Repertoriul jurisprudenței

CONCLUZIILE AVOCATULUI GENERAL
HENRIK SAUGMANDSGAARD ØE
prezentate la 19 iulie 2016 [1]

Cauzele conexate C-203/15 și C-698/15

Tele2 Sverige AB
împotriva
Post- och telestyrelsen (C-203/15)
și
Secretary of State for the Home Department
împotriva
Tom Watson,
Peter Brice,
Geoffrey Lewis (C-698/15)
cu participarea
Open Rights Group,
Privacy International,
Law Society of England and Wales

[cereri de decizie preliminară formulate de Kammarrätten i Stockholm (Curtea Administrativă de Apel din Stockholm, Suedia) și Court of Appeal (England & Wales) (Civil Division) [Curtea de Apel (Anglia și Țara Galilor) (Secția civilă), Regatul Unit]

„Trimitere preliminară — Directiva 2002/58/CE — Prelucrarea datelor cu caracter personal și protejarea confidențialității în sectorul comunicațiilor electronice — Legislație națională care prevede o obligație generală de păstrare a datelor referitoare la comunicațiile electronice — Articolul 15 alineatul (1) — Carta drepturilor fundamentale a Uniunii Europene — Articolul 7 — Dreptul la respectarea vieții private — Articolul 8 — Dreptul la protecția datelor cu caracter personal — Ingerință gravă — Justificare — Articolul 52 alineatul (1) — Condiții — Obiectivul legitim al combaterii infracțiunilor grave — Cerința unui temei legal în dreptul intern — Cerința caracterului strict necesar — Cerința proporționalității într-o societate democratică”

Cuprins

1 — Limba originală: franceza.

I – Introducere

1. În anul 1788, James Madison, unul dintre autorii Constituției Statelor Unite, scria: „If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself” [2].

2. Prezentele cauze ne situează în centrul „dificultății majore” identificate de Madison. Acestea privesc compatibilitatea cu dreptul Uniunii a unor regimuri naționale care prevăd, în sarcina furnizorilor de servicii de comunicații electronice accesibile publicului (denumiți în continuare „furnizorii”), o obligație de păstrare a datelor referitoare la comunicațiile electronice (denumite în continuare „datele referitoare la comunicații”) care vizează toate mijloacele de comunicare și toți utilizatorii (denumită în continuare „obligația generală de păstrare a datelor”).

3. Pe de o parte, păstrarea datelor referitoare la comunicații permite „guvernării să îi controleze pe cei guvernați”, oferind autorităților competente un mijloc de cercetare care poate prezenta o anumită utilitate în combaterea infracțiunilor grave și în special în combaterea terorismului. În esență, păstrarea acestor date conferă autorităților o capacitate limitată de „a examina trecutul”, prin accesarea datelor referitoare la comunicațiile efectuate de o persoană înainte chiar ca aceasta să fie suspectată de legături cu o infracțiune gravă [3].

4. Totuși, pe de altă parte, este imperativ ca „guvernarea să fie obligată să se controleze pe sine” în ceea ce privește atât păstrarea, cât și accesul la datele păstrate, având în vedere riscurile grave generate de existența unor astfel de baze de date care acoperă totalitatea comunicațiilor efectuate pe teritoriul național. Astfel, aceste baze de date de o amploare considerabilă oferă oricărei persoane care are acces

2 — „Dacă oamenii ar fi îngeri, guvernarea nu ar fi necesară. Dacă îngerii ar guverna oamenii, controlul extern sau intern asupra guvernării nu ar fi necesar. În cadrul reglementării unei guvernări a oamenilor asupra oamenilor, dificultatea majoră este aceasta: mai întâi trebuie să se permită guvernării să îi controleze pe cei guvernați; iar apoi, aceasta trebuie obligată să se controleze pe sine”: Madison, J., „Federalist No. 51”, în Hamilton, A., Madison, J., și Jay, J., ed. Genovese, M. A., *The Federalist Papers*, Palsgrave Macmillan, New York, 2009, p. 120 (traducere liberă). Madison a fost unul dintre principalii autori și unul dintre cei 39 de semnatari ai Constituției Statelor Unite (1787). A devenit ulterior al patrulea președinte al Statelor Unite (din 1809 până în 1817).

3 — Această capacitate limitată de „a examina trecutul” se poate dovedi deosebit de utilă în special în scopul identificării unor eventuali complici: a se vedea punctele 178-184 din prezentele concluzii.

la acestea capacitatea de a cataloga instantaneu întreaga populație relevantă [4]. Aceste riscuri trebuie analizate cu scrupulozitate, în special prin examinarea caracterului strict necesar și a caracterului proporțional al unei obligații generale de păstrare a datelor, precum cele în discuție în litigiile principale.

5. Astfel, în cadrul prezentelor cauze, Curtea și instanțele de trimitere sunt chemate să definească un punct de echilibru între obligația care revine statelor membre de a asigura siguranța indivizilor care se află pe teritoriul lor și respectarea drepturilor fundamentale la viață privată și la protecția datelor cu caracter personal consacrate la articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”).

6. Vom examina în lumina acestei „dificultăți majore” întrebările adresate Curții în prezentele cauze. Acestea privesc, mai specific, compatibilitatea unor regimuri naționale care prevăd o obligație generală de păstrare a datelor cu Directiva 2002/58/CE [5], precum și cu articolele 7 și 8 din cartă. Pentru a răspunde la aceste întrebări, Curtea va trebui să precizeze printre altele interpretarea care trebuie dată într-un context național Hotărârii Digital Rights Ireland și alții (denumită în continuare „Hotărârea DRI”) [6], în care Marea Cameră a Curții a invalidat Directiva 2006/24/CE [7].

7. Pentru motivele pe care le vom prezenta în continuare, avem sentimentul că o obligație generală de păstrare a datelor impusă de un stat membru poate fi compatibilă cu drepturile fundamentale consacrate de dreptul Uniunii, cu condiția să fie încadrată în mod strict de o serie de garanții, pe care le vom identifica în cursul expunerii.

II – Cadrul juridic

A – *Directiva 2002/58*

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

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

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

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

4 — A se vedea punctele 252-261 din prezentele concluzii.

5 — Directiva Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor electronice (Directiva asupra confidențialității și comunicațiilor electronice) (JO 2002, L 201, p. 37, Ediție specială, 13/vol. 36, p. 63), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 (JO 2009, L 337, p. 11).

6 — Hotărârea din 8 aprilie 2014 (C-293/12 și C-594/12, EU:C:2014:238).

7 — 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).

9. Articolul 15 alineatul (1) din Directiva 2002/58, intitulat „Aplicarea anumitor dispoziții ale Directivei [95/46]”, are următorul cuprins:

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

B – *Dreptul suedez*

10. Directiva 2006/24, în prezent invalidată, a fost transpusă în dreptul suedez prin modificări aduse lagen (2003:389) om elektronisk kommunikation (Legea suedeză 2003:389 privind comunicațiile electronice, denumită în continuare „LEK”) și förordningen (2003:396) om elektronisk kommunikation (Regulamentul nr. 2003:396 privind comunicațiile electronice, denumit în continuare „FEK”), texte intrate în vigoare la 1 mai 2012.

1. Cu privire la întinderea obligației de păstrare

11. Reiese din dispozițiile articolului 16 a din capitolul 6 din LEK că furnizorii sunt obligați să păstreze datele referitoare la comunicații care sunt necesare pentru a detecta și a identifica sursa și destinația comunicației, pentru a stabili data, ora, durata și tipul comunicației, pentru a identifica echipamentele de comunicații utilizate, precum și pentru a localiza echipamentele de comunicații mobile la începutul și la sfârșitul comunicației. Tipurile de date care trebuie păstrate fac obiectul unor dispoziții mai detaliate la articolele 38-43 din FEK.

12. Această obligație de păstrare vizează datele prelucrate în cadrul unui serviciu de telefonie, al unui serviciu de telefonie care utilizează o conexiune mobilă, al unui sistem de mesagerie electronică, al unui serviciu de acces la internet, precum și al unui serviciu de furnizare a posibilității de acces la internet.

13. Datele care trebuie păstrate includ nu numai toate datele care trebuiau păstrate în cadrul Directivei 2006/24, ci și pe cele privind comunicațiile nereușite, precum și pe cele referitoare la locul în care a fost terminat un apel în rețelele mobile. La fel precum în cazul regimului prevăzut de această directivă, datele care trebuie păstrate nu includ conținutul comunicațiilor.

2. Cu privire la accesul la datele păstrate

14. Accesul la datele păstrate este reglementat de trei texte, și anume LEK, rättegångsbalken (Codul de procedură judiciară, denumit în continuare „RB”) și lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (Legea suedeză 2012:278 privind colectarea datelor referitoare la comunicațiile electronice în activitățile de investigare desfășurate de autoritățile represive, denumită în continuare „Legea 2012:278”).

a) LEK

15. Potrivit dispozițiilor articolului 22 primul paragraf punctul 2 din capitolul 6 din LEK, orice furnizor trebuie să comunice datele referitoare la un abonament la cererea organului de urmărire penală, a poliției, a Säkerhetspolisen (Serviciul Suedez de Securitate, denumit în continuare „Säpo”) sau a oricărei alte autorități căreia îi revine responsabilitatea combaterii criminalității, dacă datele respective au legătură cu o suspiciune privind o infracțiune. Potrivit acestor dispoziții, nu este necesar să fie vorba despre o infracțiune gravă.

16. Date referitoare la un abonament înseamnă în esență datele referitoare la numele, titlul, adresa poștală, numărul de telefon și adresa IP ale abonatului.

17. În temeiul LEK, predarea datelor referitoare la un abonament nu este subordonată unui control prealabil, însă poate face obiectul unui control administrativ ulterior. Pe de altă parte, numărul autorităților care pot avea acces la date nu este limitat.

b) RB

18. RB reglementează monitorizarea comunicațiilor electronice în cadrul urmăririi penale.

19. În esență, monitorizarea comunicațiilor electronice poate fi dispusă doar atunci când există motive rezonabile pentru a suspecta că o persoană a săvârșit o infracțiune pentru care se prevede o pedeapsă cu închisoarea de cel puțin șase luni sau alte infracțiuni enumerate în mod specific, iar această măsură prezintă o importanță deosebită pentru necesitățile urmăririi.

20. Pe lângă aceste situații, se poate realiza o astfel de monitorizare în vederea urmăririi oricărei persoane atunci când există motive serioase pentru care aceasta este suspectată de săvârșirea unei infracțiuni pentru care se prevede o pedeapsă cu închisoarea de cel puțin doi ani, dacă măsura prezintă o importanță deosebită pentru necesitățile urmăririi.

21. În conformitate cu articolul 21 din capitolul 27 din RB, ca regulă generală, parchetul trebuie să obțină autorizație din partea instanței competente înainte de a proceda la monitorizarea comunicațiilor electronice.

22. Cu toate acestea, dacă există motive să se creadă că obținerea autorizării din partea instanței competente înainte de a proceda la monitorizarea comunicațiilor electronice – măsură de importanță esențială pentru necesitățile urmăririi – ar fi incompatibilă cu urgența acesteia sau ar crea obstacole, autorizarea este acordată de parchet în așteptarea deciziei instanței competente. Parchetul trebuie să notifice de îndată în scris instanței luarea măsurii. Instanța trebuie apoi să analizeze în mod prompt dacă măsura este justificată.

c) Legea 2012:278

23. În contextul strângerii de informații și în conformitate cu articolul 1 din Legea 2012:278, poliția națională, Säpo și Tullverket (Autoritatea Vamală Suedeză) pot, sub rezerva condițiilor prevăzute de această lege, să colecteze date referitoare la comunicații fără știrea furnizorului.

24. Potrivit articolelor 2 și 3 din Legea 2012:278, datele pot fi colectate dacă împrejurările sunt de așa natură încât măsura prezintă o importanță deosebită pentru prevenirea, evitarea sau detectarea unor fapte penale care includ una sau mai multe infracțiuni pentru care pedeapsa este de cel puțin doi ani de închisoare sau una dintre faptele enumerate la articolul 3 (incluzând printre altele diverse forme de sabotaj și spionaj).

25. Decizia de a lua o astfel de măsură revine șefului autorității relevante sau oricărei persoane delegate în acest scop.

26. Decizia trebuie să precizeze faptele penale și perioada în discuție, precum și numărul de telefon, orice altă adresă, echipamentul de comunicații electronice sau zona geografică pe care le vizează. Durata autorizării nu poate fi mai lungă decât este necesar și nu poate, în cazul unei perioade ulterioare deciziei de autorizare, să depășească o lună.

27. Acest tip de măsură nu necesită niciun control prealabil. Totuși, potrivit articolului 6 din Legea 2012:278, Säkerhets och integritetsskyddsnämnden (Comisia pentru Securitate și Protecția Integrității, Suedia) trebuie să fie informată despre orice decizie privind colectarea de date. În conformitate cu articolul 1 din lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Legea 2007:980 privind supravegherea anumitor activități represive), acest organism trebuie să supravegheze aplicarea legii de către autoritățile cărora le revine această responsabilitate.

3. Cu privire la perioada de păstrare a datelor

28. Reiese din dispozițiile articolului 16 d din capitolul 6 din LEK că datele la care se face referire la articolul 16 a din același capitol trebuie să fie păstrate pentru o perioadă de șase luni, calculată de la data finalizării comunicării. Datele trebuie apoi să fie șterse imediat, cu excepția cazului în care articolul 16 d al doilea paragraf (din capitolul 6) din LEK prevede altfel. În conformitate cu această din urmă dispoziție, datele solicitate înainte de expirarea perioadei de păstrare, dar care încă nu au fost predate, trebuie să fie șterse imediat după ce a avut loc predarea lor.

4. Cu privire la protecția și securitatea datelor păstrate

29. Articolul 20 primul paragraf din capitolul 6 din LEK interzice oricărei persoane să transmită sau să utilizeze fără autorizație datele referitoare la comunicații.

30. Potrivit dispozițiilor articolului 3 a din capitolul 6 din LEK, furnizorii trebuie să ia măsurile tehnice și organizatorice adecvate pentru a asigura protejarea datelor păstrate aflate în curs de prelucrare. Din lucrările pregătitoare referitoare la aceste dispoziții rezultă că nu este permis să se stabilească nivelul de protecție prin punerea în balanță a considerațiilor de ordin tehnic, a costurilor și a riscurilor de piratare și de încălcare a confidențialității.

31. Norme suplimentare privind securitatea datelor figurează la articolul 37 din FEK, precum și în instrucțiunile și în orientările generale ale Post- och telestyrelsen (Autoritatea Suedeză de Reglementare a Poștei și Telecomunicațiilor, denumită în continuare „PTS”) referitoare la garanțiile pentru păstrarea și prelucrarea datelor în scopul aplicării legii (PTSFS 2012:4). Din aceste texte reiese printre altele că furnizorii trebuie să ia măsuri pentru protejarea datelor împotriva distrugerii neintenționate sau neautorizate, împotriva stocării, prelucrării, accesării sau divulgării lor neautorizate. Furnizorii trebuie totodată să efectueze operațiuni de securitate cu caracter continuu și sistematic, având în vedere riscurile deosebite legate de obligația de păstrare.

32. În dreptul suedez nu există dispoziții care să reglementeze locul în care trebuie să fie stocate datele.

33. În conformitate cu capitolul 7 din LEK, autoritatea de reglementare poate, în cazul nerespectării de către un furnizor a obligațiilor sale, să ia măsuri de punere în aplicare sau de interdicție, eventual însoțite de penalități, precum și să decidă încetarea totală sau parțială a activității.

C – *Dreptul Regatului Unit*

34. Dispozițiile care reglementează păstrarea datelor se găsesc în Data Retention and Investigatory Powers Act 2014 (Legea din 2014 privind păstrarea datelor și competențele de investigare, denumită în continuare „DRIPA”), în Data Retention Regulations 2014 (SI 2014/2042) (Regulamentul din 2014 privind păstrarea datelor, denumit în continuare „Regulamentul din 2014”), precum și în Retention of Communications Data Code of Practice („Ghidul de bune practici privind păstrarea datelor privind comunicațiile”).

35. Dispozițiile care reglementează accesul la date se găsesc în capitolul 2 din partea I din Regulation of Investigatory Powers Act 2000 (Legea din 2000 privind reglementarea competențelor de investigare, denumită în continuare „RIPA”), în Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480) [Ordinul din 2010 privind reglementarea competențelor de investigare a datelor privind comunicațiile], astfel cum a fost modificat prin Regulation of Investigatory Powers (Communications Data) (Amendement) Order 2015 (SI 2015/228), precum și în Acquisition and Disclosure of Communications Data Code of Practice (Ghidul de bune practici privind obținerea și divulgarea datelor privind comunicațiile, denumit în continuare „Ghidul privind obținerea datelor”).

1. Cu privire la întinderea obligației de păstrare

36. În temeiul articolului 1 din DRIPA, Secretary of State for the Home Department (ministrul de interne, Regatul Unit, denumit în continuare „ministrul”) poate impune furnizorilor o obligație de păstrare a tuturor datelor privind comunicațiile. În esență, această obligație poate privi toate datele generate cu ocazia unei comunicații transmise prin intermediul unui serviciu poștal sau al unui sistem de telecomunicații, cu excepția conținutului comunicației. Aceste date includ printre altele locul în care se află utilizatorul serviciului, precum și datele care permit să se determine adresa IP (protocol internet) sau orice alt identificator care aparține expeditorului sau destinatarului unei comunicații.

37. Scopurile care pot justifica adoptarea unei astfel de măsuri de păstrare includ interesele siguranței naționale, prevenirea sau detectarea infracțiunilor sau prevenirea dezordinii, interesele bunăstării economice a Regatului Unit, în măsura în care aceste interese sunt relevante și pentru interesele siguranței naționale, interesele siguranței publice, protecția sănătății publice, evaluarea sau colectarea oricăror taxe, contribuții sau a altor impozite datorate unei administrații publice, prevenirea, în caz de urgență, a prejudiciilor aduse sănătății fizice sau mentale a unei persoane, sprijinirea anchetelor desfășurate în ceea ce privește presupusele erori judiciare, identificarea unei persoane care a decedat în alt mod decât în urma unei infracțiuni sau care nu poate fi identificată din cauza unei afecțiuni fizice sau psihice, alta decât una care rezultă dintr-o infracțiune (cum ar fi o catastrofă naturală sau un accident), exercitarea funcțiilor referitoare la organizarea serviciilor și a piețelor financiare sau la stabilitatea financiară, precum și orice alt obiectiv stabilit printr-un ordin emis de ministru în temeiul articolului 22 alineatul (2) din DRIPA.

38. Nu există nicio cerință în legislația națională conform căreia emiterea unui act de păstrare trebuie să fie supusă unei autorizări judiciare sau independente prealabile. Ministrul trebuie să se asigure că obligația de păstrare este „necesară și proporțională” pentru unul sau mai multe dintre scopurile pentru care pot fi păstrate datele relevante privind comunicațiile.

2. Cu privire la accesul la datele păstrate

39. Potrivit articolului 22 alineatul (4) din RIPA, autoritățile publice pot, printr-un act, să solicite furnizorilor să le comunice date privind comunicațiile. Forma și conținutul unor astfel de acte sunt reglementate la articolul 23 alineatul (2) din RIPA. Un asemenea act este limitat în timp, conținând dispoziții care reglementează anularea și prelungirea sa.

40. Colectarea datelor privind comunicațiile trebuie să fie necesară și proporțională cu unul sau mai multe dintre scopurile prevăzute la articolul 22 din RIPA, care corespund obiectivelor pentru care pot fi păstrate date menționate la punctul 37 din prezentele concluzii.

41. Reiese din Ghidul privind colectarea datelor că o hotărâre judecătorească este necesară în cazul unei cereri de acces care este formulată în scopul de a identifica sursa folosită de un jurnalist, precum și în cazul cererilor de acces formulate de autoritățile locale.

42. În afara acestor ipoteze, accesul autorităților publice este condiționat de obținerea unei autorizații acordate de persoanele desemnate în acest scop din cadrul autorității publice competente. O persoană desemnată în acest scop este persoana care deține o funcție, un rang sau o poziție în cadrul unei autorități publice competente, care a fost desemnată în scopul colectării de date privind comunicațiile în conformitate cu Ordinul din 2015 privind reglementarea competențelor de investigare a datelor privind comunicațiile, astfel cum a fost modificat.

43. Nicio autorizație judiciară sau a unei entități independente nu este necesară pentru a accesa datele privind comunicațiile protejate de un secret profesional legal sau datele privind comunicațiile referitoare la medici, la membri ai Parlamentului sau la membri ai cultelor religioase. Ghidul privind obținerea datelor precizează doar că trebuie să se acorde o atenție deosebită în ceea ce privește necesitatea și proporționalitatea unei cereri de acces la astfel de date.

3. Cu privire la durata păstrării datelor

44. Articolul 1 alineatul 5 din DRIPA și articolul 4 alineatul 2 din Regulamentul din 2014 prevăd o perioadă maximă de păstrare a datelor de 12 luni. Potrivit ghidului de bune practici privind păstrarea datelor, perioada trebuie să fie strict atât de lungă cât este necesar și proporțional. Articolul 6 din Regulamentul din 2014 impune ca actul de păstrare a datelor să facă obiectul unei examinări din partea ministrului.

4. Cu privire la protecția și securitatea datelor păstrate

45. În conformitate cu articolul 1 din DRIPA, furnizorii nu trebuie să divulge datele păstrate, cu excepția cazului în care acest lucru este în conformitate cu capitolul 2 din partea 1 din RIPA, cu o decizie judecătorească sau cu orice altă autorizație sau mandat judiciar ori cu un regulament adoptat de ministru în conformitate cu articolul 1 din DRIPA.

46. În temeiul articolelor 7 și 8 din Regulamentul din 2014, furnizorii trebuie să asigure integritatea și securitatea datelor păstrate, protecția lor împotriva distrugerii accidentale sau ilegale, pierderii accidentale sau modificării, depozitării, prelucrării, accesării sau divulgării neautorizate sau ilicite, distrugerea datelor, astfel încât să devină imposibilă accesarea lor în cazul în care păstrarea datelor încetează să mai fie autorizată, precum și punerea în aplicare a unor sisteme de securitate. Articolul 9 din Regulamentul din 2014 impune în sarcina Information Commissioner (comisarul pentru informații) obligația de a verifica respectarea acestor obligații de către furnizori.

47. Autoritățile cărora furnizorii le comunică date privind comunicațiile trebuie să prelucreze și să păstreze aceste date, precum și toate copiile, extrasele sau sintezele acestora în siguranță. În conformitate cu ghidul privind obținerea datelor, cerințele cuprinse în Legea privind protecția datelor (Data Protection Act, denumită în continuare „DPA”), care a pus în aplicare Directiva 95/46, trebuie să fie respectate.

48. RIPA instituie un Interception of Communications Commissioner (comisar pentru interceptarea comunicațiilor, denumit în continuare „comisarul pentru interceptare”), a cărui competență este aceea de a supraveghea în mod independent exercitarea și îndeplinirea competențelor și a atribuțiilor prevăzute în capitolul II din partea I din RIPA. Comisarul pentru interceptare nu supraveghează aplicarea articolului 1 din DRIPA. Prevederea se aplică în ceea ce privește rapoartele periodice adresate publicului și Parlamentului [articolul 57 alineatul 2 și articolul 58 din RIPA], precum și în ceea ce privește păstrarea și raportarea înregistrărilor efectuate de autoritățile publice (Ghidul privind obținerea datelor, punctele 6.1-6.8). Plângerile pot fi formulate de asemenea la Investigatory Powers Tribunal (Tribunalul pentru Litigii referitoare la Competențele de Investigare) în cazul în care există convingerea că datele au fost colectate în mod necorespunzător (articolul 65 din RIPA).

49. Reiese din ghidul privind obținerea datelor că comisarul pentru interceptare nu are competența de a trimite o cauză la acest Tribunal, ci poate doar să informeze o persoană în legătură cu presupusa utilizare nelegală a competențelor, în cazul în care acesta poate „stabili că o persoană a fost afectată în mod negativ de o încălcare intenționată sau din culpă”. Totuși, chiar dacă este convins că a existat o încălcare intenționată sau din culpă, comisarul pentru interceptare nu poate să divulge acest lucru în cazul în care siguranța națională ar fi pusă în pericol prin această divulgare.

III – Litigiile principale și întrebările preliminare

A – *Cauza C-203/15*

50. La 9 aprilie 2014, mai exact în ziua următoare datei pronunțării Hotărârii DRI, Tele2 Sverige a notificat PTS decizia sa de a înceta să păstreze datele la care face referire capitolul 6 din LEK. Tele2 Sverige urma totodată să șteargă datele care au fost păstrate anterior în temeiul acestui capitol. Tele2 Sverige considera că legislația suedeză care transpune Directiva 2006/24 nu era conformă cu carta.

51. La 15 aprilie 2014, Rikspolisstyrelsen (Direcția Generală a Poliției Naționale, Suedia, denumită în continuare „RPS”) a sesizat PTS cu o plângere pentru motivul că Tele2Sverige încetase să comunice serviciilor sale datele referitoare la anumite comunicații electronice. În această plângere, RBS arăta că refuzul Tele2 Sverige ar avea consecințe majore asupra activităților represive desfășurate de poliție.

52. Prin decizia din 27 iunie 2014, PTS a impus Tele2 Sverige ca până la 25 iulie 2014 cel târziu să reînceapă să păstreze datele în conformitate cu articolul 16 a din capitolul 6 din LEK și cu articolele 37-43 din FEK.

53. Tele2 Sverige a formulat la Förvaltningsrätten i Stockholm (Tribunalul Administrativ din Stockholm, Suedia) o acțiune împotriva deciziei PTS. Prin hotărârea din 13 octombrie 2014, Förvaltningsrätten i Stockholm a respins această acțiune.

54. Tele2 Sverige a formulat apel împotriva hotărârii pronunțate de Förvaltningsrätten i Stockholm la instanța de trimitere, având ca obiect anularea deciziei contestate.

55. Constatând că există argumente atât în favoarea, cât și împotriva punctului de vedere potrivit căruia o astfel de obligație extinsă de păstrare cum este cea prevăzută la articolul 16 a din capitolul 6 din LEK este compatibilă cu articolul 15 alineatul (1) din Directiva 2002/58, precum și cu articolul 7, articolul 8 și articolul 52 alineatul (1) din cartă, Kammarrätten i Stockholm (Curtea Administrativă de Apel din Stockholm, Suedia) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„1) O obligație generală de păstrare a datelor de transfer care include toate persoanele, toate mijloacele de comunicații electronice și toate datele de transfer fără niciun fel de distincții, limitări sau excepții, în vederea combaterii criminalității [astfel cum este descrisă la punctele 13-18 din cererea de decizie preliminară], este compatibilă cu articolul 15 alineatul (1) din Directiva 2002/58, ținând seama de articolul 7, de articolul 8 și de articolul 52 alineatul (1) din cartă?

2) În cazul unui răspuns negativ la prima întrebare, se poate permite totuși păstrarea atunci când:

a) modul de acces al autorităților naționale la datele păstrate este stabilit astfel cum se arată la punctele 19-36 [din cererea de decizie preliminară] și

b) cerințele de securitate sunt reglementate astfel cum se arată la punctele 38-43 [din cererea de decizie preliminară] și

c) toate datele relevante trebuie să fie păstrate pentru o perioadă de șase luni, calculată de la data la care s-a terminat comunicația, iar ulterior să fie șterse astfel cum se arată la punctul 37 [din cererea de decizie preliminară]?”

B – *Cauza C-698/15*

56. Domnii Watson, Brice și Lewis au formulat la High Court of Justice (England & Wales), Queen’s Bench Division (Administrative Court) [Curtea Supremă de Justiție (Anglia și Țara Galilor), Secția Queen’s Bench (Camera administrativă)], cereri de control jurisdicțional („judicial review”) al legalității regimului de păstrare a datelor prevăzut la articolul 1 din DRIPA, prin care ministrul este abilitat să impună operatorilor de telecomunicații publice păstrarea tuturor datelor privind comunicațiile pentru o perioadă maximă de 12 luni, păstrarea conținutului comunicațiilor respective fiind exclusă.

57. Open Rights Group, Privacy International și Law Society of England and Wales au fost autorizate să intervină în cadrul fiecărei acțiuni.

58. Prin hotărârea din 17 iulie 2015, această instanță a constatat că regimul menționat nu este compatibil cu dreptul Uniunii, în măsura în care nu respectă cerințele stabilite de Hotărârea DRI, considerând că acestea din urmă sunt aplicabile reglementărilor statelor membre în materie de păstrare a datelor privind comunicațiile electronice și de acces la astfel de date. Ministrul a formulat apel împotriva acestei hotărâri la instanța de trimitere.

59. În hotărârea din 20 noiembrie 2015, Court of Appeal (England & Wales) (Civil Division) [Curtea de Apel (Anglia și Țara Galilor) (Secția civilă), Regatul Unit] a apreciat, cu titlu provizoriu, că Hotărârea DRI nu a stabilit cerințe imperative ale dreptului Uniunii pe care legislațiile naționale trebuie să le respecte, ci doar a identificat și a descris garanții care nu figurau în regimul armonizat al Uniunii.

60. Cu toate acestea, considerând că răspunsurile la aceste probleme de drept al Uniunii nu erau clare și erau necesare pentru a se pronunța în cadrul acestor proceduri, Court of Appeal (England & Wales) (Civil Division) [Curtea de Apel (Anglia și Țara Galilor) (Secția civilă), Regatul Unit] a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„1) Hotărârea [DRI] (inclusiv în special punctele 60-62 din aceasta) stabilește cerințe imperative ale dreptului Uniunii aplicabile regimului național al unui stat membru care reglementează accesul la datele păstrate în conformitate cu legislația națională, în vederea respectării articolelor 7 și 8 din [cartă]?

2) Hotărârea [DRI] extinde domeniul de aplicare al articolelor 7 și/sau 8 din cartă dincolo de cel al articolului 8 din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, astfel cum este stabilit în jurisprudența Curții Europene a Drepturilor Omului?”

IV – Procedura în fața Curții

61. Cererile de decizie preliminară au fost înregistrare la grefa Curții la 4 mai 2015 în cauza C-203/15 și la 28 decembrie 2015 în cauza C-698/15.

62. Prin Ordonanța din 1 februarie 2015, Curtea a decis judecarea cauzei C-698/15 potrivit procedurii accelerate prevăzute la articolul 105 alineatul (1) din Regulamentul de procedură al Curții.

63. În cauza C-203/15, au depus observații scrise Tele2 Sverige, guvernele belgian, ceh, danez, german, eston, irlandez, spaniol, francez, maghiar, neerlandez, suedez și al Regatului Unit, pre cum și Comisia Europeană.

64. În cauza C-698/15, au depus observații scrise domnii Watson, Brice și Lewis, Open Rights Group, Privacy International și Law Society of England and Wales, guvernele ceh, danez, german, eston, irlandez, francez, cipriot, polonez, finlandez și al Regatului Unit, precum și Comisia.

65. Prin Decizia Curții din 10 martie 2016, aceste două cauze au fost conexate pentru buna desfășurare a procedurii orale și în vederea pronunțării hotărârii.

66. La ședința de audiere a pledoariilor din 12 aprilie 2016 s-au prezentat pentru a formula observații reprezentanții Tele2 Sverige, ai domnilor Watson, Brice și Lewis, ai Open Rights Group, Privacy International și Law Society of England and Wales, ai guvernelor ceh, danez, german, eston, irlandez, spaniol, francez, finlandez, suedez și al Regatului Unit, precum și ai Comisiei.

V – Analiza întrebărilor preliminare

67. Prin intermediul primei întrebări adresate în cauza C-203/15, instanța de trimitere solicită Curții să stabilească dacă, în lumina Hotărârii DRI, articolul 15 alineatul (1) din Directiva 2002/58, precum și articolul 7, articolul 8 și articolul 52 alineatul (1) din cartă trebuie interpretate în sensul că se opun posibilității unui stat membru de a impune furnizorilor o obligație generală de păstrare a datelor, precum cele în discuție în litigiile principale, indiferent de eventualele garanții care ar însoți această obligație.

68. În cazul unui răspuns negativ la această întrebare, a doua întrebare adresată în cauza C-203/15 și prima întrebare adresată în cauza C-698/15 urmăresc să se stabilească dacă aceste dispoziții trebuie interpretate în sensul că se opun posibilității unui stat membru de a impune furnizorilor o obligație generală de păstrare a datelor în cazul în care această obligație nu este însoțită de ansamblul garanțiilor specificate de Curte la punctele 60-68 din Hotărârea DRI referitoare la accesul la date, la durata de păstrare, precum și la protecția și securitatea datelor.

69. În măsura în care aceste trei întrebări sunt strâns legate, le vom examina împreună în cele ce urmează.

70. În schimb, a doua întrebare adresată în cauza C-698/15 necesită o examinare separată. Prin intermediul acestei întrebări, instanța de trimitere solicită Curții să stabilească dacă Hotărârea DRI a extins domeniul de aplicare al articolelor 7 și/sau 8 din cartă dincolo de cel al articolului 8 din CEDO. Vom arăta în secțiunea următoare motivele pentru care considerăm că această întrebare trebuie respinsă ca inadmisibilă.

71. Înainte de a începe examinarea acestor întrebări, considerăm util să reamintim tipul de date vizate de obligațiile de păstrare în discuție în litigiile principale. Potrivit constatărilor efectuate de instanțele de trimitere, întinderea acestor obligații este în esență echivalentă cu cea a obligației care era prevăzută la articolul 5 din Directiva 2006/24[8]. În mod schematic, datele referitoare la comunicațiile care fac obiectul acestor obligații de păstrare pot fi încadrate în patru categorii[9]:

— datele care permit identificarea atât a sursei, cât și a destinației comunicației;

— datele care permit localizarea atât a sursei, cât și a destinației comunicației;

— datele referitoare la data, ora și durata comunicației și

— datele care permit să se stabilească tipul comunicației și tipul de echipament utilizat.

72. Conținutul comunicațiilor este exclus de la obligațiile generale de păstrare a datelor în discuție în litigiile principale, la fel cum prevedea articolul 5 alineatul (2) din Directiva 2006/24.

A – *Cu privire la admisibilitatea celei de a doua întrebări adresate în cauza C-698/15*

73. Cea de a doua întrebare adresată în cauza C-698/15 invită Curtea să precizeze dacă Hotărârea DRI extinde domeniul de aplicare al articolelor 7 și/sau 8 din cartă dincolo de cel al articolului 8 din CEDO, astfel cum este interpretat de Curtea Europeană a Drepturilor Omului.

74. Această întrebare reflectă în special un argument invocat de ministru în fața instanței de trimitere, potrivit căruia jurisprudența Curții Europene a Drepturilor Omului nu impune, pe de o parte, ca accesul la date să fie condiționat de o autorizare prealabilă a unui organ independent și nici, pe de altă parte, ca păstrarea datelor și accesul la acestea să se limiteze la combaterea infracțiunilor grave.

75. Apreciem că această întrebare trebuie respinsă ca inadmisibilă pentru motivele următoare. În mod evident, motivele și soluția adoptate de Curte în Hotărârea DRI prezintă o importanță decisivă pentru soluționarea litigiilor principale. Totuși, împrejurarea că această hotărâre a extins eventual domeniul de aplicare al articolelor 7 și/sau 8 din cartă dincolo de cel al articolului 8 din CEDO nu este, în sine, relevantă pentru soluționarea acestor litigii.

8 — Această echivalență este de înțeles, având în vedere că regimurile naționale respective urmăreau să transpună directiva menționată, în prezent declarată nevalidă.

9 — A se vedea descrierea regimurilor naționale în discuție în litigiile principale de la punctele 11-13 și 36 din prezentele concluzii.

76. În această privință, trebuie amintit că, în temeiul articolului 6 alineatul (3) TUE, drepturile fundamentale, astfel cum sunt garantate de CEDO, constituie principii generale ale dreptului Uniunii. Totuși, în lipsa aderării Uniunii la convenția menționată, aceasta nu constituie un instrument juridic integrat formal în ordinea juridică a Uniunii [10].

77. Desigur, prima teză a articolul 52 alineatul (3) din cartă prevede o normă de interpretare potrivit căreia, în măsura în care carta conține drepturi ce corespund unor drepturi garantate prin CEDO, „înțelesul și întinderea lor sunt aceleași ca și cele prevăzute de convenția menționată”.

78. Totuși, potrivit celei de a doua teze a articolului 52 alineatul (3) din cartă, „[a]ceastă dispoziție nu împiedică dreptul Uniunii să confere o protecție mai largă”. În opinia noastră, rezultă din această teză că, în cazul în care consideră necesar în contextul dreptului Uniunii, Curtea are posibilitatea să extindă domeniul de aplicare al dispozițiilor cartei dincolo de cel al dispozițiilor corespunzătoare din CEDO.

79. Adăugăm, cu titlu subsidiar, că articolul 8 din cartă, interpretat de Curte în Hotărârea DRI, prevede un drept care nu corespunde niciunui drept garantat prin CEDO, și anume dreptul la protecția datelor cu caracter personal, fapt confirmat, pe de altă parte, de explicațiile referitoare la articolul 52 din cartă [11]. Prin urmare, norma de interpretare prevăzută la articolul 52 alineatul (3) prima teză din cartă nu este, în orice caz, aplicabilă interpretării articolului 8 din cartă, astfel cum au arătat domnii Brice și Lewis, Open Rights Group și Privacy International, Law Society of England and Wales, precum și guvernele ceh, irlandez și finlandez.

80. Rezultă din ceea ce precedă că dreptul Uniunii nu se opune acordării prin articolele 7 și 8 din cartă a unei protecții mai extinse decât cea prevăzută de CEDO. Prin urmare, împrejurarea că Hotărârea DRI a extins eventual domeniul de aplicare al acestor dispoziții din cartă dincolo de cel al articolului 8 din CEDO nu este, în sine, relevantă pentru soluționarea litigiilor principale. Soluția care trebuie dată acestor litigii depinde în esență de condițiile în care o obligație generală de păstrare a datelor poate fi considerată compatibilă cu articolul 15 alineatul (1) din Directiva 2002/58, precum și cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din cartă, interpretate în lumina Hotărârii DRI, aspect care face tocmai obiectul celorlalte trei întrebări adresate în prezentele cauze.

81. Potrivit unei jurisprudențe constante, respingerea unei cereri formulate de o instanță națională este posibilă numai dacă este evident că interpretarea solicitată a dreptului Uniunii nu are nicio legătură cu realitatea sau cu obiectul litigiului principal ori atunci când problema este de natură ipotetică ori Curtea nu dispune de elementele de fapt și de drept necesare pentru a răspunde în mod util la întrebările care i-au fost adresate [12].

82. În speță, pentru motivele prezentate anterior, a doua întrebare adresată în cauza C-698/15 prezintă, în opinia noastră, doar un interes teoretic, având în vedere că un eventual răspuns la această întrebare nu ar permite să se deducă elemente de interpretare a dreptului Uniunii pe care instanța de trimitere ar putea să le aplice în mod util pentru a soluționa, în funcție de dreptul Uniunii, litigiul aflat pe rolul său [13].

10 — Avizul 2/13 din 18 decembrie 2014 (EU:C:2014:2454, punctul 179) și Hotărârea din 15 februarie 2016, N. (C-601/15 PPU, EU:C:2016:84, punctul 45 și jurisprudența citată).

11 — În conformitate cu articolul 6 alineatul (1) al treilea paragraf TUE și cu articolul 52 alineatul (7) din cartă, explicațiile referitoare la cartă trebuie luate în considerare în vederea interpretării acesteia (a se vedea Hotărârea din 26 februarie 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, punctul 20), și Hotărârea din 15 februarie 2016, N. (C-601/15 PPU, EU:C:2016:84, punctul 47). Potrivit acestor explicații, articolul 7 din cartă corespunde articolului 8 din CEDO, în timp ce articolul 8 din cartă nu corespunde niciunui drept din CEDO.

12 — A se vedea printre altele Hotărârea din 9 noiembrie 2010, Volker und Markus Schecke și Eifert (C-92/09 și C-93/09, EU:C:2010:662, punctul 40 și jurisprudența citată), precum și Hotărârea din 24 aprilie 2012, Kamberaj (C-571/10, EU:C:2012:233, punctul 42 și jurisprudența citată).

13 — A se vedea printre altele Hotărârea din 16 septembrie 1982, Vlaeminck (132/81, EU:C:1982:294, punctul 13), Ordonanța din 24 martie 2011, Abt și alții (C-194/10, EU:C:2011:182, punctele 36 și 37, precum și jurisprudența citată), și Hotărârea din 24 octombrie 2013, Stoilov i Ko (C-180/12, EU:C:2013:693, punctul 46 și jurisprudența citată).

83. În aceste condiții, considerăm că întrebarea menționată trebuie respinsă ca fiind inadmisibilă, astfel cum au arătat în mod întemeiat domnul Watson, Law Society of England and Wales și guvernul ceh.

B – *Cu privire la compatibilitatea unei obligații generale de păstrare a datelor cu regimul prevăzut de Directiva 2002/58*

84. Prezenta secțiune privește posibilitatea statelor membre de a utiliza opțiunea conferită la articolul 15 alineatul (1) din Directiva 2002/58 pentru a impune o obligație generală de păstrare a datelor. În schimb, aceasta nu examinează cerințele specifice care trebuie respectate de statele membre care doresc să utilizeze această opțiune, care vor fi analizate pe larg într-o secțiune ulterioară [14].

85. Astfel, Open Rights Group și Privacy International au susținut că o astfel de obligație ar fi incompatibilă cu regimul armonizat prevăzut de Directiva 2002/58, independent de respectarea cerințelor care decurg din articolul 15 alineatul (1) din Directiva 2002/58, pentru motivul că ar anula esența drepturilor și a regimului prevăzute de această directivă.

86. Înainte de a examina acest argument, este necesar să se verifice dacă o obligație generală de păstrare a datelor intră în domeniul de aplicare al acestei directive.

1. Cu privire la includerea unei obligații generale de păstrare a datelor în domeniul de aplicare al Directivei 2002/58

87. Niciuna dintre părțile care au prezentat observații Curții nu a contestat faptul că o obligație generală de păstrare a datelor, precum cele în discuție în litigiile principale, intră în noțiunea „prelucr[are] de date personale legate de furnizarea de servicii de comunicații electronice prin intermediul rețelelor de comunicații electronice din cadrul [Uniunii]” în sensul articolului 3 din Directiva 2002/58.

88. Totuși, guvernele ceh, francez, polonez și al Regatului Unit au susținut că o obligație generală de păstrare a datelor intră sub incidența excluderii prevăzute la articolul 1 alineatul (3) din Directiva 2002/58. Pe de o parte, dispozițiile naționale care reglementează accesul la date și utilizarea acestora de către autoritățile de poliție sau judiciare ale statelor membre ar privi siguranța publică, apărarea sau siguranța statului sau cel puțin ar face parte din dreptul penal. Pe de altă parte, singurul obiectiv al păstrării datelor ar fi de a permite acestor autorități de poliție sau judiciare să aibă acces la acestea și să le utilizeze. Prin urmare, o obligație de păstrare a datelor ar fi exclusă din domeniul de aplicare al acestei directive în temeiul dispoziției citate anterior.

89. Acest raționament nu ni se pare convingător, pentru motivele următoare.

90. În primul rând, modul de redactare a articolului 15 alineatul (1) din Directiva 2002/58 confirmă că obligațiile de păstrare impuse de statele membre intră în domeniul de aplicare al acestei directive. Astfel, potrivit acestei dispoziții, „statele membre pot adopta, *inter alia*, măsuri legislative care să permită reținerea de date, pe perioadă limitată, pentru motivele arătate anterior în acest alineat”. Ni se pare cel puțin dificil să se susțină că obligațiile de păstrare sunt excluse din domeniul de aplicare al acestei directive, în măsura în care chiar articolul 15 alineatul (1) din directiva menționată reglementează posibilitatea de a adopta astfel de obligații.

14 — A se vedea punctele 126-262 din prezentele concluzii.

91. În realitate, astfel cum au susținut domnul Watson, domnii Brice și Lewis, guvernele belgian, danez, german, finlandez, precum și Comisia, o obligație generală de păstrare a datelor, precum cele în discuție în litigiile principale, constituie o punere în aplicare a articolului 15 alineatul (1) din Directiva 2002/58.

92. În al doilea rând, faptul că dispozițiile care reglementează accesul pot intra sub incidența excluderii prevăzute la articolul 1 alineatul (3) din Directiva 2002/58 [15] nu presupune că obligația de păstrare intră de asemenea sub incidența acesteia și că, prin urmare, se situează în afara domeniului de aplicare al acestei directive.

93. În această privință, Curtea a avut deja ocazia de a preciza că activitățile menționate la articolul 3 alineatul (2) prima liniuță din Directiva 95/46/CE [16], al cărui text are un domeniu de aplicare echivalent cu cel al articolului 1 alineatul (3) din Directiva 2002/58, sunt activități proprii statelor sau autorităților statale, străine de domeniile de activitate ale particularilor [17].

94. Or, obligațiile de păstrare în discuție în litigiile principale sunt impuse unor operatori privați în cadrul unor activități private de furnizare de servicii de comunicații electronice, astfel cum a arătat Comisia. În plus, aceste obligații sunt impuse independent de orice cerere de acces din partea autorităților de poliție sau judiciare, precum și, mai general, independent de orice act al autorităților statale legat de siguranța publică, de apărare, de siguranța statului sau de dreptul penal.

95. În al treilea rând, soluția adoptată de Curte în Hotărârea Irlanda/Parlamentul și Consiliul confirmă că o obligație generală de păstrare a datelor nu face parte din domeniul penal [18]. Astfel, Curtea a statuat că Directiva 2006/24, care prevedea o astfel de obligație, nu făcea parte din domeniul penal, ci viza funcționarea pieței interne, astfel încât articolul 95 CE (devenit articolul 114 TFUE) constituia temeiul juridic adecvat pentru adoptarea acestei directive.

96. Pentru a ajunge la această concluzie, Curtea a constatat printre altele că dispozițiile acestei directive se limitau în esență la activitățile furnizorilor de servicii și nu reglementau nici accesul la date și nici exploatarea acestora de către autoritățile de poliție sau judiciare ale statelor membre [19]. Deducem din aceasta că nici dispozițiile de drept intern care prevăd o obligație de păstrare similară celei prevăzute de Directiva 2006/24 nu fac parte din domeniul penal.

97. Având în vedere cele ce precedă, considerăm că o obligație generală de păstrare a datelor nu intră sub incidența excluderii prevăzute la articolul 1 alineatul (3) din Directiva 2002/58 și, prin urmare, intră în domeniul de aplicare al acestei directive.

2. Cu privire la posibilitatea de a deroga de la regimul prevăzut de Directiva 2002/58 prin stabilirea unei obligații generale de păstrare a datelor

98. Trebuie să se stabilească în continuare dacă o obligație generală de păstrare a datelor este compatibilă cu regimul prevăzut de Directiva 2002/58.

99. Problema care se ridică cu privire la acest aspect este aceea dacă un stat membru poate utiliza opțiunea conferită la articolul 15 alineatul (1) din Directiva 2002/58 pentru a impune o astfel de obligație.

15 — A se vedea punctele 123-125 din prezentele concluzii.

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).

17 — Hotărârea din 6 noiembrie 2003, Lindqvist (C-101/01, EU:C:2003:596, punctele 43 și 44).

18 — Hotărârea din 10 februarie 2009 (C-301/06, EU:C:2009:68).

19 — Hotărârea din 10 februarie 2009, Irlanda/Parlamentul și Consiliul (C-301/06, EU:C:2009:68, punctul 80).

100. Au fost invocate patru argumente împotriva unei astfel de posibilități, în special de Open Rights Group și Privacy International.

101. Potrivit unui prim argument, acordarea în favoarea statelor membre a competenței de a adopta o obligație generală de păstrare a datelor ar repune în discuție obiectivul de armonizare care constituie rațiunea de a fi a Directivei 2002/58. Astfel, în conformitate cu articolul 1 alineatul (1), această directivă prevede armonizarea dispozițiilor naționale, lucru necesar în vederea asigurării unui nivel echivalent de protecție a drepturilor și a libertăților fundamentale, în special a dreptului la confidențialitate și la respectarea vieții private, în domeniul prelucrării de date cu caracter personal în sectorul comunicațiilor electronice și al asigurării liberei circulații a acestor date și a serviciilor și echipamentelor de comunicații electronice în interiorul Uniunii.

102. Astfel, articolul 15 alineatul (1) din Directiva 2002/58 nu ar putea fi interpretat în sensul că ar conferi statelor membre competența de a adopta o derogare de la regimul prevăzut de această directivă de o asemenea amploare încât acest efort de armonizare ar fi privat de orice efect util.

103. Potrivit unui al doilea argument, modul de redactare a articolului 15 alineatul (1) din Directiva 2002/58 s-ar opune de asemenea unei interpretări atât de largi a posibilității statelor membre de a deroga de la regimul prevăzut de această directivă. Astfel, potrivit acestei dispoziții, „[s]tatele membre pot adopta măsuri legislative pentru a *restrânge sfera de aplicare* a drepturilor și obligațiilor prevăzute la articolul 5, articolul 6, articolul 8 alineatele (1), (2), (3) și (4) și articolul 9 ale [acestei] directive” (sublinierea noastră).

104. Or, o obligație generală de păstrare a datelor nu s-ar limita la a „restrânge sfera de aplicare” a drepturilor și a obligațiilor menționate de această dispoziție, ci ar anula complet aceste drepturi și obligații. Situația ar fi aceasta pentru:

— obligația de a asigura confidențialitatea datelor de transfer și obligația de a solicita acordul utilizatorului pentru stocarea informațiilor, prevăzute la articolul 5 alineatul (1) și, respectiv, alineatul (3) din Directiva 2002/58,

— obligația de a șterge sau de a trece în anonimat datele de transfer, prevăzută la articolul 6 alineatul (1) din această directivă și

— obligația de a trece în anonimat datele de localizare sau de a obține acordul utilizatorului pentru prelucrarea acestor date, impusă la articolul 9 alineatul (1) din directiva menționată.

105. Considerăm că aceste două prime argumente trebuie respinse, pentru motivele următoare.

106. Pe de o parte, modul de redactare a articolului 15 alineatul (1) din Directiva 2002/58 evocă posibilitatea statelor membre de a adopta „măsuri legislative care să permită reținerea de date, pe perioadă limitată”. Această referire explicită la obligațiile de păstrare a datelor confirmă că astfel de obligații nu sunt în sine incompatibile cu regimul prevăzut de Directiva 2002/58. Deși această formulare nu prevede în mod expres posibilitatea de a adopta o obligație *generală* de păstrare a datelor, trebuie să se constate că nici nu se opune acesteia.

107. Pe de altă parte, considerentul (11) al Directivei 2002/58 precizează că aceasta nu aduce atingere „echilibrului existent între dreptul indivizilor la confidențialitate și posibilitatea ca statele membre să ia măsurile stipulate la articolul 15 alineatul (1) al [acestei] directive, posibilitate necesară în vederea protejării siguranței publice, a apărării și a siguranței statului (inclusiv a bunăstării economice a acestuia, în cazul în care activitățile respective sunt legate de chestiuni de siguranța statului) și a întăririi legii penale”. În consecință, „directiv[a] [menționată] nu interzice statelor membre să efectueze interceptări legale ale comunicațiilor electronice sau să ia alte măsuri pentru atingerea scopurilor menționate anterior, dacă acest lucru este necesar și în conformitate cu [CEDO]”.

108. Rezultă, în opinia noastră, din acest considerent (11) că intenția legiuitorului Uniunii nu a fost de a aduce atingere posibilității statelor membre de a adopta măsurile prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, ci de a condiționa această posibilitate de anumite cerințe care privesc în special scopurile urmărite și proporționalitatea acestor măsuri. Cu alte cuvinte, o obligație generală de păstrare a datelor nu este, în opinia noastră, incompatibilă cu regimul prevăzut de această directivă, cu condiția ca aceasta să respecte anumite condiții.

109. Potrivit unui al treilea argument, articolul 15 alineatul (1) din Directiva 2002/58, constituind o excepție de la regimul prevăzut de această directivă, ar trebui, în temeiul unei norme de interpretare care rezultă dintr-o jurisprudență constantă a Curții, să fie de strictă interpretare. Această normă de interpretare strictă ar interzice interpretarea acestei dispoziții în sensul că ar conferi posibilitatea de a impune o obligație generală de păstrare a datelor.

110. Cu privire la acest aspect, avem sentimentul că posibilitatea prevăzută la articolul 15 alineatul (1) din Directiva 2002/58 nu poate fi calificată drept excepție și, în consecință, nu poate fi interpretată strict, astfel cum a susținut în mod întemeiat Comisia. Astfel, ni se pare dificil ca această posibilitate să fie calificată drept excepție, având în vedere considerentul (11) menționat mai sus, potrivit căruia această directivă nu aduce atingere posibilității statelor membre de a adopta măsurile prevăzute de această dispoziție. Subliniem, pe de altă parte, că articolul 15 din directiva menționată este intitulat „Aplicarea anumitor dispoziții ale Directivei 95/46”, în timp ce articolul 10 din aceeași directivă este intitulat în mod explicit „Excepții”. Aceste titluri ne întăresc convingerea că posibilitatea prevăzută la articolul 15 menționat nu poate fi calificată drept „excepție”.

111. Potrivit unui al patrulea și ultim argument, incompatibilitatea unei obligații generale de păstrare a datelor cu regimul prevăzut de Directiva 2002/58 ar fi confirmată de adăugarea articolului 15 alineatul (1a) din această directivă prin adoptarea Directivei 2006/24, declarată nevalidă de Hotărârea DRI. În temeiul acestui argument, această incompatibilitate este cea care ar fi determinat legiuitorul Uniunii să declare că articolul 15 alineatul (1) din Directiva 2002/58 nu este aplicabil regimului de păstrare generală prevăzut de Directiva 2006/24.

112. Acest argument pare a decurge dintr-o înțelegere eronată a sensului articolului 15 alineatul (1a) din Directiva 2002/58. Potrivit acestei dispoziții, „[articolul 15 alineatul (1) din Directiva 2002/58] nu se aplică datelor solicitate în mod specific de Directiva [2006/24] pentru a fi păstrate în scopurile menționate la articolul 1 alineatul (1) din această directivă”.

113. Interpretarea noastră referitoare la această dispoziție este următoarea. În ceea ce privește datele a căror păstrare era impusă de Directiva 2006/24, în scopurile prevăzute de aceasta, statele membre pierdeau posibilitatea, prevăzută la articolul 15 alineatul (1) din Directiva 2002/58, de a restrânge mai mult sfera de aplicare a drepturilor și obligațiilor prevăzute de această dispoziție, în special prin intermediul unor obligații suplimentare de păstrare a datelor. Altfel spus, articolul 15 alineatul (1a) prevedea o armonizare exhaustivă în ceea ce privește datele a căror păstrare era impusă de Directiva 2006/24, în scopurile prevăzute de aceasta.

114. Considerăm că această interpretare este confirmată de considerentul (12) al Directivei 2006/24, potrivit căruia „articolul 15 alineatul (1) din Directiva [2002/58] *se aplică în continuare* datelor, inclusiv datele referitoare la încercări nereușite de apeluri telefonice, date a căror păstrare nu este cerută în mod specific în temeiul prezentei directive și *care, prin urmare, nu fac parte din domeniul de aplicare al acesteia*, precum și păstrării acestora *în scopuri*, inclusiv judiciare, *altele decât cele reglementate de prezenta directivă*” (sublinierea noastră).

115. Astfel, introducerea articolului 15 alineatul (1a) din Directiva 2002/58 nu atestă incompatibilitatea unei obligații generale de păstrare a datelor cu regimul prevăzut de această directivă, ci voința legiuitorului Uniunii de a efectua o armonizare exhaustivă prin adoptarea Directivei 2006/24.

116. Având în vedere ceea ce precedă, considerăm că o obligație generală de păstrare a datelor este compatibilă cu regimul prevăzut de Directiva 2002/58 și, prin urmare, că un stat membru poate utiliza opțiunea conferită la articolul 15 alineatul (1) din această directivă pentru a impune o astfel de obligație [20]. Totuși, recurgerea la această posibilitate este condiționată de respectarea unor cerințe stricte, care decurg nu numai din această dispoziție, ci și din dispozițiile relevante ale cartei interpretate în lumina Hotărârii DRI și care vor fi examinate într-o secțiune ulterioară [21].

C – *Cu privire la aplicabilitatea cartei în privința unei obligații generale de păstrare a datelor*

117. Înainte de a examina conținutul cerințelor impuse de cartă, în coroborare cu articolul 15 alineatul (1) din Directiva 2002/58, atunci când un stat optează pentru instituirea unei obligații generale de păstrare a datelor, trebuie să se verifice dacă carta este aplicabilă unei astfel de obligații.

118. Aplicabilitatea cartei în privința unei obligații generale de păstrare a datelor depinde în esență de aplicabilitatea Directivei 2002/58 în privința unei astfel de obligații.

119. Astfel, potrivit articolului 51 alineatul (1) prima teză din aceasta, „dispozițiile [cartei] se adresează statelor membre numai în cazul în care aceste state pun în aplicare dreptul Uniunii”. Explicațiile referitoare la articolul 51 din cartă fac trimitere, în această privință, la jurisprudența Curții, potrivit căreia statelor membre le este impusă obligația de a respecta drepturile fundamentale definite în cadrul Uniunii numai în cazul în care pun în aplicare dreptul Uniunii [22].

120. Guvernele ceh, francez, polonez și al Regatului Unit, care au contestat aplicabilitatea Directivei 2002/58 în privința unei obligații generale de păstrare a datelor [23], au susținut de asemenea că carta nu este aplicabilă unei astfel de obligații.

121. Am prezentat deja motivele pentru care considerăm că o obligație generală de păstrare a datelor constituie o punere în aplicare a posibilității prevăzute la articolul 15 alineatul (1) din Directiva 2002/58 [24].

122. În consecință, considerăm că dispozițiile cartei sunt aplicabile măsurilor naționale prin care se instituie o astfel de obligație, în conformitate cu articolul 51 alineatul (1) din cartă, astfel cum au arătat domnul Watson, domnii Brice și Lewis, Open Rights Group și Privacy International, guvernele danez, german, finlandez, precum și Comisia [25].

20 — Dat fiind că Directiva 2002/58 poate fi calificată drept „*lex specialis*” în raport cu Directiva 95/46 [a se vedea în această privință articolul 1 alineatul (2) din Directiva 2002/58], nu considerăm necesară verificarea compatibilității unei obligații generale de păstrare a datelor cu regimul prevăzut de Directiva 95/46, care, de altfel, nu face obiectul întrebărilor adresate Curții. Din motive de exhaustivitate, dorim totuși să precizăm că modul de redactare a articolului 13 alineatul (1) din Directiva 95/46 oferă statelor membre o marjă de decizie mai largă decât cea conferită de articolul 15 alineatul (1) din Directiva 2002/58, care precizează sfera de aplicare a acesteia în cadrul furnizării de servicii de comunicații electronice accesibile publicului. Având în vedere că posibilitatea prevăzută la articolul 15 alineatul (1) din Directiva 2002/58 permite unui stat membru să adopte o obligație generală de păstrare a datelor, deducem din aceasta că articolul 13 alineatul (1) din Directiva 95/46 permite de asemenea acest lucru.

21 — A se vedea punctele 126-262 din prezentele concluzii.

22 — Rezultă, astfel, dintr-o jurisprudență constantă a Curții că drepturile fundamentale garantate de ordinea juridică a Uniunii au vocația de a fi aplicate în toate situațiile reglementate de dreptul Uniunii, însă nu în afara unor asemenea situații. În această măsură, Curtea a amintit deja că nu poate aprecia, din perspectiva cartei, o reglementare națională care nu se situează în cadrul dreptului Uniunii. În schimb, de îndată ce o asemenea reglementare intră în domeniul de aplicare al acestui drept, Curtea, sesizată cu titlu preliminar, trebuie să furnizeze toate elementele de interpretare necesare aprecierii de către instanța națională a conformității acestei reglementări cu drepturile fundamentale a căror respectare o asigură (a se vedea Hotărârea din 26 februarie 2013, Åkerberg Fransson, EU:C:2013:105, C-617/10, punctul 19 și jurisprudența citată).

23 — A se vedea punctul 88 din prezentele concluzii.

24 — A se vedea punctele 90-97 din prezentele concluzii.

25 — Mai precis, articolul 51 alineatul (1) a doua teză din cartă prevede că statele membre trebuie să respecte drepturile garantate de aceasta în cazul în care pun în aplicare dreptul Uniunii.

123. Această concluzie nu este repusă în discuție de faptul că dispozițiile naționale care reglementează accesul la datele păstrate nu intră, ca atare, în domeniul de aplicare al cartei.

124. Desigur, în măsura în care acestea privesc „activități[e] statului în domeniul legii penale", dispozițiile naționale care reglementează accesul la datele păstrate de autoritățile de poliție și judiciare în vederea combaterii infracțiunilor grave intră, în opinia noastră, sub incidența excluderii prevăzute la articolul 1 alineatul (3) din Directiva 2002/58 [26]. În consecință, asemenea dispoziții naționale nu pun în aplicare dreptul Uniunii, astfel încât carta nu le este aplicabilă.

125. Cu toate acestea, rațiunea de a fi a unei obligații de păstrare a datelor este de a permite autorităților represive să aibă acces la datele păstrate, astfel încât problematica păstrării și cea a accesului nu pot fi complet disociate. Astfel cum a subliniat în mod întemeiat Comisia, dispozițiile care reglementează accesul prezintă o importanță decisivă pentru a aprecia compatibilitatea cu carta a dispozițiilor care instituie o obligație generală de păstrare a datelor, care pun în aplicare articolul 15 alineatul (1) din Directiva 2002/58. Mai precis, dispozițiile care reglementează accesul trebuie luate în considerare în vederea aprecierii necesității și a proporționalității unei astfel de obligații [27].

D – *Cu privire la compatibilitatea unei obligații generale de păstrare a datelor cu cerințele prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, precum și la articolul 7, la articolul 8 și la articolul 52 alineatul (1) din cartă*

126. Rămâne să abordăm, în continuare, problema dificilă a compatibilității unei obligații generale de păstrare a datelor cu cerințele prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, precum și la articolul 7, la articolul 8 și la articolul 52 alineatul (1) din cartă, interpretate în lumina Hotărârii DRI. Acest aspect privește, într-un mod mai general, adaptarea necesară a cadrului legal care reglementează capacitățile de monitorizare ale statelor membre, care au fost multiplicate de progresele tehnologice recente [28].

127. În acest context, prima etapă a oricărei analize rezidă în constatarea ingerinței în drepturile consacrate de Directiva 2002/58 și în drepturile fundamentale consacrate la articolele 7 și 8 din cartă.

128. Astfel, o asemenea obligație constituie o ingerință gravă în dreptul la respectarea vieții private, consacrat la articolul 7 din cartă, și în dreptul la protecția datelor cu caracter personal, garantat la articolul 8 din cartă. Nu considerăm util să insistăm asupra acestei constatări a ingerinței, care a fost formulată cu claritate de Curte la punctele 32-37 din Hotărârea DRI [29]. În același mod, o obligație generală de păstrare a datelor constituie o ingerință în mai multe drepturi consacrate de Directiva 2002/58 [30].

129. A doua etapă a analizei constă în a se stabili dacă și în ce condiții poate fi justificată această ingerință gravă în drepturile consacrate de Directiva 2002/58, precum și în drepturile fundamentale consacrate la articolele 7 și 8 din cartă.

26 — Cu privire la domeniul de aplicare al acestei excluderi, a se vedea punctele 90-97 din prezentele concluzii.

27 — A se vedea punctele 185-262 din prezentele concluzii.

28 — A se vedea printre altele Consiliul Organizației Națiunilor Unite pentru drepturile omului, Raportul raportorului special privind promovarea și protecția dreptului la libertatea de opinie și de exprimare, 17 aprilie 2013, A/HRC/23/40, nr. 33: „Progresele tehnologice permit statului să se angajeze în activități de monitorizare care nu mai sunt limitate de criterii de amploare sau de durată. […] În consecință, statul dispune în prezent mai mult ca oricând de mijloace extinse pentru a desfășura actvități de monitorizare simultane, care atentează la viața privată, direcționate și la scară largă. […]". A se vedea de asemenea nr. 50: „În general, legislația nu a urmat ritmul modificărilor tehnologice. În cea mai mare parte a statelor, normele juridice sunt fie inexistente, fie inadecvate pentru a face față condițiilor moderne de monitorizare a comunicațiilor. […]"

29 — Vom reveni totuși asupra riscurilor specifice generate de constituirea unor baze de date de o asemenea amploare în cadrul cerinței privind proporționalitatea, într-o societate democratică, a unei obligații generale de păstrare a datelor precum cele în discuție în litigiile principale: a se vedea punctele 252-261 din prezentele concluzii.

30 — A se vedea cu privire la acest aspect argumentul invocat de Open Rights Group și Privacy International, rezumat la punctul 104 din prezentele concluzii.

130. Două dispoziții prevăd condițiile care trebuie îndeplinite pentru ca această dublă ingerință să fie justificată: articolul 15 alineatul (1) din Directiva 2002/58, care reglementează posibilitatea statelor membre de a restrânge sfera de aplicare a anumitor drepturi prevăzute de această directivă, și articolul 52 alineatul (1) din cartă, interpretat în lumina Hotărârii DRI, care reglementează orice restrângere a exercițiului drepturilor consacrate de cartă.

131. Dorim să subliniem că aceste cerințe sunt *cumulative*. Astfel, respectarea cerințelor prevăzute la articolul 15 alineatul (1) din Directiva 2002/58 nu implică, în sine, că cerințele prevăzute la articolul 52 alineatul (1) din cartă sunt îndeplinite și invers [31]. În consecință, o obligație generală de păstrare a datelor va putea fi considerată compatibilă cu dreptul Uniunii doar dacă respectă atât cerințele prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, cât și pe cele prevăzute la articolul 52 alineatul (1) din cartă, astfel cum a subliniat Law Society of England and Wales [32].

132. Împreună, aceste două dispoziții prevăd șase cerințe care trebuie respectate pentru ca ingerința cauzată de o obligație generală de păstrare a datelor să fie justificată:

— obligația de păstrare trebuie să aibă un temei legal;

— trebuie să respecte substanța drepturilor consacrate de cartă;

— trebuie să urmărească un obiectiv de interes general;

— trebuie să fie adecvată urmăririi acestui obiectiv;

— trebuie să fie necesară pentru urmărirea obiectivului menționat și

— trebuie să fie proporțională, în cadrul unei societăți democratice, în raport cu urmărirea aceluiași obiectiv.

133. Mai multe dintre aceste condiții au fost deja evocate de Curte în Hotărârea DRI. Din motive de claritate și ținând seama de particularitățile prezentelor cauze în raport cu cauza DRI, dorim totuși să revenim asupra fiecăreia dintre ele, examinând mai detaliat cerințele referitoare la temeiul legal, la caracterul necesar, precum și la caracterul proporțional în cadrul unei societăți democratice al unei obligații generale de păstrare a datelor.

1. Cu privire la cerința unui temei legal în dreptul intern

134. Atât articolul 52 alineatul (1) din cartă, cât și articolul 15 alineatul (1) din Directiva 2002/58 prevăd cerințe cu privire la temeiul legal care trebuie utilizat de un stat membru în vederea adoptării unei obligații generale de păstrare a datelor.

135. În primul rând, orice restrângere a exercitării drepturilor recunoscute de cartă trebuie să fie „prevăzută de lege” în temeiul articolului 52 alineatul (1). Precizăm că această cerință nu a fost examinată în mod formal de Curte în Hotărârea DRI, care privea o ingerință prevăzută de o directivă.

31 — Găsim confirmarea acestei naturi cumulative în ultima teză a articolului 15 alineatul (1) din Directiva 2002/58, potrivit căreia „[t]oate măsurile menționate în acest alineat trebuie să fie conforme cu principiile generale ale legislației comunitare, inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) [TUE]”. În temeiul articolului 6 alineatul (1) TUE, „Uniunea recunoaște drepturile, libertățile și principiile prevăzute în [cartă], care are aceeași valoare juridică cu cea a tratatelor”.

32 — Rezultă în mod logic din această natură cumulativă că, în măsura în care cerințele prevăzute de aceste două dispoziții se suprapun, se impune aplicarea cerinței celei mai stricte sau, altfel spus, a cerinței care protejează cel mai bine drepturile respective.

136. Până la recenta Hotărâre WebMindLicenses [33], Curtea nu se pronunțase niciodată cu privire la domeniul exact de aplicare al acestei cerințe, nici măcar când constatase în mod expres că această cerință era [34] sau nu era [35] îndeplinită. La punctul 81 din această hotărâre, Camera a treia a Curții s-a pronunțat după cum urmează:

„În această privință, trebuie subliniat că cerința potrivit căreia orice restrângere a exercitării acestui drept trebuie să fie prevăzută de lege presupune ca temeiul juridic care permite utilizarea probelor menționate la punctul anterior de administrația fiscală să fie suficient de clar și de precis și ca, prin faptul că definește ea însăși întinderea restrângerii exercitării dreptului garantat de articolul 7 din cartă, aceasta să ofere o anumită protecție împotriva eventualelor atingeri arbitrare din partea respectivei administrații (a se vedea în special Curtea Europeană a Drepturilor Omului, Hotărârea Malone împotriva Regatului Unit din 2 august 1984, seria A nr. 82, § 67, precum și Hotărârea Gillan și Quinton împotriva Regatului Unit din 12 ianuarie 2010, nr. 4158/05, § 77, CEDO 2010)”.

137. Invităm Marea Cameră a Curții să confirme această interpretare în prezentele cauze, pentru motivele următoare.

138. Astfel cum a arătat în mod întemeiat avocatul general Cruz Villalón în Concluziile prezentate în cauza Scarlet Extended [36], Curtea Europeană a Drepturilor Omului a elaborat o bogată jurisprudență referitoare la această cerință în contextul CEDO, care se caracterizează printr-o accepțiune materială, iar nu formală, a termenului „lege” [37].

139. Potrivit acestei jurisprudențe, expresia „prevăzută de lege” presupune ca temeiul legal să fie suficient de accesibil și de previzibil, adică formulat cu destulă precizie pentru a permite individului – apelând la nevoie la consiliere adecvată – să își ajusteze conduita. Acest temei legal trebuie de asemenea să furnizeze o protecție corespunzătoare împotriva arbitrarului și, în consecință, să definească cu suficientă claritate întinderea și modalitățile de exercitare a puterii conferite autorităților competente (principiul preeminenței dreptului) [38].

140. Or, în opinia noastră, este necesar ca expresiei „prevăzută de lege”, utilizată la articolul 52 alineatul (1) din cartă, să i se atribuie un domeniu de aplicare similar celui pe care îl implică această expresie în contextul CEDO, pentru motivele următoare.

33 — Hotărârea din 17 decembrie 2015 (C-419/14, EU:C:2015:832).

34 — A se vedea printre altele Hotărârea din 17 octombrie 2013, Schwarz (C-291/12, EU:C:2013:670, punctul 35) (ingerință prevăzută de un regulament european), Hotărârea din 27 mai, Spasic (C-129/14 PPU, EU:C:2014:586, punctul 57) (ingerință prevăzută de Convenția de punere în aplicare a Acordului Schengen din 14 iunie 1985 între guvernele statelor Uniunii Economice Benelux, Republicii Federale Germania și Republicii Franceze privind eliminarea treptată a controalelor la frontierele comune, semnată la Schengen la 19 iunie 1990 și intrată în vigoare la 26 martie 1995), Hotărârea din 6 octombrie 2015, Delvigne (C-650/13, EU:C:2015:648, punctul 47) (ingerință prevăzută de Codul electoral și de Codul penal francez), și Hotărârea din 17 decembrie 2015, Neptune Distribution (C-157/14, EU:C:2015:823, punctul 69) (ingerință prevăzută de un regulament și de o directivă europeană).

35 — Hotărârea din 1 iulie 2010, Knauf Gips/Commisia (C-407/08 P, EU:C:2010:389, punctele 87-92) (ingerință lipsită de temei legal).

36 — C-70/10, EU:C:2011:255, punctele 94-100.

37 — A se vedea printre altele Curtea Europeană a Drepturilor Omului, Hotărârea Sanoma Uitgevers B. V. împotriva Țărilor de Jos din 14 septembrie 2010, CE:ECHR:2010:0914JUD003822403, § 83.

38 — A se vedea printre altele Curtea Europeană a Drepturilor Omului, Hotărârea din 26 martie 1987, Leander împotriva Suediei, CE:ECHR:1987:0326JUD000924881, § 50 și 51, Curtea Europeană a Drepturilor Omului, Hotărârea Hassan și Tchaouch împotriva Bulgariei din 26 octombrie 2000, CE:ECHR:2000:1026JUD003098596, § 84, Curtea Europeană a Drepturilor Omului, Hotărârea S. și Marper împotriva Regatului Unit din 4 decembrie 2008, CE:ECHR:2008:1204JUD003056204, § 95, Curtea Europeană a Drepturilor Omului, Hotărârea Sanoma Uitgevers B. V. împotriva Țărilor de Jos din 14 septembrie 2010, CE:ECHR:2010:0914JUD003822403, § 81-83, Curtea Europeană a Drepturilor Omului, Hotărârea Stoyanov și alții împotriva Bulgariei din 31 martie 2016, CE:ECHR:2016:0331JUD005538810, § 124-126.

141. Pe de o parte, în temeiul articolului 53 din cartă și al explicațiilor referitoare la acest articol, nivelul de protecție oferit de cartă nu poate fi niciodată inferior celui garantat de CEDO. Această interdicție de a depăși „pragul CEDO” presupune ca interpretarea de către Curte a expresiei „prevăzută de lege” utilizată la articolul 52 alineatul (1) din cartă trebuie să fie cel puțin la fel de strictă precum cea a Curții Europene a Drepturilor Omului în contextul CEDO [39].

142. Pe de altă parte, având în vedere natura orizontală a acestei cerințe, care poate fi aplicată unor numeroase tipuri de ingerințe atât în contextul cartei, cât și în cel al CEDO [40], ar fi inoportun ca statele membre să fie supuse unor criterii diferite după cum ingerința este examinată în raport cu unul sau altul dintre aceste instrumente [41].

143. Prin urmare, considerăm, astfel cum au arătat guvernul eston și Comisia, că expresia „prevăzută de lege” menționată la articolul 52 alineatul (1) din cartă trebuie să fie interpretată, în lumina jurisprudenței Curții Europene a Drepturilor Omului rezumată la punctul 139 din prezentele concluzii, în sensul că o obligație generală de păstrare a datelor, precum cele în discuție în litigiile principale, trebuie să fie prevăzută de un temei legal suficient de accesibil și de previzibil, pe de o parte, și care să ofere o protecție corespunzătoare împotriva arbitrarului, pe de altă parte.

144. În al doilea rând, trebuie să se stabilească conținutul cerințelor impuse la articolul 15 alineatul (1) din Directiva 2002/58 în ceea ce privește temeiul legal care trebuie utilizat de un stat membru care dorește să utilizeze posibilitatea oferită de această dispoziție.

145. Este necesar să evidențiem, cu privire la acest aspect, existența unei divergențe între versiunile lingvistice ale primei teze a acestei dispoziții.

146. În versiunile în limbile engleză („legislative measures”), franceză („mesures législatives”), italiană („disposizioni legislative”), portugheză („medidas legislativas”), română („măsuri legislative”) și suedeză („genom lagstiftning vidta åtgärder”), articolul 15 alineatul (1) prima teză din Directiva 2002/58 impune, în opinia noastră, adoptarea unor măsuri care emană de la puterea legislativă.

147. În schimb, versiunile în limbile daneză („retsforskrifter”), germană („Rechtsvorschriften”), neerlandeză („wettelijke maatregele”) și spaniolă („medidas legales”) ale acestei teze pot fi interpretate în sensul că impun adoptarea fie a unor măsuri care emană de la puterea legislativă, fie a unor măsuri de reglementare care emană de la puterea executivă.

148. Conform unei jurisprudențe constante, necesitatea unei aplicări și, prin urmare, a unei interpretări uniforme a unui act al Uniunii Europene exclude posibilitatea ca acesta să fie privit în mod izolat în una dintre versiunile sale, impunând, dimpotrivă, ca el să fie interpretat atât în funcție de voința reală a autorului, cât și în funcție de scopul urmărit de acesta din urmă, în special în lumina versiunilor întocmite în toate celelalte limbi oficiale. În caz de divergențe între aceste versiuni, dispoziția în cauză trebuie interpretată în funcție de economia generală și de finalitatea reglementării din care face parte [42].

39 — Mai precis, Curtea nu poate, în opinia noastră, să adopte o interpretare a acestei cerințe care să fie mai permisivă decât cea a Curții Europene a Drepturilor Omului, ceea ce ar avea drept consecință să permită un număr de ingerințe mai ridicat decât cel care ar rezulta din interpretarea acestei cerințe de către Curtea Europeană a Drepturilor Omului.

40 — Această expresie „prevăzută de lege” este utilizată la articolul 8 alineatul (2) (dreptul la respectarea vieții private și de familie), la articolul 9 alineatul (2) (libertatea de gândire, de conștiință și de religie), la articolul 10 alineatul (2) (libertatea de exprimare) și la articolul 11 alineatul (2) (libertatea de întrunire și de asociere) din CEDO. În contextul cartei, articolul 52 alineatul (1) se aplică oricărei restrângeri a exercitării drepturilor consacrate de aceasta, presupunând că restrângerea respectivă este permisă.

41 — A se vedea în acest sens Peers, S., „Article 52 – Scope of guaranteed rights”, în Peers, S., și alții, *The EU Charter of Fundamental Rights: a Commentary*, Oxford, OUP, 2014, nr. 52.39.

42 — A se vedea printre altele Hotărârea din 30 mai 2013, Asbeek Brusse și de Man Garabito (C-488/11, EU:C:2013:341, punctul 26), Hotărârea din 24 iunie 2015, Hotel Sava Rogaška (C-207/14, EU:C:2015:414, punctul 26), și Hotărârea din 26 februarie 2015, Christie's France (C-41/14, EU:C:2015:119, punctul 26).

149. În speță, articolul 15 alineatul (1) din Directiva 2002/58 reglementează posibilitatea statelor membre de a deroga de la drepturile fundamentale consacrate la articolele 7 și 8 din cartă, a căror protecție este pusă în aplicare prin această directivă. Prin urmare, considerăm oportună interpretarea cerinței unui temei legal impusă la articolul 15 alineatul (1) din Directiva 2002/58 în lumina cartei și în special a articolului 52 alineatul (1) din aceasta.

150. Astfel, „măsurile” impuse la articolul 15 alineatul (1) din Directiva 2002/58 trebuie să aibă obligatoriu calitățile accesibilității, previzibilității și protecției corespunzătoare împotriva arbitrarului, evocate la punctul 143 din prezentele concluzii. Rezultă prin altele din aceste calități și în special din cerința protecției corespunzătoare împotriva arbitrarului că aceste măsuri trebuie să fie *obligatorii* pentru autoritățile naționale cărora le este conferită competența de acces la datele păstrate. În mod special, nu ar fi suficient ca garanțiile care însoțesc accesul la aceste date să fie prevăzute în ghiduri sau orientări interne care nu au un astfel de caracter obligatoriu, astfel cum a subliniat în mod întemeiat Law Society of England and Wales.

151. În plus, considerăm că expresia „statele membre pot adopta măsuri”, comună tuturor versiunilor lingvistice ale articolului 15 alineatul (1) prima teză din Directiva 2002/58, exclude posibilitatea ca o jurisprudență națională, chiar constantă fiind, să constituie un temei legal suficient pentru punerea în aplicare a acestei dispoziții. Subliniem că, în această măsură, dispoziția menționată depășește cerințele care rezultă din jurisprudența Curții Europene a Drepturilor Omului [43].

152. Adăugăm că pare de dorit ca, având în vedere gravitatea ingerințelor în drepturile fundamentale consacrate la articolele 7 și 8 din cartă pe care le implică o obligație generală de păstrare a datelor, substanța regimului în discuție și în special cea a garanțiilor care însoțesc această obligație să fie prevăzute într-o măsură adoptată de puterea legislativă, puterea executivă având sarcina de a stabili modalitățile de aplicare a acesteia.

153. Având în vedere ceea ce precedă, considerăm că articolul 15 alineatul (1) din Directiva 2002/58 și articolul 52 alineatul (1) din cartă trebuie interpretate în sensul că regimul care instituie o obligație generală de păstrare a datelor, precum cele în discuție în litigiile principale, trebuie să fie prevăzut de măsuri legislative sau de reglementare care au calitățile accesibilității, previzibilității și protecției corespunzătoare împotriva arbitrarului.

154. Revine instanțelor de trimitere sarcina de a verifica respectarea acestei cerințe, având în vedere poziția privilegiată a acestora în vederea evaluării regimurilor naționale respective.

2. Cu privire la respectarea substanței drepturilor recunoscute la articolele 7 și 8 din cartă

155. Potrivit articolului 52 alineatul (1), orice restrângere a exercițiului drepturilor recunoscute de cartă trebuie „să respecte substanța acestor drepturi” [44]. Acest aspect, care a fost examinat de Curte la punctele 39 și 40 din Hotărârea DRI în contextul Directivei 2006/24, nu ni se pare că ridică probleme în cadrul prezentelor cauze, astfel cum au arătat guvernele spaniol și irlandez, precum și Comisia.

156. La punctul 39 din Hotărârea DRI, Curtea a statuat că această directivă nu aducea atingere substanței dreptului la respectarea vieții private și a celorlalte drepturi consacrate la articolul 7 din cartă, având în vedere că nu permitea cunoașterea conținutului comunicațiilor electronice ca atare.

43 — A se vedea în special Curtea Europeană a Drepturilor Omului, Hotărârea Sanoma Uitgevers B. V. împotriva Țărilor de Jos din 14 septembrie 2010, CE:ECHR:2010:0914JUD003822403, § 83: „[termenul «lege» menționat la articolele 8-11 din CEDO include] «dreptul scris», care cuprinde atât texte de rang infralegislativ, cât și acte de reglementare adoptate de un ordin profesional, prin delegare de către legiuitor în cadrul competenței normative autonome a acestuia, și «dreptul nescris». «Legea» trebuie să fie înțeleasă ca incluzând textul scris și «dreptul elaborat» de instanțe”.

44 — O astfel de cerință nu reiese din modul de redactare a articolului 15 alineatul (1) din Directiva 2002/58, nici din economia acestei directive, pentru motivele prezentate la punctele 99-116 din prezentele concluzii.

157. Această apreciere poate fi transpusă, în opinia noastră, regimurilor naționale în discuție în litigiile principale, dat fiind că nici acestea nu permit cunoașterea conținutului comunicațiilor electronice ca atare [45].

158. La punctul 40 din Hotărârea DRI, Curtea a considerat că Directiva 2006/24 nu aducea atingere substanței dreptului fundamental la protecția datelor cu caracter personal, consacrat la articolul 8 din cartă, având în vedere principiile de protecție și de securitate a datelor care trebuie să fie respectate de furnizori în temeiul articolului 7 din această directivă, principii în temeiul cărora statele membre asigură adoptarea de măsuri tehnice și organizaționale adecvate împotriva distrugerii accidentale sau ilegale, a pierderii sau a modificării accidentale a datelor.

159. Considerăm, din nou, că această apreciere poate fi transpusă regimurilor naționale în discuție în litigiile principale, dat fiind că acestea prevăd, în opinia noastră, garanții comparabile în ceea ce privește protecția și securitatea datelor păstrate de furnizori, aceste garanții trebuind să permită protejarea în mod eficient a datelor cu caracter personal împotriva riscurilor de abuz, precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date [46].

160. Revine totuși instanțelor de trimitere sarcina să verifice dacă regimurile naționale în discuție în litigiile principale respectă efectiv substanța drepturilor recunoscute la articolele 7 și 8 din cartă, în lumina considerațiilor care precedă.

3. Cu privire la existența unui obiectiv de interes general recunoscut de Uniune care poate justifica o obligație generală de păstrare a datelor

161. Atât articolul 15 alineatul (1) din Directiva 2002/58, cât și articolul 52 alineatul (1) din cartă impun ca orice ingerință în drepturile consacrate prin aceste instrumente să urmărească un obiectiv de interes general.

162. La punctele 41-44 din Hotărârea DRI, Curtea a considerat, pe de o parte, că obligația generală de păstrare a datelor impusă de Directiva 2006/24 contribuia „la combaterea criminalității grave și astfel, în final, la siguranța publică” și, pe de altă parte, că această combatere constituia un obiectiv de interes general al Uniunii.

163. Reiese, astfel, din jurisprudența Curții că combaterea terorismului internațional pentru menținerea păcii și a securității internaționale constituie un obiectiv de interes general al Uniunii. Același lucru este valabil în ceea ce privește combaterea criminalității grave în scopul garantării siguranței publice. Pe de altă parte, trebuie arătat în această privință că articolul 6 din cartă prevede dreptul oricărei persoane nu doar la libertate, ci și la siguranță [47].

164. Această apreciere poate fi transpusă în privința obligațiilor generale de păstrare a datelor în discuție în litigiile principale, care pot fi justificate de obiectivul combaterii infracțiunilor grave.

165. Cu toate acestea, având în vedere unele argumente prezentate Curții, este necesar să se stabilească dacă o astfel de obligație poate fi justificată de un alt obiectiv de interes general decât combaterea infracțiunilor grave.

45 — A se vedea descrierea regimurilor naționale în discuție în litigiile principale, în special la punctele 13 și 36 din prezentele concluzii.

46 — Hotărârea DRI, punctul 54. A se vedea descrierea regimurilor naționale în discuție în litigiile principale, în special la punctele 29-33, precum și 45 și 46 din prezentele concluzii.

47 — Hotărârea DRI, punctul 42 și jurisprudența citată.

166. În această privință, formularea articolului 52 alineatul (1) din cartă evocă, la modul general, „obiectivel[e] de interes general recunoscute de Uniune” și „necesit[atea] protejării drepturilor și libertăților celorlalți”.

167. Formularea articolului 15 alineatul (1) din Directiva 2002/58 este mai precisă în ceea ce privește obiectivele care pot justifica o ingerință în drepturile prevăzute de această directivă. Astfel, potrivit acestei dispoziții, măsurile în discuție trebuie să contribuie la „a proteja securitatea națională (de exemplu siguranța statului), apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice, în conformitate cu articolul 13 alineatul (1) al Directivei 95/46/CE”.

168. În plus, în Hotărârea Promusicae [48], Curtea a statuat că această dispoziție trebuie interpretată în lumina articolului 13 alineatul (1) din Directiva 95/46, care autorizează derogările de la drepturile prevăzute de această directivă atunci când sunt justificate de „protecția drepturilor și libertăților altora”. În consecință, Curtea a considerat că articolul 15 alineatul (1) din Directiva 2002/58 oferă statelor membre posibilitatea de a prevedea obligația unui furnizor de a divulga date cu caracter personal în vederea stabilirii, în cadrul unei proceduri civile, a existenței unei încălcări a drepturilor de autor referitoare la înregistrări muzicale și audiovizuale.

169. Guvernul Regatului Unit a dedus din această hotărâre argumentul potrivit căruia o obligație generală de păstrare a datelor poate fi justificată de orice obiectiv menționat fie la articolul 15 alineatul (1) din Directiva 2002/58, fie la articolul 13 alineatul (1) din Directiva 95/46. Potrivit guvernului menționat, o astfel de obligație ar putea fi justificată de utilitatea datelor păstrate în combaterea infracțiunilor „simple” (spre deosebire de cele „grave”) sau chiar în contextul unor proceduri nepenale în raport cu obiectivele menționate de aceste dispoziții.

170. Acest argument nu ni se pare convingător, pentru următoarele motive.

171. În primul rând, astfel cum au subliniat în mod întemeiat domnul Watson, precum și Open Rights Group și Privacy International, abordarea adoptată de Curte în Hotărârea Promusicae [49] nu poate fi transpusă în prezentele cauze, având în vedere că această hotărâre privea o cerere de acces, formulată de o asociație de titulari de drepturi de autor, la date păstrate în mod spontan de către un furnizor, și anume Telefónica de España. Altfel spus, această hotărâre nu privea obiectivele care pot justifica ingerințele grave în drepturile fundamentale pe care le implică o obligație generală de păstrare a datelor, precum cele în discuție în litigiile principale.

172. În al doilea rând, considerăm că cerința proporționalității într-o societate democratică exclude posibilitatea justificării unei obligații generale de păstrare a datelor prin combaterea infracțiunilor simple sau prin buna desfășurare a procedurilor nepenale. Astfel, riscurile considerabile pe care le implică o astfel de obligație sunt disproporționate în raport cu avantajele pe care le-ar aduce în ceea ce privește combaterea infracțiunilor simple sau în contextul procedurilor nepenale [50].

173. Având în vedere ceea ce precedă, considerăm că articolul 15 alineatul (1) din Directiva 2002/58 și articolul 52 alineatul (1) din cartă trebuie interpretate în sensul că combaterea infracțiunilor grave constituie un obiectiv de interes general care poate justifica o obligație generală de păstrare a datelor, spre deosebire de combaterea infracțiunilor simple sau de buna desfășurare a procedurilor nepenale.

174. În consecință, este necesar să se examineze caracterul adecvat, necesar și proporțional al unei astfel de obligații în lumina obiectivului combaterii infracțiunilor grave.

48 — Hotărârea din 29 ianuarie 2008 (C-275/06, EU:C:2008:54, punctele 50-54).

49 — Hotărârea din 29 ianuarie 2008 (C-275/06, EU:C:2008:54).

50 — A se vedea punctele 252-261 din prezentele concluzii.

4. Cu privire la caracterul adecvat al unei obligații generale de păstrare a datelor în raport cu combaterea infracțiunilor grave

175. Cerințele referitoare la caracterul adecvat, necesar [51] și proporțional [52] decurg atât din articolul 15 alineatul (1) din Directiva 2002/58, cât și din articolul 52 alineatul (1) din cartă.

176. În temeiul primei cerințe, o obligație generală de păstrare a datelor precum cele în discuție în litigiile principale trebuie să fie aptă să contribuie la obiectivul de interes general identificat anterior, și anume combaterea infracțiunilor grave.

177. Această cerință nu creează dificultăți deosebite în contextul prezentelor cauze. Astfel cum a arătat Curtea în esență la punctul 49 din Hotărârea DRI, datele păstrate permit autorităților naționale competente în materie penală să dispună de un mijloc suplimentar de investigare pentru prevenirea și elucidarea infracțiunilor grave. Prin urmare, o astfel de obligație contribuie la combaterea infracțiunilor grave.

178. Dorim totuși să precizăm utilitatea pe care o poate avea o obligație generală de păstrare a datelor în scopul combaterii infracțiunilor grave. După cum a susținut în mod întemeiat guvernul francez, o astfel de obligație permite, într-o anumită măsură, autorităților represive să „se examineze trecutul” prin consultarea datelor păstrate, spre deosebire de măsurile de monitorizare direcționate.

179. O măsură de monitorizare direcționată vizează persoane care au fost identificate în prealabil ca având o posibilă legătură, chiar și indirectă sau îndepărtată, cu o infracțiune gravă. Astfel de măsuri direcționate permit autorităților competente să aibă acces la datele referitoare la comunicațiile efectuate de aceste persoane și chiar la conținutul acestor comunicații. Totuși, prin ipoteză, acest acces nu poate viza decât comunicațiile efectuate de astfel de persoane *ulterior* identificării lor.

180. În schimb, o obligație generală de păstrare a datelor privește ansamblul comunicațiilor efectuate de ansamblul utilizatorilor, fără a fi necesară o legătură cu o infracțiune gravă. O astfel de obligație permite autorităților competente să aibă acces la istoricul comunicațiilor efectuate de o persoană înainte de a fi fost identificată ca având o astfel de legătură. În acest sens, o astfel de obligație conferă autorităților represive o capacitate limitată de a examina trecutul, oferindu-le acces la comunicațiile efectuate de aceste persoane *anterior* identificării lor [53].

181. Altfel spus, utilitatea pe care o are o obligație generală de păstrare a datelor în scopul combaterii infracțiunilor grave rezidă în această capacitate limitată de a examina trecutul prin intermediul datelor care refac istoricul comunicațiilor efectuate de o persoană înainte chiar de a fi suspectată de legături cu o infracțiune gravă [54].

51 — Cu privire la caracterul necesar, a se vedea punctele 185-245 din prezentele concluzii.

52 — Cu privire la caracterul proporțional *stricto sensu*, a se vedea punctele 246-262 din prezentele concluzii.

53 — Comisia a subliniat de asemenea că valoarea adăugată a unei obligații generale de păstrare a datelor în raport cu o păstrare direcționată a datelor rezidă în această capacitate limitată de a examina trecutul: a se vedea Commission Staff Working Document prezentat în anexa la propunerea de directivă care a condus la adoptarea Directivei 2006/24, SEC(2005) 1131, 21 septembrie 2005, nr. 3.6, „Data Preservation versus Data Retention”: „[W]ith only data preservation as a tool, it is impossible for investigators to go back in time. Data preservation is only useful as of the moment when suspects have been identified – data retention is indispensable in many cases to actually identify those suspects”.

54 — Guvernul francez a făcut referire, în această privință, la Raportul Conseil d'État, *Le numérique et les droits fondamentaux*, 2014, p. 209 și 210. Conseil d'État (Franța) subliniază că un mecanism de măsuri de monitorizare direcționate „ar fi cu mult mai puțin eficient decât păstrarea sistematică din perspectiva siguranței naționale și a căutării autorilor infracțiunilor. Astfel, acesta nu ar permite accesul retrospectiv la schimburile care au avut loc înainte ca autoritatea să identifice o amenințare sau o infracțiune: caracterul său operațional ar depinde, așadar, de capacitatea autorităților de a anticipa identitatea persoanelor ale căror date de conectare ar putea fi utile, ceea ce nu este posibil în cadrul poliției judiciare. În ceea ce privește, spre exemplu, o crimă, autoritatea judiciară nu ar putea avea acces la comunicațiile anterioare acesteia, informație totuși prețioasă și adesea chiar indispensabilă pentru identificarea autorului acesteia și a complicilor săi, astfel cum au arătat câteva cazuri recente de atentate teroriste. În domeniul prevenirii atingerilor aduse siguranței naționale, noile programe tehnice se bazează pe o capacitate de detectare a semnalelor slabe, incompatibilă cu ideea predirecționării către persoane periculoase”.

182. Cu ocazia prezentării propunerii de directivă care a condus la adoptarea Directivei 2006/24, Comisia a ilustrat această utilitate cu ajutorul mai multor exemple concrete de anchete referitoare printre altele la acte de terorism, de asasinat, de răpire și de pornografie infantilă [55].

183. Mai multe exemple similare au fost prezentate Curții în cadrul prezentelor cauze, în special de către guvernul francez, care a subliniat obligația pozitivă care revine statelor membre de a asigura siguranța persoanelor care se află pe teritoriul acestora. Potrivit acestui guvern, în cadrul unor anchete privind dezmembrarea filierelor care organizează plecarea unor rezidenți francezi către zone de conflict din Irak sau Siria, accesul la datele păstrate joacă un rol decisiv în identificarea persoanelor care au facilitat astfel de plecări. Guvernul menționat adaugă că accesul la datele referitoare la comunicațiile persoanelor implicate în atentatele teroriste recente din ianuarie și din noiembrie 2015 din Franța a fost extrem de util anchetatorilor pentru a descoperi complicii autorilor acestor atentate. Tot astfel, în cadrul căutării unei persoane dispărute, datele referitoare la localizarea acestei persoane din cadrul comunicațiilor efectuate anterior dispariției sale ar putea avea un rol decisiv în vederea desfășurării anchetei.

184. Având în vedere considerațiile care precedă, considerăm că o obligație generală de păstrare a datelor este aptă să contribuie la combaterea infracțiunilor grave. Rămâne totuși de verificat dacă o astfel de obligație este în același timp necesară și proporțională cu acest obiectiv.

5. Cu privire la caracterul necesar al unei obligații generale de păstrare a datelor în raport cu combaterea infracțiunilor grave

185. Potrivit unei jurisprudențe constante, o măsură poate fi considerată necesară numai în lipsa oricărei alte măsuri care ar fi la fel de adecvată, fiind în același timp mai puțin constrângătoare [56].

186. Cerința referitoare la caracterul adecvat se referă la evaluarea eficacității „absolute” – independent de orice altă măsură posibilă – a unei obligații generale de păstrare a datelor în raport cu combaterea infracțiunilor grave. Cerința necesității duce, la rândul său, la aprecierea eficienței – sau eficacitatea „relativă”, mai precis în comparație cu orice altă măsură posibilă – a unei astfel de obligații [57].

187. În contextul prezentelor cauze, testul necesității impune să se verifice, pe de o parte, dacă alte măsuri ar putea fi la fel de eficiente precum o obligație generală de păstrare a datelor în combaterea infracțiunilor grave și, pe de altă parte, dacă aceste eventuale măsuri afectează în mai mică măsură drepturile consacrate de Directiva 2002/58 și la articolele 7 și 8 din cartă [58].

188. Reamintim, în plus, jurisprudența constantă amintită la punctul 52 din Hotărârea DRI, potrivit căreia protecția dreptului fundamental la viața privată impune ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele „strictului necesar” [59].

55 — Commission Staff Working Document prezentat în anexa la propunerea de directivă care a condus la adoptarea Directivei 2006/24, SEC(2005) 1131, 21 septembrie 2005, nr. 1.2, „The importance of traffic data for law enforcement”.

56 — A se vedea printre altele Hotărârea din 22 ianuarie 2013, Sky Österreich (C-283/11, EU:C:2013:28, punctele 54-57), Hotărârea din 13 noiembrie 2014, Reindl (C-443/13, EU:C:2014:2370, punctul 39), și Hotărârea din 16 iulie 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480, punctele 120-122). În doctrină, a se vedea în special Pirker, B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, p. 29: „Under a necessity test, the adjudicator examines whether there exists an alternative measure which achieves the same degree of satisfaction for the first value while entailing a lower degree of non-satisfaction of the second value”.

57 — A se vedea Rivers, J., „Proportionality and variable intensity of review”, 65(1) *Cambridge Law Journal* (2006) 174, p. 198: „The test of necessity thus expresses the idea of efficiency or Pareto-optimality. A distribution is efficient or Pareto-optimal if no other distribution could make at least one person better off without making any one else worse off. Likewise an act is necessary if no alternative act could make the victim better off in terms of rights-enjoyment without reducing the level of realisation of some other constitutional interest”.

58 — Cu privire la existența acestor două componente în cadrul testului necesității, a se vedea Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, p. 323-331.

59 — A se vedea printre altele Hotărârea din 9 noiembrie 2010, Volker und Markus Schecke și Eifert (C-92/09 și C-93/09, EU:C:2010:662, punctele 77 și 86), și Hotărârea din 7 noiembrie 2013, IPI (C-473/12, EU:C:2013:715, punctul 39).

189. În legătură cu cerința strictei necesități în contextul prezentelor cauze, au fost amplu dezbătute de părțile care au prezentat observații Curții două problematici, care corespund în esență celor două întrebări adresate de instanța de trimitere în cauza C-203/15:

— pe de o parte, trebuie să se considere, în lumina punctelor 56-59 din Hotărârea DRI, că o obligație generală de păstrare a datelor depășește ca atare limitele strictului necesar în vederea combaterii infracțiunilor grave, independent de eventualele garanții care însoțesc această obligație?

— pe de altă parte, presupunând că se poate considera că o astfel de obligație nu depășește ca atare limitele strictului necesar, aceasta trebuie să fie însoțită de ansamblul garanțiilor specificate de Curte la punctele 60-68 din Hotărârea DRI pentru a limita la strictul necesar atingerea adusă drepturilor consacrate de Directiva 2002/58 și la articolele 7 și 8 din cartă?

190. Înainte de a aborda aceste întrebări, considerăm oportună respingerea unui argument invocat de guvernul Regatului Unit, potrivit căruia criteriile stabilite în Hotărârea DRI ar fi lipsite de relevanță în contextul prezentelor cauze, pentru motivul că această hotărâre nu privea un regim național, ci un regim instituit de legiuitorul Uniunii.

191. În această privință, subliniem că Hotărârea DRI a interpretat articolul 7, articolul 8 și articolul 52 alineatul (1) din cartă și că aceste dispoziții fac de asemenea obiectul întrebărilor adresate în litigiile principale. Or, în opinia noastră, este imposibil ca dispozițiile cartei să fie interpretate diferit după cum regimul în discuție a fost instituit la nivelul Uniunii sau la nivel național, astfel cum au subliniat în mod întemeiat domnii Brice și Lewis, precum și Law Society of England and Wales. În cazul în care s-a constatat aplicabilitatea cartei, cum este situația în prezentele cauze [60], aceasta trebuie să fie aplicată în mod identic indiferent de regimul în discuție. Prin urmare, criteriile evidențiate de Curte în Hotărârea DRI sunt relevante în scopul aprecierii regimurilor naționale în discuție în prezentele cauze, astfel cum au arătat în special guvernele danez și irlandez, precum și Comisia.

a) Cu privire la caracterul strict necesar al unei obligații generale de păstrare a datelor

192. Potrivit unei prime abordări, susținută de Tele2 Sverige, precum și de Open Rights Group și Privacy International, trebuie să se considere, în urma Hotărârii DRI, că o obligație generală de păstrare a datelor depășește ca atare limitele a ceea ce este strict necesar în vederea combaterii infracțiunilor grave, independent de eventualele garanții care însoțesc această obligație.

193. Potrivit unei a doua abordări, susținută de majoritatea celorlalte părți care au prezentat observații Curții, o astfel de obligație nu depășește limitele strictului necesar, cu condiția să fie însoțită de anumite garanții referitoare la accesul la date, la perioada de păstrare, precum și la protecția și securitatea datelor.

194. Următoarele motive ne determină să adoptăm a doua abordare.

195. În primul rând, potrivit interpretării noastre cu privire la Hotărârea DRI, Curtea a considerat că o obligație generală de păstrare a datelor depășește limitele a ceea ce este strict necesar în cazul în care *nu este însoțită* de garanții stricte referitoare la accesul la date, la perioada de păstrare, precum și la protecția și securitatea datelor. În schimb, Curtea nu s-a pronunțat cu privire la compatibilitatea cu dreptul Uniunii a unei obligații generale de păstrare a datelor care ar fi *însoțită* de astfel de garanții, întrucât un astfel de regim nu făcea obiectul întrebărilor adresate Curții în această cauză.

60 — A se vedea punctele 117-125 din prezentele concluzii.

196. În această privință, subliniem că punctele 56-59 din Hotărârea DRI nu cuprind nicio declarație a Curții în sensul că o obligație generală de păstrare a datelor ar depăși ca atare limitele strictului necesar.

197. La punctele 56 și 57 din această hotărâre, Curtea constată că obligația de păstrare prevăzută de Directiva 2006/24 vizează toate mijloacele de comunicare electronică, toți utilizatorii, precum și toate datele de trafic, fără a face vreo diferențiere, limitare sau excepție în funcție de obiectivul combaterii infracțiunilor grave.

198. La punctele 58 și 59 din hotărârea menționată, Curtea prezintă în mod mai detaliat implicațiile practice ale acestei lipse de diferențiere. Pe de o parte, această obligație de păstrare privește chiar și persoane în privința cărora nu există niciun indiciu de natură să sugereze că comportamentul lor ar putea avea o legătură, chiar indirectă sau îndepărtată, cu infracțiuni grave. Pe de altă parte, această directivă nu impune existența unei relații între datele a căror păstrare este prevăzută și o amenințare pentru siguranța publică și în special aceasta nu se limitează la păstrarea unor date aferente unei perioade temporale și/sau unei zone geografice determinate și/sau unui cerc de persoane determinate care ar putea fi implicate, într-un mod sau altul, într-o infracțiune gravă.

199. Astfel, Curtea constată că o obligație generală de păstrare a datelor se caracterizează prin lipsa unei diferențieri în funcție de obiectivul combaterii infracțiunilor grave. Totuși, aceasta nu s-a pronunțat în sensul că lipsa de diferențiere respectivă înseamnă că o astfel de obligație depășește ca atare limitele strictului necesar.

200. În realitate, abia la finalul examinării regimului prevăzut de Directiva 2006/24 și după ce a constatat absența anumitor garanții pe care le vom examina în continuare [61], Curtea a statuat, la punctul 69 din Hotărârea DRI:

„*Având în vedere ansamblul considerațiilor care precedă*, trebuie să se considere că, prin adoptarea Directivei 2006/24, legiuitorul Uniunii a *depășit limitele* impuse de respectarea principiului proporționalității în lumina articolelor 7 și 8 și a articolului 52 alineatul (1) din cartă” (sublinierea noastră).

201. Astfel cum au arătat guvernele german și neerlandez, în cazul în care simpla păstrare generalizată a datelor ar fi fost suficientă pentru a atrage invaliditatea Directivei 2006/24, Curtea nu ar fi trebuit să examineze, în mod detaliat, lipsa garanțiilor specificate la punctele 60-68 din această hotărâre.

202. Prin urmare, obligația generală de păstrare a datelor prevăzută de Directiva 2006/24 nu depășea ca atare limitele strictului necesar. Această directivă depășea limitele strictului necesar ca urmare a *efectului combinat* al păstrării generalizate a datelor și al lipsei garanțiilor vizând limitarea la strictul necesar a atingerii aduse drepturilor consacrate la articolele 7 și 8 din cartă. Ca urmare a acestui efect combinat, directiva a trebuit declarată nevalidă în totalitate [62].

61 — A se vedea punctele 216-245 din prezentele concluzii.

62 — A se vedea Hotărârea DRI, punctul 65: „Prin urmare, trebuie să se constate că această directivă conține o ingerință în aceste drepturi fundamentale, care este de o mare amploare și de o gravitate deosebită în ordinea juridică a Uniunii, *fără ca* o astfel de ingerință să fie încadrată în mod precis de dispoziții care să permită garantarea faptului că ea este limitată efectiv la strictul necesar” (sublinierea noastră).

203. În al doilea rând, considerăm că această interpretare este confirmată de punctul 93 din Hotărârea Schrems [63], pe care îl reproducem în continuare:

„Astfel, nu este limitată la strictul necesar o reglementare care autorizează în mod generalizat stocarea integralității datelor cu caracter personal ale tuturor persoanelor ale căror date au fost transferate din Uniune către Statele Unite, *fără* a se face vreo diferențiere, limitare sau excepție în funcție de obiectivul urmărit și *fără* a se prevedea un criteriu obiectiv care să permită delimitarea accesului autorităților publice la date și utilizarea lor ulterioară în scopuri precise, strict restrânse și susceptibile să justifice ingerința pe care o implică atât accesarea, cât și utilizarea acestor date [a se vedea în acest sens, în ceea ce privește Directiva 2006/24, Hotărârea DRI, punctele 57-61]” (sublinierea noastră).

204. Din nou, Curtea nu s-a pronunțat în sensul că regimul în discuție în această cauză depășea limitele strictului necesar doar pentru motivul că acesta autoriza o păstrare generalizată a datelor cu caracter personal. În speță, limitele strictului necesar erau depășite ca urmare a efectului combinat al posibilității unei astfel de păstrări generalizate și al lipsei garanțiilor referitoare la acces în vederea reducerii ingerinței la strictul necesar.

205. Deducem din ceea ce precedă că nu trebuie să se considere că o obligație generală de păstrare a datelor depășește întotdeauna, ca atare, limitele a ceea ce este strict necesar în vederea combaterii infracțiunilor grave. În schimb, o astfel de obligație depășește întotdeauna limitele a ceea ce este strict necesar atunci când nu este însoțită de garanții referitoare la accesul la date, la perioada de păstrare, precum și la protecția și securitatea datelor.

206. În al treilea rând, opinia noastră cu privire la acest aspect este confirmată de necesitatea de a verifica în mod concret respectarea cerinței strictei necesități în contextul regimurilor naționale în discuție în litigiile principale.

207. Astfel cum am arătat la punctul 187 din prezentele concluzii, cerința strictei necesități impune să se examineze dacă alte măsuri ar putea fi la fel de eficiente precum o obligație generală de păstrare a datelor în combaterea infracțiunilor grave, afectând în același timp în mai mică măsură drepturile consacrate de Directiva 2002/58 și la articolele 7 și 8 din cartă.

208. Or, o astfel de apreciere trebuie realizată în contextul specific al fiecărui regim național care prevede o obligație generală de păstrare a datelor. Pe de o parte, această apreciere necesită compararea eficacității acestei obligații cu cea a oricărei alte măsuri posibile în contextul național, ținând seama de faptul că obligația menționată conferă autorităților competente o capacitate limitată de a examina trecutul prin intermediul datelor păstrate [64].

209. Având în vedere cerința strictei necesități, este imperativ ca aceste instanțe să nu se limiteze la a verifica simpla utilitate a unei obligații generale de păstrare a datelor, ci să verifice în mod strict că nicio altă măsură sau combinație de măsuri și în special o obligație direcționată de păstrare a datelor însoțită de alte instrumente de investigare nu pot oferi aceeași eficacitate în combaterea infracțiunilor grave. Subliniem, în această privință, că mai multe studii supuse atenției Curții repun în discuție necesitatea acestui tip de obligație în vederea combaterii infracțiunilor grave [65].

63 — Hotărârea din 6 octombrie 2015, Schrems (C-362/14, EU:C:2015:650).

64 — A se vedea punctele 178-183 din prezentele concluzii.

65 — A se vedea Comisarul pentru drepturile omului din cadrul Consiliului Europei, „Issue paper on the rule of law on the Internet and in the wider digital world”, decembrie 2014, CommDH/IssuePaper(2014)1, p. 115; Consiliul Organizației Națiunilor Unite pentru drepturile omului, Raportul Înaltului Comisariat al Organizației Națiunilor Unite pentru drepturile omului cu privire la dreptul la viața privată în era digitală, 30 iunie 2014, A/HRC/27/37, nr. 26; Adunarea generală a Organizației Națiunilor Unite, Raportul raportorului special privind promovarea și protecția drepturilor omului și a libertăților fundamentale în cadrul combaterii terorismului, 23 septembrie 2014, A/69/397, nr. 18 și 19.

210. Pe de altă parte, presupunând că alte măsuri ar putea fi la fel de eficiente în combaterea infracțiunilor grave, revine din nou instanțelor de trimitere sarcina de a stabili dacă acestea afectează în mai mică măsură drepturile fundamentale în discuție decât o obligație generală de păstrare a datelor, în conformitate cu jurisprudența constantă amintită la punctul 185 din prezentele concluzii.

211. În lumina punctului 59 din Hotărârea DRI, revine instanțelor naționale sarcina de a evalua în special posibilitatea de a limita întinderea materială a obligației de păstrare, menținând în același timp eficacitatea acestei măsuri în combaterea infracțiunilor grave [66]. Aceste obligații pot avea, astfel, o întindere materială mai mare sau mai mică, în funcție de utilizatori, de zonele geografice și de mijloacele de comunicare avute în vedere [67].

212. În opinia noastră, ar fi de dorit în special, în cazul în care tehnologia o permite, să se excludă obligația de păstrare a datelor deosebit de sensibile din perspectiva drepturilor fundamentale în discuție în prezentele cauze, cum sunt datele supuse secretului profesional sau datele care permit să se identifice sursele jurnaliștilor.

213. Totuși, trebuie să se aibă în vedere că o limitare substanțială a întinderii unei obligații generale de păstrare a datelor riscă să reducă în mod considerabil utilitatea pe care o prezintă un astfel de regim în combaterea infracțiunilor grave. Pe de o parte, mai multe guverne au subliniat dificultatea sau chiar imposibilitatea de a stabili dinainte datele care ar putea avea legătură cu o infracțiune gravă. Prin urmare, o astfel de limitare este susceptibilă să excludă păstrarea datelor care s-ar putea dovedi relevante în vederea combaterii infracțiunilor grave.

214. Pe de altă parte, astfel cum a susținut guvernul eston, criminalitatea gravă este un fenomen dinamic, capabil de a se adapta la instrumentele de investigație de care dispun autoritățile represive. Astfel, o limitare la o zonă geografică sau la un mijloc de comunicare determinate ar risca să provoace o deplasare a activităților legate de infracțiuni către o zonă geografică și/sau un mijloc de comunicare care nu se află sub incidența acestui regim.

215. În măsura în care necesită o evaluare complexă a regimurilor naționale în discuție în litigiile principale, considerăm că această apreciere trebuie să fie efectuată de instanțele naționale, astfel cum au subliniat guvernele ceh, eston, irlandez, francez, neerlandez, precum și Comisia.

b) Cu privire la caracterul imperativ al garanțiilor specificate de Curte la punctele 60-68 din Hotărârea DRI în raport cu cerința strictei necesități

216. Presupunând că o obligație generală de păstrare a datelor poate fi considerată ca fiind strict necesară în contextul regimului național în discuție, aspect a cărui apreciere revine instanței naționale, trebuie să se mai stabilească dacă o astfel de obligație trebuie să fie însoțită de ansamblul garanțiilor specificate de Curte la punctele 60-68 din Hotărârea DRI pentru a limita la strictul necesar atingerea adusă drepturilor consacrate de Directiva 2002/58 și la articolele 7 și 8 din cartă.

217. Aceste garanții privesc normele care reglementează accesul la datele păstrate de autoritățile competente și utilizarea acestora (punctele 60-62 din Hotărârea DRI), durata de păstrare a datelor (punctele 63 și 64 din această hotărâre), precum și securitatea și protecția datelor păstrate de furnizori (punctele 66-68 din această hotărâre).

66 — Această observație privește numai obligațiile generale de păstrare a datelor (care pot viza orice persoană, independent de existența unei legături cu o infracțiune gravă), iar nu măsurile de monitorizare direcționate (care vizează persoane care au fost identificate în prealabil ca având o legătură cu o infracțiune gravă): cu privire la această distincție, a se vedea punctele 178-183 din prezentele concluzii.

67 — Guvernul german a precizat în ședința de audiere a pledoariilor printre altele că Parlamentul german a exclus mesajele electronice de la obligația de păstrare impusă de legislația germană, însă acest regim privește toți utilizatorii și întregul teritoriu național.

218. În cadrul observațiilor prezentate Curții, au existat două teze contrare cu privire la natura acestor garanții.

219. Potrivit unei prime teze, susținută de domnul Watson, domnii Brice și Lewis, precum și de Open Rights Group și Privacy International, garanțiile specificate de Curte la punctele 60-68 din Hotărârea DRI sunt imperative. Potrivit acestei teze, Curtea a stabilit garanții minime care trebuie să fie *toate* îndeplinite de regimul național în discuție pentru ca atingerea adusă drepturilor fundamentale să fie limitată la strictul necesar.

220. Potrivit unei a doua teze, susținută de guvernele german, eston, irlandez, francez și al Regatului Unit, garanțiile specificate de Curte la punctele 60-68 din Hotărârea DRI sunt doar orientative. Curtea ar fi efectuat o „apreciere de ansamblu" a garanțiilor care lipsesc din cadrul regimului prevăzut de Directiva 2006/24, fără ca vreuna dintre aceste garanții să poată fi considerată, în mod izolat, ca fiind imperativă în raport cu cerința strictei necesități. Pentru a ilustra această teză, guvernul german a evocat imaginea „vaselor comunicante", în temeiul căreia o abordare mai flexibilă a unuia dintre cele trei aspecte identificate de Curte (de exemplu accesul la datele păstrate) ar putea fi compensată de o abordare mai strictă în ceea ce privește celelalte două aspecte (durata de păstrare, precum și securitatea și protecția datelor).

221. Avem convingerea că această teză a „vaselor comunicante" trebuie să fie respinsă și că *toate* garanțiile specificate de Curte la punctele 60-68 din Hotărârea DRI trebuie să fie considerate ca fiind imperative, pentru motivele următoare.

222. În primul rând, limbajul utilizat de Curte în cadrul examinării caracterului strict necesar al regimului instituit de Directiva 2006/24 nu permite o astfel de interpretare. În special, Curtea nu face nicăieri referire, în cadrul punctelor 60-68 din hotărârea menționată, la o posibilitate de a „compensa" o abordare mai flexibilă cu privire la unul dintre cele trei aspecte identificate de Curte printr-o abordare mai strictă în ceea ce privește celelalte două aspecte.

223. În realitate, teza „vaselor comunicante" ne pare că provine dintr-o confuzie între cerința necesității și cea a proporționalității *stricto sensu*, care nu a fost examinată de Curte în Hotărârea DRI. Astfel, după cum am indicat la punctul 186 din prezentele concluzii, cerința necesității constă în respingerea oricărei măsuri ineficiente. Nu se poate pune, în acest context, problema unei „aprecieri de ansamblu", a „compensării" sau a „evaluării comparative", procedee care nu intervin decât în stadiul proporționalității *stricto sensu*[68].

224. În al doilea rând, această teză a „vaselor comunicante" ar anula efectul util al garanțiilor menționate de Curte la punctele 60-68 din Hotărârea DRI, astfel încât persoanele ale căror date au fost păstrate nu ar mai dispune de garanții suficiente care să permită protejarea în mod eficient a datelor lor cu caracter personal împotriva riscurilor de abuz, precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date, astfel cum impune punctul 54 din această hotărâre.

225. Efectul distructiv al acestei teze poate fi ilustrat cu ușurință cu ajutorul exemplelor următoare. Un regim național care restrânge în mod strict accesul numai în scopul combaterii terorismului și care limitează durata de păstrare la trei luni (abordare strictă în ceea ce privește accesul și durata de păstrare), însă care nu ar obliga furnizorii să păstreze datele pe teritoriul național și într-un format criptat (abordare flexibilă în privința securității), ar expune întreaga sa populație la un risc crescut de acces ilegal la datele păstrate. În același mod, un regim național care prevede o durată de păstrare de

68 — A se vedea Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, p. 344: „The first three components of proportionality deal mainly with the relation between the limiting law's purpose and the means to fulfil that purpose. […] Accordingly, those tests are referred to as means-end analysis. *They are not based on balancing*. The test of proportionality stricto sensu is different. […] It focuses on the relation between the benefit in fulfilling the law's purpose and the harm caused by limiting the constitutional right. *It is based on balancing*" (sublinierea noastră).

trei luni, precum și păstrarea datelor pe teritoriul național și într-un format criptat (abordări stricte în ceea ce privește durata și securitatea), însă care ar permite tuturor angajaților tuturor autorităților publice să aibă acces la datele păstrate (abordare flexibilă cât privește accesul), ar expune întreaga sa populație la un risc crescut de abuz din partea autorităților naționale.

226. În opinia noastră, din aceste exemple reiese că menținerea efectului util al garanțiilor specificate de Curte la punctele 60-68 din Hotărârea DRI impune să se considere că *fiecare* dintre acestea este imperativă. Curtea Europeană a Drepturilor Omului a subliniat de asemenea importanța fundamentală a acestor garanții în Hotărârea recentă Szabó și Vissy împotriva Ungariei, făcând trimitere în mod expres la Hotărârea DRI [69].

227. În al treilea rând, considerăm că punerea în aplicare a acestor garanții de către statele membre care doresc să impună o obligație generală de păstrare a datelor nu ridică dificultăți practice majore. În realitate, aceste garanții ne par în multe privințe „minime”, astfel cum a susținut domnul Watson.

228. Mai multe dintre aceste garanții au fost dezbătute în fața Curții în considerarea posibilei lor lipse din cadrul regimurilor naționale în discuție in litigiile principale.

229. În primul rând, reiese din cuprinsul punctelor 61 și 62 din Hotărârea DRI că accesul la datele păstrate și utilizarea ulterioară a acestora trebuie să fie restricționate în mod strict la scopul prevenirii și al detectării infracțiunilor grave delimitate precis sau al desfășurării urmăririi penale aferente acestora.

230. Potrivit Tele2 Sverige și Comisiei, această cerință nu ar fi respectată de regimul suedez în discuție în cauza C-203/15, care ar permite accesul la datele păstrate în vederea combaterii infracțiunilor simple. O critică similară este formulată de domnii Brice și Lewis, precum și de domnul Watson împotriva regimului din Regatul Unit în discuție în cauza C-698/15, care ar autoriza accesul în vederea combaterii infracțiunilor simple și chiar în lipsa unei infracțiuni.

231. Deși nu revine Curții sarcina de a se pronunța cu privire la conținutul acestor regimuri naționale, îi revine aceea de a identifica obiectivele de interes general care pot justifica o ingerință gravă în drepturile consacrate de directivă și la articolele 7 și 8 din cartă. În speță, am prezentat deja motivele pentru care considerăm că *numai* combaterea infracțiunilor grave poate justifica o astfel de ingerință [70].

232. În al doilea rând, potrivit punctului 62 din Hotărârea DRI, accesul la datele păstrate trebuie să fie condiționat de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă prin a căror decizie se urmărește limitarea accesului la date și a utilizării lor la ceea ce este strict necesar în vederea atingerii obiectivului urmărit. În plus, acest control prealabil trebuie să intervină în urma unei cereri motivate a acestor autorități formulate în cadrul procedurilor de prevenire, de detectare sau de urmărire penală.

69 — Curtea Europeană a Drepturilor Omului, Hotărârea Szabó și Vissy împotriva Ungariei din 12 ianuarie 2016, CE:ECHR:2016:0112JUD003713814, § 68: „Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information”.

70 — A se vedea punctele 170-173 din prezentele concluzii.

233. Potrivit observațiilor formulate de Tele2 Sverige și de Comisie, această garanție a unui control independent și prealabil accesului ar lipsi în parte din cadrul regimului suedez în discuție în cauza C-203/15. Aceeași constatare, a cărei veridicitate nu este contestată de guvernul Regatului Unit, este făcută de domnii Brice și Lewis, de domnul Watson, precum și de Open Rights Group și Privacy International cu privire la regimul din Regatul Unit în discuție în cauza C-698/15.

234. Nu vedem niciun motiv pentru care această cerință a controlului prealabil de către o entitate independentă, care rezultă în mod incontestabil din limbajul utilizat de Curte la punctul 62 din Hotărârea DRI [71], ar trebui să devină mai flexibilă. Mai întâi, această cerință este dictată de gravitatea ingerinței și a riscurilor generate de constituirea unor baze de date care acoperă cvasitotalitatea populației vizate [72]. Arătăm că mai mulți experți în domeniul protecției drepturilor omului în cadrul combaterii terorismului au criticat tendința actuală care constă în a înlocui procedurile tradiționale de autorizare independentă și de supraveghere efectivă prin sisteme de „autoautorizare” a accesului la date de către serviciile de informații și de poliție [73].

235. În plus, un control independent și prealabil al accesului la date este necesar pentru a permite o prelucrare de la caz la caz a datelor deosebit de sensibile din perspectiva drepturilor fundamentale în discuție în prezentele cauze, cum sunt datele supuse secretului profesional sau datele care permit să se identifice sursele jurnaliștilor, astfel cum au subliniat Law Society of England and Wales, precum și guvernele francez și german. Acest control prealabil al accesului este cu atât mai necesar în ipoteza în care este dificil din punct de vedere tehnic să se excludă toate aceste date în stadiul păstrării [74].

236. În sfârșit, adăugăm că, din punct de vedere practic, niciuna dintre cele trei părți vizate de o cerere de acces nu este în măsură să exercite un control efectiv în ceea ce privește accesul la datele păstrate. Autoritățile competente în materia aplicării legii au tot interesul să solicite un acces cât mai larg posibil la aceste date. Furnizorii, care nu cunosc dosarul de cercetare, nu pot verifica dacă cererea de acces se limitează la strictul necesar. În ceea ce privește persoanele ale căror date sunt consultate, acestea nu au nicio posibilitate de a afla că fac obiectul unei astfel de măsuri de cercetare, chiar și în cazul unei utilizări abuzive sau ilicite, astfel cum au subliniat domnul Watson, precum și domnii Brice și Lewis. Această configurație a intereselor în joc impune, în opinia noastră, intervenția unei entități independente anterior consultării datelor păstrate, pentru a proteja persoanele ale căror date sunt păstrate împotriva oricărui acces abuziv din partea autorităților competente.

71 — Precizăm totuși că această cerință a unui control prealabil și independent nu poate avea, în opinia noastră, temeiul în articolul 8 alineatul (3) din cartă, din moment ce carta nu este aplicabilă ca atare dispozițiilor naționale care reglementează accesul la datele păstrate: a se vedea punctele 123-125 din prezentele concluzii.

72 — A se vedea punctele 252-261 din prezentele concluzii.

73 — Consiliul Organizației Națiunilor Unite pentru drepturile omului, Raportul raportorului special privind promovarea și protecția drepturilor omului și a libertăților fundamentale în cadrul combaterii terorismului, 28 decembrie 2009, A/HRC/13/37, nr. 62: „Nu trebuie să existe niciun sistem secret de monitorizare care să nu fie supravegheat de o instanță de control eficientă și nicio ingerință care să nu fie autorizată prin intermediul unui organism independent” (a se vedea de asemenea nr. 51). A se vedea de asemenea Adunarea generală a Organizației Națiunilor Unite, Raportul raportorului special privind promovarea și protecția drepturilor omului și a libertăților fundamentale în cadrul combaterii terorismului, 23 septembrie 2014, A/69/397, nr. 61.

74 — A se vedea punctul 212 din prezentele concluzii. În ceea ce privește sursele jurnaliștilor, Curtea Europeană a Drepturilor Omului a subliniat necesitatea unei autorizări prealabile de o entitate independentă, în măsura în care un control *a posteriori* nu permite restabilirea încrederii acestor surse: a se vedea Curtea Europeană a Drepturilor Omului, Hotărârea Telegraaf Media Nederland Landelijke Media B. V. și alții împotriva Țărilor de Jos din 22 noiembrie 2012, CE:ECHR:2012:1122JUD003931506, § 101, și Curtea Europeană a Drepturilor Omului, Hotărârea Szabó și Vissy împotriva Ungariei din 12 ianuarie 2016, CE:ECHR:2016:0112JUD003713814, § 77. În Hotărârea Kopp împotriva Elveției, care privea monitorizarea liniilor telefonice ale unui avocat, Curtea Europeană a Drepturilor Omului a criticat faptul că un funcționar care aparține administrației este însărcinat, în lipsa controlului de către un magistrat independent, să filtreze informațiile supuse secretului profesional: a se vedea Curtea Europeană a Drepturilor Omului, Hotărârea Kopp împotriva Elveției, CE:ECHR:1998:0325JUD002322494, § 74.

237. În aceste condiții, ne pare rezonabil să considerăm că situațiile punctuale de extremă urgență, evocate de guvernul Regatului Unit, pot justifica un acces imediat la datele păstrate al autorităților represive fără un control prealabil, în vederea prevenirii săvârșirii unor infracțiuni grave sau a urmăririi autorilor unor astfel de infracțiuni [75]. În măsura posibilului, este imperativă menținerea cerinței autorizării prealabile prin instituirea unei proceduri de urgență în cadrul entității independente în vederea prelucrării acestui tip de cerere de acces. Cu toate acestea, dacă simplul fapt de a sesiza această entitate cu o cerere de acces pare incompatibil cu extrema urgență a situației, accesul la date și utilizarea acestora vor trebui să facă obiectul unui control *a posteriori* de către această entitate, în cel mai scurt timp posibil.

238. În al treilea rând, punctul 68 din Hotărârea DRI stabilește, în sarcina furnizorilor, o obligație de a păstra datele pe teritoriul Uniunii, în scopul garantării controlului exercitat de o autoritate independentă, impus la articolul 8 alineatul (3) din cartă, al respectării cerințelor de protecție și de securitate menționate la punctele 66 și 67 din această hotărâre.

239. Tele2 Sverige și Comisia au arătat că păstrarea datelor pe teritoriul național nu ar fi garantată în cadrul regimului suedez în discuție în cauza C-203/15. Aceeași critică este formulată de domnii Brice și Lewis, precum și de domnul Watson împotriva regimului din Regatul Unit în discuție în cauza C-698/15.

240. În această privință, pe de o parte, nu vedem niciun motiv pentru care această cerință stabilită la punctul 68 din Hotărârea DRI ar trebui atenuată, din moment ce păstrarea datelor în afara teritoriului Uniunii nu ar permite să se garanteze persoanelor ale căror date sunt păstrate nivelul de protecție oferit de Directiva 2002/58 și la articolul 7, la articolul 8 și la articolul 52 alineatul (1) din cartă [76].

241. Pe de altă parte, considerăm rezonabilă adaptarea acestei cerințe, exprimată de Curte în contextul Directivei 2006/24, la contextul regimurilor naționale prin dispoziții care să prevadă păstrarea datelor pe teritoriul național, astfel cum au arătat guvernele german și francez, precum și Comisia. Astfel, în temeiul articolului 8 alineatul (3) din cartă, revine fiecărui stat membru obligația de a asigura controlul de către o autoritate independentă al respectării cerințelor de protecție și securitate de către furnizorii vizați de regimul național. Or, în lipsa unei coordonări la nivelul Uniunii, o astfel de autoritate națională s-ar putea afla în imposibilitatea de a-și duce la bun sfârșit misiunile de control pe teritoriul unui alt stat membru.

242. În al patrulea rând, în ceea ce privește durata de păstrare, instanțele de trimitere vor trebui să aplice criteriile definite de Curte la punctele 63 și 64 din Hotărârea DRI. Pe de o parte, aceste instanțe trebuie să stabilească dacă datele păstrate pot fi diferențiate în funcție de utilitatea lor și, dacă este cazul, dacă durata de păstrare a fost adaptată în funcție de acest criteriu. Pe de altă parte, instanțele menționate trebuie să verifice dacă durata de păstrare este întemeiată pe criterii obiective care să permită garantarea limitării acesteia la strictul necesar.

243. Subliniem că, în recenta Hotărâre Roman Zakharov împotriva Rusiei, Curtea Europeană a Drepturilor Omului a considerat rezonabilă o durată maximă de păstrare de șase luni, exprimându-și în același timp regretul cu privire la inexistența obligației de a distruge imediat datele care nu au legătură cu scopul pentru care au fost colectate [77]. Adăugăm, cu privire la acest aspect, că regimurile

75 — A se vedea în această privință mecanismul descris la punctul 22 din prezentele concluzii. Subliniem că această problematică nu a fost abordată de Curte în Hotărârea DRI.

76 — A se vedea în această privință Hotărârea din 6 octombrie 2015, Schrems (C-362/14, EU:C:2015:650).

77 — A se vedea, în această privință, Curtea Europeană a Drepturilor Omului, Hotărârea Roman Zakharov împotriva Rusiei din 4 decembrie 2015, CE:ECHR:2015:1204JUD004714306, § 254 și 255. Potrivit dreptului rus, distrugerea elementelor interceptate trebuia să intervină la finalul unei perioade de păstrare de șase luni dacă persoana în cauză nu fusese inculpată pentru o infracțiune. Curtea Europeană a Drepturilor Omului a considerat rezonabilă durata maximă de păstrare, și anume șase luni, stabilită de dreptul rus pentru astfel de date. Totuși, aceasta și-a exprimat regretul cu privire la inexistența obligației de a distruge pe loc datele care nu au legătură cu scopul pentru care au fost colectate, precizând că păstrarea automată timp de șase luni a datelor vădit lipsite de interes nu poate fi considerată justificată în raport cu articolul 8 din CEDO.

naționale în discuție în litigiile principale trebuie să prevadă o obligație de distrugere în mod iremediabil a tuturor datelor păstrate din momentul în care nu mai sunt strict necesare în vederea combaterii infracțiunilor grave. Această obligație trebuie să fie respectată nu numai de furnizorii care păstrează date, ci și de autoritățile care au avut acces la date păstrate.

244. Având în vedere considerațiile care precedă, considerăm că toate garanțiile specificate de Curte la punctele 60-68 din Hotărârea DRI au un caracter imperativ și trebuie, prin urmare, să însoțească o obligație generală de păstrare a datelor în vederea limitării la strictul necesar a atingerii aduse drepturilor consacrate de Directiva 2002/58 și la articolele 7 și 8 din cartă.

245. Revine instanțelor de trimitere sarcina să verifice dacă regimurile naționale în discuție în litigiile principale includ fiecare dintre aceste garanții.

6. Cu privire la caracterul proporțional, într-o societate democratică, al unei obligații de păstrare a datelor în raport cu obiectivul combaterii infracțiunilor grave

246. După verificarea caracterului necesar al regimurilor naționale în discuție în litigiile principale, va reveni instanțelor de trimitere și sarcina de a verifica caracterul proporțional, într-o societate democratică, al acestora în raport cu obiectivul combaterii infracțiunilor grave. Acest aspect nu a fost examinat de Curte în Hotărârea DRI, întrucât regimul prevăzut de Directiva 2006/24 depășea limitele a ceea ce este strict necesar în vederea combaterii infracțiunilor grave.

247. Această cerință a proporționalității într-o societate democratică – sau proporționalitate *stricto sensu* – decurge în același timp de la articolul 15 alineatul (1) din Directiva 2002/58, de la articolul 52 alineatul (1) din cartă și dintr-o jurisprudență constantă. Potrivit acestei jurisprudențe constante, o măsură care aduce atingere unor drepturi fundamentale poate fi considerată proporțională doar dacă inconvenientele cauzate de aceasta nu sunt disproporționate în raport cu scopurile vizate [78].

248. Spre deosebire de cerințele referitoare la caracterul adecvat și necesar al măsurilor în discuție, care evaluează eficacitatea acestora în raport cu obiectivul urmărit, cerința proporționalității *stricto sensu* constă în a evalua comparativ, pe de o parte, avantajele care rezultă din această măsură în raport cu obiectivul legitim urmărit și, pe de altă parte, inconvenientele care decurg din aceasta în raport cu drepturile fundamentale consacrate într-o societate democratică [79]. Această cerință inițiază, astfel, o dezbatere cu privire la valorile care trebuie să prevaleze într-o societate democratică și, în definitiv, cu privire la tipul de societate în care dorim să trăim [80].

78 — A se vedea printre altele Hotărârea din 15 februarie 2016, N. (C-601/15 PPU, EU:C:2016:84, punctul 54; caracterul necesar este examinat la punctele 56-67, iar caracterul proporțional la punctele 68 și 69), Hotărârea din 16 iulie 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480, punctul 123; caracterul necesar este examinat la punctele 120-122, iar caracterul proporțional la punctele 123-127), și Hotărârea din 22 ianuarie 2013, Sky Österreich (C-283/11, EU:C:2013:28, punctul 50; caracterul necesar este examinat la punctele 54-57, iar caracterul proporțional la punctele 58-67).

79 — A se vedea Rivers, J., „Proportionality and variable intensity of review”, 65(1) *Cambridge Law Journal* (2006) 174, p. 198: „It is vital to realise that the test of balance has a totally different function from the test of necessity. The test of necessity rules out inefficient human rights limitations. It filters out cases in which the same level of realisation of a legitimate aim could be achieved at less cost to rights. By contrast, the test of balance is strongly evaluative. It asks whether the combination of certain levels of rights-enjoyment combined with the achievement of other interests is good or acceptable.”

80 — A se vedea Pirker, B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, p. 30: „In its simple form, one could state that proportionality *stricto sensu* leads to a weighing between competing values to assess which value should prevail.”

249. Prin urmare, astfel cum am indicat la punctul 223 din prezentele concluzii, aprecierea în ansamblu a regimului în discuție trebuie efectuată în etapa examinării proporționalității în sens strict, iar nu în etapa examinării necesității, astfel cum au susținut adepții tezei „vaselor comunicante” [81].

250. În conformitate cu jurisprudența amintită la punctul 247 din prezentele concluzii, este necesar să se evalueze comparativ avantajele și inconvenientele, într-o societate democratică, ale unei obligații generale de păstrare a datelor. Aceste avantaje și inconveniente sunt strâns legate de caracteristica esențială a unei astfel de obligații, pentru care reprezintă oarecum partea pozitivă și partea întunecată, și anume faptul că ea privește toate comunicațiile efectuate de toți utilizatorii, fără a fi necesară vreo legătură cu o infracțiune gravă.

251. Pe de o parte, am arătat deja, la punctele 178-183 din prezentele concluzii, avantajele pe care le aduce, în ceea ce privește combaterea infracțiunilor grave, păstrarea datelor referitoare la ansamblul comunicațiilor efectuate pe teritoriul național.

252. Pe de altă parte, inconvenientele unei obligații generale de păstrare a datelor decurg din faptul că imensa majoritate a datelor păstrate privesc persoane care nu vor avea niciodată o legătură cu o infracțiune gravă. Este important de precizat, în această privință, natura inconvenientelor care vor afecta aceste persoane. Or, aceste inconveniente sunt de natură diferită, în funcție de nivelul de ingerință în drepturile fundamentale ale acestora la respectarea vieții private și la protecția datelor cu caracter personal.

253. În cadrul unei ingerințe „individuale”, care afectează un individ determinat, inconvenientele care rezultă dintr-o obligație generală de păstrare a datelor au fost descrise cu mare precizie de avocatul general Cruz Villalón la punctele 72-74 din Concluziile prezentate în cauza DRI [82]. Pentru a relua termenii utilizați de acesta, exploatarea acestor date face posibilă „stabilirea unei cartografii atât fidele, cât și exhaustive a unei părți importante a comportamentelor unei persoane care țin strict de viața sa privată, chiar de un portret complet și precis al identității sale private”.

254. Altfel spus, într-un context individual, o obligație generală de păstrare a datelor permite ingerințe tot atât de grave precum măsurile de monitorizare direcționate, inclusiv cele care interceptează conținutul comunicațiilor efectuate.

255. Deși gravitatea unor astfel de ingerințe individuale nu poate fi subestimată, ni se pare totuși că riscurile specifice generate de o obligație generală de păstrare a datelor se dezvăluie în contextul ingerințelor „în masă”.

256. Astfel, spre deosebire de măsurile de monitorizare direcționate, o astfel de obligație poate facilita considerabil ingerințele în masă, mai exact ingerințele care afectează o parte substanțială sau chiar întreaga populație relevantă, ceea ce se poate ilustra cu ajutorul exemplelor următoare.

81 — Specificitatea cerinței proporționalității *stricto sensu* în raport cu cerințele referitoare la caracterul adecvat și necesar poate fi ilustrată prin exemplul următor. Să ne imaginăm că un stat membru impune injectarea unui cip electronic de geolocalizare tuturor persoanelor care au reședința pe teritoriul său, acest cip permițând autorităților să reconstituie deplasările efectuate de purtătorul acestuia pe parcursul anului anterior. O astfel de măsură ar putea fi considerată ca fiind „necesară” dacă nicio altă măsură nu permite atingerea aceluiași grad de eficiență în combaterea infracțiunilor grave. Totuși, în opinia noastră, o astfel de măsură ar fi disproporționată într-o societate democratică, dat fiind că inconvenientele rezultate din atingerea adusă drepturilor la integritate fizică, la respectarea vieții private și la protecția datelor cu caracter personal ar fi disproporționate în raport cu avantajele care ar decurge pentru combaterea infracțiunilor grave.

82 — C-293/12 și C-594/12, EU:C:2013:845. A se vedea de asemenea Hotărârea DRI, punctele 27 și 37.

257. Să presupunem, în primul rând, că o persoană care are acces la datele păstrate are intenția de a identifica, în cadrul populației statului membru, toți indivizii afectați de probleme de ordin psihologic. Analiza, în acest scop, a conținutului tuturor comunicațiilor efectuate pe teritoriul național ar necesita resurse considerabile. În schimb, exploatarea bazelor de date referitoare la comunicații ar permite să se identifice instantaneu toți indivizii care au contactat un psiholog în cursul perioadei de păstrare a datelor [83]. Adăugăm că această tehnică ar putea fi extinsă la fiecare dintre specializările medicale înregistrate într-un stat membru [84].

258. Să presupunem, în al doilea rând, că aceeași persoană dorește să identifice indivizii care se opun politicii guvernului în exercițiu. Din nou, analiza în acest scop a conținutului comunicațiilor ar necesita resurse considerabile. În schimb, exploatarea datelor referitoare la comunicații ar permite să se identifice toți indivizii înscriși pe listele de distribuție a mesajelor electronice care critică politica guvernului. În plus, aceste date ar permite de asemenea identificarea indivizilor care participă la orice manifestare publică de opoziție față de guvern [85].

259. Dorim să subliniem că riscurile legate de accesul la datele referitoare la comunicații (sau „metadate”) pot fi echivalente sau chiar superioare celor care decurg din accesul la conținutul acestor comunicații, astfel cum au subliniat Open Rights Group și Privacy International, Law Society of England and Wales, precum și un raport recent al Înaltului Comisariat al Organizației Națiunilor Unite pentru drepturile omului [86]. În special, astfel cum arată exemplele menționate anterior, „metadatele” permit o catalogare aproape instantanee a întregii populații, ceea ce conținutul comunicațiilor nu permite.

260. Adăugăm că riscurile de acces abuziv sau nelegal la datele păstrate nu sunt deloc teoretice. Pe de o parte, riscul de acces abuziv din partea autorităților competente trebuie raportat la numărul extrem de ridicat de cereri de acces menționate în observațiile prezentate Curții. În contextul regimului suedez, Tele2 Sverige a indicat ca a primit aproximativ 10 000 de cereri de acces pe lună, număr care nu include cererile primite de alți furnizori activi pe teritoriul suedez. În ceea ce privește regimul din

83 — Astfel, datele păstrate includ identitatea sursei și a destinatarului unei comunicații, date care ar fi suficient să fie confruntate cu lista numerelor de telefon ale psihologilor care își desfășoară activitatea pe teritoriul național.

84 — A se vedea în această privință Consiliul Organizației Națiunilor Unite pentru drepturile omului, Raportul raportorului special privind promovarea și protecția drepturilor omului și a libertăților fundamentale în cadrul combaterii terorismului, 28 decembrie 2009, A/HRC/13/37, nr. 42: „[Î]n Germania, studiile au semnalat o consecință îngrijorătoare a politicilor de păstrare a datelor: 52 % dintre persoanele interogate au indicat că este puțin probabil că vor utiliza telecomunicațiile pentru a lua legătura cu un toxicolog, un psihoterapeut sau un consilier conjugal ca urmare a legilor privind păstrarea datelor.”

85 — Întrucât datele păstrate includ localizarea sursei și a destinatarului unei comunicații, orice persoană care inițiază sau primește o comunicație cu ocazia unei manifestații va putea fi identificată cu ușurință grație datelor păstrate. În această privință, Marc Goodman, expert FBI și Interpol în domeniul riscurilor legate de noile tehnologii, relatează că, recent, guvernul ucrainian a procedat, cu ocazia unei manifestații a opoziției, la identificarea tuturor telefoanelor mobile localizate în apropierea ciocnirilor stradale dintre forțele de ordine și opozanții guvernului. Toate aceste numere de telefon au primit atunci un mesaj pe care autorul îl descrie ca fiind, posibil, mesajul cel mai „orwellian” trimis vreodată de un guvern: „Stimate abonat, sunteți înregistrat ca participant la o tulburare gravă a ordinii publice” (Goodman, M., *Future Crimes*, Anchor Books, New York, 2016, p. 153, traducere liberă). A se vedea de asemenea Consiliul Organizației Națiunilor Unite pentru drepturile omului, Raportul raportorului special privind promovarea și protecția dreptului la libertatea de opinie și de exprimare, 17 aprilie 2013, A/HRC/23/40, nr. 75, și Consiliul Organizației Națiunilor Unite pentru drepturile omului, Raportul Înaltului Comisariat al Organizației Națiunilor Unite pentru drepturile omului cu privire la dreptul la viața privată în era digitală, 30 iunie 2014, A/HRC/27/37, nr. 3.

86 — A se vedea, în această privință, Consiliul Organizației Națiunilor Unite pentru drepturile omului, Raportul Înaltului Comisariat al Organizației Națiunilor Unite pentru drepturile omului cu privire la dreptul la viața privată în era digitală, 30 iunie 2014, A/HRC/27/37, nr. 19: „În aceeași ordine de idei, unii susțin că interceptarea - sau colectarea - de date referitoare la o comunicație, iar nu la conținutul comunicației nu constituie în sine o imixtiune în viața privată. Or, din perspectiva dreptului la viața privată, această diferențiere nu este convingătoare. Acumulările de informații denumite în mod uzual «metadate» pot oferi indicații cu privire la conduita unui individ, la relațiile sale sociale, la preferințele private și la identitatea sa *care depășesc cu mult ceea ce se obține prin accesarea conținutului* unei comunicații private” (sublinierea noastră). A se vedea de asemenea Adunarea generală a Organizației Națiunilor Unite, Raportul raportorului special privind promovarea și protecția drepturilor omului și a libertăților fundamentale în cadrul combaterii terorismului, 23 septembrie 2014, A/69/397, nr. 53.

Regatul Unit, domnul Watson a reprodus numere extrase dintr-un raport oficial care indica 517 236 de autorizații și 55 346 de autorizații orale urgente doar pentru anul 2014. Pe de altă parte, riscul accesării nelegale de către orice persoană este inseparabil de însăși existența bazelor de date păstrate pe suporturi informatice [87].

261. Revine, în opinia noastră, instanțelor de trimitere sarcina de a aprecia dacă inconvenientele cauzate de obligațiile generale de păstrare a datelor în discuție în litigiile principale nu sunt disproporționate, într-o societate democratică, în raport cu scopurile urmărite, în conformitate cu jurisprudența amintită la punctul 247 din prezentele concluzii. În cadrul acestei aprecieri, aceste instanțe vor trebui să evalueze comparativ riscurile și avantajele legate de o astfel de obligație, și anume:

— pe de o parte, avantajele legate de conferirea unei capacități limitate de a examina trecutul, autorităților implicate în combaterea infracțiunilor grave [88] și

— pe de altă parte, riscurile grave rezultate, într-o societate democratică, din posibilitatea de a cartografia viața privată a unui individ și din posibilitatea de a cataloga o populație în ansamblul său.

262. Această apreciere trebuie să fie efectuată în raport cu toate caracteristicile relevante ale regimurilor naționale în discuție în litigiile principale. Subliniem, în această privință, că garanțiile imperative specificate de Curte la punctele 60-68 din Hotărârea DRI constituie doar garanții minime în vederea limitării la strictul necesar a atingerii aduse drepturilor consacrate de Directiva 2002/58 și la articolele 7 și 8 din cartă. Prin urmare, nu este exclus ca un regim național care prezintă ansamblul acestor garanții să trebuiască să fie considerat totuși disproporționat în cadrul unei societăți democratice, pentru motivul disproporției dintre riscurile grave generate de această obligație într-o societate democratică și avantajele care decurg din aceasta pentru combaterea infracțiunilor grave.

VI – Concluzie

263. Având în vedere ceea ce precedă, propunem Curții să răspundă la întrebările preliminare adresate de Kammarrätten i Stockholm (Curtea Administrativă de Apel din Stockholm, Suedia) și de Court of Appeal (England & Wales) (Civil Division) [Curtea de Apel (Anglia și Țara Galilor) (Secția civilă), Regatul Unit] după cum urmează:

„Articolul 15 alineatul (1) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor electronice (Directiva asupra confidențialității și comunicațiilor electronice), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009, precum și articolul 7, articolul 8 și articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene trebuie interpretate în sensul că nu se opun posibilității unui stat

87 — A se vedea în special Consiliul Organizației Națiunilor Unite pentru drepturile omului, Raportul raportorului special privind promovarea și protecția dreptului la libertatea de opinie și de exprimare, 17 aprilie 2013, A/HRC/23/40, nr. 67: „Bazele de date de comunicații devin vulnerabile la furt, la fraudă și la divulgarea accidentală”.

88 — A se vedea punctele 178-183 din prezentele concluzii.

membru de a impune furnizorilor de servicii de comunicații electronice o obligație de păstrare a tuturor datelor referitoare la comunicațiile efectuate de utilizatorii serviciilor lor atunci când sunt îndeplinite toate condițiile următoare, aspect a cărui verificare revine instanței de trimitere, în lumina tuturor caracteristicilor relevante ale regimurilor naționale în discuție în litigiile principale:

— această obligație și garanțiile care o însoțesc trebuie să fie prevăzute de măsuri legislative sau de reglementare care au calitățile accesibilității, previzibilității și protecției corespunzătoare împotriva arbitrarului;

— această obligație și garanțiile care o însoțesc trebuie să respecte substanța drepturilor recunoscute la articolele 7 și 8 din Carta drepturilor fundamentale;

— această obligație trebuie să fie strict necesară în vederea combaterii infracțiunilor grave, ceea ce presupune că nicio altă măsură sau combinație de măsuri nu ar putea fi la fel de eficientă în combaterea infracțiunilor grave, afectând în același timp în mai mică măsură drepturile consacrate de Directiva 2002/58 și la articolele 7 și 8 din Carta drepturilor fundamentale;

— această obligație trebuie să fie însoțită de toate garanțiile specificate de Curte la punctele 60-68 din Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238), referitoare la accesul la date, la durata de păstrare, precum și la protecția și securitatea datelor, în vederea limitării la strictul necesar a atingerii aduse drepturilor consacrate de Directiva 2002/58 și la articolele 7 și 8 din Carta drepturilor fundamentale și

— această obligație trebuie să fie proporțională, într-o societate democratică, cu obiectivul combaterii infracțiunilor grave, ceea ce presupune că riscurile grave generate de această obligație într-o societate democratică nu trebuie să fie disproporționate în raport cu avantajele care decurg din aceasta pentru combaterea infracțiunilor grave.”