Repertoriul jurisprudenței

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

Cauza C-520/18

Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,
UA,
Liga voor Mensenrechten ASBL,
Ligue des Droits de l'Homme ASBL,
VZ,
WY,
XX
împotriva
Conseil des ministres,
cu intervenția:
Child Focus

[cerere de decizie preliminară formulată de Cour constitutionnelle (Curtea Constituțională, Belgia)]

„Întrebare 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 (1) – Articolul 4 alineatul (2) TUE – Carta drepturilor fundamentale a Uniunii Europene – Articolele 4, 6, 7, 8 și 11 și articolul 52 alineatul (1) – Obligație de păstrare generalizată și nediferențiată a datelor de transfer și de localizare – Efectivitatea investigațiilor penale și alte obiective de interes public”

1. În ultimii ani, Curtea a menținut o linie jurisprudențială constantă cu privire la păstrarea și la accesarea datelor cu caracter personal, în cadrul căreia 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 permitea o ingerință disproporționată în drepturile consacrate la articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene.

1 Limba originală: spaniola.

2 Cauzele C-293/12 și C-594/12, denumită 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. 53, p. 51).

– 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].

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

2. Aceste hotărâri (în special cea de a doua) preocupă autoritățile anumitor state membre, deoarece, în opinia lor, le privează de un instrument pe care îl consideră necesar pentru protecția securității naționale și pentru combaterea infracționalității și a terorismului. Prin urmare, o parte dintre respectivele state membre solicită schimbarea sau nuanțarea acelei jurisprudențe.

3. Anumite instanțe din statele membre au pus în evidență aceeași preocupare în patru trimiteri preliminare [7], în privința cărora prezentăm astăzi concluziile noastre.

4. În cele patru cauze se ridică mai întâi 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 drepturile referitoare la respectarea vieții private pe care ea le protejează. În sfârșit, va trebui să se analizeze măsura în care 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.

5. Ca urmare a pronunțării Hotărârii Digital Rights, Cour constitutionnelle (Curtea Constituțională, Belgia) a anulat reglementarea națională care a transpus parțial în dreptul național Directiva 2006/24, declarată nevalidă prin hotărârea respectivă. Legiuitorul belgian a adoptat apoi o nouă reglementare, a cărei compatibilitate cu dreptul Uniunii este pusă din nou sub semnul îndoielii în lumina Hotărârii Tele2 Sverige și Watson.

6. O specificitate a prezentei trimiteri preliminare constă în faptul că aceasta ridică problema privind posibilitatea de a amâna în mod provizoriu efectele unei norme interne a cărei anulare de către instanțele naționale se impune ca urmare a incompatibilității sale cu dreptul Uniunii.

I. Cadrul normativ

A. Dreptul Uniunii

7. Facem trimitere la secțiunea corespunzătoare din Concluziile noastre prezentate în cauzele C-511/18 și C-512/18.

4 Cauzele C-203/15 și C-698/15, denumită 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. 36, p. 63).

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

7 În afara de prezenta cauză (cauza C-520/18, Ordre des barreaux francophones et germanophone și alții), este vorba despre cauzele C-511/18 și C-512/18, La Quadrature du Net și alții, și despre cauza C-623/17, Privacy International.

8 Cauza C-623/17, Privacy International.

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

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

B. Dreptul național. Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques [11]

8. Articolul 4 prevede că articolul 126 din loi du 13 juin 2005 relative aux communications électroniques [12] va fi redactat după cum urmează:

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

Prezentul articol nu privește conținutul comunicațiilor.

[…]

2. Numai următoarele autorități pot obține, la cerere, de la furnizorii și de la operatorii menționați la alineatul 1 primul paragraf, date păstrate în temeiul prezentului articol, în scopurile și în condițiile enumerate mai jos:

1° autoritățile judiciare, în vederea investigării, a instrucției și a urmăririi penale a infracțiunilor, pentru executarea măsurilor prevăzute la articolele 46*bis* și 88*bis* din Code d'instruction criminelle (Codul de procedură penală) și în condițiile prevăzute la aceste articole;

2° serviciile de informații și de securitate, pentru a îndeplini misiunile de informare prin recurgerea la metodele de colectare a datelor prevăzute la articolele 16/2, 18/7 și 18/8 din loi du 30 novembre 1998 organique des services de renseignement et de sécurité[13] și în condițiile stabilite prin această lege;

3° orice ofițer de poliție judiciară din cadrul Institut [belge des services postaux et des télécommunications (Institutul belgian al Poștei și al Telecomunicațiilor)] în vederea investigării, a instrucției și a urmăririi penale a infracțiunilor referitoare la [normele de securitate a rețelelor] și la prezentul articol;

4° serviciile de urgență care oferă asistență la fața locului, atunci când, în urma unui apel de urgență, acestea nu obțin de la furnizorul sau de la operatorul respectiv datele de identificare a apelantului […] sau obțin date incomplete sau incorecte. Numai datele de identificare a apelantului pot fi solicitate și în cel mult 24 de ore de la efectuarea apelului;

11 Legea din 29 mai 2016 privind colectarea și păstrarea datelor în sectorul comunicațiilor electronice, denumită în continuare „Legea din 29 mai 2016" (Moniteur belge din 18 iulie 2016, p. 44717).

12 Legea din 13 iunie 2005 privind comunicațiile electronice, denumită în continuare „Legea din 2005" (*Moniteur belge* din 20 iunie 2005, p. 28070).

13 Legea organică din 30 noiembrie 1998 privind serviciile de informații și de securitate, denumită în continuare „Legea din 1998" (*Moniteur belge* din 18 decembrie 1998, p. 40312).

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

6° Serviciul de mediere pentru telecomunicații, în vederea identificării persoanei care a utilizat cu rea-credință o rețea sau un serviciu de comunicații electronice […]. Numai datele de identificare pot fi solicitate.

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

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

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

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

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

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

4. În vederea păstrării datelor prevăzute la alineatul 3, furnizorii și operatorii menționați la alineatul 1 primul paragraf:

1° garantează că datele păstrate sunt de aceeași calitate și sunt supuse acelorași cerințe de securitate și de protecție ca datele din rețea;

2° se asigură că datele păstrate sunt supuse unor măsuri tehnice și organizaționale adecvate pentru a fi protejate împotriva distrugerii accidentale sau ilicite, pierderii sau modificării accidentale, depozitării, prelucrării, accesării sau divulgării neautorizate sau ilicite;

3° garantează că la datele păstrate pentru a răspunde solicitărilor autorităților menționate la alineatul 2 au acces doar unul sau mai mulți membri ai Celulei de coordonare prevăzute la articolul 126/1 alineatul 1;

4° păstrează datele pe teritoriul Uniunii Europene;

5° pun în aplicare măsuri de protecție tehnologică care fac ca datele păstrate să devină, de la înregistrarea lor, ilizibile și inutilizabile de orice persoană care nu este autorizată să aibă acces la acestea;

6° distrug datele păstrate de pe orice suport la expirarea perioadei de păstrare aplicabile acestor date, stabilită la alineatul 3, fără a aduce atingere articolelor 122 și 123;

7° asigură o trasabilitate a exploatării datelor păstrate pentru fiecare solicitare de obținere a acestor date din partea unei autorități menționate la alineatul 2.

Trasabilitatea prevăzută la alineatul 1 punctul 7 se realizează cu ajutorul unui jurnal. Institutul și Comisia pentru protecția vieții private pot să consulte acest jurnal sau să solicite o copie a întregului jurnal sau a unei părți a acestuia. Institutul și Comisia pentru protecția vieții private încheie un protocol de colaborare privind luarea la cunoștință și controlul conținutului jurnalului.

5. Ministrul și ministrul justiției transmit anual Camerei Reprezentanților statistici privind păstrarea datelor cu caracter personal generate sau prelucrate în cadrul furnizării de servicii sau de rețele publice de comunicații.

Aceste statistici conțin în special:

1° cazurile în care s-au transmis date autorităților competente în conformitate cu dispozițiile legale aplicabile;

2° perioada scursă între data începând cu care s-au păstrat datele și data la care autoritățile competente au solicitat transmiterea lor;

3° cazurile în care nu s-a putut da curs cererilor de date.

Statisticile respective nu pot conține date cu caracter personal.

[…]”

9. Articolul 5 prevede includerea articolului 126/1 în Legea din 2005, cu următorul conținut:

„1. În cadrul fiecărui operator și al fiecărui furnizor menționat la articolul 126 alineatul 1 primul paragraf se constituie o Celulă de coordonare responsabilă cu furnizarea către autoritățile belgiene abilitate prin lege, la cerere, a datelor păstrate în temeiul articolelor 122, 123 și 126, a datelor de identificare a apelantului în temeiul articolului 107 alineatul 2 primul paragraf sau a datelor care pot fi solicitate în temeiul articolelor 46*bis*, 88*bis* și 90*ter* din Codul de procedură penală și al articolelor 18/7, 18/8, 18/16 și 18/17 din [Legea din 1998].

[…]

2. Fiecare operator și fiecare furnizor menționat la articolul 126 alineatul 1 primul paragraf stabilește o procedură internă pentru a răspunde solicitărilor autorităților privind accesul la datele cu caracter personal ale utilizatorilor. La cerere, aceștia oferă Institutului informații

privind procedurile respective, numărul de solicitări primite, temeiul juridic invocat și răspunsul la acestea.

[…]

3. Fiecare furnizor și fiecare operator menționat la articolul 126 alineatul 1 primul paragraf desemnează unul sau mai mulți prepuși pentru protecția datelor cu caracter personal, care trebuie să îndeplinească condițiile cumulative enumerate la alineatul 1 al treilea paragraf.

[…]

În exercitarea misiunilor sale, prepusul pentru protecția datelor cu caracter personal acționează cu deplină independență și are acces la toate datele cu caracter personal transmise autorităților, precum și la toate sediile relevante ale furnizorului sau ale operatorului.

[…]

4. Regele stabilește, prin decret adoptat în cadrul Conseil des ministres, după avizul Comisiei pentru protecția vieții private și al Institutului:

[…]

2° cerințele pe care trebuie să le îndeplinească Celula de coordonare, ținând seama de situația operatorilor și a furnizorilor care primesc puține solicitări de la autoritățile judiciare, care nu au un sediu în Belgia sau care operează în principal din străinătate;

3° informațiile care trebuie furnizate Institutului și Comisiei pentru protecția vieții private în conformitate cu alineatele 1 și 3, precum și autoritățile care au acces la aceste informații;

4° celelalte norme care reglementează colaborarea operatorilor și a furnizorilor menționați la articolul 126 alineatul 1 primul paragraf cu autoritățile belgiene sau cu unele dintre acestea în vederea furnizării datelor prevăzute la alineatul 1, inclusiv, dacă este necesar și pentru fiecare autoritate în cauză, forma și conținutul cererii.

[…]”

10. Articolul 8 prevede că articolul 46*bis* alineatul 1 din Codul de procedură penală va avea următorul cuprins:

„1. În cadrul investigării infracțiunilor, procurorul, printr-o decizie scrisă motivată, solicitând la nevoie sprijinul operatorului unei rețele de comunicații electronice sau al unui furnizor al unui serviciu de comunicații electronice ori al unui serviciu de poliție desemnat de Rege, în temeiul tuturor datelor pe care le deține sau prin intermediul accesului la fișierele clienților operatorului sau furnizorului serviciului, poate să procedeze sau să dispună să se procedeze la:

1° identificarea abonatului sau a utilizatorului obișnuit al unui serviciu de comunicații electronice sau al mijlocului de comunicare electronică utilizat;

2° identificarea serviciilor de comunicații electronice la care este abonată o anumită persoană sau care sunt utilizate în mod obișnuit de o anumită persoană.

Măsura adoptată trebuie să fie proporțională, având în vedere respectarea vieții private, și subsidiară oricărei alte obligații impuse de investigație.

În caz de extremă urgență, orice ofițer de poliție judiciară, cu acordul verbal și prealabil al procurorului, poate solicita aceste date printr-o decizie motivată și scrisă. Ofițerul de poliție judiciară comunică procurorului această decizie motivată și scrisă, precum și informațiile pe care le-a obținut în 24 de ore și, pe de altă parte, motivează extrema urgență.

Pentru infracțiunile care nu sunt de natură să aibă drept consecință o pedeapsă principală cu închisoarea de un an sau o pedeapsă mai severă, procurorul sau, în caz de extremă urgență, ofițerul de poliție judiciară poate solicita datele prevăzute la alineatul 1 numai pentru o perioadă de șase luni anterior deciziei sale.

2. Fiecare operator al unei rețele de comunicații electronice și fiecare furnizor al unui serviciu de comunicații electronice căruia i se solicită să comunice datele menționate la alineatul 1 furnizează procurorului sau ofițerului de poliție judiciară datele care au fost solicitate într-un termen care este stabilit de Rege […].

[…]

Orice persoană care, în virtutea funcției, are cunoștință despre măsură sau participă la punerea în aplicare a acesteia are obligația de a păstra secretul. Orice încălcare a secretului se pedepsește conform articolului 458 din Codul penal.

Refuzul comunicării datelor se pedepsește cu amendă de la 26 de euro la 10 000 de euro.”

11. Articolul 9 conferă următorul mod de redactare articolului 88*bis* din Codul de procedură penală:

„1. În cazul în care există indicii temeinice în sensul că infracțiunile sunt de natură să aibă drept consecință o pedeapsă principală cu închisoarea de un an sau o pedeapsă mai severă și atunci când judecătorul de instrucție apreciază că există circumstanțe care fac ca reperarea comunicațiilor electronice sau localizarea originii sau a destinației comunicațiilor electronice să fie necesară pentru aflarea adevărului, acesta poate dispune, solicitând la nevoie, direct sau prin intermediul unui serviciu de poliție desemnat de Rege, asistența tehnică a operatorului unei rețele de comunicații electronice sau a unui furnizor al unui serviciu de comunicații electronice:

1° reperarea datelor de transfer ale mijloacelor de comunicare electronică de la care sau către care sunt sau au fost adresate comunicații electronice;

2° localizarea originii sau a destinației comunicațiilor electronice.

În cazurile prevăzute la primul paragraf, pentru fiecare mijloc de comunicare electronică ale cărui date de apel sunt reperate sau a cărui origine sau destinație a telecomunicațiilor este localizată, ziua, ora, durata și, dacă este necesar, locul comunicației electronice sunt indicate și consemnate într-un proces-verbal.

Judecătorul de instrucție indică într-o ordonanță motivată împrejurările de fapt ale cauzei care justifică măsura, caracterul său proporțional având în vedere respectarea vieții private și subsidiar oricărei alte obligații impuse de investigație.

Acesta precizează de asemenea perioada pentru care măsura se va putea aplica în viitor, această perioadă neputând depăși două luni de la data ordonanței, fără a aduce atingere unei reînnoiri, și, dacă este cazul, perioada din trecut pe care o acoperă ordonanța, în conformitate cu alineatul 2.

[…]

2. În ceea ce privește aplicarea măsurii prevăzute la alineatul 1 primul paragraf în privința datelor de transfer sau de localizare păstrate în temeiul articolului 126 din Legea din […] 2005 […], se aplică următoarele dispoziții:

– pentru o infracțiune prevăzută în cartea II titlul I*ter* din Codul penal, judecătorul de instrucție poate solicita date, prin ordonanță, pentru o perioadă de douăsprezece luni anterior ordonanței;

– pentru o infracțiune prevăzută la articolul 90*ter* alineatele 2-4, care nu este vizată la prima liniuță, sau pentru o infracțiune care este săvârșită în cadrul unui grup infracțional organizat menționat la articolul 324*bis* din Codul penal sau pentru o infracțiune care este de natură să aibă drept consecință o pedeapsă principală cu închisoarea corecțională de cinci ani sau o pedeapsă mai severă, judecătorul de instrucție poate solicita date, prin ordonanță, pentru o perioadă de nouă luni anterior ordonanței;

– pentru celelalte infracțiuni, judecătorul de instrucție poate solicita date numai pentru o perioadă de șase luni anterior ordonanței.

3. Măsura nu poate privi mijloacele de comunicare electronică ale unui avocat sau ale unui medic decât dacă acesta este suspectat el însuși de săvârșirea unei infracțiuni prevăzute la alineatul 1 sau de participarea la aceasta sau dacă există indicii concrete în sensul că terți suspectați de săvârșirea unei infracțiuni prevăzute la alineatul 1 utilizează mijloacele de comunicare electronică ale acestuia.

Măsura nu poate fi pusă în aplicare fără ca decanul Baroului sau reprezentantul ordinului provincial al medicilor, după caz, să fie înștiințat. Aceleași persoane vor fi informate de judecătorul de instrucție cu privire la elementele considerate de acesta ca ținând de secretul profesional. Aceste elemente nu sunt consemnate în procesul-verbal.

4. […]

Orice persoană care, în virtutea funcției, are cunoștință despre măsură sau își dă concursul la aceasta are obligația de a păstra secretul. Orice încălcare a secretului se pedepsește conform articolului 458 din Codul penal.

[…]”

12. În conformitate cu articolul 12, articolul 13 din Legea din 1998 are următorul cuprins:

„Serviciile de informații și de securitate pot căuta, colecta, primi și prelucra informații și date cu caracter personal care pot fi utile îndeplinirii misiunilor lor și pot păstra o documentație actualizată referitoare în special la evenimente, la grupări și la persoane care prezintă interes pentru îndeplinirea misiunilor lor.

Informațiile cuprinse în documentație trebuie să aibă legătură cu finalitatea stocării și trebuie să se limiteze la cerințele care decurg din aceasta.

Serviciile de informații și de securitate asigură securitatea datelor care au legătură cu sursele lor și a informațiilor și a datelor cu caracter personal furnizate de aceste surse.

Agenții serviciilor de informații și de securitate au acces la informațiile și la datele cu caracter personal colectate și prelucrate de serviciile lor, în măsura în care acestea sunt utile pentru exercitarea funcției sau a misiunii lor."

13. Articolul 14 conferă un nou mod de redactare articolului 18/3, care prevede în prezent:

„1. Metodele specifice de colectare de date prevăzute la articolul 18/2 alineatul 1 pot fi puse în aplicare ținând seama de amenințarea potențială la care face referire articolul 18/1, în cazul în care metodele obișnuite de colectare de date sunt considerate insuficiente pentru a permite colectarea informațiilor necesare pentru finalizarea unei misiuni de informare. Metoda specifică trebuie să fie aleasă în funcție de gravitatea amenințării potențiale pentru care este pusă în aplicare.

Metoda specifică poate fi pusă în aplicare numai în urma unei decizii scrise și motivate a șefului serviciului și după notificarea acestei decizii către Comisie.

2. Decizia șefului serviciului trebuie să menționeze:

1° natura metodei specifice;

2° după caz, persoanele fizice sau juridice, asociațiile sau grupările, obiectele, locurile, evenimentele sau informațiile care sunt vizate de metoda specifică;

3° amenințarea potențială care justifică utilizarea metodei specifice;

4° împrejurările de fapt care justifică metoda specifică, motivarea privind caracterul subsidiar și proporțional, inclusiv legătura dintre punctele 2 și 3;

5° perioada în care poate fi aplicată metoda specifică începând de la notificarea deciziei către Comisie;

[…]

9° dacă este cazul, indiciile temeinice care atestă că avocatul, medicul sau jurnalistul participă sau a participat personal și activ la nașterea sau la dezvoltarea amenințării potențiale;

10° în cazul în care se aplică articolul 18/8, motivarea duratei perioadei în care are loc colectarea de date;

[…]

8. Șeful serviciului dispune încetarea metodei specifice atunci când amenințarea potențială care o justifică a dispărut, atunci când metoda nu mai este utilă pentru finalitatea pentru care a fost

aplicată sau atunci când s-a constatat o nelegalitate. Acesta informează în cel mai scurt timp Comisia cu privire la decizia sa."

14. Articolul 18/8 din Legea din 1988 are următorul mod de redactare:

„1. În vederea îndeplinirii misiunilor lor și, la nevoie, solicitând în acest scop asistență tehnică din partea operatorului unei rețele de comunicații electronice sau a furnizorului unui serviciu de comunicații electronice, serviciile de informații și de securitate pot proceda sau pot dispune să se procedeze la:

1° reperarea datelor de transfer ale mijloacelor de comunicare electronică de la care sau către care sunt sau au fost adresate comunicații electronice;

2° localizarea originii sau a destinației comunicațiilor electronice.

[…]

2. În ceea ce privește aplicarea metodei prevăzute la alineatul 1 în privința datelor păstrate în temeiul articolului 126 din Legea din […] 2005 […], se aplică următoarele dispoziții:

1° în cazul unei amenințări potențiale care privește o activitate care poate fi legată de grupuri infracționale organizate sau de organizații sectare nocive, șeful serviciului poate solicita prin decizia sa datele pentru o perioadă de șase luni anterior deciziei;

2° în cazul unei alte amenințări potențiale decât cele prevăzute la punctele 1 și 3, șeful serviciului poate solicita prin decizia sa datele pentru o perioadă de nouă luni anterior deciziei;

3° în cazul unei amenințări potențiale care privește o activitate care poate fi legată de terorism sau de extremism, șeful serviciului poate solicita prin decizia sa datele pentru o perioadă de douăsprezece luni anterior deciziei. […]".

II. Situația de fapt și întrebările preliminare adresate

15. Prin hotărârea din 11 iunie 2015 [14], Cour constitutionnelle (Curtea Constituțională) a anulat noua versiune a articolului 126 din Legea din 2005, pentru aceleași motive care au determinat Curtea să declare nevaliditatea Directivei 2006/24 prin Hotărârea Digital Rights.

16. Ca urmare a anulării respective, legiuitorul național a adoptat (înainte de pronunțarea Hotărârii Tele2 Sverige și Watson) Legea din 29 mai 2016.

17. VZ și alții, Ordre des barreaux francophones et germanophone (denumit în continuare „Ordre des barreaux"), Liga voor Mensenrechten ASBL (denumită în continuare „LMR"), Ligue des Droits de l'Homme ASBL (denumită în continuare „LDH") și Académie Fiscale ASBL (denumită în continuare „Académie Fiscale") au sesizat instanța de trimitere cu mai multe acțiuni în declararea neconstituționalității legii menționate, susținând în esență că aceasta depășea ceea ce este strict necesar și nu stabilea garanții suficiente de protecție.

[14] Hotărârea nr. 84/2015, *Moniteur belge* din 11 august 2015.

18. În acest context, Cour constitutionnelle (Curtea Constituțională) a adresat Curții următoarele întrebări:

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

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

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

III. Procedura în fața Curții

19. Trimiterea preliminară a fost înregistrată la grefa Curții la 2 august 2018.

20. Au prezentat observații scrise VZ și alții, Académie Fiscale, LMR, LDH, Ordre des barreaux, Fondation pour Enfants Disparus et Sexuellement Exploités (Child Focus), guvernele german, belgian, britanic, ceh, cipriot, danez, spaniol, estonian, francez, maghiar, irlandez, neerlandez, polonez și suedez, precum și Comisia.

21. La 9 septembrie 2019 s-a organizat o ședință publică împreună cu cele din cauzele C-511/18, C-512/18 și C-623/17, în care s-au prezentat părțile din cele patru trimiteri preliminare, guvernele menționate anterior și guvernul Norvegiei, precum și Comisia și Autoritatea Europeană pentru Protecția Datelor.

IV. Analiză

22. Prima întrebare adresată în prezenta trimitere preliminară coincide în esență cu cele formulate în cauzele C-511/18 și C-512/28. Totuși, ea diferă de acestea din urmă în ceea ce privește obiectivele pe care le urmărește reglementarea națională: nu este vorba numai despre combaterea terorismului și a formelor cele mai grave de criminalitate sau despre protecția securității naționale, ci și despre „apărarea teritoriului, securitatea publică, investigarea, depistarea și urmărirea penală a infracțiunilor minore” și, cu caracter general, despre orice alt obiectiv prevăzut la articolul 23 alineatul (1) din Regulamentul 2016/679.

23. A doua întrebare se leagă de prima, însă o completează în sensul că se solicită să se stabilească dacă obligațiile pozitive care revin autorității publice în ceea ce privește investigarea și sancționarea abuzurilor sexuale asupra minorilor ar justifica măsurile în litigiu.

24. A treia întrebare este formulată în ipoteza în care norma națională este declarată incompatibilă cu dreptul Uniunii. Instanța de trimitere solicită să se stabilească dacă, în această ipoteză, efectele Legii din 29 mai 2016 ar putea fi menținute în mod provizoriu.

25. Vom aborda aceste întrebări analizând, în primul rând, aplicabilitatea Directivei 2002/58, motiv pentru care vom face trimitere la concluziile noastre prezentate în celelalte trimiteri preliminare menționate. În al doilea rând, vom indica principalele orientări din jurisprudența Curții în această materie și modurile în care ele pot fi dezvoltate. În ultimul rând, vom da răspunsul la fiecare dintre întrebările preliminare.

A. Aplicabilitatea Directivei 2002/58

26. La fel ca în celelalte trei trimiteri preliminare, și în aceasta s-a ridicat problema aplicabilității Directivei 2002/58. Având în vedere identitatea dintre abordările statelor membre în această privință, facem trimitere în acest sens la Concluziile prezentate în cauzele C-511/18 și C-512/18 [15].

[15] Punctul 40 și următoarele.

B. Jurisprudența Curții cu privire la păstrarea datelor personale și accesul autorităților publice la aceste date în contextul Directivei 2002/58

1. Principiul confidențialității comunicațiilor și a datelor conexe

27. Dispozițiile Directivei 2002/58 „precizează și completează" Directiva 95/46/CE [16] cu scopul de a garanta un nivel ridicat de protecție a datelor cu caracter personal în contextul prestării serviciilor de comunicații electronice [17].

28. Articolul 5 alineatul (1) din Directiva 2002/58 prevede că statele membre trebuie să asigure, prin legislația internă, confidențialitatea comunicațiilor transmise prin intermediul unei rețele de comunicații publice sau al unor servicii publice de comunicații electronice, precum și confidențialitatea datelor de transfer aferente.

29. Confidențialitatea informațiilor implică, printre altele [articolul 5 alineatul (1) a doua teză din Directiva 2002/58], o interdicție pentru orice alte persoane decât utilizatorii de a stoca, fără acordul acestora, datele de transfer aferente comunicațiilor electronice. Sunt exceptate „persoanele autorizate în mod legal […] și stocarea tehnică necesară pentru transmisia comunicației" [18].

30. Articolele 5 și 6 și articolul 9 alineatul (1) din Directiva 2002/58 urmăresc să asigure confidențialitatea comunicațiilor și a datelor de transfer și să minimizeze riscurile de abuz. Sfera lor de aplicare trebuie apreciată în lumina considerentului (30) al acestei directive, potrivit căruia „[s]istemele de furnizare de servicii și rețele de comunicații electronice trebuie astfel construite încât să limiteze cantitatea de date personale necesare la un *minimum* strict" [19].

31. În ceea ce privește datele respective, se pot distinge:

– datele de *transfer*, a căror prelucrare și stocare sunt permise numai în măsura și pe durata de timp necesare facturării serviciilor, comercializării acestora și furnizării unor servicii cu valoare adăugată (articolul 6 din Directiva 2002/58). Odată expirată această perioadă, datele care au fost prelucrate și stocate trebuie șterse sau anonimizate [20];

– datele de *localizare* altele decât datele de transfer, care pot fi prelucrate numai în anumite condiții și doar dacă au fost anonimizate sau există acordul utilizatorilor sau abonaților respectivi [articolul 9 alineatul (1) din Directiva 2002/58] [21].

16 Directiva Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO 1995, L 281, p. 31, Ediție specială, 13/vol. 17, p. 10). A se vedea articolul 1 alineatul (2) din Directiva 2002/58. Directiva 95/46 a fost abrogată începând cu 25 mai 2018 prin Regulamentul 2016/679. Astfel, în măsura în care Directiva 2002/58 face trimitere la Directiva 95/46 sau nu stabilește măsuri proprii, trebuie să se ia în considerare dispozițiile regulamentului respectiv [a se vedea articolul 94 alineatele (1) și (2) din Regulamentul 2016/679].

17 Hotărârea Tele2 Sverige și Watson, punctele 82 și 83.

18 *Ibidem*, punctul 85 și jurisprudența citată.

19 *Ibidem*, punctul 87. Sublinierea noastră.

20 *Ibidem*, punctul 86 și jurisprudența citată.

21 *Ibidem*, punctul 86, *in fine*.

2. Clauza de limitare prevăzută la articolul 15 alineatul (1) din Directiva 2002/58

32. În temeiul articolului 15 alineatul (1) din Directiva 2002/58, 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” din această directivă.

33. Orice limitare trebuie să 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]”.

34. Această enumerare a obiectivelor are un caracter exhaustiv [22]: cu titlu de exemplu („*inter alia*”), se pot adopta „măsuri legislative care să permită reținerea de date, pe perioadă limitată, pentru motivele arătate anterior în acest alineat”.

35. În orice caz, „[t]oate măsurile menționate [la articolul 15 alineatul (1) din această directivă] trebuie să fie conforme cu principiile generale ale legislației [Uniunii], inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) [TUE]”. Prin urmare, articolul 15 alineatul (1) din Directiva 2002/58 trebuie interpretat în lumina drepturilor fundamentale garantate de cartă [23].

36. Dintre drepturile consacrate de cartă, Curtea a menționat, în acest context, dreptul la respectarea vieții private (articolul 7), dreptul la protecția datelor cu caracter personal (articolul 8) și dreptul la libertatea de exprimare (articolul 11) [24].

37. Curtea a subliniat de asemenea, drept criteriu de interpretare a articolului 15 alineatul (1) din Directiva 2002/58, că limitele obligației de garantare a confidențialității comunicațiilor și a datelor de transfer aferente trebuie interpretate în mod strict.

38. Concret, Curtea a statuat că nu se poate ca „derogarea de la această obligație de principiu și în special de la interdicția de a stoca aceste date, prevăzută la articolul 5 din directiva menționată, să devină regula, fără a vida semnificativ această din urmă dispoziție de conținutul său” [25].

39. În opinia noastră, această dublă observație este decisivă pentru a înțelege motivele pentru care Curtea a considerat că păstrarea generalizată și nediferențiată a datelor de transfer și de localizare privind comunicațiile electronice este incompatibilă cu Directiva 2002/58.

40. Prin această constatare, Curtea nu a făcut altceva decât să aplice în mod „strict” [26] criteriul proporționalității, pe care îl utilizase și în trecut [27]: „protecția dreptului fundamental la respectarea vieții private la nivelul Uniunii impune ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele strictului necesar” [28].

22 *Ibidem*, punctul 90.

23 *Ibidem*, punctul 91 și jurisprudența citată.

24 *Ibidem*, punctul 93 și jurisprudența citată.

25 *Ibidem*, punctul 89.

26 Utilizarea acestui adverb în Hotărârea Tele2 Sverige și Watson, punctul 95, provine din considerentul (11) al Directivei 2002/58.

27 Hotărârea Digital Rights, punctul 48: „ținând seama, pe de o parte, de rolul important pe care îl are protecția datelor cu caracter personal în lumina dreptului fundamental la respectarea vieții private și, pe de altă parte, de amploarea și de gravitatea ingerinței în acest drept cauzate de Directiva 2006/24, puterea de apreciere a legiuitorului Uniunii este redusă, astfel încât este necesară efectuarea unui control strict”.

28 Hotărârea Tele2 Sverige și Watson, punctul 96 și jurisprudența citată.

3. Caracterul proporțional al păstrării datelor

a) Caracterul disproporționat al unei păstrări generalizate și nediferențiate

41. Potrivit Curții, combaterea infracționalității grave, în special combaterea crimei organizate și a terorismului, are o importanță majoră pentru garantarea securității publice, iar eficacitatea sa poate să depindă în mare măsură de utilizarea tehnicilor moderne de investigație. Aceasta a adăugat că „un astfel de obiectiv de interes general, oricât de fundamental ar fi, nu poate justifica *per se* faptul de a considera o măsură de păstrare precum cea instituită de Directiva 2006/24 ca fiind necesară în scopul combaterii menționate”[29].

42. Pentru a determina dacă o astfel de măsură se limitează la strictul necesar, Curtea a subliniat, în primul rând, ingerința de mare amploare în drepturile fundamentale consacrate la articolele 7 și 8 din cartă[30]. Această amploare rezultă chiar din faptul că reglementarea națională prevedea „o păstrare generalizată și nediferențiată a *ansamblului datelor de transfer și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică* și că îi oblig[a] pe furnizorii de servicii de comunicații electronice să păstreze aceste date *în mod sistematic și continuu, fără nicio excepție*”[31].

43. Ingerința pe care o implica măsura respectivă în viața cetățenilor se reflectă în constatările Curții cu privire la efectele păstrării datelor.

Aceste date[32]

– „permit să se găsească și să se identifice sursa unei comunicații și destinația acesteia, să se determine data, ora, durata și tipul unei comunicații, dispozitivele de comunicații ale utilizatorilor, precum și să se localizeze dispozitivele de comunicații mobile”[33];

– „permit în special stabilirea persoanei cu care a comunicat un abonat sau un utilizator înregistrat și prin ce mijloace, precum și stabilirea duratei comunicației și a locului de unde a fost inițiată aceasta. În plus, acestea permit să se cunoască frecvența comunicațiilor abonatului sau ale utilizatorului înregistrat cu anumite persoane într-o perioadă determinată”[34];

– „permit deducerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, precum obiceiurile din viața cotidiană, locurile de ședere permanente sau temporare, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele”[35];

– „furnizează mijloacele de a stabili […] profilul persoanelor în cauză, informație la fel de sensibilă, din perspectiva dreptului la respectarea vieții private, ca și conținutul însuși al comunicațiilor”[36].

29 Hotărârea Digital Rights, punctul 51. În același sens, Hotărârea Tele2 Sverige și Watson, punctul 103.

30 Hotărârea Digital Rights, punctul 65, și Hotărârea Tele2 Sverige și Watson, punctul 100.

31 Hotărârea Tele2 Sverige și Watson, punctul 97. Sublinierea noastră.

32 Printre aceste date figurează numele și adresa abonatului sau a utilizatorului înregistrat, numărul de telefon al apelantului și numărul apelat, precum și o adresă IP pentru serviciile internet.

33 Hotărârea Tele2 Sverige și Watson, punctul 98.

34 *Ibidem*, punctul 98.

35 *Ibidem*, punctul 99.

36 *Ibidem*, punctul 99 *in fine*.

44. În plus, ingerința este susceptibilă să genereze „în mintea persoanelor vizate sentimentul că viața lor privată face obiectul unei supravegheri constante”, deoarece „păstrarea datelor este efectuată fără ca utilizatorii serviciilor de comunicații electronice să fie informați cu privire la aceasta” [37].

45. Având în vedere gravitatea ingerinței, numai combaterea infracționalității grave poate justifica o măsură constând în păstrarea datelor cu aceste caracteristici [38]. Totuși, măsura respectivă nu poate deveni regula generală, întrucât „sistemul instituit de Directiva 2002/58 impune ca această conservare a datelor să fie excepția” [39].

46. În plus, au existat două caracteristici care decurgeau din faptul că măsura în litigiu nu prevedea „nicio diferențiere, limitare sau excepție în funcție de obiectivul urmărit” [40] și „nu impune[a] nicio relație între datele a căror păstrare este prevăzută și o amenințare pentru securitatea publică” [41]:

– pe de o parte, aceasta privea „în mod global ansamblul persoanelor care utilizează servicii de comunicații electronice, fără ca aceste persoane să se regăsească, fie și în mod indirect, într-o situație susceptibilă să declanșeze începerea urmăririi penale […] În plus, aceasta nu prevede[a] nicio excepție, astfel încât ea se aplic[a] chiar și acelor persoane ale căror comunicații sunt supuse, potrivit normelor dreptului național, secretului profesional” [42];

– pe de altă parte, „[…] aceasta nu [era] 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” [43].

47. În aceste condiții, reglementarea națională analizată depășea limitele strictului necesar. Prin urmare, ea nu putea fi considerată justificată într-o societate democratică, astfel cum prevede articolul 15 alineatul (1) din Directiva 2002/58, în lumina articolelor 7, 8, 11 și a articolului 52 alineatul (1) din cartă [44].

b) Caracterul viabil al unei păstrări selective a datelor

48. Curtea a admis conformitatea cu dreptul Uniunii a unei reglementări naționale care „să permită, cu titlu preventiv, *păstrarea direcționată* a datelor de transfer și a datelor de localizare, în scopul combaterii infracționalității grave” [45].

49. Această păstrare direcționată a datelor este validă cu condiția „să fie, în ceea ce privește categoriile de date care trebuie păstrate, mijloacele de comunicare vizate, persoanele în cauză, precum și durata de păstrare reținută, limitată la strictul necesar”.

37 *Ibidem*, punctul 100.
38 *Ibidem*, punctul 102.
39 *Ibidem*, punctul 104.
40 *Ibidem*, punctul 105.
41 *Ibidem*, punctul 106.
42 *Ibidem*, punctul 105.
43 *Ibidem*, punctul 106.
44 *Ibidem*, punctul 107.
45 *Ibidem*, punctul 108. Sublinierea noastră.

50. Orientările oferite de Hotărârea Tele2 Sverige și Watson pentru a stabili dacă sunt îndeplinite condițiile respective nu sunt (probabil nu puteau fi) exhaustive și sunt formulate în termeni mai degrabă generali. Pentru a le respecta, statele membre:

– trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea unei astfel de măsuri de păstrare a datelor [46];

– trebuie să fixeze „criterii obiective, care să stabilească un raport între datele care trebuie păstrate și obiectivul urmărit” [47], și

– trebuie „să se întemeieze pe elemente obiective care să permită să fie vizat un public ale cărui date pot prezenta o legătură, cel puțin indirectă, cu acte de infracționalitate gravă, să contribuie într-un mod sau altul la combaterea infracționalității grave sau să prevină un risc grav pentru securitatea publică” [48].

51. În ceea ce privește elementele obiective, Curtea oferă drept exemplu posibilitatea de a utiliza un criteriu geografic pentru a stabili publicul și situațiile eventual vizate. Invocarea acestui criteriu, care a fost foarte criticat de anumite state membre, nu are drept scop, în opinia noastră, limitarea exclusiv la el a listei de criterii de selecție admisibile.

4. Caracterul proporțional al accesului la date

a) Hotărârea Tele2 Sverige și Watson

52. Curtea abordează *accesul* autorităților naționale la date independent de întinderea obligației de *păstrare* impusă furnizorilor de servicii de comunicații electronice și în special de caracterul generalizat sau specific al păstrării datelor respective [49].

53. Astfel, chiar dacă scopul păstrării este de a facilita accesul ulterior la date, păstrarea și accesul pot conduce la încălcări diferite ale drepturilor fundamentale consacrate de cartă. Această diferențiere nu implică totuși că anumite considerații privind păstrarea nu sunt aplicabile și în ceea ce privește accesul la datele păstrate.

54. În acest sens, accesul:

– „trebuie să urmărească în mod efectiv și strict unul dintre aceste obiective” prevăzute la articolul 15 alineatul (1) prima teză din Directiva 2002/58. Trebuie să existe de asemenea o concordanță între gravitatea ingerinței în drepturile fundamentale și finalitatea acesteia. Dacă ingerința este considerată gravă, aceasta poate fi justificată numai de combaterea infracționalității grave [50];

46 *Ibidem*, punctul 109. În special, acestea trebuie să indice „în ce împrejurări și în ce condiții poate fi luată, cu titlu preventiv, o măsură de păstrare a datelor, garantând astfel că o asemenea măsură este limitată la strictul necesar”.

47 *Ibidem*, punctul 110.

48 *Ibidem*, punctul 111.

49 *Ibidem*, punctul 113.

50 *Ibidem*, punctul 115.

– este permis numai în limitele strictului necesar [51]. În plus, măsurile legislative trebuie să prevadă „norme clare și precise care să indice în ce împrejurări și în ce condiții furnizorii de servicii de comunicații electronice trebuie să acorde autorităților naționale competente accesul la date. De asemenea, o măsură de această natură trebuie să fie obligatorie din punct de vedere juridic în dreptul intern” [52];

– mai exact, reglementările naționale trebuie să prevadă „condițiile materiale și procedurale care guvernează accesul autorităților naționale competente la datele păstrate” [53].

55. Din cele de mai sus rezultă că „un acces general la toate datele păstrate, independent de orice legătură, chiar indirectă, cu scopul urmărit, nu poate fi considerat limitat la strictul necesar” [54].

56. Potrivit Curții, „reglementarea națională în cauză trebuie să se întemeieze pe criterii obiective pentru a defini împrejurările și condițiile în care trebuie să se acorde autorităților naționale competente accesul la datele abonaților sau ale utilizatorilor înregistrați” [55]. În această privință, „accesul nu poate fi acordat, în principiu, în raport cu obiectivul de combatere a infracționalității, decât la *datele persoanelor bănuite că ar pregăti, că ar săvârși sau că ar fi săvârșit o infracțiune gravă ori că ar fi implicate în orice mod într-o astfel de infracțiune*” [56].

57. Cu alte cuvinte, normele naționale care acordă autorităților naționale competente acces la datele păstrate trebuie să aibă un domeniu de aplicare suficient de limitat. Trebuie să existe o legătură între persoanele afectate și obiectivul urmărit, astfel încât accesul să nu vizeze un număr semnificativ de persoane sau să includă toate persoanele, toate mijloacele de comunicații electronice și toate datele stocate.

58. Totuși, aceste reguli pot fi nuanțate în anumite condiții. Curtea menționează „situații speciale, precum cele în care interese vitale privind securitatea națională, apărarea sau securitatea publică sunt amenințate prin activități teroriste”. În astfel de situații, „ar putea de asemenea să fie permis accesul la datele altor persoane în cazul în care există elemente obiective care permit să se considere că aceste date ar putea aduce, într-un caz concret, o contribuție efectivă la combaterea unor asemenea activități” [57].

59. Această clarificare a Curții permite statelor membre să instituie un regim special de acces la date mai amplu, atunci când este absolut necesar pentru a combate amenințările la adresa intereselor primordiale ale statului (securitatea națională, apărarea și securitatea publică) [58], astfel încât să se aplice inclusiv persoanelor care au o legătură doar indirectă cu riscurile respective.

51 *Ibidem*, punctul 116.

52 *Ibidem*, punctul 117.

53 *Ibidem*, punctul 118.

54 *Ibidem*, punctul 119.

55 *Idem.*

56 *Idem*. Sublinierea noastră.

57 *Idem.*

58 În afara activităților teroriste, acest caracter excepțional ar putea fi justificat de alte evenimente, precum un atac informatic la scară largă împotriva infrastructurilor critice ale statului sau o amenințare legată de proliferarea nucleară.

60. Accesul autorităților naționale la datele stocate trebuie să fie supus, indiferent de tipul său, următoarelor trei condiții:

– trebuie să fie, „în principiu, cu excepția unor situații de urgență justificate corespunzător, condiționat de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă". Decizia acestei instanțe sau a acestei entități trebuie să fie adoptată „în urma unei cereri motivate formulate de autoritățile respective, printre altele în cadrul unor proceduri de prevenire, de detectare sau de urmărire penală" [59];

– se impune ca „autoritățile naționale competente cărora le-a fost acordat accesul la datele păstrate să informeze persoanele în cauză, în cadrul procedurilor naționale aplicabile, din momentul în care această comunicare nu poate compromite anchetele desfășurate de autoritățile respective" [60];

– statele membre trebuie să adopte norme cu privire la securitatea și la protecția datelor deținute de furnizorii de comunicații electronice, cu scopul de a evita folosirea necorespunzătoare și accesul ilicit la date [61].

b) Hotărârea Ministerio Fiscal

61. În cauza respectivă s-a ridicat problema compatibilității cu articolul 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7 și 8 din cartă, a unei norme naționale care prevede accesul autorităților competente la date privind identitatea civilă a titularilor anumitor cartele SIM.

62. Curtea a declarat că articolul 15 alineatul (1) prima teză din Directiva 2002/58 nu limitează obiectivul privind prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor numai la combaterea infracțiunilor grave, ci se referă la „infracțiuni" în general [62].

63. Aceasta a adăugat că, pentru a justifica accesul autorităților naționale competente la date, trebuie să existe o legătură între gravitatea ingerinței și gravitatea infracțiunilor respective. Prin urmare:

– „o ingerință gravă nu poate fi justificată […] decât prin obiectivul privind combaterea infracționalității care trebuie calificată drept «gravă»" [63];

– în schimb, „dacă ingerința pe care o implică un asemenea acces nu este gravă, respectivul acces este susceptibil să fie justificat de un obiectiv privind prevenirea, investigarea, detectarea și urmărirea penală a unor «infracțiuni» în general" [64].

59 Hotărârea Tele2 Sverige și Watson, punctul 120.

60 *Ibidem*, punctul 121.

61 *Ibidem*, punctul 122.

62 Hotărârea Ministerio Fiscal, punctul 53.

63 *Ibidem*, punctul 56.

64 *Ibidem*, punctul 57.

64. Plecând de la această premisă și spre deosebire de situația din Hotărârea Tele2 Sverige și Watson, Curtea nu a calificat drept „gravă" ingerința în drepturile consacrate la articolele 7 și 8 din cartă, întrucât cererea de acces „avea drept unic obiect să identifice titularii cartelelor SIM activate, într-o perioadă de douăsprezece zile, cu codul IMEI al telefonului mobil furat" [65].

65. Pentru a sublinia gravitatea minoră a ingerinței, Curtea a explicat că „datele vizate de cererea de acces în discuție în litigiul principal permit doar să se pună în legătură, pe o perioadă determinată, cartela sau cartelele SIM activate cu telefonul mobil furat cu identitatea civilă a titularilor acestor cartele SIM. Fără o verificare încrucișată a datelor aferente comunicațiilor efectuate cu respectivele cartele SIM și a datelor de localizare, aceste date nu permit să se cunoască nici data, ora, durata și destinatarii comunicațiilor efectuate cu cartela sau cu cartelele SIM în cauză, nici locurile în care aceste comunicații au avut loc sau frecvența acestora cu anumite persoane într-o perioadă determinată. Prin urmare, aceste date nu permit să se tragă concluzii precise cu privire la viața privată a persoanelor ale căror date sunt vizate" [66].

66. În cauza soluționată prin Hotărârea Ministerio Fiscal nu se ridica problema privind aspectul dacă datele cu caracter personal au fost păstrate de furnizorii de comunicații electronice în conformitate cu condițiile prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, interpretate în lumina articolelor 7 și 8 din cartă [67]. De asemenea, nu s-a abordat nici problema dacă erau sau nu îndeplinite celelalte condiții de acces rezultate din articolul respectiv.

67. Prin urmare, lectura Hotărârii Ministerio Fiscal nu permite deducerea vreunei modificări a jurisprudenței Curții cu privire la incompatibilitatea cu dreptul Uniunii a unui regim național care autorizează stocarea generalizată și nediferențiată a datelor, în sensul Hotărârii Tele2 Sverige și Watson.

68. Cu toate acestea, considerăm că, atunci când Curtea recunoaște validitatea regimului de acces limitat la anumite date personale (cele referitoare la identitatea civilă a titularilor de cartele SIM), aceasta acceptă în mod implicit păstrarea datelor respective de către furnizorii serviciului.

C. Principalele critici aduse jurisprudenței Curții

69. Atât instanța de trimitere, cât și majoritatea statelor membre care au formulat observații solicită Curții să clarifice, să nuanțeze sau inclusiv să reconsidere anumite aspecte ale jurisprudenței sale în această materie, care face obiectul criticilor lor.

70. Majoritatea acestor critici, aduse fie în mod voalat, fie în mod direct, au fost deja exprimate cu ocazia Hotărârii Digital Rights și au fost respinse prin Hotărârea Tele2 Sverige și Watson. Ele revin acum în discuție pentru a sublinia în esență că ar fi suficient să se adopte norme riguroase privind accesul la datele deținute de furnizorii de servicii de comunicații electronice, care ar putea compensa într-o anumită măsură gravitatea ingerinței pe care o presupune păstrarea generalizată și nediferențiată a datelor respective.

65 *Ibidem*, punctul 59. Era vorba despre accesul „la numerele de telefon corespunzătoare acestor cartele SIM, precum și la datele referitoare la identitatea civilă a titularilor cartelelor menționate, cum ar fi numele, prenumele și, dacă este cazul, adresa lor. În schimb, aceste date nu prive[au], după cum au confirmat în ședință atât guvernul spaniol, cât și procurorul, comunicațiile efectuate cu telefonul mobil furat și nici localizarea acestuia".

66 *Ibidem*, punctul 60.

67 Hotărârea Ministerio Fiscal, punctul 49.

71. În mai multe dintre aceste critici se subliniază de asemenea necesitatea de a adopta măsuri realmente eficiente pentru combaterea amenințărilor grave la adresa siguranței și a infracționalității în general și se solicită Curții să ia în considerare dreptul la siguranță (articolul 6 din cartă), precum și marja de apreciere a statelor membre privind protecția securității naționale. În orice caz, astfel cum se adaugă, Curtea nu a apreciat caracterul preventiv al intervenției serviciilor de securitate și de informații.

D. Opinia noastră cu privire la criticile respective și la nuanțele care ar putea fi introduse în jurisprudența Curții

72. În opinia noastră, Curtea ar trebui să mențină abordarea de principiu pe care a adoptat-o în hotărârile anterioare: o obligație generalizată și nediferențiată de păstrare a datelor de transfer și de localizare ale tuturor abonaților și utilizatorilor înregistrați încalcă în mod disproporționat drepturile fundamentale protejate de articolele 7, 8 și 11 din cartă.

73. *A sensu contrario*, o reglementare națională care stabilește restricții adecvate cu privire la păstrarea anumitor date, generate în contextul furnizării de servicii de comunicații electronice, ar putea fi compatibilă cu dreptul Uniunii. Prin urmare, elementul-cheie este *păstrarea limitată* a datelor respective.

74. Pentru motivele pe care le vom prezenta în continuare, păstrarea limitată nu ar trebui să aibă ca obiect numai o zonă geografică sau o categorie de persoane concrete: diferendele privind criteriile de păstrare denotă faptul că acestea fie ar putea fi nerealizabile sau ineficiente pentru scopurile urmărite, fie ar putea deveni o sursă de discriminare.

75. Trebuie subliniat de la început că nu împărtășim argumentul critic care promovează binomul „păstrare mai îndelungată în schimbul unui acces mai restrâns”. Raționamentul Curții, cu care suntem de acord, este că păstrarea și accesul la date constituie două tipuri diferite de ingerință. Chiar dacă sensul păstrării datelor îl reprezintă un posibil acces ulterior al autorităților competente, fiecare dintre ingerințele respective trebuie justificată în mod separat, în cadrul unei analize specifice și în lumina obiectivului urmărit.

76. Prin urmare, un sistem național care prevede stocarea generalizată și nediferențiată a datelor nu poate fi justificat prin faptul că normele respective stabilesc în același timp cerințe de formă și procedurale stricte cu privire la accesul la datele respective.

77. Trebuie să existe, așadar, norme care să vizeze în mod direct păstrarea datelor și care să supună această activitate anumitor condiții astfel încât să nu dobândească un caracter generalizat și nediferențiat. Numai în acest mod s-ar garanta compatibilitatea sa cu articolul 15 alineatul (1) din Directiva 2002/58, în lumina articolelor 7, 8 și 11 și a articolului 52 alineatul (1) din cartă.

78. În fond, aceasta este abordarea grupurilor de lucru reunite în cadrul Consiliului pentru a stabili norme privind păstrarea și accesul compatibile cu jurisprudența Curții, examinând în paralel cele două tipuri de ingerințe [68].

[68] Statele membre participă din anul 2017 într-un grup de lucru al cărui scop este de a-și adapta legislațiile la criteriile stabilite în jurisprudența Curții în această materie [Groupe Échange d'informations et protection des données (DAPIX)].

79. Prin aplicarea unor limitări în cazul fiecăruia dintre cele două tipuri de ingerințe, s-ar putea aprecia dacă posibilul efect cumulativ al acestora, combinat cu garanții solide, este de natură să diminueze impactul păstrării datelor asupra drepturilor fundamentale protejate de articolele 7, 8 și 11 din cartă, asigurând în același timp eficacitatea investigațiilor.

80. Pentru a proteja aceste drepturi, sistemul trebuie:

– să prevadă o păstrare a datelor care să conțină anumite limitări și diferențe în funcție de obiectivul urmărit;

– să reglementeze accesul la aceste date numai în măsura strict necesară pentru obiectivul urmărit și sub controlul unei instanțe sau al unei autorități administrative independente.

81. Justificarea furnizorilor de servicii de comunicații electronice de a păstra anumite date, și nu numai pentru îndeplinirea obligațiilor lor contractuale față de utilizatori, crește în paralel cu evoluțiile tehnologice. Dacă se admite că această păstrare este utilă pentru combaterea infracționalității (ceea ce este greu de contestat[69]), nu ar fi logic ca ea să se limiteze la simpla utilizare a datelor păstrate de operatori pentru desfășurarea activităților lor comerciale și numai pe perioada necesară desfășurării activităților menționate.

82. Odată ce se recunoaște utilitatea unei obligații de păstrare a datelor pentru protejarea securității naționale și combaterea infracționalității, dincolo de cea pe care o pot realiza operatorii pentru necesitățile lor tehnice și comerciale, este indispensabil să se definească întinderea acestei obligații.

83. Fiecare regim de păstrare trebuie să fie adaptat cu strictețe scopului urmărit, astfel încât să nu se ajungă la o păstrare nediferențiată[70]. Este necesar de asemenea să se excludă ca totalitatea acestor date să permită conturarea unui *portret* al persoanei afectate (și anume al activităților sale obișnuite și al relațiilor sale sociale) apropiat sau similar celui obținut dacă s-ar cunoaște conținutul comunicațiilor.

84. Pentru a clarifica anumite confuzii și neînțelegeri, este important să se ia în considerare ceea ce Curtea *nu a statuat* în Hotărârile Digital Rigths și Tele2 Sverige și Watson. Prin acestea nu a fost dezavuată existența, ca atare, a unui regim de păstrare a datelor drept instrument util pentru combaterea infracționalității. Dimpotrivă, s-a recunoscut caracterul legitim al obiectivului de prevenție și de combatere a infracțiunilor, precum și utilitatea unui regim de păstrare a datelor pentru îndeplinirea obiectivului respectiv.

85. Astfel cum am menționat, ceea ce s-a respins în mod ferm prin hotărârile respective este posibilitatea ca, în temeiul acestui obiectiv, Uniunea sau statele sale membre să impună păstrarea nediferențiată a *tuturor* datelor generate în contextul furnizării serviciilor de comunicații electronice și accesul general la datele respective.

86. Prin urmare, este necesar să se identifice modalități de păstrare a datelor care să o îndepărteze de calificativele („generalizată și nediferențiată”) incompatibile cu protecția prevăzută la articolele 7, 8 și 11 din cartă.

69 În orice caz, stabilirea tehnicilor de investigație și aprecierea eficacității lor intră în marja de apreciere a statelor membre.

70 Hotărârea Digital Rights, punctul 57, și Hotărârea Tele2 Sverige și Watson, punctul 105.

87. Una dintre aceste modalități ar fi păstrarea *selectivă* a datelor referitoare fie la un public concret (teoretic, cel care are anumite legături mai mult sau mai puțin directe cu amenințările mai grave), fie la o anumită zonă geografică.

88. Totuși, această abordare prezintă anumite dificultăți:

– identificarea unui grup de potențiali atacatori ar fi probabil insuficientă dacă aceștia utilizează tehnici de anonimizare sau își falsifică identitatea. Alegerea acestor grupuri ar putea conduce de asemenea la instaurarea unui regim de suspiciune generală cu privire la anumite segmente ale populației și la calificarea sa drept discriminatorie, în funcție de algoritmul utilizat;

– selectarea pe bază de criterii geografice (care, pentru a fi eficientă, ar trebui să vizeze zone foarte mici) ridică aceleași probleme și adaugă altele, astfel cum a arătat în ședință Autoritatea Europeană pentru Protecția Datelor, deoarece ar putea stigmatiza anumite zone.

89. În plus, ar putea exista anumite contradicții între caracterul preventiv al păstrării care vizează un anumit public sau o zonă geografică și faptul că nu se cunosc în prealabil autorii infracțiunilor și nici locul și momentul săvârșirii lor.

90. În orice caz, nu trebuie exclusă posibilitatea identificării unor formule de păstrare selectivă bazate pe criteriile respective, care să fie utile pentru îndeplinirea obiectivelor menționate anterior. Revine puterii legislative, în fiecare stat membru sau pe tot teritoriul Uniunii, sarcina să stabilească formule care să respecte protecția drepturilor fundamentale garantată de Curte.

91. Ar fi o greșeală să se considere că păstrarea selectivă a datelor aferente unui grup specific sau unei anumite zone geografice este unica formulă pe care Curtea o consideră compatibilă cu articolul 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7 și 8 din cartă.

92. Astfel cum am menționat, este posibil să existe alte modalități de păstrare selectivă a datelor, dincolo de cele axate pe grupuri specifice de persoane sau de zone geografice. De fapt, aceasta este interpretarea grupurilor de lucru ale Consiliului la care am făcut referire anterior: ele au avut în vedere în special, drept ipoteze de lucru, limitarea categoriilor de date păstrate [71], pseudonimizarea datelor [72], stabilirea unor perioade de păstrare limitate [73], excluderea anumitor categorii de furnizori de servicii de comunicații electronice [74], reînnoirea autorizațiilor de stocare [75],

[71] Datele care nu sunt absolut indispensabile și în mod obiectiv necesare pentru combaterea și urmărirea penală a infracțiunilor și pentru protecția securității publice ar fi excluse de la obligația de păstrare. În special, ar trebui precizat, în funcție de obiectivul urmărit, ce tipuri de date privind abonații, de date de transfer și de date de localizare ar trebui să fie păstrate în mod obligatoriu pentru îndeplinirea obiectivului respectiv. În special, ar fi excluse datele care nu sunt considerate indispensabile pentru investigarea și urmărirea penală a infracțiunilor.

[72] Metodă prin care numele sunt înlocuite cu un alias și astfel datele nu mai sunt asociate cu acesta. Spre deosebire de anonimizare, pseudonimizarea permite reasocierea datelor cu numele persoanei vizate.

[73] S-ar putea analiza posibilitatea de a modifica perioadele de păstrare în funcție de diferitele categorii de date, luând în considerare caracterul lor mai mult sau mai puțin invaziv în viața privată a indivizilor. În plus, ar trebui să se stabilească eliminarea permanentă a datelor la finalul perioadei de păstrare.

[74] S-ar putea lua în considerare posibilitatea de a nu impune obligația de păstrare a datelor tuturor furnizorilor de servicii de comunicații electronice, ci de a stabili această obligație în funcție de dimensiunea lor și de tipul serviciilor pe care le oferă, excluzându-le, de exemplu, pe cele care oferă servicii foarte specializate.

[75] Sistemele de autorizare s-ar putea baza pe evaluări periodice ale amenințărilor din fiecare stat membru. Trebuie să se garanteze că legătura dintre datele păstrate și obiectivul urmărit este creată și adaptată pentru situația specifică fiecărui stat membru. Prin urmare, autorizațiile de păstrare acordate furnizorilor ar putea conduce la păstrarea anumitor tipuri de date pentru o perioadă determinată, în funcție de evaluarea amenințării. Aceste autorizații ar putea fi acordate de o instanță sau de o autoritate administrativă independentă și ar determina revizuirea periodică a caracterului indispensabil al păstrării respective.

impunerea obligației de păstrare a datelor stocate pe teritoriul Uniunii sau controlul sistematic și regulat de către o autoritate administrativă independentă al garanțiilor oferite de furnizorii de servicii de comunicații electronice împotriva utilizării abuzive a datelor.

93. În opinia noastră, pentru a asigura compatibilitatea cu jurisprudența Curții, ar trebui să se opteze pentru o păstrare temporară a anumitor *categorii* de date de transfer și de localizare, limitate în funcție de necesitățile stricte de securitate, care să nu permită, în ansamblul lor, obținerea unei imagini exacte și detaliate în privința vieții persoanelor afectate.

94. În practică, aceasta presupune că, în ceea ce privește cele două categorii principale (date de transfer și date de localizare), trebuie să se păstreze, prin aplicarea filtrelor corespunzătoare, numai datele *minime* considerate absolut indispensabile pentru combaterea și controlul eficiente ale infracțiunilor și pentru protecția securității naționale.

95. Revine statelor membre sau instituțiilor Uniunii sarcina de a realiza, pe cale legislativă (cu ajutorul propriilor experți), această operațiune de selectare, renunțând la orice tentativă de a impune o stocare generalizată și nediferențiată a tuturor datelor de transfer și de localizare.

96. În afara acestei limitări în funcție de categorii, datele colectate pot fi păstrate numai pentru o perioadă de stocare, pentru a nu permite să se ofere o imagine detaliată în privința vieții persoanelor afectate. În plus, această perioadă de păstrare trebuie adaptată în funcție de natura datelor, astfel încât cele care oferă informații mai exacte privind stilurile de viață și obiceiurile persoanelor respective să fie depozitate pentru o perioadă mai scurtă [76].

97. Cu alte cuvinte, diferențierea între perioada de păstrare a fiecărei categorii de date, în funcție de utilitatea lor pentru atingerea obiectivelor de securitate, este o metodă care trebuie analizată. Prin limitarea perioadei în care cele două categorii de informații sunt stocate în mod simultan (și, prin urmare, pot fi utilizate pentru a efectua corelații care relevă stilul de viață al persoanelor afectate) se asigură o protecție mai extinsă a dreptului consacrat la articolul 8 din cartă.

98. Aceasta a fost opinia Autorității Europene pentru Protecția Datelor, exprimată în ședință: cu cât există mai multe categorii de metadate stocate și cu cât este mai mare perioada de stocare, cu atât va fi mai simplu de stabilit profilul unei persoane, și viceversa [77].

99. În fond, astfel cum s-a arătat în ședință, este greu să se stabilească granița dintre anumite metadate ale comunicațiilor electronice și conținutul acestor comunicații. Anumite metadate pot fi la fel sau chiar mai revelatoare decât conținutul însuși al comunicațiilor respective: acesta ar putea fi cazul adreselor (URL) paginilor web vizitate [78]. Prin urmare, acest tip de date și altele similare ar trebui să primească o atenție specială, pentru a limita la maximum necesitatea păstrării lor și durata acesteia.

[76] Acesta este, aparent, sistemul aplicat în Republica Federală Germania, al cărei guvern a menționat în cadrul ședinței că, în conformitate cu legislația națională, perioada de păstrare a datelor de transfer este de zece săptămâni, în timp ce perioada de păstrare a datelor de localizare este de numai patru săptămâni. Dimpotrivă, în opinia Republicii Franceze, este necesară o perioadă de un an de stocare a datelor de transfer și de localizare. Potrivit acestui stat membru, reducerea acestui termen sub un an ar avea ca efect diminuarea eficacității serviciilor de poliție judiciară.

[77] Desigur, trebuie să se garanteze că furnizorii de servicii de comunicații electronice șterg în mod permanent datele la finalul perioade de păstrare (cu excepția celor care pot să rămână stocate în scopuri comerciale, în conformitate cu Directiva 2002/58).

[78] În ședință, guvernul francez a afirmat că URL-urile erau excluse din datele de conectare pentru care legislația prevede o obligație generală de păstrare.

100. Găsirea unei soluții echilibrate nu este ușoară, deoarece tehnica de încrucișare și de corelare a datelor stocate permite serviciilor de investigații și de supraveghere să identifice un suspect sau o amenințare, după caz. Chiar și astfel, există o diferență de intensitate între păstrarea datelor în vederea identificării suspectului sau a amenințării respective și cea care are drept rezultat oferirea unui portret detaliat al vieții unei persoane.

101. În așteptarea unei reglementări comune în acest domeniu specific pe tot teritoriul Uniunii, considerăm că nu i se poate solicita Curții să își asume funcții de reglementare și să indice în mod detaliat ce categorii de date se pot păstra și pentru cât timp. Odată stabilite limitele care, potrivit Curții, rezultă din cartă, revine instituțiilor Uniunii și statelor membre sarcina de a identifica soluția corectă pentru obținerea unui echilibru între protecția securității și drepturile fundamentale consacrate de cartă.

102. Desigur, dacă s-ar renunța la informațiile care pot fi deduse dintr-un număr mai mare de date păstrate, combaterea posibilelor amenințări ar putea fi mai dificilă în anumite cazuri. Totuși, acesta este un preț la fel ca altele, care trebuie plătit de autoritățile publice atunci când își asumă obligația de a proteja drepturile fundamentale.

103. La fel cum nimeni nu ar susține o obligație *ex ante* de păstrare generalizată și nediferențiată a *conținuturilor* comunicațiilor electronice private (nici măcar atunci când legile ar garanta accesul ulterior limitat la conținuturile respective), nici metadatele aferente acestor comunicații, care pot să reflecte informații la fel de sensibile precum conținuturile, nu pot face obiectul unei stocări nediferențiate și generalizate.

104. Dificultatea legislativă – pe care o recunoaștem – de a configura cu precizie situațiile și condițiile în care trebuie realizată o păstrare selectivă nu justifică faptul ca statele membre, făcând din excepție o regulă, să transforme păstrarea generalizată a datelor cu caracter personal în principiul central al legislațiilor lor. Într-un astfel de caz, s-ar admite existența pe termen nedeterminat a unei încălcări relevante a dreptului la protecția datelor cu caracter personal.

105. Trebuie adăugat că, în situații cu adevărat *excepționale*, caracterizate de o amenințare iminentă sau de un risc extraordinar care justifică declararea oficială a situației de urgență într-un stat membru, legislația națională prevede, pentru o perioadă limitată, posibilitatea de a impune o obligație de păstrare a datelor atât de amplă și de generală cât se consideră necesar.

106. În acest context, s-ar putea adopta o legislație care să permită în mod specific o păstrare a datelor (și o accesare a acestora) mai amplă, în conformitate cu condițiile și cu procedurile care conferă acestor măsuri un caracter extraordinar, din perspectiva domeniului lor de aplicare material și a duratei lor, precum și garanțiile jurisdicționale corespunzătoare.

107. Analiza comparativă a sistemelor legislative aplicabile situațiilor constituționale de urgență relevă că nu este imposibilă delimitarea situațiilor de fapt care pot determina aplicarea unui regim de reglementare special, prin stabilirea autorității care poate adopta această decizie, a condițiilor în care această decizie poate fi adoptată și a modului în care ea este controlată [79].

[79] Ackerman, B., „The Emergency Constitution”, în *Yale Law Journal*, vol. 113, 2004, p. 1029-1092; Ferejohn, J., și Pasquino, P., „The Law of the Exception: A typology of Emergency Powers”, în *International Journal of Constitutional Law*, vol. 2, 2004, p. 210-239.

E. Răspunsurile specifice la cele trei întrebări preliminare

1. Considerație introductivă

108. Instanța de trimitere solicită o interpretare a articolului 15 alineatul (1) din Directiva 2002/58 în legătură cu mai multe drepturi garantate de cartă: dreptul la respectarea vieții private și de familie (articolul 7), dreptul la protecția datelor cu caracter personal (articolul 8) și dreptul la libertatea de exprimare și de informare (articolul 11).

109. Astfel cum arătăm în Concluziile prezentate în cauzele C-511/18 și C-512/18, acestea sunt, de fapt, drepturile care, potrivit Curții, ar putea fi afectate în asemenea cazuri.

110. Cu toate acestea, Cour constitutionnelle (Curtea Constituțională) face trimitere de asemenea la articolele 4 și 6 din cartă, la care se referă a doua și, respectiv, prima întrebare preliminară.

111. În ceea ce privește articolul 6 din cartă, care garantează dreptul la libertate și la siguranță, acesta a fost invocat și în cauzele C-511/18 și C-512/18 și ne-am pronunțat deja cu privire la importanța sa în concluziile prezentate în cauzele respective, la care facem trimitere [80].

112. În ceea ce privește articolul 4 din cartă, având în vedere că răspunsul nu depinde atât de analiza legislației naționale, în vederea comparării sale cu dreptul Uniunii, cât de interpretarea acelei dispoziții, considerăm că este oportun să abordăm în primul rând această chestiune.

2. A doua întrebare preliminară

113. Astfel, referirea la interzicerea torturii și a pedepselor sau a tratamentelor inumane sau degradante, garantată la articolul 4 din cartă, se face exclusiv în prezenta trimitere preliminară, ceea ce ne determină să îi acordăm atenție.

114. Prin referirea la articolul 4 din cartă, instanța de trimitere dorește să sublinieze că reglementarea națională are de asemenea scopul de a aduce la îndeplinire *obligația pozitivă* care îi revine autorității publice, ce constă în instituirea „unui cadru legal care să permită o urmărire penală efectivă și o reprimare efectivă a abuzului sexual asupra minorilor și care să permită efectiv identificarea autorului infracțiunii, chiar și atunci când sunt utilizate mijloace de comunicare electronică” [81].

115. În opinia noastră, această *obligație pozitivă* concretă nu este foarte diferită de fiecare dintre sarcinile specifice pe care le implică, pentru stat, proclamarea unui catalog de drepturi fundamentale. Dreptul la viață (articolul 2 din cartă), dreptul la integritate fizică (articolul 3 din cartă) sau dreptul la protecția datelor (articolul 8 din cartă), asemenea libertății de exprimare (articolul 11 din cartă) și libertății de gândire, de conștiință și de religie (articolul 10 din cartă)

[80] Concluziile prezentate în cauzele C-511/18 și C-512/18, punctul 95 și următoarele.

[81] Enunțul celei de a doua întrebări *in fine*. Referirea la mijloacele de comunicare electronică justifică trimiterea din cuprinsul întrebării la o a doua *obligație pozitivă* a statelor membre, și anume cea impusă la articolul 8 din cartă în ceea ce privește protecția datelor cu caracter personal. Dubla referire la articolul 8 din cartă relevă că instanța de trimitere atribuie drepturilor garantate de cartă, în funcție de natura lor, o dublă funcție: cea de *limitare* și cea de *justificare* a obligației în litigiu.

implică pentru stat obligația de a crea un cadru de reglementare în care acestea să fie garantate, dacă este cazul, prin aplicarea forței monopolizate de către autoritatea publică împotriva oricui încearcă să împiedice sau să îngreuneze exercitarea lor [82].

116. În ceea ce privește abuzurile sexuale asupra copiilor, Curtea Europeană a Drepturilor Omului (denumită în continuare Curtea EDO) consideră că minorii și alte persoane vulnerabile beneficiază de un drept extins la protecție din partea statului, prin intermediul adoptării unor norme penale care sancționează în mod eficient și cu efecte disuasive săvârșirea infracțiunilor respective [83].

117. Acest drept extins la protecție nu se întemeiază numai pe articolul 4 din cartă, ci poate fi invocat în mod firesc și articolul 1 (demnitatea umană) sau articolul 3 (dreptul la integritatea fizică și psihică).

118. Cu toate că obligația pozitivă a autorităților publice de a garanta protecția copiilor și a altor persoane vulnerabile nu poate fi ignorată cu ocazia aprecierii bunurilor juridice afectate de reglementarea națională [84], aceasta nu poate implica „sarcini excesive” [85] pentru autoritățile publice și nu poate fi îndeplinită prin încălcarea legii sau a celorlalte drepturi fundamentale [86].

3. Prima întrebare preliminară

119. Instanța de trimitere solicită să se stabilească în esență dacă dreptul Uniunii se opune legii naționale cu privire la care trebuie să se pronunțe în cadrul unei acțiuni în declararea neconstituționalității.

120. Întrucât Curtea a oferit deja o interpretare a Directivei 2002/58 conformă cu dispozițiile corelative din cartă, răspunsul la această întrebare preliminară trebuie să aibă în vedere jurisprudența stabilită prin Hotărârea Tele2 Sverige și Watson, dacă este cazul cu nuanțele adăugate în prezentele concluzii.

121. Plecând de la această premisă, regulile de interpretare care pot fi puse la dispoziția Cour constitutionnelle (Curtea Constituțională) pentru ca ea însăși să aprecieze compatibilitatea normei naționale cu dreptul Uniunii trebuie să se refere în mod separat la păstrarea datelor și la accesul la date, astfel cum sunt ele reglementate de norma națională respectivă.

82 Această obligație de eficiență presupune o obligație de rezultat pentru autoritatea publică în statul bazat pe un sistem de prestații sociale, în care, dincolo de recunoașterea formală a drepturilor, se urmărește asigurarea practică a conținutului lor material.

83 Hotărârea Curții EDO din 2 decembrie 2008, K.U. împotriva Finlandei, (ECHR:2008:1202JUD000287202), § 46.

84 În acest sens, considerăm că drepturilor invocate de instanța de trimitere (ca *limite* privind obligația în litigiu, iar nu ca *justificare* a acesteia) li s-ar putea adăuga dreptul la o cale de atac eficientă (articolul 47 din cartă) și dreptul la apărare (articolul 48 din cartă), a căror eventuală încălcare a fost de asemenea dezbătută în procedurile principale. Cu toate acestea, în dispozitivul deciziei de trimitere se face referire numai la articolele 7, 8 și 11 și la articolul 52 alineatul (1) din cartă.

85 Hotărârea Curții EDO din 28 octombrie 1998, Osman împotriva Regatului Unit (CE:ECHR:1998:1028JUD002345294), § 116.

86 *Ibidem* § 116 *in fine*: „[este necesar] să se garanteze că autoritățile polițienești își exercită competența privind combaterea și prevenirea infracționalității cu respectarea deplină a modalităților legale și a celorlalte garanții care limitează în mod legitim întinderea actelor lor de urmărire penală”. A se vedea de asemenea Hotărârea Curții EDO din 2 decembrie 2008, K.U. împotriva Finlandei (CE:ECHR:2008:1202JUD000287202), § 48. În același sens, Curtea a statuat în Hotărârea din 29 iulie 2019, Gambino și Hyka (C-38/18, EU:C:2019:628, punctul 49), că drepturile prevăzute în beneficiul victimei unei infracțiuni nu pot afecta exercitarea efectivă a drepturilor procedurale recunoscute persoanei acuzate.

a) Condițiile de păstrare a datelor

122. Guvernul belgian subliniază că a dorit să stabilească un cadru juridic clar, care să includă garanțiile necesare pentru protecția vieții private, în loc să se bazeze pe practica operatorilor de servicii de comunicații electronice privind păstrarea datelor în vederea facturării și a soluționării cererilor de informare ale clienților.

123. În opinia guvernului respectiv, obligația generală și preventivă de păstrare a datelor nu are drept scop numai instrucția, investigarea și urmărirea penală a faptelor care țin de infracționalitatea gravă, ci și garantarea securității naționale, apărarea teritoriului și a securității publice, investigarea, detectarea și urmărirea penală a altor fapte decât cele care țin de infracționalitatea gravă sau prevenirea unei utilizări interzise a sistemelor de comunicații electronice [87] ori realizarea unui alt obiectiv identificat la articolul 23 alineatul (1) din Regulamentul (UE) 2016/679.

124. Potrivit guvernului belgian:

– păstrarea datelor ca atare nu permite extragerea unor concluzii foarte exacte cu privire la viața privată a persoanelor afectate: posibilitatea de a extrage concluziile respective ar exista numai dacă s-ar facilita și accesul la datele păstrate;

– legea conține garanții prin care se urmărește protejarea vieții private; printre altele, păstrarea datelor nu afectează conținutul comunicațiilor; garanțiile privind justificarea păstrării, dreptul de acces, dreptul de rectificare și altele sunt pe deplin aplicabile; furnizorii și operatorii trebuie să supună datele stocate acelorași obligații și măsuri de siguranță și de protecție ca cele aplicabile datelor din rețea, prevenind distrugerea accidentală sau ilegală, pierderea sau deteriorarea accidentală a acestora;

– datele pot fi stocate pentru o perioadă de douăsprezece luni (la finalul căreia trebuie distruse) și numai pe teritoriul Uniunii;

– furnizorii și operatorii trebuie să aplice măsuri de protecție tehnică prin care datele păstrate să devină, imediat după înregistrarea lor, ilizibile și inutilizabile de către orice persoană care nu este autorizată să le acceseze;

– în orice caz, operațiunile se efectuează sub supravegherea autorității belgiene de reglementare în domeniile poștei și telecomunicațiilor și de Autoritatea pentru protecția datelor.

125. În pofida acestor garanții, este cert că legislația belgiană impune operatorilor și furnizorilor de servicii de comunicații electronice obligația generală și nediferențiată de a păstra datele de transfer și de localizare, în sensul Directivei 2002/58, prelucrate în contextul prestării serviciilor respective. Perioada de păstrare este, astfel cum am menționat, în general de douăsprezece luni: nu se prevede nicio limitare temporală în funcție de categoriile de date păstrate.

126. Această obligație de păstrare generală și nediferențiată se aplică în mod permanent și continuu. Chiar dacă obiectivul său constă în prevenirea, investigarea și urmărirea penală a oricărui tip de infracțiuni (de la cele referitoare la securitatea națională, la apărare sau cele

[87] Aceasta este justificată și pentru a răspunde unui apel la un serviciu de urgență sau pentru a găsi o persoană dispărută, a cărei integritate fizică este în pericol iminent.

deosebit de grave până la cele în privința cărora se aplică o pedeapsă cu închisoarea mai mică de un an), o obligație cu aceste caracteristici nu respectă jurisprudența Curții, astfel încât nu poate fi considerată compatibilă cu carta.

127. Pentru a se adapta jurisprudenței respective, legiuitorul belgian va trebui să exploreze alte modalități (precum cele menționate anterior) care să instituie formule de păstrare limitată. Aceste formule, care ar varia în funcție de categoriile de date, trebuie să respecte principiul conform căruia trebuie să se păstreze numai *minimul* necesar de date, în funcție de risc sau de amenințare, și pentru o perioadă limitată, care va depinde de natura informațiilor stocate. În orice caz, păstrarea nu poate oferi o *cartografiere* exactă a vieții private, a obiceiurilor, a comportamentului sau a relațiilor sociale ale persoanelor afectate.

b) Condițiile de acces al autorităților publice la datele păstrate

128. În opinia noastră, condițiile enunțate în Hotărârea Tele2 Sverige și Watson [88] sunt în continuare relevante în ceea ce privește accesul: reglementarea națională trebuie să stabilească cerințele de fond și procedurale care reglementează accesul autorităților competente la datele păstrate [89].

129. Guvernul belgian menționează că articolul 126 alineatul 2 din Legea din 2005 (privind comunicațiile electronice) [90] stabilește în mod restrictiv autoritățile naționale care pot primi datele stocate în conformitate cu alineatul 1 al articolului respectiv.

130. Printre aceste autorități figurează cele propriu-zis judiciare și Ministerul Public, forțele de securitate ale statului, Serviciul General de Informații și Securitate, aflat sub controlul mai multor comisii independente, ofițerii de poliție judiciară din cadrul Institutului belgian al Poștei și al Telecomunicațiilor, serviciile de urgență, ofițerii de poliție judiciară din cadrul Unității pentru persoane dispărute a Poliției Federale, Serviciul de mediere pentru telecomunicații și organul de supraveghere a sectorului financiar.

131. În general, guvernul belgian susține că legislația națională nu permite ca diverse servicii să aibă acces la date în vederea urmăririi active a amenințărilor neidentificate sau lipsite de indicații concrete. Prin urmare, autoritățile naționale nu ar putea să acceseze pur și simplu date de comunicații brute și să le prelucreze în mod automat pentru a obține informații și pentru a combate în mod activ amenințările la adresa securității.

132. Potrivit guvernului respectiv, accesul la date este supus unor condiții stricte, în funcție de statutul fiecărei autorități naționale competente.

133. Răspunsul la prima întrebare preliminară nu necesită, în opinia noastră, efectuarea unei analize exhaustive de către Curte cu privire la condițiile aplicabile pentru ca fiecare dintre autoritățile respective să poată obține datele păstrate. Această sarcină revine mai degrabă instanței de trimitere, care va trebui să o execute în lumina orientărilor oferite de jurisprudența stabilită prin Hotărârile Tele2 Sverige și Watson și Ministerio Fiscal.

88 A se vedea punctul 60 din prezentele concluzii.

89 Hotărârea Tele2 Sverige și Watson, punctul 118.

90 Articolul 126, în versiunea modificată prin Legea din 29 mai 2016.

134. De altfel, conform informațiilor furnizate de guvernul belgian, există diferențe notabile între condițiile de acces aplicabile autorităților judiciare sau Ministerului Public [91] în vederea investigării, a instrucției și a urmăririi penale a infracțiunilor, în conformitate cu articolele 46*bis* [92] și 88*bis* [93] din Codul de procedură penală, și cele aplicabile altor autorități.

135. În ceea ce privește serviciile de informații și de securitate, în conformitate cu Legea din 1998, cererea de acces la datele de trafic și de localizare deținute de operatori trebuie să se întemeieze pe criterii obiective pentru a garanta că se limitează la strictul necesar, pe baza unei amenințări identificate în prealabil [94]. Sunt prevăzute diverse perioade de acces la date (de șase, de nouă sau de douăsprezece luni), în funcție de amenințarea potențială, iar cererea trebuie să respecte principiile proporționalității și subsidiarității. S-a instituit de asemenea un mecanism de control de către o autoritate independentă [95].

136. În ceea ce privește ofițerii de poliție judiciară din cadrul Institutului belgian al Poștei și al Telecomunicațiilor (BIPT), accesul acestora la datele deținute de operatorii de telecomunicații este posibil, sub supravegherea procurorului, în cazuri concrete foarte limitate [96], fără ca, potrivit guvernului belgian, activitatea lor să afecteze persoanele ale căror date se păstrează.

137. În ceea ce privește serviciile de urgență care oferă asistență la fața locului, acestea pot solicita datele autorului unui apel de urgență atunci când, după primirea apelului, nu obțin de la furnizor sau de la operator datele de identificare ale persoanei respective sau când acestea sunt incomplete sau incorecte.

138. În ceea ce privește ofițerii de poliție judiciară din cadrul Unității pentru persoane dispărute a Poliției Federale, ei pot solicita operatorului datele necesare pentru găsirea unei persoane dispărute a cărei integritate fizică este în pericol iminent. Accesul, supus unor condiții stricte, este limitat la datele care permit identificarea utilizatorului și la cele referitoare la accesul și la conectarea terminalelor la rețea și la serviciu, precum și la localizarea acestor echipamente și se limitează la cele stocate pe o perioadă de 48 de ore de la depunerea cererii.

91 Capacitatea procurorilor de a adopta măsuri de acest tip este dezbătută în trimiterea preliminară formulată în cauza C-746/18, HK/Prokuratur, care este pendinte.

92 În ceea ce privește solicitările de date de identificare adresate operatorilor, este competent procurorul, care, printr-o decizie motivată și scrisă (orală în cazuri de urgență), trebuie să ateste caracterul proporțional al măsurii în ceea ce privește respectarea vieții private și caracterul subsidiar al acesteia în raport cu orice altă obligație impusă de investigare. În cazul infracțiunilor care nu sunt susceptibile de o pedeapsă cu închisoarea de un an sau de o pedeapsă mai gravă, procurorul poate solicita datele numai pentru o perioadă de șase luni anterior deciziei sale.

93 În ceea ce privește solicitările adresate operatorilor cu privire la reperarea comunicațiilor electronice sau a datelor de trafic și de localizare păstrate, este competent judecătorul de instrucție, care poate dispune această măsură în cazul în care există dovezi serioase privind săvârșirea unei infracțiuni pasibile de anumite pedepse și care se pronunță prin ordonanță motivată și scrisă (sau orală în caz de urgență), supusă acelorași cerințe de proporționalitate și subsidiaritate ca cele aplicabile procurorului. Există unele excepții atunci când măsura este îndreptată împotriva anumitor categorii profesionale protejate (de exemplu, avocați sau medici).

94 Decizia trebuie să specifice, de la caz la caz, persoanele fizice sau juridice, asociațiile de fapt sau grupurile, obiectele, locurile, evenimentele sau informațiile care fac obiectul metodei specifice. Aceasta trebuie să menționeze de asemenea legătura dintre scopul datelor solicitate și amenințarea potențială care justifică această metodă în special.

95 Comisia administrativă pentru supravegherea metodelor specifice și excepționale de colectare a datelor de către serviciile de informații și de securitate (Comisia BIM) și Comitetul permanent pentru controlul serviciilor de informații (Comitetul R). Potrivit guvernului belgian, Comisia BIM este responsabilă de monitorizarea metodelor de căutare utilizate de serviciile de informații și de securitate, față de care exercită un control de prim grad. Această comisie, formată din judecători, își îndeplinește sarcinile în mod total independent. Este organizat de asemenea un control de gradul al doilea, care revine în sarcina Comitetului R.

96 Este permisă pentru investigarea, instrucția și urmărirea penală a infracțiunilor prevăzute la articolul 114 (siguranța rețelelor), la articolul 124 (confidențialitatea comunicațiilor electronice) și la articolul 126 (păstrarea datelor și accesul) din Legea din 13 iunie 2005 privind comunicațiile electronice.

139. În ceea ce privește Serviciul de mediere pentru telecomunicații, acesta poate solicita numai datele de identificare ale persoanei care a utilizat cu rea-credință o rețea sau un serviciu de comunicații electronice. Nu există, în acest caz, un control prealabil efectuat de o autoritate judiciară sau administrativă independentă (alta decât serviciul însuși).

140. În sfârșit, în vederea combaterii infracțiunilor financiare, organul de supraveghere a sectorului financiar poate obține accesul la datele de transfer și de localizare, care este supus autorizației prealabile a judecătorului de instrucție.

141. Prezentarea acestor modalități și condiții de acces la datele păstrate, aplicabile fiecăreia dintre autoritățile autorizate sa le obțină, relevă o varietate de situații și de garanții, revenind instanței de trimitere sarcina de a efectua o analiză detaliată privind compatibilitatea lor cu criteriile utilizate de Curte în jurisprudența sa [97].

142. Observăm de exemplu că, în contextul reglementării în litigiu, nu se precizează că autoritățile naționale competente au obligația să informeze în mod sistematic persoanele afectate (cu excepția cazului în care informațiile respective compromit investigațiile în curs) cu privire la faptul că datele lor au fost consultate. Nu pare, cel puțin în anumite cazuri, precum cele referitoare la infracțiunile financiare, nici să existe reguli predeterminate cu privire la gravitatea acestora, pentru a justifica accesul la datele corespunzătoare. Relația dintre gravitatea ingerinței și gravitatea infracțiunii investigate, în sensul Hotărârii Ministerio Fiscal, nu este evidentă în toate situațiile.

143. În orice caz, apreciem că argumentele referitoare la accesul autorităților la date trec pe un plan secund atunci când, pentru motivele prezentate anterior, păstrarea generalizată și nediferențiată a acestor date constituie motivul principal pentru care reglementarea națională la care se referă prezenta trimitere preliminară nu respectă dreptul Uniunii.

4. A treia întrebare preliminară

144. Cour constitutionnelle (Curtea Constituțională) solicită să se stabilească dacă, în ipoteza în care, în lumina răspunsului Curții, se constată că reglementarea națională este incompatibilă cu dreptul Uniunii, ar putea menține în mod provizoriu efectele reglementării respective. Astfel, s-ar evita insecuritatea juridică și s-ar permite ca datele colectate și păstrate să continue să fie utilizate pentru obiectivele urmărite.

145. Potrivit unei jurisprudențe constante, „numai Curtea poate, cu titlu excepțional și pentru considerații imperative de securitate juridică, să acorde o suspendare provizorie a efectului de înlăturare avut de o normă din dreptul Uniunii asupra dreptului național contrar acesteia”. Dacă „instanțele naționale ar avea puterea de a conferi dispozițiilor naționale supremație în raport cu dreptul Uniunii contrar acestora, chiar și numai cu titlu provizoriu, s-ar aduce atingere aplicării uniforme a dreptului Uniunii” [98].

146. Comisia consideră că, întrucât Curtea nu a limitat efectele în timp ale interpretării articolului 15 alineatul (1) din Directiva 2002/58, răspunsul la această întrebare a instanței de trimitere ar trebui să fie negativ [99].

97 Facem trimitere la punctul 60 din prezentele concluzii.

98 Hotărârea din 28 iulie 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, punctul 33).

99 Punctul 100 din observațiile scrise ale Comisiei.

147. Cu toate acestea, în Hotărârea din 28 februarie 2012, Inter-Environnement Wallonie și Terre wallonne [100], Curtea a statuat că, ținând seama de existența unei cerințe imperative legate de protecția mediului, instanța de trimitere poate fi în mod excepțional autorizată să facă uz de dispoziția sa națională care îi permite să mențină anumite efecte ale unui act național anulat, ca urmare a încălcării unei reglementări a Uniunii [101].

148. Această abordare jurisprudențială a fost confirmată prin Hotărârea din 29 iulie 2019, Inter-Environnement Wallonie și Bond Beter Leefmilieu Vlaanderen [102]. Cu toate că hotărârea menționată a fost adoptată în domeniul protecției mediului și se întemeiază pe securitatea furnizării de energie electrică, considerăm că nu există motive pentru a respinge aplicabilitatea sa în alte domenii ale dreptului Uniunii, în special în cele analizate în prezenta cauză.

149. Împrejurarea că o „cerință imperativă legată de protecția mediului" poate justifica menținerea cu titlu excepțional de către instanțele naționale a anumitor efecte ale unei dispoziții naționale incompatibile cu dreptul Uniunii se datorează faptului că protecția mediului constituie „unul dintre obiectivele esențiale ale Uniunii și care are un caracter atât transversal, cât și fundamental" [103].

150. Or, printre obiectivele Uniunii figurează și crearea unui spațiu de securitate (articolul 3 TUE), care include respectarea funcțiilor esențiale ale statului, în special cele care au scopul de a asigura ordinea publică și de a proteja securitatea națională [articolul 4 alineatul (2) TUE]. Este vorba despre un obiectiv la fel de „transversal și fundamental" precum protecția mediului, deoarece îndeplinirea sa constituie condiția necesară pentru instituirea unui cadru normativ capabil să garanteze exercitarea efectivă a drepturilor și a libertăților fundamentale.

151. În opinia noastră, motivele imperative legate de protecția securității naționale ar putea justifica, în prezenta cauză, decizia Curții de a autoriza în mod excepțional instanța de trimitere să mențină cel puțin o parte dintre efectele legii în litigiu.

152. Această menținere ar presupune ca instanța de trimitere, în lumina hotărârii Curții, să considere că norma națională este incompatibilă cu dreptul Uniunii și să aprecieze ca fiind extrem de perturbatoare efectele pe care le-ar putea avea asupra securității publice sau a securității statului anularea imediată a acesteia (în cazul în care anularea ar fi, în dreptul național, consecința incompatibilității respective) sau neaplicarea sa.

153. Pentru menținerea provizorie (în tot sau în parte) a efectelor normei naționale ar fi necesar de asemenea ca:

– scopul prelungirii respective să constea în evitarea unui vid normativ cu efecte la fel de dăunătoare precum cele care decurg din aplicarea reglementării în litigiu, vid imposibil de acoperit prin alte mijloace și care ar implica privarea autorităților naționale de un instrument valoros pentru garantarea securității naționale și

100 Cauza C-41/11, EU:C:2012:103.

101 Hotărârea din 28 februarie 2012, Inter-Environnement Wallonie și Terre wallonne (C-41/11, EU:C:2012:103, punctul 58). În Hotărârea din 28 iulie 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, punctul 34), Curtea a dedus din această afirmație că „a înțeles să recunoască unei instanțe naționale, de la caz la caz și cu titlu excepțional, posibilitatea de a organiza efectele anulării unei dispoziții naționale considerate incompatibilă cu dreptul Uniunii".

102 Cauza C-411/17 (EU:C:2019:622, punctul 178).

103 Hotărârea din 28 februarie 2012, Inter-Environnement Wallonie și Terre wallonne (C-41/11, EU:C:2012:103, punctul 57).

– menținerea să se realizeze pe perioada strict necesară pentru punerea în aplicare a unor măsuri care să permită remedierea incompatibilității constatate cu dreptul Uniunii [104].

154. În plus, această soluție este justificată de dificultatea pe care o presupune adaptarea reglementărilor naționale la jurisprudența stabilită în cauza Tele2 Sverige și Watson [105] și de faptul că voința legiuitorului belgian de a se conforma Hotărârii Digital Rights s-a concretizat prin modificarea legislației naționale. Acest precedent ne determină să credem că legiuitorul belgian va proceda și la adaptarea Legii din 29 mai 2016 (adoptată înaintea Hotărârii Tele2 Sverige și Watson) la jurisprudența stabilită prin aceasta din urmă.

V. Concluzie

155. În temeiul considerațiilor anterioare, propunem Curții să răspundă Cour constitutionnelle (Curtea Constituțională, Belgia) după cum urmează:

„1) Articolul 15 alineatul (1) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) coroborat cu articolele 7, 8 și 11 și cu articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene trebuie interpretat în sensul că:

– se opune unei reglementări naționale care 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 și utilizatorilor, în legătură cu toate mijloacele de comunicații electronice;

– această concluzie nu poate fi infirmată de faptul că reglementarea respectivă nu are ca obiect numai investigarea, depistarea și urmărirea penală a infracțiunilor, grave sau minore, ci și garantarea securității naționale, a apărării teritoriului și a securității publice, prevenirea unei utilizări interzise a sistemelor de comunicații electronice ori realizarea unui alt obiectiv identificat la articolul 23 alineatul (1) din 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);

– această concluzie nu poate fi infirmată nici de faptul că accesul la datele păstrate este supus unor garanții reglementate în mod precis. Revine instanței de trimitere sarcina de a verifica dacă reglementarea națională care stabilește condițiile privind accesul autorităților competente limitează accesul respectiv la situații specifice a căror gravitate determină ca ingerința să fie indispensabilă, dacă îl supune controlului prealabil (cu excepția situațiilor de urgență) al unei instanțe sau al unei autorități independente și dacă prevede că persoanele afectate trebuie informate cu privire la acest acces, în măsura în care această informare nu compromite acțiunea autorităților respective.

104 Hotărârea din 28 februarie 2012, Inter-Environnement Wallonie și Terre wallonne (C-41/11, EU:C:2012:103, punctul 62).

105 Punctul 45 din observațiile guvernului danez.

2) Articolele 4 și 6 din Carta drepturilor fundamentale a Uniunii Europene nu afectează interpretarea articolului 15 alineatul (1) din Directiva 2002/58 coroborat cu celelalte articole menționate din cartă astfel încât să împiedice stabilirea incompatibilității cu dreptul Uniunii a unei reglementări naționale precum cea în discuție în litigiul principal.

3) O instanță națională poate, în cazul în care dreptul național îi permite, să mențină cu titlu excepțional și provizoriu efectele unei reglementări precum cea în discuție în litigiul principal, chiar dacă aceasta este incompatibilă cu dreptul Uniunii, dacă menținerea respectivă este justificată de considerații imperative legate de amenințările la adresa securității naționale, care nu ar putea fi combătute prin alte mijloace și prin alte metode. Menținerea respectivă se poate realiza pe perioada strict necesară pentru remedierea incompatibilității invocate cu dreptul Uniunii.”