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

Cauza C-623/17

Privacy International
împotriva
Secretary of State for Foreign and Commonwealth Affairs,
Secretary of State for the Home Department,
Government Communications Headquarters,
Security Service,
Secret Intelligence Service

[cerere de decizie preliminară formulată de Investigatory Powers Tribunal (Tribunalul pentru Competențe de Investigare, Regatul Unit)]

„Trimitere preliminară – Prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice – Directiva 2002/58/CE – Domeniu de aplicare – Articolul 1 alineatul (3) – Articolul 15 alineatul (3) – Carta drepturilor fundamentale a Uniunii Europene – Articolele 7, 8 și 51 și articolul 52 alineatul (1) – Articolul 4 alineatul (2) TUE – Transmitere generalizată și nediferențiată către serviciile de securitate a datelor de conectare ale utilizatorilor unui serviciu de comunicații electronice”

1. În ultimii ani, Curtea a menținut o orientare jurisprudențială constantă cu privire la păstrarea și la accesarea datelor cu caracter personal, următoarele hotărâri reprezentând repere majore:

– Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții[2], în care a declarat nevaliditatea Directivei 2006/24/CE[3], deoarece aceasta permitea o ingerință disproporționată în drepturile consacrate la articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene.

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

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

1 Limba originală: spaniola.

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

3 Directiva 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. 053, p. 51).

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

5 Directiva 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. 036, p. 63).

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

2. Hotărârile respective (în special a doua) preocupă autoritățile din anumite state membre, deoarece, în opinia lor, au drept consecință faptul că le privează de un instrument pe care îl consideră indispensabil pentru protecția securității naționale și pentru combaterea terorismului. Prin urmare, o parte dintre acele 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 concluziile noastre din această zi.

4. În cele patru cauze se ridică, în primul rând, problema aplicării Directivei 2002/58 în ceea ce privește 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 în ce măsură diversele legislații naționale (cea britanică [8], cea belgiană [9] și cea franceză [10]) în această materie respectă dreptul Uniunii, astfel cum a fost interpretat de Curte.

I. Cadrul normativ

A. Dreptul Uniunii

5. Facem trimitere la punctul corespunzător din Concluziile noastre prezentate în cauzele C-511/18 și C-512/18.

B. Dreptul național (aplicabil în prezenta speță)

1. Telecommunications Act 1984 [11]

6. În conformitate cu articolul 94, secretarul de stat poate da operatorului unei rețele publice de comunicații electronice instrucțiunile generale sau specifice pe care le consideră necesare în interesul securității naționale sau al relațiilor cu guvernul unei țări sau al unui teritoriu situat în afara Regatului Unit.

2. Data Retention and Investigatory Powers Act 2014 [12]

7. Articolul 1 prevede:

„(1) Secretarul de stat poate, în temeiul unui ordin de păstrare, să solicite unui operator de telecomunicații publice să păstreze date relevante referitoare la comunicații în cazul în care consideră că solicitarea respectivă este necesară și proporțională în raport cu unul sau mai multe dintre obiectivele prevăzute la articolul 22 alineatul (2) literele (a)-(h) din Regulation of Investigatory Powers Act 2000 [Legea din 2000 de reglementare a competențelor de investigare, denumită în continuare «RIPA»].

7 În afară de prezenta cauză, este vorba despre cauzele C-511/18 și C-512/18, La Quadrature du Net și alții, și 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.

11 Legea din 1984 privind telecomunicațiile, denumită în continuare „Legea din 1984”.

12 Legea din 2014 privind păstrarea datelor și competențele de investigare; denumită în continuare „DRIPA”.

(2) Un ordin de păstrare poate:

(a) să se refere la un operator în particular sau la orice categorie de operatori;

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

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

(d) să conțină alte cerințe sau restricții în legătură cu păstrarea datelor;

(e) să prevadă dispoziții diferite în scopuri diferite;

(f) să se refere la date care există sau nu la data adoptării sau intrării în vigoare a ordinului de păstrare.

(3) Secretarul de stat poate, prin intermediul unui regulament, să adopte dispoziții suplimentare referitoare la păstrarea datelor relevante referitoare la comunicații.

(4) Aceste dispoziții pot privi în special:

(a) cerințele anterioare adoptării ordinului de păstrare;

(b) perioada maximă în care urmează să fie păstrate datele în temeiul unui ordin de păstrare;

(c) conținutul, adoptarea, intrarea în vigoare, reexaminarea, modificarea sau revocarea unui ordin de păstrare;

(d) integritatea, securitatea sau protecția datelor păstrate în aplicarea prezentului articol, accesul la aceste date, precum și divulgarea sau distrugerea lor;

(e) respectarea cerințelor sau a restricțiilor relevante sau verificarea conformității cu acestea;

(f) un cod de bune practici privind cerințele, restricțiile sau competențele relevante;

(g) rambursarea de către secretarul de stat (în anumite condiții sau nu) a cheltuielilor suportate de operatorii de telecomunicații publice, efectuate în vederea conformării cu cerințele sau cu restricțiile relevante;

[…]

(5) Perioada maximă prevăzută în aplicarea alineatului (4) litera (b) nu trebuie să depășească 12 luni începând de la data indicată în raport cu datele vizate de regulamentele menționate la alineatul (3).

(6) Un operator de telecomunicații publice care păstrează date relevante referitoare la comunicații în aplicarea prezentului articol nu poate divulga datele respective, cu excepția cazului în care:

(a) le divulgă în conformitate cu:

(i) capitolul 2 partea 1 din [RIPA] sau

(ii) o hotărâre judecătorească sau cu orice altă autorizație ori ordin judecătoresc sau

(b) este prevăzut de regulamentele menționate la alineatul (3).

(7) Secretarul de stat poate, pe cale normativă, să adopte măsuri cu privire la oricare dintre dispozițiile adoptate (sau care pot fi adoptate) în aplicarea alineatului (4) literele (d)-(g) sau a alineatului (6), în legătură cu datele referitoare la comunicații păstrate de furnizorii de servicii de telecomunicații pe baza unui cod de bune practici, în temeiul articolului 102 din Legea din 2001 privind combaterea terorismului, criminalitatea și securitatea [Anti-terrorism, Crime and Security Act 2001]".

3. RIPA

8. Articolul 21 prevede:

„[…]

(4) În prezentul capitol, «date privind comunicațiile» înseamnă oricare dintre următoarele:

(a) orice dată privind transferul inclusă în sau anexată la o comunicație (fie de către expeditor, fie în alt mod) pentru orice serviciu poștal sau sistem de telecomunicații prin intermediul căruia este transmisă sau poate fi transmisă;

(b) orice informație care nu include nimic din conținutul unei comunicații [cu excepția oricărei informații care intră în domeniul de aplicare al literei (a)] și care se referă la utilizarea de către orice persoană:

(i) a oricărui serviciu poștal sau de telecomunicații sau

(ii) în legătură cu furnizarea sau cu utilizarea de către orice persoană a oricărui serviciu de telecomunicații, a oricărei părți dintr-un sistem de telecomunicații;

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

[…]

(6) În această secțiune, noțiunea de «dată privind transferul», cu privire la orice comunicație, se referă la:

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

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

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

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

[…]"

9. Articolul 22 prevede:

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

(2) Pentru motive care intră sub incidența prezentului alineat, este necesar să se obțină date din cadrul unei comunicații dacă acestea sunt necesare:

(a) în interesul securității naționale;

(b) în vederea prevenirii sau a detectării criminalității sau în vederea prevenirii tulburărilor aduse ordinii publice;

(c) în interesul bunăstării economice a Regatului Unit, cu condiția ca aceste interese să fie de asemenea relevante pentru interesele securității naționale;

(d) în interesul securității publice;

(e) în vederea protecției sănătății publice;

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

(g) în scopul prevenirii, în caz de urgență, de deces, de vătămare ori în cazul oricăror prejudicii aduse sănătății fizice sau mentale a unei persoane sau în vederea reducerii oricărei vătămări sau a oricărui prejudiciu adus sănătății fizice sau mentale a unei persoane fizice;

(h) în orice alt scop [care nu intră sub incidența literelor (a)-(g)] precizat într-un ordin emis de secretarul de stat în conformitate cu articolul 22 alineatul 2 litera (h) din [DRIPA].

[…]

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

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

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

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

10. În conformitate cu articolul 65, se pot formula plângeri la Investigatory Powers Tribunal (Tribunalul pentru Competențe de Investigare, Regatul Unit) dacă există motive pentru a considera că datele au fost colectate în mod necorespunzător.

II. Situația de fapt și întrebările preliminare

11. Potrivit instanței de trimitere, litigiul principal se referă la obținerea și la utilizarea de către United Kingdom Security and Intelligence Agencies (agențiile de securitate și de informații din Regatul Unit, denumite în continuare „ASI") a datelor referitoare la comunicații în masă.

12. Aceste date includ informații de tipul „cine" utilizează telefonul și internetul, precum și „când, unde, cum și cu cine" le utilizează. Ele cuprind localizarea telefoanelor mobile și fixe de pe care se efectuează sau pe care se primesc apeluri, precum și a computerelor de pe care se realizează accesul la internet. Ele nu includ conținutul comunicațiilor, care poate fi obținut numai printr-un ordin judecătoresc.

13. Reclamanta din procedura principală (Privacy International, organizație non-guvernamentală pentru apărarea drepturilor omului) a formulat o acțiune în fața instanței de trimitere, susținând că obținerea și utilizarea datelor menționate de către ASI încalcă dreptul la respectarea vieții private consacrat la articolul 8 din Convenția europeană a drepturilor omului (denumită în continuare „CEDO") și sunt incompatibile cu dreptul Uniunii.

14. Autoritățile pârâte [13] susțin că exercitarea competenței lor în această materie este legală și esențială, printre altele, pentru protecția securității naționale.

15. Potrivit informațiilor din decizia de trimitere, în temeiul instrucțiunilor emise de secretarul de stat în conformitate cu articolul 94 din Legea din 1984, ASI primesc datele referitoare la comunicațiile în masă prin intermediul operatorilor rețelelor publice de comunicații electronice.

16. Aceste date includ informații privind transferul și localizarea, precum și activitățile sociale, comerciale și financiare, comunicațiile și călătoriile utilizatorilor. Odată intrate în posesia ASI, datele respective sunt păstrate în siguranță de acestea, prin utilizarea unor tehnici (de exemplu, filtrarea și agregarea) generalizate, adică nedirecționate spre obiective specifice și cunoscute.

17. Instanța de trimitere consideră dovedit faptul că aceste tehnici sunt esențiale pentru activitatea ASI în cadrul combaterii amenințărilor grave la adresa siguranței publice, în special a terorismului, a contraspionajului și a proliferării nucleare. Capacitatea ASI de a obține și de a utiliza datele respective este esențială pentru protecția securității naționale a Regatului Unit.

18. Potrivit instanței de trimitere, măsurile în litigiu respectă dreptul național și articolul 8 din CEDO. Totuși, aceasta are îndoieli cu privire la compatibilitatea lor cu dreptul Uniunii, având în vedere Hotărârea Tele2 Sverige și Watson.

19. În acest context, instanța de trimitere adresează Curții următoarele întrebări preliminare:

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

13 Secretary of State for Foreign and Commonwealth Affairs (secretarul de stat pentru Afaceri Externe și Commonwealth, Regatul Unit), Secretary of State for the Home Department (secretarul de stat pentru Afaceri Interne, Regatul Unit) și cele trei ASI din Regatul Unit, și anume, Government Communications Headquarters (Cartierul General pentru Comunicații din Regatul Unit) (GCHQ), Security Service (Serviciul de Securitate, Regatul Unit) (MI5) și Secret Intelligence Service (Serviciul Secret de Informații, Regatul Unit) (MI6).

2) În cazul în care răspunsul la prima întrebare este afirmativ, unei astfel de instrucțiuni transmise de secretarul de stat i se aplică vreuna dintre cerințele prevăzute de Hotărârea Watson[14] sau orice altă cerință suplimentară față de cele impuse de CEDO? Dacă răspunsul este afirmativ, în ce mod și în ce măsură se aplică aceste cerințe, luând în considerare nevoia absolută a ASI de a utiliza tehnicile de obținere în masă și de prelucrare automată pentru a proteja securitatea națională, și în ce măsură astfel de capacități, dacă din alte puncte de vedere sunt conforme cu CEDO, pot fi grav afectate de impunerea acestor cerințe?"

20. Instanța de trimitere motivează întrebările sale după cum urmează:

„a) capacitățile [ASI] de a utiliza [datele referitoare la comunicații în masă] care le sunt furnizate sunt esențiale pentru a proteja securitatea națională a Regatului Unit, inclusiv în domeniul combaterii terorismului, a contraspionajului și a proliferării nucleare;

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

c) furnizorul unei rețele de comunicații electronice nu are apoi obligația de a păstra datele menționate (dincolo de perioada în care trebuie să le păstreze în vederea exercitării activității sale obișnuite), care sunt păstrate numai de către stat (ASI);

d) instanța națională a constatat (sub rezerva anumitor aspecte rămase în pronunțare) că garanțiile legate de utilizarea [acestor date] de către ASI sunt conforme cu dispozițiile CEDO și

e) instanța națională a constatat că impunerea cerințelor specificate în Hotărârea [Tele2 Sverige și Watson], dacă este cazul, ar submina măsurile luate pentru apărarea securității naționale de către ASI și astfel ar periclita securitatea națională a Regatului Unit."

III. Procedura în fața Curții

21. Cererea de decizie preliminară a fost înregistrată la grefa Curții la 31 octombrie 2017.

22. Au prezentat observații scrise guvernele german, belgian, britanic, ceh, cipriot, spaniol, estonian, francez, maghiar, irlandez, leton, neerlandez, norvegian, polonez, portughez și suedez, precum și Comisia.

23. La 9 septembrie 2019 a avut loc o ședință publică, desfășurată împreună cu cele din cauzele C-511/18, C-512/18 și C-520/18, în care s-au prezentat părțile din cele patru cauze preliminare, guvernele menționate anterior, precum și Comisia și Autoritatea Europeană pentru Protecția Datelor.

14 *Id est*, jurisprudența stabilită prin Hotărârea Tele2 Sverige și Watson.

IV. Analiză

A. Cu privire la domeniul de aplicare al Directivei 2002/58 și la excluderea securității naționale (prima întrebare preliminară)

24. În Concluziile noastre prezentate la aceeași dată în cauzele C-511/18 și C-512/18, explicăm motivele pentru care, în opinia noastră, 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” [15].

25. În prezentarea argumentelor noastre, facem referire la incidența Hotărârilor Curții din 30 mai 2006, Parlamentul/Consiliul și Comisia [16], și Tele2 Sverige și Watson și alții, susținând o interpretare care le include pe ambele [17].

26. În aceleași concluzii, odată constatată aplicabilitatea Directivei 2002/58, examinăm excluderea securității naționale, prevăzută de aceasta, și incidența articolului 4 alineatul (2) TUE [18].

27. Fără a aduce atingere aspectelor prezentate în continuare, facem trimitere la cele afirmate în concluziile menționate și în cele prezentate în cauza C-520/18.

1. Aplicarea Directivei 2002/58 în prezenta cauză

28. Conform dispozițiilor în discuție în speță, furnizorii de servicii de comunicații electronice sunt destinatarii unei obligații care implică, pe lângă păstrarea datelor deținute ca urmare a serviciului prestat utilizatorilor rețelelor publice de comunicații ale Uniunii, și prelucrarea lor [19].

29. Astfel, operatorii menționați trebuie să transmită în mod obligatoriu către ASI datele respectivele. Problema care se ridică aici se referă la aspectul dacă articolul 15 alineatul (1) din Directiva 2002/58 permite ca această transmitere, având în vedere scopul său, să fie pur și simplu exclusă din domeniul de aplicare al dreptului Uniunii.

30. Noi credem că nu. Păstrarea datelor menționate, urmată de transmiterea lor ulterioară, poate fi calificată drept prelucrare de date cu caracter personal realizată de furnizorii de servicii de telecomunicații electronice, motiv pentru care intră în mod firesc în domeniul de aplicare al Directivei 2002/58.

31. După cum sugerează instanța de trimitere, motivele de securitate națională nu pot prevala asupra acestei constatări, astfel încât obligația în litigiu să nu mai intre în domeniul de aplicare al dreptului Uniunii. În opinia noastră, astfel cum am menționat, furnizorii sunt obligați să efectueze o prelucrare de date în legătură cu furnizarea de servicii de comunicații electronice destinate publicului prin intermediul rețelelor publice de comunicații din cadrul Uniunii, ceea ce corespunde chiar domeniului de aplicare al Directivei 2002/58, conform articolului 3 alineatul (1) din aceasta.

15 Concluziile prezentate în cauzele C-511/18 și C-512/18, punctul 42.

16 Cauzele C-317/04 și C-318/04, EU:C:2006:346.

17 Concluziile prezentate în cauzele C-511/18 și C-512/18, punctele 44-76.

18 *Ibidem*, punctele 77-90.

19 În temeiul articolului 2 din Directiva 2002/58, în sensul acestei directive, se aplică definițiile prevăzute de Directiva 95/46. În conformitate cu articolul 2 litera (b) din aceasta din urmă, „prelucrarea datelor cu caracter personal” înseamnă „orice operațiune sau serie de operațiuni efectuate cu privire la datele cu caracter personal, indiferent dacă se realizează prin mijloace automate sau nu, precum colectarea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, recuperarea, consultarea, utilizarea, *divulgarea prin transmitere*, diseminare sau *punere la dispoziție în alt mod*, alinierea sau combinarea, blocarea, ștergerea sau distrugerea” (sublinierea noastră).

32. Plecând de la această premisă, dezbaterea privește nu activitățile ASI (care, astfel cum am menționat anterior, ar putea să nu intre sub incidența dreptului Uniunii în cazul în care nu ar viza operatorii de comunicații electronice), ci păstrarea și transmiterea ulterioară a datelor deținute de operatorii respectivi. Din această perspectivă, intră în joc drepturile fundamentale garantate de Uniune.

33. Elementul-cheie pentru soluționarea acestei dezbateri este, încă o dată, obligația de păstrare generalizată și nediferențiată a datelor cu caracter personal la care au acces autoritățile publice.

2. Invocarea securității naționale

34. Având în vedere că, în prezenta cauză, instanța de trimitere acordă o atenție specială activității ASI din domeniul securității naționale, ne permitem să reproducem unele dintre punctele din Concluziile noastre prezentate la aceeași dată în cauzele C-511/18 și C-512/18, referitoare la această chestiune:

„77. Securitatea națională […] 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.

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». […]

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.

[…]

82. […][C]onsiderăm că poate fi utilizat în scop orientativ criteriul stabilit în Decizia-cadru 2006/960/JAI […], 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 […].

[…]

84. Există […] 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 [al unsprezecelea 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.

[…]

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.”

3. Consecințele aplicării Hotărârii Tele2 Sverige și Watson în prezenta cauză

35. Instanța de trimitere s-a concentrat pe interpretarea realizată de Curte în Hotărârea Tele2 Sverige și Watson, prezentând dificultățile pe care le-ar implica, în opinia sa, aplicarea acesteia în prezenta cauză.

36. Hotărârea Tele2 Sverige și Watson a stabilit astfel condițiile pe care trebuie să le îndeplinească o reglementare națională care instituie obligația de a păstra date de transfer și de localizare pentru accesarea ulterioară a acestora de către autoritățile publice.

37. La fel ca în cauzele C-511/18 și C-512/18 și pentru motive similare, considerăm că normele naționale vizate de prezenta trimitere preliminară nu respectă condițiile stabilite în Hotărârea Tele2 Sverige și Watson, deoarece acestea prevăd o păstrare generalizată și nediferențiată a datelor cu caracter personal care facilitează o descriere detaliată a vieții persoanelor afectate, pentru o perioadă îndelungată.

38. În concluziile prezentate în cele două cauze ridicăm problema dacă ar fi posibilă nuanțarea sau completarea jurisprudenței menționate în hotărârea respectivă, având în vedere consecințele sale asupra combaterii terorismului sau a protejării statului de alte amenințări similare la adresa securității naționale.

39. Ne permitem de asemenea să reproducem în continuare o parte dintre punctele din concluziile respective, în care susținem în esență că, având în vedere că este posibilă nuanțarea jurisprudenței respective, se impune confirmarea sa în ceea ce privește aspectele esențiale:

„135. Deși este dificil, nu este imposibil să se determine cu exactitate și în conformitate cu criterii obiective nici categoriile de date a căror păstrare este considerată indispensabilă, nici 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 […] 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. […]

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 […], 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.

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 […]. 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. […]

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 […]. 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.”

B. Cu privire la a doua întrebare preliminară

40. Instanța de trimitere formulează a doua întrebare preliminară pentru eventualitatea în care se va răspunde în sens afirmativ la prima. În acest caz, solicită să se stabilească ce „altă cerință suplimentară față de cele impuse de CEDO” sau față de cele care decurg din Hotărârea Tele2 Sverige și Watson ar trebui prevăzută.

41. În acest sens, ea subliniază că impunerea condițiilor stabilite în Hotărârea Tele2 Sverige și Watson „ar submina măsurile luate pentru protejarea securității naționale de către ASI”.

42. Având în vedere că răspunsul pe care îl propunem la prima întrebare este negativ, nu este necesar să o abordăm pe cea de a doua. Aceasta din urmă, astfel cum subliniază instanța de trimitere însăși, este condiționată de constatarea compatibilității cu dreptul Uniunii a „tehnicil[or] de obținere și de prelucrare automată în masă” a datelor cu caracter personal ale tuturor utilizatorilor din Regatul Unit, pe care operatorii serviciilor de comunicații electronice ar trebui să le transmită către ASI.

43. În cazul în care Curtea apreciază că este necesar să se răspundă la cea de a doua întrebare preliminară, considerăm că ar trebui să confirmăm condițiile menționate în Hotărârea Tele2 Sverige și Watson în legătură cu:

– interzicerea accesului generalizat la date;

– necesitatea unei autorizații prealabile emise de un judecător sau de o autoritate independentă pentru legitimarea accesului respectiv;

– obligația de a informa persoanele afectate, cu excepția cazului în care prin aceasta s-ar compromite eficacitatea măsurii;

– păstrarea datelor în cadrul Uniunii.

44. Ar fi suficient, astfel cum am menționat, să confirmăm aceste condiții, a căror aplicare este obligatorie, pentru motivele menționate în Concluziile prezentate în cauzele C-511/18 și C-512/18 și, respectiv, C-520/18, fără a fi necesar să adăugăm „altele” suplimentare, în sensul la care face referire instanța de trimitere.

V. Concluzie

45. În temeiul considerațiilor anterioare, propunem Curții să răspundă Investigatory Powers Tribunal (Tribunalul pentru Competențe de Investigare, Regatul Unit) după cum urmează:

„Articolul 4 TUE și articolul 1 alineatul (3) 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) trebuie interpretate în sensul că se opun unei reglementări naționale care impune furnizorului unei rețele de comunicații electronice obligația de a furniza «date referitoare la comunicații în masă» către agențiile de securitate și de informații dintr-un stat membru, care implică colectarea prealabilă a acestora în mod generalizat și nediferențiat.”

Cu titlu subsidiar:

„Accesul agențiilor de securitate și de informații dintr-un stat membru la datele cu caracter personal transmise de furnizorii de rețele de comunicații electronice trebuie să respecte condițiile stabilite în Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson (C-203/15 și C-698/15, EU:C:2016:970).”