată în cauza C-511/18 este formulată chiar „într-un context marcat de amenințări grave și persistente la adresa siguranței naționale și în special de riscul terorismului”.

120. Or, luând în considerare *contextul factual* în care se impune obligația de păstrare a datelor cu caracter personal, este cert că, în *contextul normativ* al acesteia, terorismul nu este singurul avut în vedere. Regimul de păstrare și de accesare a datelor în discuție în procedura desfășurată în fața Conseil d'État (Consiliul de Stat) condiționează obligația respectivă de scopul investigării, al constatării și al urmăririi penale a infracțiunilor cu caracter general.

121. În orice caz, amintim că lupta împotriva terorismului a constituit unul dintre argumentele prezentate în Hotărârea Tele2 Sverige și Watson și că, în contextul respectiv, Curtea nu a considerat că acel tip de infracțiune necesită vreo modificare a jurisprudenței sale [73].

122. Prin urmare și în principiu, considerăm că întrebarea instanței de trimitere, axată pe specificitatea amenințării teroriste, ar trebui să primească același răspuns precum cel dat de Curte în Hotărârea Tele2 Sverige și Watson.

123. Astfel cum am arătat în Concluziile prezentate în cauza Stichting Brein, „[c]ertitudinea privind aplicarea legii, deși nu impune instanțelor să aplice *stare decisis* în termeni absoluți, le obligă să dea dovadă de prudență în ceea ce privește respectarea propriilor decizii, după o analiză profundă, referitoare la o problemă juridică concretă” [74].

2) Păstrare limitată a datelor ca urmare a amenințărilor la adresa securității naționale, inclusiv amenințarea teroristă.

124. Ar fi posibilă, totuși, nuanțarea sau completarea jurisprudenței, având în vedere consecințele sale asupra combaterii terorismului sau a protecției statului față de alte amenințări similare la adresa securității naționale?

72 *Ibidem*, punctul 112.

73 *Ibidem*, punctul 103.

74 Cauza C-527/15, EU:C:2016:938, punctul 41.

125. Am subliniat deja că simpla păstrare a datelor cu caracter personal implică o ingerință în drepturile garantate la articolele 7, 8 și 11 din cartă [75]. În afara faptului că, în ultimă instanță, prin aceasta se urmărește facilitarea *accesului*, în mod retrospectiv sau simultan, la datele cu caracter personal la un moment dat [76], simpla păstrare a datelor care depășesc ceea ce este strict necesar pentru transmiterea unei comunicații sau pentru facturarea serviciilor prestate de furnizor presupune nerespectarea limitelor prevăzute la articolele 5 și 6 din Directiva 2002/58.

126. Utilizatorii acestor servicii (în realitate, cvasi-totalitatea cetățenilor din societățile mai dezvoltate) beneficiază sau trebuie să beneficieze de o așteptare legitimă în sensul că, dacă nu își dau consimțământul, nu se vor păstra mai multe date despre aceștia decât cele stocate în conformitate cu dispozițiile respective. Derogările prevăzute la articolul 15 alineatul (1) din Directiva 2002/58 trebuie interpretate plecând de la această premisă.

127. Astfel cum am arătat, în Hotărârea Tele2 Sverige și Watson, Curtea a respins păstrarea generalizată și nediferențiată a datelor cu caracter personal inclusiv în legătură cu combaterea terorismului [77].

128. Ca urmare a criticilor primite, nu considerăm că jurisprudența stabilită prin hotărârea respectivă subestimează amenințarea teroristă, ca formă infracțională deosebit de gravă, care implică un scop explicit de subminare a autorității statului și de destabilizare și distrugere a instituțiilor sale. Lupta împotriva terorismului este literalmente vitală pentru un stat și pentru existența sa, reprezentând un obiectiv de interes general indispensabil pentru un stat de drept.

129. Practic, toate guvernele care s-au înfățișat în procedură, precum și Comisia, au subliniat că, dincolo de dificultățile sale tehnice, o păstrare parțială și diferențiată a datelor cu caracter personal ar priva serviciile naționale de informații de posibilitatea de a accesa informații indispensabile pentru identificarea amenințărilor la adresa securității publice și pentru apărarea statului, precum și pentru urmărirea penală a autorilor atentatelor teroriste [78].

130. Având în vedere această abordare, considerăm că este important să subliniem că lupta împotriva terorismului nu trebuie invocată numai din perspectiva eficacității sale. Din aceasta decurge dificultatea, dar și importanța ei atunci când mijloacele și metodele sale respectă cerințele statului de drept, care constă în principal în exercitarea puterii și a forței în limitele prevăzute de lege și, în special, de o ordine juridică care are drept finalitate apărarea drepturilor fundamentale.

131. Dacă, în ceea ce privește terorismul, singurul criteriu care justifică mijloacele sale este efectivitatea clară (și maximă) a atacurilor asupra ordinii stabilite, pentru statul de drept eficacitatea este apreciată în condiții care nu permit să se renunțe, în vederea apărării sale, la procedurile și la garanțiile care o califică drept ordine legitimă. Statul de drept și-ar pierde calitatea distinctivă dacă s-ar concentra pur

75 Astfel cum a amintit Curtea în Avizul nr. 1/15, punctul 124, „comunicarea de date cu caracter personal unui terț, precum o autoritate publică, constituie o ingerință în dreptul fundamental consacrat la articolul 7 din cartă, indiferent de utilizarea ulterioară a informațiilor comunicate. Același lucru este valabil și în privința păstrării datelor cu caracter personal, în special de către prestatorii de servicii de comunicații electronice, precum și în privința accesului la datele respective pentru utilizarea lor de către autoritățile publice. În acest sens, este irelevant dacă informațiile vizate referitoare la viața privată prezintă sau nu prezintă un caracter sensibil sau dacă persoanele interesate au suferit sau nu au suferit eventuale inconveniente ca urmare a acestei ingerințe”.

76 Astfel cum sublinia avocatul general Cruz Villalón în Concluziile prezentate în cauza Digital Rights, C-293/12 și C-594/12 (EU:C:2013:845, punctul 72), „colectarea și, mai ales, păstrarea, în baze de date foarte mari, a unor date multiple generate sau prelucrate în cadrul celei mai mari părți a comunicațiilor electronice curente ale cetățenilor Uniunii constituie o ingerință individualizată în viața lor privată, chiar dacă aceasta nu ar face decât să creeze condițiile posibilității unui control retrospectiv al activităților lor atât personale, cât și profesionale. Colectarea acestor date creează condițiile unei supravegheri care, deși nu se exercită decât retrospectiv cu ocazia exploatării acestora, amenință totuși permanent, pe întreaga perioadă de păstrare a acestora, dreptul cetățenilor Uniunii la confidențialitate în ceea ce privește viața lor privată. Sentimentul difuz de supraveghere generat ridică într-un mod deosebit de acut problema perioadei de păstrare a datelor”.

77 Hotărârea Tele2 Sverige și Watson, punctul 103: „nu poate […] să justifice ca o reglementare națională care prevede păstrarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare să fie considerată necesară în scopul acestei combateri”.

78 Astfel interpretează de exemplu guvernul francez, care ilustrează această afirmație cu exemple concrete privind utilitatea păstrării generalizate a datelor, care a permis statului să reacționeze la atacurile teroriste majore comise în Franța în ultimii ani (punctele 107 și 122-126 din observațiile guvernului francez).

și simplu pe simpla eficacitate și ar putea deveni el însuși, în situații extreme, o amenințare pentru cetățeni. Nu există nicio garanție în sensul că după înzestrarea autorității publice cu instrumente excesive pentru urmărirea penală a infracțiunilor, prin intermediul cărora ar putea ignora sau aduce atingere drepturilor fundamentale, acțiunile sale, care nu sunt supuse niciunui control și sunt complet arbitrare, ar aduce atingere în cele din urmă libertății tuturor.

132. Astfel cum am menționat, drepturile fundamentale ale cetățenilor constituie un obstacol major în calea eficienței autorității publice, iar restrângerile lor, conform articolului 52 alineatul (1) din cartă, pot fi stabilite numai prin lege și cu respectarea conținutului lor esențial „numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți” [79].

133. În ceea ce privește condițiile în care, conform Hotărârii Tele2 Sverige și Watson, ar fi permisă o păstrare *selectivă* a datelor, facem trimitere la Concluziile noastre prezentate în cauza C-520/18 [80].

134. Împrejurările în care informațiile aflate la dispoziția serviciilor de securitate confirmă suspiciunile întemeiate privind pregătirea unui atentat terorist pot constitui o situație legitimă de impunere a obligației de păstrare a anumitor date. Acest lucru este cu atât mai mult valabil în cazul comiterii efective a unui atentat. Dacă, în acest din urmă caz, repetarea infracțiunii poate constitui în sine o împrejurare care justifică adoptarea măsurii respective, ca urmare a simplei suspiciuni privind un eventual atentat, ar fi necesar ca împrejurările care o justifică să ofere un grad minim de verosimilitate, necesar pentru o apreciere obiectivă a indiciilor care o pot justifica.

135. Deși este dificil, nu este imposibil de determinat cu exactitate și în conformitate cu criterii obiective atât categoriile de date a căror păstrare este considerată indispensabilă, cât și cercul persoanelor afectate. Desigur, cel mai *practic și mai eficient* ar fi să se păstreze în mod generalizat și nediferențiat toate datele cu caracter personal colectate de furnizorii de servicii de comunicații electronice, însă am subliniat deja că problema nu poate fi soluționată din perspectiva *eficacității practice*, ci a *eficacității juridice*, și în contextul unui stat de drept.

136. Această activitate de determinare este în general de natură legislativă și se încadrează în limitele stabilite de jurisprudența Curții. Facem trimitere din nou la considerațiile noastre în această privință din Concluziile prezentate în cauza C-520/18 [81].

79 Hotărârea din 15 februarie 2016, N. (C-601/15 PPU, EU:C:2016:84, punctul 50). Este vorba, așadar, despre echilibrul dificil între ordinea publică și libertatea la care am făcut referire și la care aspiră în principiu orice reglementare a Uniunii. Un exemplu în acest sens este Directiva (UE) 2017/541 a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO 2017, L 88, p. 6). În timp ce articolul 20 alineatul (1) din aceasta prevede că statele membre trebuie să se asigure că cei responsabili de investigarea sau urmărirea penală a infracțiunilor de terorism „dispun de instrumente eficace de investigare”, în considerentul (21) al acesteia se arată că utilizarea acestor instrumente eficace „ar trebui să fie specifică, să țină seama de principiul proporționalității, precum și de natura și gravitatea infracțiunilor investigate și să respecte dreptul la protecția datelor cu caracter personal”.

80 Punctele 87-95.

81 Punctele 100-107.

3) Accesul la datele cu caracter personal păstrate

137. Plecând de la premisa că operatorii au colectat datele în conformitate cu dispozițiile Directivei 2002/58 și că acestea au fost păstrate în temeiul articolului 15 alineatul (1) din aceasta [82], accesul autorităților competente la informațiile respective trebuie să se realizeze în condițiile impuse de Curte și analizate de noi în Concluziile prezentate în cauza C-520/18, la care facem trimitere [83].

138. Prin urmare, în prezenta cauză este necesar de asemenea ca legislația națională să stabilească cerințele de fond și procedurale care reglementează accesul autorităților competente la datele păstrate [84]. În contextul prezentelor trimiteri preliminare, cerințele respective ar permite accesul la datele persoanelor suspectate că planifică, vor comite, au comis sau pot fi implicate într-un act terorist [85].

139. Cu toate acestea, este esențial ca, exceptând situațiile de urgență justificate în mod corespunzător, accesul la datele cu caracter personal în cauză să fie supus controlului prealabil al unei instanțe sau al unei autorități administrative independente, prin a cărei decizie se soluționează o cerere motivată formulată de autoritățile competente [86]. Astfel, în cazul în care nu se poate realiza o analiză *in abstracto* a legii, se asigură analiza *in concreto* efectuată de autoritatea independentă respectivă, care trebuie să aibă în vedere în egală măsură garantarea securității naționale și protejarea drepturilor fundamentale ale cetățenilor.

4) Obligația de păstrare a datelor care permit identificarea autorilor conținuturilor, în lumina Directivei 2000/31 (a doua întrebare preliminară din cauza C-512/18)

140. Instanța de trimitere face referire la Directiva 2000/31 ca punct de referință pentru a stabili dacă este posibil să se impună anumitor persoane [87] și operatorilor care oferă servicii de comunicații publice 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”.

141. Împărtășim opinia Comisiei, potrivit căreia nu ar fi posibilă examinarea compatibilității obligației respective cu Directiva 2000/31 [88], având în vedere că articolul 1 alineatul (5) litera (b) din aceasta exclude din domeniul său de aplicare „chestiunile referitoare la serviciile societății informaționale reglementate de Directivele 95/46/CE și 97/66/CE”, norme cărora le corespund în prezent Regulamentul 2006/679 și Directiva 2002/58 [89], fiind necesară, în opinia noastră, o interpretare a articolului 23 alineatul (1) din acest regulament și a articolului 15 alineatul (1) din această directivă în termenii menționați anterior.

82 Având în vedere că sunt respectate condițiile menționate la punctul 122 din Hotărârea Tele2 Sverige și Watson: Curtea a amintit că articolul 15 alineatul (1) din Directiva 2002/58 nu admite exceptarea articolului 4 alineatele (1) și (1a), care impune furnizorilor obligația de a adopta măsuri care permit garantarea protecției datelor păstrate împotriva riscului de abuz și a accesării lor ilegale. În acest sens, Curtea statua că „[ț]inând seama de cantitatea datelor păstrate, de caracterul sensibil al respectivelor date, precum și de riscul de acces ilicit la acestea, furnizorii de servicii de comunicații electronice trebuie, în scopul de a asigura deplina integritate și confidențialitate a datelor menționate, să garanteze un nivel deosebit de ridicat de protecție și de securitate prin măsuri tehnice și organizatorice adecvate. În special, reglementarea națională trebuie să prevadă păstrarea pe teritoriul Uniunii, precum și distrugerea iremediabilă a datelor la finalul duratei de păstrare a acestora”.

83 Punctele 52-60.

84 Hotărârea Tele2 Sverige și Watson, punctul 118.

85 *Ibidem*, punctul 119.

86 *Ibidem*, punctul 120.

87 Cele care „asigură […], 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 […]”.

88 Directiva în cauză este menționată, în termeni generici și fără să se indice vreo dispoziție, de instanța de trimitere în a doua întrebare preliminară din cauza C-512/18.

89 Punctele 112 și 113 din observațiile Comisiei.

2. Cu privire la obligația de colectare în timp real a datelor de trafic și de localizare (a doua întrebare preliminară din cauza C-511/18)

142. În opinia instanței de trimitere, articolul L. 851-2 din Codul privind securitatea internă permite, exclusiv în scopul combaterii terorismului, colectarea în timp real a informațiilor cu privire la persoanele identificate în prealabil ca fiind susceptibile să aibă legătură cu o amenințare teroristă. În mod analog, articolul L. 851-4 din codul respectiv permite transmiterea în timp real, de către operatori, a datelor tehnice referitoare la localizarea echipamentelor terminale.

143. Potrivit instanței de trimitere, aceste tehnici nu impun furnizorilor o obligație de păstrare suplimentară față de cea necesară pentru facturarea și comercializarea serviciilor lor.

144. În plus, conform articolului L. 851-3 din Codul privind securitatea internă, operatorii de comunicații electronice și furnizorii de servicii tehnice pot fi obligați „să efectueze în rețelele lor prelucrări automatizate de date destinate, în funcție de parametrii stabiliți în autorizație, să detecteze conexiuni care pot indica o amenințare teroristă”. Această tehnică nu presupune o păstrare generalizată și nediferențiată a datelor și urmărește colectarea într-un timp limitat a datelor de conectare care ar putea avea legătură cu o infracțiune de natură teroristă.

145. În opinia noastră, condițiile necesare pentru accesul la datele cu caracter personal păstrate trebuie să se aplice de asemenea în ceea ce privește accesul în timp real la datele generate în cursul comunicațiilor electronice. Facem trimitere, prin urmare, la cele arătate cu privire la acest aspect. Este irelevant dacă este vorba despre date păstrate sau despre date obținute pe loc, deoarece, în ambele cazuri, se ia cunoștință de datele cu caracter personal, neavând importanță dacă acestea sunt anterioare sau actuale.

146. Concret, dacă accesul în timp real ar fi consecința unor conexiuni detectate prin intermediul unei prelucrări automatizate, precum cea prevăzută la articolul L. 851-3 din Codul privind securitatea internă, este necesar ca modelele și criteriile prestabilite pentru această prelucrare să fie specifice, fiabile și nediscriminatorii, pentru a facilita identificarea indivizilor cu privire la care ar putea exista o bănuială rezonabilă de participare la infracțiuni de terorism [90].

3. Cu privire la obligația de a informa persoanele afectate (a treia întrebare preliminară din cauza C-511/18)

147. Curtea a statuat că autoritățile cărora li se acordă acces la date trebuie să informeze persoanele afectate despre împrejurarea respectivă, cu condiția de a nu se compromite anchetele în curs. Motivul acestei obligații constă în faptul că informația respectivă este necesară pentru ca acele persoane să își poată exercita dreptul la o cale de atac efectivă, menționat în mod expres la articolul 15 alineatul (2) din Directiva 2002/58, în cazul în care le sunt încălcate drepturile [91].

148. Conseil d'État (Consiliul de Stat) solicită să se stabilească, prin intermediul celei de a treia întrebări preliminare adresate în cauza C-511/18, dacă cerința respectivă privind informarea este obligatorie în orice situație sau dacă poate fi eludată în cazul în care s-au prevăzut alte garanții, precum cele menționate în decizia de trimitere.

90 Hotărârea Digital Rights, punctul 59.

91 Hotărârea Tele2 Sverige și Watson, punctul 121.

149. Conform descrierii realizate de instanța de trimitere[92], garanțiile menționate se limitează la posibilitatea ca persoanele care doresc să verifice dacă o tehnică de informare a fost aplicată în mod nelegal să sesizeze Conseil d'État (Consiliul de Stat). Această instanță ar putea, la rândul său, să anuleze autorizarea măsurii și să dispună eliminarea datelor colectate, în cadrul unei proceduri care nu prevede principiul contradictorialității specific procedurilor jurisdicționale.

150. Instanța de trimitere consideră că reglementarea respectivă nu încalcă dreptul la o cale de atac efectivă. Cu toate acestea, apreciem că s-ar putea afirma, teoretic, acest lucru în privința celor care decid să verifice dacă fac obiectul unei operațiuni de interceptare de informații. Dimpotrivă, dreptul respectiv nu este respectat în cazul în care persoanele care fac obiectul acelei operațiuni nu sunt informate cu privire la această împrejurare și, prin urmare, nu pot să verifice nici măcar dacă drepturile lor au fost sau nu încălcate.

151. Garanțiile jurisdicționale la care face referire instanța de trimitere par să fie condiționate de inițiativa celui care suspectează că face obiectul unei colectări de informații privind persoana sa. Cu toate acestea, accesul la justiție în vederea apărării propriilor drepturi ar trebui să fie conferit tuturor, ceea ce presupune că persoana care a fost supusă unei prelucrări a datelor sale cu caracter personal trebuie să aibă posibilitatea să conteste în justiție legalitatea prelucrării respective și, prin urmare, trebuie notificată cu privire la efectuarea sa.

152. Desigur, astfel cum rezultă din informațiile furnizate, acțiunea în justiție poate fi exercitată din oficiu sau în temeiul unei plângeri administrative, însă persoana afectată trebuie să aibă în orice caz posibilitatea de a fi ea însăși cea care o inițiază, motiv pentru care este necesar să i se comunice că datele sale personale au făcut obiectul unei anumite prelucrări. Apărarea drepturilor sale nu se poate baza pe împrejurarea că aceasta va fi informată cu privire la prelucrarea respectivă de către terți sau prin mijloace proprii.

153. Prin urmare, în măsura în care nu se compromite cursul investigațiilor în scopul cărora s-a acordat accesul la datele păstrate, persoana afectată trebuie să fie informată cu privire la accesul respectiv.

154. Pe de altă parte, în cazul în care, în urma introducerii unei acțiuni în justiție de către persoana afectată, după ce i s-a adus la cunoștință accesarea datelor sale, procedura jurisdicțională subsecventă respectă cerințele de confidențialitate și de discreție, inerente procedurilor penale privind acțiunile autorităților publice în domenii sensibile, precum cel al siguranței și al apărării statului. Totuși, această chestiune nu are legătură cu prezentele trimiteri preliminare, astfel încât, în opinia noastră, Curtea nu trebuie să se pronunțe în acest sens.

92 Punctele 8-11 din decizia de trimitere.

V. Concluzie

155. În temeiul considerațiilor prezentate, propunem Curții să răspundă Conseil d'État (Consiliul de Stat, Franța) după cum urmează:

„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) coroborat cu articolele 7, 8 și 11 și articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene trebuie interpretat în sensul că:

1) se opune unei reglementări naționale care, într-un context marcat de amenințări grave și persistente la adresa securității naționale, în special de riscul terorismului, impune operatorilor și furnizorilor de servicii de comunicații electronice obligația de a păstra în mod general și nediferențiat datele de transfer și de localizare ale tuturor abonaților, precum și datele care permit identificarea creatorilor conținuturilor oferite de furnizorii serviciilor respective;

2) se opune unei reglementări naționale care nu impune obligația de informare a persoanelor afectate cu privire la prelucrarea datelor lor personale realizată de autoritățile competente, cu excepția cazului în care această comunicare compromite acțiunile autorităților respective;

3) nu se opune unei reglementări naționale care permite colectarea în timp real a datelor de transfer și de localizare a anumitor persoane, în măsura în care acțiunile respective se realizează în conformitate cu procedurile stabilite pentru accesul la datele cu caracter personal păstrate în mod legal și cu aceleași garanții."