Repertoriul jurisprudenței

CONCLUZIILE AVOCATULUI GENERAL
YVES BOT
prezentate la 23 septembrie 2015 [1]

Cauza C-362/14

Maximillian Schrems
împotriva
Data Protection Commissioner

[cerere de decizie preliminară formulată de High Court (Irlanda)]

„Trimitere preliminară — Date cu caracter personal — Protecția persoanelor fizice în ceea ce privește prelucrarea acestor date — Carta drepturilor fundamentale a Uniunii Europene — Articolele 7, 8 și 47 — Directiva 95/46/CE — Articolul 25 — Decizia 2000/520/CE — Transfer de date cu caracter personal către Statele Unite — Evaluarea caracterului adecvat sau inadecvat al nivelului de protecție — Plângere formulată de o persoană fizică ale cărei date au fost transferate către o țară terță — Autoritatea națională de supraveghere — Competențe”

I – **Introducere**

1. Astfel cum a constatat Comisia Europeană în Comunicarea din 27 noiembrie 2013 [2], „[t]ransferurile de date cu caracter personal constituie un element important și necesar al relației transatlantice. Acestea fac parte integrantă din schimburile comerciale transatlantice inclusiv în noile sectoare din domeniul digital aflate în continuă dezvoltare, cum ar fi mijloacele de comunicare sociale sau tehnologia de tip cloud, care implică transferul unor cantități mari de date dinspre UE către SUA” [3].

2. Schimburile comerciale fac obiectul Deciziei 2000/520/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță” privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al SUA [4]. Această decizie furnizează un temei juridic pentru transferul de date cu caracter personal din Uniune către întreprinderi stabilite în Statele Unite care aderă la principiile sferei de siguranță.

3. Decizia menționată se confruntă în prezent cu provocarea care constă în autorizarea fluxurilor de date dintre Uniune și Statele Unite, garantând totodată un nivel ridicat de protecție pentru aceste date, astfel cum impune dreptul Uniunii.

1 — Limba originală: franceza.

2 — Comunicare a Comisiei către Parlamentul European și Consiliu intitulată „Restabilirea încrederii în fluxurile de date dintre UE și SUA” [COM(2013) 846 final].

3 — Pagina 2.

4 — JO L 215, p. 7, rectificare în JO 2001, L 115, p. 14, Ediție specială, 16/vol. 1, p. 64.

4. Astfel, anumite dezvăluiri au evidențiat recent existența unor programe americane de colectare a informațiilor pe scară largă. Aceste dezvăluiri au semănat confuzie cu privire la respectarea normelor dreptului Uniunii cu ocazia unor transferuri de date cu caracter personal către întreprinderi stabilite în Statele Unite și cu privire la punctele slabe ale sistemului sferei de siguranță.

5. Prezenta trimitere preliminară solicită Curții să precizeze ce atitudine trebuie să adopte autoritățile naționale de supraveghere și Comisia atunci când se confruntă cu disfuncționalități în aplicarea Deciziei 2000/520.

6. Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date [5] prevede, în capitolul IV, norme referitoare la transferul datelor cu caracter personal către țări terțe.

7. În cadrul acestui capitol, principiul instituit la articolul 25 alineatul (1) din directiva menționată este cel potrivit căruia transferul către o țară terță de date cu caracter personal care fac obiectul prelucrării sau sunt destinate prelucrării după transfer nu poate avea loc decât dacă țara terță în cauză asigură un nivel adecvat de protecție a unor astfel de date.

8. În caz contrar, astfel cum arată legiuitorul Uniunii în considerentul (57) al directivei menționate, trebuie interzis transferul datelor cu caracter personal către o țară terță care nu asigură un nivel de protecție adecvat.

9. Potrivit articolului 25 alineatul (2) din Directiva 95/46, „[c]aracterul adecvat al nivelului de protecție oferit de o țară terță se evaluează având în vedere toate circumstanțele referitoare la un transfer sau la o categorie de transferuri de date; în special sunt luate în considerare natura datelor, scopul și durata prelucrării sau prelucrărilor propuse, țările de origine și țările de destinație, normele de drept atât generale, cât și sectoriale în vigoare în țara terță în cauză, precum și normele profesionale și măsurile de securitate respectate în țara respectivă”.

10. În temeiul articolului 25 alineatul (6) din această directivă, Comisia poate constata că o țară terță asigură, în temeiul legislației interne sau al angajamentelor sale internaționale, un nivel adecvat de protecție a datelor cu caracter personal. În cazul în care Comisia adoptă o decizie în acest sens, transferul de date cu caracter personal către țara terță în cauză poate avea loc.

11. În temeiul acestei dispoziții, Comisia a adoptat Decizia 2000/520. Din cuprinsul articolului 1 alineatul (1) din această decizie rezultă că se consideră că „principiile «sferei de siguranță» privind protecția vieții private”, puse în aplicare în conformitate cu orientările furnizate de „întrebările de bază” [6], asigură un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune către întreprinderi stabilite în Statele Unite ale Americii.

12. În consecință, Decizia 2000/520 permite transferul de date cu caracter personal din statele membre către întreprinderi stabilite în Statele Unite care s-au angajat să respecte principiile sferei de siguranță.

13. Decizia 2000/520 prevede, în anexa I, anumite principii la care întreprinderile pot subscrie în mod voluntar, însoțite de limite și de un sistem de control specific. Numărul întreprinderilor care au subscris la ceea ce ar putea fi calificat drept „cod de conduită” depășea cifra de 3 200 în anul 2013.

14. Sistemul sferei de siguranță se întemeiază pe o soluție care combină autocertificarea, precum și autoevaluarea efectuate de întreprinderile private și intervenția autorității publice.

5 — JO L 281, p. 31, Ediție specială, 13/vol. 17, p. 10. Directivă astfel cum a fost modificată prin Regulamentul (CE) nr. 1882/2003 al Parlamentului European și al Consiliului din 29 septembrie 2003 (JO L 284, p. 1, denumită în continuare „Directiva 95/46”).

6 — Frequently asked questions, denumite în continuare „FAQ”.

15. Principiile sferei de siguranță au fost elaborate „prin consultări cu întreprinderile și publicul larg în scopul facilitării comerțului și relațiilor de afaceri dintre Statele Unite ale Americii și Uniune […]. Ele sunt destinate exclusiv organizațiilor din Statele Unite ale Americii care primesc date cu caracter personal din Uniune […] cu scopul de a permite acestor organizații să îndeplinească condițiile privind «sfera de siguranță» și prezumția de «nivel de protecție adecvat» pe care aceasta o creează” [7].

16. Principiile sferei de siguranță, care figurează în anexa I la Decizia 2000/520, prevăd printre altele:

— o obligație de informare potrivit căreia „[o]rice organizație trebuie să informeze persoanele în cauză cu privire la motivele strângerii și utilizării informațiilor cu caracter personal, la modul în care pot contacta organizația pentru orice întrebări sau plângeri, la terții cărora le sunt comunicate informațiile, la opțiunile și mijloacele pe care organizația le oferă persoanelor în cauză pentru limitarea utilizării și divulgării acestor date. Notificarea […] [t]rebuie comunicată persoanelor în cauză atunci când acestea sunt invitate pentru prima dată să furnizeze informații cu caracter personal sau cât mai curând posibil după această invitație, dar, în orice caz, înainte ca datele să fie folosite într-un scop diferit de cel pentru care au fost inițial strânse sau prelucrate de organizația care a efectuat transferul sau înainte ca ele să fie comunicate pentru prima dată unui terț” [8];

— o obligație a organizațiilor de a conferi persoanelor în cauză posibilitatea de a decide dacă datele lor pot fi divulgate unui terț sau pot fi utilizate într-un scop incompatibil cu scopul sau scopurile pentru care au fost inițial strânse sau într-un scop aprobat ulterior de persoana în cauză. În ceea ce privește informațiile sensibile, „orice persoană trebuie să aibă în mod pozitiv sau expres posibilitatea de a decide (consimțământ) dacă datele pot fi divulgate unui terț sau pot fi utilizate într-un scop care diferă de obiectivul inițial pentru care au fost strânse sau într-un scop aprobat ulterior de persoana în cauză prin exercitarea dreptului de consimțământ” [9];

— norme referitoare la transferul ulterior de date. Astfel, „[p]entru a divulga informații unui terț, organizațiile trebuie să aplice principiile notificării și opțiunii” [10];

— în ceea ce privește securitatea datelor, o obligație a „[o]rganizațiil[or] care creează, administrează, utilizează sau difuzează date cu caracter personal [de a lua] măsurile necesare pentru a preveni pierderea, utilizarea abuzivă, consultarea neautorizată, divulgarea, modificarea și distrugerea acestor date” [11];

— în ceea ce privește integritatea datelor, o obligație a organizațiilor, „[de a lua] măsurile necesare pentru a asigura fiabilitatea datelor în raport cu utilizarea prevăzută, precum și acuratețea, exhaustivitatea și actualitatea lor” [12];

— că o persoană ale cărei date sunt deținute de o organizație trebuie, în principiu, „să aibă acces la informațiile cu caracter personal […] și să le poată corecta, modifica sau șterge atunci când sunt incorecte” [13];

7 — Al doilea paragraf al anexei I la Decizia 2000/520.

8 — A se vedea anexa I secțiunea „Notificarea”.

9 — A se vedea anexa I secțiunea „Opțiunea”.

10 — A se vedea anexa I secțiunea „Transferul ulterior”.

11 — A se vedea anexa I secțiunea „Securitatea”.

12 — A se vedea anexa I secțiunea „Integritatea datelor”.

13 — A se vedea anexa I secțiunea „Accesul”.

— o obligație de a prevedea „mecanisme care să permită asigurarea respectării principiilor «sferei de siguranță», posibilitatea de recurs pentru persoanele în cauză care au fost afectate de nerespectarea principiilor și de sancționare a organizațiilor care nu au respectat principiile atunci când s-au angajat să le aplice” [14].

17. O organizație americană care dorește să adere la principiile sferei de siguranță este obligată să prevadă, în politica de protecție a vieții private, că declară în mod public faptul că aderă la principiile respective și că se conformează efectiv acestora și să se autocertifice, notificând Departamentului Comerțului al Statelor Unite că este în conformitate cu principiile amintite [15].

18. Organizațiile dispun de mai multe mijloace pentru a se conforma principiilor sferei de siguranță. Astfel, acestea pot, de exemplu, să „particip[e] la un program privind protecția confidențialității pus la punct de sectorul privat care aderă la principii [sau] se pot conforma acestor condiții și prin elaborarea propriilor regulamente privind protecția datelor, cu condiția ca acestea să fie conforme cu principiile. […] Pe lângă aceasta, organizațiile care se supun unui ansamblu de dispoziții juridice, de reglementare, administrative sau de alt tip (ori unui ansamblu de reguli) care asigură o protecție eficientă a datelor cu caracter personal pot, de asemenea, beneficia de avantajele «sferei de siguranță»” [16].

19. Mai multe mecanisme, care combină arbitrajul privat și controlul efectuat de autoritățile publice, există pentru verificarea respectării principiilor sferei de siguranță. Controlul poate fi asigurat astfel prin intermediul unui sistem de soluționare extrajudiciară a litigiilor de către un terț independent. Pe de altă parte, întreprinderile se pot angaja să coopereze cu comitetul Uniunii privind protecția datelor. În sfârșit, Comisia Federală pentru Comerț (Federal Trade Commission, denumită în continuare „FTC”), pe baza competențelor care îi sunt conferite în temeiul articolului 5 din Legea privind Comisia Federală a Comerțului (Federal Trade Commission Act), și Departamentul Transporturilor (Department of Transportation), pe baza competențelor care îi sunt conferite în temeiul articolului 41712 din Codul Statelor Unite (United States Code), care figurează în titlul 49, sunt competente să soluționeze plângerile.

20. Potrivit celui de al patrulea paragraf din anexa I la Decizia 2000/520, aderarea la principiile sferei de siguranță poate fi limitată printre altele de „cerințele privind securitatea națională, interesul public și respectarea legilor Statelor Unite ale Americii” și de „textele legislative, regulamentele administrative sau jurisprudența care creează obligații contradictorii sau prevăd autorizații exprese, cu condiția ca organizația care a recurs la o asemenea autorizație să poată demonstra că nerespectarea principiilor se limitează la măsurile necesare pentru garantarea intereselor legitime superioare pe care această autorizație urmărește să le servească” [17].

21. În plus, posibilitatea autorităților competente ale statelor membre de a suspenda fluxurile de date este supusă mai multor condiții care sunt prevăzute la articolul 3 alineatul (1) din Decizia 2000/520.

22. Prezenta cerere de decizie preliminară ne determină să reflectăm asupra semnificației Deciziei 2000/520 în raport cu articolele 7, 8 și 47 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”), precum și cu articolul 25 alineatul (6) și cu articolul 28 din Directiva 95/46. Această cerere a fost formulată în cadrul unui litigiu între domnul Schrems și Data Protection Commissioner (Comisarul pentru protecția datelor, denumit în continuare „Comisarul”) cu privire la refuzul acestuia din urmă de a investiga o plângere formulată de domnul Schrems ca urmare a faptului că Facebook Ireland Ltd. (denumită în continuare „Facebook Ireland”) păstrează datele cu caracter personal ale utilizatorilor săi pe servere situate în Statele Unite.

14 — A se vedea anexa I secțiunea „Aplicarea”.

15 — Articolul 1 alineatele (2) și (3) din Decizia 2000/520. A se vedea și anexa II, FAQ 6.

16 — Al treilea paragraf al anexei I.

17 — A se vedea de asemenea anexa IV secțiunea B.

23. Domnul Schrems este un resortisant austriac și are reședința în Austria. Acesta este utilizator al rețelei sociale Facebook din anul 2008.

24. Tuturor utilizatorilor Facebook care au reședința pe teritoriul Uniunii li se solicită să semneze un contract cu Facebook Ireland, care este o filială a societății-mamă Facebook Inc., situată în Statele Unite (denumită în continuare „Facebook USA”). Datele utilizatorilor Facebook Ireland care au reședința pe teritoriul Uniunii sunt, în tot sau în parte, transferate pe serverele Facebook USA, situate pe teritoriul Statelor Unite ale Americii, unde sunt păstrate.

25. Domnul Schrems a depus, la 25 iunie 2013, o plângere la Comisar, susținând, în esență, că dreptul și practicile din Statele Unite nu asigură nicio protecție reală a datelor păstrate pe teritoriul Statelor Unite împotriva supravegherii statului. Aceasta ar rezulta din dezvăluirile făcute de domnul Snowden începând din luna mai 2013 cu privire la activitățile serviciilor de informații americane și în special cele ale National Security Agency (denumită în continuare „NSA”).

26. Rezultă printre altele din aceste dezvăluiri că NSA ar fi stabilit un program denumit „PRISM” în cadrul căruia această agenție ar fi obținut un acces liber la datele de masă stocate pe serverele situate în Statele Unite, care sunt deținute sau controlate de o serie de societăți care își desfășoară activitatea în domeniul internetului și al tehnologiei, precum Facebook USA.

27. Comisarul a considerat că nu era obligat să investigheze plângerea, dat fiind că aceasta era lipsită de temei juridic. Acesta a apreciat că nu existau dovezi că NSA are acces la datele domnului Schrems. În plus, plângerea trebuia să fie respinsă, în opinia sa, având în vedere Decizia 2000/520, prin care Comisia a constatat că Statele Unite asigură, în cadrul sistemului sferei de siguranță, un nivel adecvat de protecție a datelor cu caracter personal transferate. Orice problemă referitoare la caracterul adecvat al protecției acestor date în Statele Unite ar trebui soluționată în conformitate cu această decizie, care l-ar împiedica să examineze problema ridicată de plângere.

28. Legislația națională care a determinat Comisarul să respingă plângerea este următoarea.

29. Articolul 10 alineatul (1) din Legea din 1988 privind protecția datelor (Data Protection Act 1988), astfel cum a fost modificată prin Legea din 2003 privind protecția datelor [Data Protection (Amendment) Act 2003, denumită în continuare „Legea privind protecția datelor”], îi conferă competența de a examina plângerile și prevede:

„(a) Comisarul poate examina sau poate solicita să se examineze dacă dispoziții ale prezentei legi au fost, sunt sau riscă să fie încălcate în ceea ce privește o anumită persoană, fie în cazul în care această persoană formulează în fața sa o plângere privind încălcarea oricăreia dintre aceste dispoziții, fie în cazul în care Comisarul consideră că o astfel de încălcare poate exista.

(b) Atunci când o persoană formulează o plângere în fața Comisarului în temeiul literei (a) a prezentului alineat, Comisarul:

(i) cercetează sau solicită să se cerceteze plângerea, cu excepția situației în care aceasta concluzionează că este hazardată sau vexatorie, și

(ii) în cazul în care acesta sau aceasta nu poate obține, într-un termen rezonabil, din partea părților în cauză o soluționare amiabilă a obiectului plângerii, notifică în scris reclamantului decizia pe care o adoptă cu privire la aceasta, indicând că, dacă decizia respectivă îi cauzează prejudicii, reclamantul poate formula împotriva sa o acțiune în justiție în temeiul articolului 26 din prezenta lege, în termen de 21 de zile de la primirea notificării.”

30. În speță, Comisarul a concluzionat că plângerea formulată de domnul Schrems era „hazardată sau vexatorie” în sensul că aceasta era sortită eșecului întrucât era lipsită de temei juridic. În acest temei, a refuzat să examineze plângerea respectivă.

31. Articolul 11 din Legea privind protecția datelor reglementează transferul datelor cu caracter personal în afara teritoriului național. Articolul 11 alineatul (2) litera (a) din legea menționată prevede:

„Atunci când, în cadrul oricărei proceduri reglementate de prezenta lege, se ridică o problemă:

(i) pentru a stabili dacă nivelul adecvat de protecție prevăzut la alineatul 1 al prezentului articol este asigurat de o țară sau de un teritoriu în afara Spațiului Economic European [(SEE)] căruia urmează să i se transfere date cu caracter personal și

(ii) o constatare a Uniunii a fost efectuată în ceea ce privește tipul de transferuri în discuție,

problema va fi soluționată în conformitate cu această constatare.”

32. Articolul 11 alineatul (2) litera (b) din Legea privind protecția datelor definește noțiunea de constatare a Uniunii după cum urmează:

„La litera (a) a prezentului alineat, «constatarea Uniunii» înseamnă o constatare pe care Comisia […] a făcut-o în sensul alineatului (4) sau al alineatului (6) al articolului 25 din Directiva [95/46], în cadrul procedurii prevăzute la articolul 31 alineatul (2) din [aceasta] pentru a se stabili dacă nivelul adecvat de protecție prevăzut la alineatul (1) al prezentului articol este asigurat de o țară sau de un teritoriu din afara [SEE].”

33. Comisarul a observat că Decizia 2000/520 era o „constatare a Uniunii” în sensul articolului 11 alineatul (2) litera (a) din Legea privind protecția datelor, astfel încât, în temeiul acestei legi, orice problemă referitoare la caracterul adecvat al protecției datelor în țara terță în care acestea sunt transferate trebuia soluționată în conformitate cu respectiva constatare. Întrucât aceasta constituia esența plângerii formulate de domnul Schrems, și anume faptul că date cu caracter personal erau transferate către o țară terță care nu asigura în practică un nivel de protecție adecvat, Comisarul a considerat că natura și însăși existența Deciziei 2000/520 îl împiedicau să examineze această problemă.

34. Domnul Schrems a introdus o acțiune la High Court împotriva deciziei Comisarului de a respinge plângerea sa. După ce a examinat probele prezentate în procedura principală, această instanță a constatat că supravegherea electronică și interceptarea datelor cu caracter personal răspund unor finalități necesare și indispensabile pentru interesul public, și anume menținerea securității naționale și prevenirea infracțiunilor grave. High Court arată, în această privință, că supravegherea și interceptarea datelor cu caracter personal transferate din Uniune către Statele Unite servesc unor obiective legitime legate de combaterea terorismului.

35. Potrivit aceleiași instanțe, dezvăluirile făcute de domnul Snowden au demonstrat însă că NSA și alte organe similare săvârșiseră excese considerabile. Deși Foreign Intelligence Surveillance Court (denumită în continuare „FISC”), care intervine în cadrul Legii din 1978 privind supravegherea serviciilor de informații străine (Foreign Intelligence Surveillance Act of 1978) [18], exercită competențe

18 — A se vedea articolul 702 din această lege, astfel cum a fost modificată prin Legea din 2008 (Foreign Intelligence Surveillance Act of 2008). În temeiul acestui articol, NSA deține o bază de date cunoscută sub denumirea „PRISM” (a se vedea report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection din 27 noiembrie 2013).

de supraveghere, procedura în fața acesteia ar fi însă secretă și necontradictorie. În plus, pe lângă faptul că deciziile referitoare la accesul la date cu caracter personal ar fi adoptate în temeiul dreptului american, cetățenii Uniunii nu ar dispune de niciun drept efectiv de a fi ascultați cu privire la problema supravegherii și interceptării datelor lor.

36. Ar reieși cu claritate din documente voluminoase care însoțesc declarațiile solemne efectuate în litigiul principal că nu se contestă exactitatea unui număr semnificativ de dezvăluiri ale domnului Snowden. În consecință, High Court a concluzionat că, odată ce datele cu caracter personal sunt transferate către Statele Unite, NSA, precum și alte agenții de securitate americane cum ar fi Biroul Federal de Investigații (FBI) pot avea acces la acestea în cadrul supravegherii și interceptării de masă nediferențiate.

37. High Court constată că, în dreptul irlandez, importanța drepturilor constituționale la viață privată și la inviolabilitatea domiciliului impune ca orice ingerință în aceste drepturi să fie conformă cu cerințele prevăzute de lege și proporțională. Accesul în masă și nediferențiat la date cu caracter personal nu ar respecta nicidecum cerința proporționalității și, prin urmare, ar trebui considerat ca fiind contrar Constituției irlandeze [19].

38. High Court arată că, pentru ca interceptări de comunicații electronice să poată fi considerate constituționale, ar trebui să se demonstreze că anumite interceptări de comunicații și supravegherea anumitor persoane sau a anumitor grupuri de persoane sunt justificate în mod obiectiv în interesul securității naționale și combaterii criminalității și că există garanții adecvate și verificabile.

39. În consecință, High Court arată că, în cazul în care prezenta cauză ar trebuie abordată doar în temeiul dreptului irlandez, o problemă considerabilă s-ar ridica în ceea ce privește aspectul dacă Statele Unite „asigură un nivel adecvat de protecție a vieții private și a drepturilor și libertăților fundamentale”, în sensul articolului 11 alineatul (1) din Legea privind protecția datelor. În consecință, în temeiul dreptului irlandez și în special al cerințelor constituționale, Comisarul nu ar fi putut respinge plângerea formulată de domnul Schrems, ci ar fi trebuit să examineze această problemă.

40. Totuși, High Court constată că această cauză cu care este sesizată privește punerea în aplicare a dreptului Uniunii în sensul articolului 51 alineatul (1) din cartă, astfel încât legalitatea deciziei Comisarului ar trebui apreciată în raport cu dreptul Uniunii.

41. Problema cu care Comisarul s-a confruntat este explicată de High Court după cum urmează. În temeiul articolului 11 alineatul (2) litera (b) din Legea privind protecția datelor, Comisarul trebuie să soluționeze problema caracterului adecvat al protecției din țara terță „în conformitate” cu o constatare a Uniunii realizată de Comisie potrivit articolului 25 alineatul (6) din Directiva 95/46. În consecință, Comisarul nu s-ar putea îndepărta de o asemenea constatare. Întrucât Comisia a constatat, în Decizia 2000/520, că Statele Unite garantează un nivel de protecție adecvat în ceea ce privește prelucrarea datelor de către societăți care aderă la principiile sferei de siguranță, o plângere care dovedește caracterul inadecvat al unei asemenea protecții ar trebui respinsă în mod necesar de către Comisar.

42. Constatând totodată că Comisarul a făcut astfel dovada unei fidelități scrupuloase față de textul Directivei 95/46 și al Deciziei 2000/520, High Court arată că domnul Schrems obiectează în realitate mai mult cu privire la cerințele sistemului sferei de siguranță însuși decât cu privire la modul în care Comisarul l-a aplicat, subliniind totodată că nu a contestat în mod direct validitatea Directivei 95/46 și nici pe cea a Deciziei 2000/520.

19 — High Court face trimitere în special la respectarea demnității umane și la libertatea persoanei (preambul), la autonomia personală (articolul 40 alineatul 3 punctele 1 și 2), la inviolabilitatea domiciliului [articolul 40 alineatul (5)] și la protecția vieții de familie (articolul 41).

43. Potrivit High Court, problema esențială ar fi, așadar, dacă, având în vedere dreptul Uniunii și ținând seama în special de intrarea în vigoare ulterioară a articolelor 7 și 8 din cartă, Comisarul este ținut în mod absolut de constatarea Comisiei enunțată în Decizia 2000/520 referitoare la caracterul adecvat al dreptului și al practicilor în domeniul protecției datelor cu caracter personal în Statele Unite.

44. High Court precizează în plus că, în cadrul acțiunii cu care este sesizată, nicio critică nu a fost invocată în privința acțiunilor Facebook Ireland și Facebook USA ca atare. Or, articolul 3 alineatul (1) litera (b) din Decizia 2000/520, care permite autorităților naționale competente să solicite unei întreprinderi să suspende fluxurile de date către o țară terță, s-ar aplica, potrivit acestei instanțe, doar în circumstanțe în care plângerea este îndreptată împotriva comportamentului întreprinderii în cauză, ceea ce nu s-ar regăsi în speță.

45. High Court subliniază, în consecință, că obiecția efectivă este îndreptată nu împotriva comportamentului Facebook USA ca atare, ci mai degrabă împotriva faptului că Comisia a considerat că dreptul și practicile în domeniul protecției datelor în Statele Unite garantează o protecție adecvată, în condițiile în care dezvăluirile domnului Snowden dovedesc cu claritate că autoritățile americane pot avea acces în masă și în mod nediferențiat la datele cu caracter personal ale populației care locuiește pe teritoriul Uniunii [20].

46. Cu privire la acest aspect, High Court consideră că este dificil să se imagineze modalitatea în care Decizia 2000/520 ar putea respecta, în practică, cerințele prevăzute la articolele 7 și 8 din cartă, *a fortiori* în cazul în care se ține seama de principiile formulate de Curte în Hotărârea Digital Rights Ireland și alții [21]. În special, garanția prevăzută la articolul 7 din cartă și de valorile esențiale comune tradițiilor statelor membre ar fi compromisă în cazul în care s-ar permite autorităților publice să aibă acces la comunicațiile electronice în mod aleatoriu și generalizat, fără a trebui să furnizeze o motivare obiectivă întemeiată pe motive de securitate națională sau de prevenire a criminalității legate în mod specific de indivizii în cauză și fără nicio garanție adecvată și verificabilă. Întrucât acțiunea introdusă de domnul Schrems sugerează că Decizia 2000/520 ar putea fi *in abstracto* incompatibilă cu articolele 7 și 8 din cartă, Curtea ar putea considera că este posibil să interpreteze Directiva 95/46 și în special articolul 25 alineatul (6) din aceasta, precum și Decizia 2000/520 într-un sens care să permită autorităților naționale să își efectueze propriile anchete pentru a stabili dacă transferul datelor cu caracter personal către o țară terță și păstrarea acestora în această țară respectă cerințele care decurg din articolele 7 și 8 din cartă.

47. În aceste condiții, High Court a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„În cursul analizei unei plângeri […] referitoare la faptul că date cu caracter personal sunt transferate într-o țară terță (în speță, Statele Unite) ale cărei legi și practici se pretinde că nu conțin măsuri de protecție adecvate pentru persoana în cauză, [Comisarul], având în vedere articolele 7, 8 și 47 din [cartă] și fără a aduce atingere dispozițiilor articolului 25 alineatul (6) din Directiva 95/46, este ținut în mod absolut să respecte constatarea contrară a Uniunii cuprinsă în Decizia 2000/520?

Sau, dimpotrivă, funcționarul poate și/sau trebuie să desfășoare o investigație proprie asupra problemei în lumina evoluțiilor factuale ulterioare datei la care [Decizia 2000/520] a fost publicată pentru prima dată?”

20 — High Court arată, în această privință, că principalul mijloc invocat de domnul Schrems în fața sa consta în afirmația că, ținând seama de recentele dezvăluiri ale domnului Snowden și ca urmare a faptului că date cu caracter personal au fost puse la dispoziția serviciilor de informații ale Statelor Unite la scară largă, Comisarul nu putea concluziona în mod valabil că există, în această țară terță, un nivel de protecție adecvat al acestor date.

21 — C-293/12 și C-594/12, EU:C:2014:238, punctele 65-69.

II – **Analiza noastră**

48. Cele două întrebări formulate de High Court invită Curtea să precizeze competențele de care dispun autoritățile naționale de supraveghere atunci când sunt sesizate cu o plângere cu privire la un transfer de date cu caracter personal către o întreprindere stabilită într-o țară terță și se afirmă, în susținerea acestei plângeri, că țara terță în cauză nu garantează un nivel adecvat de protecție a datelor transferate, în condițiile în care Comisia a adoptat, în temeiul articolului 25 alineatul (6) din Directiva 95/46, o decizie de recunoaștere a caracterului adecvat al nivelului de protecție asigurat de respectiva țară terță.

49. Observăm că plângerea depusă de domnul Schrems la Comisar implică o dublă dimensiune. Aceasta urmărește să împiedice transferul de date cu caracter personal de la Facebook Ireland către Facebook USA. Domnul Schrems solicită să se pună capăt acestui transfer deoarece, în opinia sa, Statele Unite nu ar asigura un nivel adecvat de protecție a datelor cu caracter personal care sunt transferate în cadrul sistemului sferei de siguranță. Mai precis, acesta reproșează țării terțe respective faptul că a pus în practică programul PRISM, care permite NSA să aibă acces în mod liber la datele de masă stocate pe servere situate în Statele Unite. Astfel, plângerea privește în special transferul de date cu caracter personal de la Facebook Ireland către Facebook USA, punând în discuție în același timp, cu titlu mai general, nivelul de protecție asigurat unor asemenea date în cadrul sistemului sferei de siguranță.

50. Comisarul a considerat că însăși existența unei decizii a Comisiei prin care se recunoaște că Statele Unite asigură, în cadrul sistemului sferei de siguranță, un nivel de protecție adecvat îl împiedica să investigheze plângerea.

51. Prin urmare, trebuie să se examineze împreună cele două întrebări care urmăresc să stabilească, în esență, dacă articolul 28 din Directiva 95/46 coroborat cu articolele 7 și 8 din cartă trebuie interpretat în sensul că existența unei decizii adoptate de Comisie în temeiul articolului 25 alineatul (6) din această directivă are drept efect să împiedice o autoritate națională de supraveghere să investigheze o plângere prin care se susține că o țară terță nu asigură un nivel adecvat de protecție a datelor cu caracter personal transferate și, dacă este cazul, să suspende transferul acestor date.

52. Articolul 7 din cartă garantează dreptul la respectarea vieții private, în timp ce articolul 8 din aceasta consacră în mod expres dreptul la protecția datelor cu caracter personal. Alineatele (2) și (3) ale acestui din urmă articol prevăd că asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege, că orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora și că respectarea acestor norme se supune controlului unei autorități independente.

A – *Cu privire la competențele autorităților naționale de supraveghere în cazul unei decizii de adecvare a Comisiei*

53. Astfel cum indică domnul Schrems în observații, în sensul plângerii în discuție în litigiul principal, problema centrală este cea a transferului de date cu caracter personal de la Facebook Ireland către Facebook USA în lumina accesului generalizat pentru NSA și alte agenții de securitate americane la datele stocate la Facebook USA în aplicarea competențelor conferite acestora de legislația americană.

54. Sesizată cu o plângere prin care se urmărește să se repună în discuție constatarea potrivit căreia o țară terță asigură un nivel adecvat de protecție a datelor transferate, autoritatea națională de supraveghere are, în opinia domnului Schrems, competența, în cazul în care dispune de elemente în sensul temeiniciei afirmațiilor conținute în această plângere, de a dispune suspendarea transferului de date realizat de întreprinderea desemnată în plângerea respectivă.

55. Ținând seama de obligațiile Comisarului de a proteja drepturile fundamentale ale domnului Schrems, acesta din urmă susține că Comisarul are obligația nu numai de a investiga, ci și, în cazul admiterii plângerii, de a-și exercita competențele pentru a suspenda fluxul de date dintre Facebook Ireland și Facebook USA.

56. Or, Comisarul a respins plângerea pe baza dispozițiilor Legii privind protecția datelor care enumeră competențele sale. Această concluzie se întemeia pe punctul de vedere al Comisarului potrivit căruia era ținut de Decizia 2000/520.

57. În consecință, problema centrală în prezenta cauză este cea dacă aprecierea Comisiei în ceea ce privește caracterul adecvat al nivelului de protecție, cuprinsă în Decizia 2000/520, este obligatorie în mod absolut pentru autoritatea națională de protecție a datelor și o împiedică să investigheze afirmațiile prin care se urmărește să se repună în discuție această constatare. Prin urmare, întrebările preliminare privesc întinderea competențelor de investigare ale autorităților naționale de protecție a datelor în prezența unei decizii de adecvare a Comisiei.

58. Potrivit Comisiei, trebuie să se țină seama de coroborarea competențelor acesteia cu cele ale autorităților naționale de protecție a datelor. Competențele acestora din urmă ar fi centrate pe aplicarea legislației în această materie în cazuri individuale, în timp ce reexaminarea generală a aplicării Deciziei 2000/520, inclusiv a oricărei decizii care implică suspendarea sau abrogarea sa, ar ține de competența Comisiei.

59. Comisia arată că domnul Schrems nu ar fi invocat argumente specifice prin care să se considere că s-ar expune unui risc iminent de a suferi prejudicii grave ca urmare a transferului de date dintre Facebook Ireland și Facebook USA. Dimpotrivă, ca urmare a naturii lor abstracte și generale, îngrijorările exprimate de domnul Schrems în privința programelor de supraveghere puse în aplicare de agențiile de securitate americane ar fi identice cu cele care au determinat Comisia să inițieze reexaminarea Deciziei 2000/520.

60. Potrivit Comisiei, autoritățile naționale de supraveghere ar afecta competențele de care dispune pentru renegocierea condițiilor prevăzute de această decizie cu Statele Unite sau, dacă este nevoie, pentru suspendarea acesteia, în cazul în care ar lua măsuri pe baza plângerilor care exprimă doar preocupări structurale și abstracte.

61. Nu suntem de acord cu punctul de vedere al Comisiei. În opinia noastră, existența unei decizii adoptate de Comisie în temeiul articolului 25 alineatul (6) din Directiva 95/46 nu poate anula și nici măcar reduce competențele de care dispun autoritățile naționale de supraveghere în temeiul articolului 28 din această directivă. Contrar susținerilor Comisiei, în cazul în care autoritățile naționale de supraveghere sunt sesizate în cadrul plângerilor individuale, aceasta nu le împiedică, în opinia noastră, în temeiul competențelor de investigare și al independenței lor, să își exprime propriul punct de vedere cu privire la nivelul general de protecție asigurat de o țară terță și să acționeze în consecință atunci când se pronunță cu privire la cazuri individuale.

62. Rezultă dintr-o jurisprudență constantă a Curții că, în vederea interpretării dispozițiilor dreptului Uniunii, trebuie să se țină seama nu numai de formularea acestora, ci și de contextul lor și de obiectivele urmărite de reglementarea din care fac parte aceste dispoziții [22].

63. Reiese din considerentul (62) al Directivei 95/46 că „instituirea în statele membre a unor autorități de supraveghere care să își exercite atribuțiile în deplină independență este un element esențial al protecției persoanelor în ceea ce privește prelucrarea datelor cu caracter personal”.

22 — A se vedea în special Hotărârea Koushkaki (C-84/12, EU:C:2013:862, punctul 34 și jurisprudența citată).

64. Potrivit articolului 28 alineatul (1) primul paragraf din această directivă, „[f]iecare stat membru prevede ca una sau mai multe autorități publice să fie responsabile de supravegherea aplicării pe teritoriul său a dispozițiilor adoptate de statele membre în temeiul prezentei directive”. Articolul 28 alineatul (1) al doilea paragraf din directiva menționată prevede că „[a]ceste autorități acționează în condiții de independență deplină în exercitarea atribuțiilor cu care sunt învestite”.

65. Articolul 28 alineatul (3) din Directiva 95/46 enumeră competențele de care dispune fiecare autoritate de supraveghere, și anume competențe de investigare, competențe efective de intervenție care îi permit printre altele interdicția temporară sau definitivă de prelucrare, precum și competența de a acționa în justiție, în cazul încălcării dispozițiilor de drept intern adoptate în temeiul acestei directive, sau competența de a sesiza autoritățile judecătorești asupra acestor încălcări.

66. Pe de altă parte, potrivit articolului 28 alineatul (4) primul paragraf din Directiva 95/46, „[f]iecare autoritate de supraveghere poate fi sesizată de orice persoană […] printr-o cerere de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal”. Articolul 28 alineatul (4) al doilea paragraf din această directivă prevede că „[f]iecare autoritate de supraveghere poate fi sesizată printr-o plângere depusă de orice persoană cu privire la legalitatea prelucrării datelor, atunci când se aplică dispozițiile de drept intern adoptate în temeiul articolului 13 din [respectiva] directivă”. Precizăm că această din urmă dispoziție permite statelor membre să adopte măsuri legislative în scopul restrângerii domeniului de aplicare al mai multor obligații și drepturi prevăzute în Directiva 95/46, atunci când o astfel de restrângere este o măsură necesară în special pentru a garanta securitatea statului, apărarea, siguranța publică, precum și prevenirea, cercetarea, depistarea și urmărirea penală a infracțiunilor.

67. Astfel cum a arătat Curtea deja, cerința supravegherii de către o autoritate independentă a respectării normelor Uniunii referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal rezultă și din dreptul primar al Uniunii, în special din cuprinsul articolului 8 alineatul (3) din cartă și din cuprinsul articolului 16 alineatul (2) TFUE [23]. Aceasta a amintit de asemenea că „[i]nstituirea în statele membre a unor autorități de supraveghere independente constituie astfel un element esențial al respectării protecției persoanelor în ceea ce privește prelucrarea datelor cu caracter personal” [24].

68. Curtea a statuat de asemenea că „articolul 28 alineatul (1) al doilea paragraf din Directiva 95/46 trebuie interpretat în sensul că autoritățile de supraveghere competente pentru supravegherea prelucrării datelor cu caracter personal trebuie să beneficieze de o independență care să le permită să își exercite atribuțiile fără a fi supuse unei influențe exterioare. Această independență exclude printre altele orice ingerință și orice altă influență exterioară, sub orice formă, fie directă, fie indirectă, care ar fi susceptibile să le orienteze deciziile și care, astfel, ar putea să pună în discuție îndeplinirea de către autoritățile menționate a sarcinii lor care constă în stabilirea unui echilibru just între protecția dreptului la viață privată și libera circulație a datelor cu caracter personal” [25].

69. Curtea a precizat de asemenea că „garanția de independență a autorităților naționale de supraveghere are în vedere să asigure eficiența și fiabilitatea supravegherii respectării dispozițiilor în domeniul protecției persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal” [26]. Această garanție de independență a fost instituită „pentru a consolida protecția persoanelor și a organismelor care sunt avute în vedere prin deciziile [acestor autorități naționale de supraveghere]” [27].

23 — A se vedea Hotărârile Comisia/Austria (C-614/10, EU:C:2012:631, punctul 36) și Comisia/Ungaria (C-288/12, EU:C:2014:237, punctul 47).

24 — A se vedea în special Hotărârea Comisia/Ungaria (C-288/12, EU:C:2014:237, punctul 48 și jurisprudența citată). A se vedea de asemenea în acest sens Hotărârea Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238, punctul 68, precum și jurisprudența citată).

25 — A se vedea în special Hotărârea Comisia/Ungaria (C-288/12, EU:C:2014:237, punctul 51 și jurisprudența citată).

26 — Hotărârea Comisia/Germania (C-518/07, EU:C:2010:125, punctul 25).

27 — *Idem.*

70. Astfel cum reiese în special din considerentul (10) și din cuprinsul articolului 1 din Directiva 95/46, aceasta urmărește să garanteze, în cadrul Uniunii, „un nivel ridicat de protecție a libertăților și a drepturilor fundamentale în ceea ce privește prelucrarea datelor cu caracter personal”[28]. Potrivit Curții, „[a]utoritățile de supraveghere prevăzute la articolul 28 din Directiva 95/46 sunt, așadar, gardieni ai drepturilor și libertăților fundamentale”[29].

71. Având în vedere importanța rolului pe care îl au autoritățile naționale de supraveghere în domeniul protecției persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, competențele lor de intervenție trebuie să rămână depline chiar și atunci când Comisia a adoptat o decizie în temeiul articolului 25 alineatul (6) din Directiva 95/46.

72. Observăm în această privință că niciun element nu arată că sistemele de transfer de date cu caracter personal către țări terțe ar fi excluse din domeniul de aplicare material al articolului 8 alineatul (3) din cartă, care consacră la cel mai înalt nivel al ierarhiei normelor în dreptul Uniunii importanța controlului exercitat de o autoritate independentă în ceea ce privește respectarea normelor referitoare la protecția datelor cu caracter personal.

73. În cazul în care autoritățile naționale de supraveghere ar fi ținute în mod absolut de deciziile adoptate de Comisie, acest fapt ar limita în mod inevitabil independența totală a acestora. În conformitate cu rolul lor de gardieni ai drepturilor fundamentale, autoritățile naționale de supraveghere trebuie să aibă posibilitatea de a investiga, în condiții de independență deplină, reclamațiile care le sunt prezentate, în interesul superior al protecției indivizilor în ceea ce privește prelucrarea datelor cu caracter personal.

74. În plus, astfel cum au arătat în mod întemeiat guvernul belgian și Parlamentul European în ședință, nu există nicio legătură ierarhică între capitolul IV din Directiva 95/46, referitor la transferul de date cu caracter personal către țări terțe, și capitolul VI din aceasta, care este consacrat în special rolului autorităților naționale de supraveghere. Niciun element din acest capitol VI nu sugerează că dispozițiile referitoare la autoritățile naționale de supraveghere ar fi subordonate într-o anumită măsură dispozițiilor distincte privind transferurile enunțate în capitolul IV din Directiva 95/46.

75. Dimpotrivă, din cuprinsul articolului 25 alineatul (1) din această directivă, care figurează în capitolul IV din aceasta, reiese în mod expres că autorizarea transferului de date cu caracter personal către o țară terță care asigură un nivel de protecție adecvat nu poate avea loc decât sub rezerva respectării dispozițiilor de drept intern adoptate în temeiul celorlalte dispoziții ale directivei menționate.

76. Reamintim în această privință că, în temeiul dispoziției menționate, statele membre trebuie să prevadă, în legislația lor națională, că transferul către o țară terță de date cu caracter personal care fac obiectul unei prelucrări sau sunt destinate să facă obiectul unei prelucrări după transfer nu poate avea loc decât dacă, sub rezerva respectării dispozițiilor de drept intern adoptate în temeiul celorlalte dispoziții ale Directivei 95/46, țara terță în cauză asigură un nivel de protecție adecvat.

77. Conform articolului 28 alineatul (1) din această directivă, autoritățile naționale de supraveghere sunt responsabile de supravegherea aplicării pe teritoriul fiecărui stat membru a dispozițiilor adoptate de statele membre în temeiul directivei menționate.

28 — *Ibidem* (punctul 22 și jurisprudența citată).

29 — *Ibidem* (punctul 23). A se vedea în acest sens Hotărârile Comisia/Austria (C-614/10, EU:C:2012:631, punctul 52) și Comisia/Ungaria (C-288/12, EU:C:2014:237, punctul 53).

78. Apropierea dintre aceste două dispoziții permite să se considere că norma enunțată la articolul 25 alineatul (1) din Directiva 95/46, potrivit căreia transferul datelor cu caracter personal nu poate avea loc decât dacă țara terță destinatară le asigură un nivel de protecție adecvat, face parte dintre normele a căror aplicare trebuie asigurată de autoritățile naționale de supraveghere.

79. Competențele autorităților naționale de supraveghere privind investigarea în condiții de independență deplină a reclamațiilor cu care sunt sesizate în temeiul articolului 28 din Directiva 95/46 trebuie interpretate în sens larg, conform articolului 8 alineatul (3) din cartă. Prin urmare, aceste competențe nu pot fi limitate de competențele acordate de legiuitorul Uniunii Comisiei, în temeiul articolului 25 alineatul (6) din această directivă, în vederea constatării caracterului adecvat al nivelului de protecție asigurat de o țară terță.

80. Având în vedere rolul lor esențial în domeniul protecției datelor cu caracter personal, autoritățile naționale de supraveghere trebuie să poată investiga atunci când sunt sesizate cu o plângere în care se menționează elemente care ar putea fi de natură să repună în discuție nivelul de protecție asigurat de o țară terță, inclusiv atunci când Comisia a constatat, într-o decizie adoptată în temeiul articolului 25 alineatul (6) din Directiva 95/46, că țara terță în cauză asigură un nivel de protecție adecvat.

81. În cazul în care, la încheierea investigațiilor care se efectuează de o autoritate națională de supraveghere, aceasta consideră că transferul de date contestat aduce atingere protecției de care trebuie să beneficieze cetățenii Uniunii în ceea ce privește prelucrarea datelor lor, autoritatea menționată are competența de a suspenda transferul de date în cauză, indiferent care este evaluarea generală realizată de Comisie în decizia sa.

82. Astfel, este cert, potrivit articolului 25 alineatul (2) din Directiva 95/46, că caracterul adecvat al nivelului de protecție asigurat de o țară terță se evaluează în funcție de un ansamblu de circumstanțe atât de fapt, cât și de drept. În cazul în care una dintre aceste circumstanțe evoluează și este de natură să repună în discuție caracterul adecvat al nivelului de protecție asigurat de o țară terță, autoritatea națională de supraveghere sesizată cu o plângere trebuie să poată acționa în consecință în raport cu transferul contestat.

83. Desigur, astfel cum a arătat Irlanda, Decizia 2000/520 este obligatorie pentru Comisar, ca și pentru celelalte autorități ale statului. Rezultă astfel din cuprinsul articolului 288 al patrulea paragraf TFUE că o decizie adoptată de o instituție a Uniunii este obligatorie în toate elementele sale. În consecință, Decizia 2000/520 se impune statelor membre cărora li se adresează.

84. Precizăm în această privință că Decizia 2000/520 însăși prevede, la articolul 5, că „[s]tatele membre iau toate măsurile necesare pentru a se conforma [acesteia] în termen de 90 de zile de la data notificării acesteia către statele membre”. În plus, articolul 6 din decizia menționată confirmă că „[aceasta] se adresează statelor membre”.

85. Considerăm însă că, având în vedere dispozițiile citate anterior ale Directivei 95/46 și ale cartei, efectul obligatoriu al Deciziei 2000/520 nu este de natură să excludă orice investigație a Comisarului cu privire la plângerile prin care se susține că anumite transferuri de date cu caracter personal efectuate către Statele Unite în cadrul acestei decizii nu prezintă garanțiile necesare de protecție impuse de dreptul Uniunii. Cu alte cuvinte, un asemenea efect obligatoriu nu este de natură să impună ca orice plângere de acest gen să fie respinsă în mod sumar, și anume de îndată și fără nicio examinare a temeiniciei sale.

86. Adăugăm că, în plus, reiese din economia articolului 25 din Directiva 95/46 că constatarea potrivit căreia o țară terță asigură sau nu asigură un nivel de protecție adecvat poate fi efectuată fie de către statele membre, fie de către Comisie. Prin urmare, este vorba despre o competență partajată.

87. Rezultă din cuprinsul articolului 25 alineatul (6) din această directivă că, în cazul în care Comisia constată că o țară terță asigură un nivel de protecție adecvat, în sensul articolului 25 alineatul (2) din directiva menționată, statele membre trebuie să ia măsurile necesare pentru a se conforma deciziei Comisiei.

88. Întrucât o asemenea decizie are drept efect să permită transferurile de date cu caracter personal către o țară terță al cărei nivel de protecție este considerat de către Comisie ca fiind adecvat, statele membre trebuie să permită, așadar, în principiu, ca astfel de transferuri să fie efectuate de întreprinderi stabilite pe teritoriul lor.

89. Articolul 25 din Directiva 95/46 nu atribuie însă Comisiei exclusivitatea în materia constatării nivelului adecvat sau inadecvat de protecție a datelor cu caracter personal transferate. Economia acestui articol dovedește că statele membre ocupă de asemenea un rol în materie. O decizie a Comisiei are, desigur, un rol important în ceea ce privește uniformizarea condițiilor de transfer valabile în cadrul statelor membre. Totuși, această uniformizare poate continua numai atât timp cât această constatare nu este repusă în discuție.

90. Argumentul uniformizării necesare a condițiilor de transfer al datelor cu caracter personal către o țară terță își are limita, în opinia noastră, într-o situație precum cea în discuție în litigiul principal, în care Comisia nu numai că este informată cu privire la faptul că constatarea sa face obiectul criticilor, ci ea însăși formulează astfel de critici și poartă negocieri pentru a le remedia.

91. Aprecierea caracterului adecvat sau inadecvat al nivelului de protecție oferit de o țară terță poate da naștere de asemenea unei cooperări între statele membre și Comisie. Articolul 25 alineatul (3) din Directiva 95/46 prevede, în această privință, că „[s]tatele membre și Comisia se informează reciproc în cazurile în care consideră că o țară terță nu asigură un nivel de protecție adecvat în sensul alineatului (2)”. Astfel cum observă Parlamentul European, aceasta demonstrează efectiv că statele membre și Comisia au un rol echivalent în ceea ce privește identificarea situațiilor în care o țară terță nu asigură un nivel de protecție adecvat.

92. Decizia de adecvare are drept obiect autorizarea transferului de date cu caracter personal către țara terță în cauză. Aceasta nu înseamnă că autoritățile de supraveghere nu mai pot fi sesizate de cetățenii Uniunii cu o cerere prin care se urmărește protejarea datelor lor cu caracter personal. Observăm, în această privință, că articolul 28 alineatul (4) primul paragraf din Directiva 95/46, potrivit căruia „[f]iecare autoritate de supraveghere poate fi sesizată de orice persoană […] printr-o cerere de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal”, nu prevede o excepție de la acest principiu în cazul existenței unei decizii adoptate de Comisie în temeiul articolului 25 alineatul (6) din această directivă.

93. Astfel, deși o decizie adoptată de Comisie în temeiul competențelor de executare care îi sunt conferite prin această din urmă dispoziție are drept efect să permită transferul de date cu caracter personal către o țară terță, în schimb, o asemenea decizie nu poate avea drept efect privarea de orice competență a statelor membre și în special a autorităților naționale de supraveghere sau chiar și numai restrângerea atribuțiilor lor, în cazul în care acestea se confruntă cu susțineri privind încălcarea unor drepturi fundamentale.

94. O autoritate națională de supraveghere trebuie să fie în măsură să își exercite competențele prevăzute la articolul 28 alineatul (3) din Directiva 95/46, inclusiv aceea de a interzice temporar sau definitiv prelucrarea datelor cu caracter personal. Deși enumerarea competențelor, care figurează în cuprinsul acestei dispoziții, nu prevede în mod explicit competențe referitoare la un transfer dintr-un stat membru către o țară terță, trebuie să se considere, în opinia noastră, că un astfel de transfer

constituie o prelucrare a datelor [30]. Astfel cum rezultă, în plus, din modul de redactare a dispoziției menționate, enumerarea nu este exhaustivă. În orice caz, având în vedere rolul esențiat al autorităților naționale de supraveghere în cadrul sistemului instituit de Directiva 95/46, acestea trebuie să dispună de competența de a suspenda un transfer de date în cazul aducerii unei atingeri dovedite sau al riscului de a se aduce o atingere drepturilor fundamentale.

95. Adăugăm că privarea autorității naționale de supraveghere de competențele sale de investigare în circumstanțe precum cele în discuție în prezenta cauză ar fi contrară nu numai principiului independenței, ci și obiectivului Directivei 95/46, astfel cum rezultă din cuprinsul articolului 1 alineatul (1) din aceasta.

96. Astfel cum a arătat Curtea, „[d]in considerentele (3), (8) și (10) ale Directivei 95/46 rezultă că legiuitorul Uniunii a înțeles să faciliteze libera circulație a datelor cu caracter personal prin apropierea legislațiilor statelor membre, protejând în același timp drepturile fundamentale ale persoanelor, în special dreptul la protejarea vieții private, și garantând un nivel ridicat de protecție în Uniune. Astfel, articolul 1 din această directivă prevede că statele membre trebuie să asigure protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viață privată, în privința prelucrării datelor cu caracter personal” [31].

97. Prin urmare, dispozițiile Directivei 95/46 trebuie interpretate în conformitate cu obiectivul acesteia prin care se urmărește garantarea unui nivel ridicat de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice, în special a vieții lor private, în ceea ce privește prelucrarea datelor cu caracter personal în cadrul Uniunii.

98. Importanța acestui obiectiv și rolul pe care statele membre trebuie să îl joace pentru a-l atinge presupune că, atunci când circumstanțe speciale constituie temeiul unei îndoieli serioase în ceea ce privește respectarea drepturilor fundamentale garantate de cartă în cazul unui transfer de date cu caracter personal către o țară terță, statele membre și, așadar, în cadrul lor, autoritățile naționale de supraveghere nu pot fi ținute în mod absolut de o decizie de adecvare a Comisiei.

99. Curtea a statuat deja că „dispozițiile Directivei 95/46, în măsura în care reglementează prelucrarea unor date cu caracter personal care pot aduce atingere libertăților fundamentale și în special dreptului la viață privată, trebuie interpretate în mod necesar în lumina drepturilor fundamentale care, potrivit unei jurisprudențe constante, fac parte integrantă din principiile generale de drept a căror respectare o asigură Curtea și care sunt în prezent înscrise în cartă” [32].

100. Ne referim, în plus, la jurisprudența potrivit căreia „statele membre au obligația nu numai de a interpreta dreptul lor național într-un mod conform dreptului Uniunii, ci și de a se asigura că nu se întemeiază pe o interpretare a unui text de drept derivat care ar intra în conflict cu drepturile fundamentale protejate de ordinea juridică a Uniunii sau cu alte principii generale ale dreptului Uniunii” [33].

30 — A se vedea Concluziile avocatului general Léger prezentate în cauza Parlamentul European/Consiliul și Comisia (C-317/04, EU:C:2005:710, punctele 92-95). A se vedea de asemenea Hotărârea Parlamentul European/Consiliul și Comisia (C-317/04 și C-318/04, EU:C:2006:346, punctul 56).

31 — A se vedea în special Hotărârea IPI (C-473/12, EU:C:2013:715, punctul 28 și jurisprudența citată).

32 — A se vedea în special Hotărârea Google Spain și Google (C-131/12, EU:C:2014:317, punctul 68 și jurisprudența citată).

33 — A se vedea în special Hotărârea N. S. și alții (C-411/10 și C-493/10, EU:C:2011:865, punctul 77, precum și jurisprudența citată).

101. Curtea a statuat astfel, în Hotărârea N. S. și alții [34], că „o aplicare a Regulamentului [(CE)] nr. 343/2003 [35] în temeiul unei prezumții irefragabile potrivit căreia drepturile fundamentale ale solicitantului de azil vor fi respectate în statul membru în mod normal competent pentru examinarea cererii sale este incompatibilă cu obligația statelor membre de a interpreta și de a aplica Regulamentul nr. 343/2003 într-un mod conform cu drepturile fundamentale” [36].

102. În această privință, Curtea a admis, în contextul statutului statelor membre ca țări de origine sigure unele în raport cu celelalte pentru problemele juridice și practice legate de dreptul de azil, că trebuie să se prezume că tratamentul aplicat solicitanților de azil în fiecare stat membru este conform cu cerințele impuse de cartă, de Convenția privind statutul refugiaților, semnată la Geneva la 28 iulie 1951 [37], precum și de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, semnată la Roma la 4 noiembrie 1950 [38]. Cu toate acestea, Curtea a statuat că „[n]u poate fi exclus […] ca, în practică, acest sistem să întâmpine dificultăți majore de funcționare într-un anumit stat membru, astfel încât să existe un risc serios ca, în cazul transferului către acest stat membru, solicitanții de azil să fie tratați într-un mod incompatibil cu drepturile lor fundamentale” [39].

103. În consecință, Curtea a statuat că „revine statelor membre, inclusiv instanțelor naționale, obligația de a nu transfera un solicitant de azil către «statul membru responsabil» în sensul Regulamentului nr. 343/2003 atunci când acestea nu pot ignora faptul că deficiențele sistemice ale procedurii de azil și ale condițiilor de primire a solicitanților de azil în acest stat membru constituie motive serioase și întemeiate să se creadă că solicitantul va fi expus unui risc real de a fi supus unor tratamente inumane sau degradante în sensul articolului 4 din cartă” [40].

104. Contribuția Hotărârii N. S. și alții [41] ne pare că poate fi extinsă la o situație precum cea în discuție în litigiul principal. Astfel, o interpretare a dreptului derivat al Uniunii care s-ar întemeia pe o prezumție irefragabilă potrivit căreia drepturile fundamentale vor fi respectate – indiferent dacă este vorba despre un stat membru, despre Comisie sau despre o țară terță – trebuie considerată ca fiind incompatibilă cu obligația statelor membre de a interpreta și de a aplica dreptul derivat al Uniunii în mod conform cu drepturile fundamentale. Prin urmare, articolul 25 alineatul (6) din Directiva 95/46 nu impune o asemenea prezumție irefragabilă de respectare a drepturilor fundamentale în ceea ce privește aprecierea Comisiei cu privire la caracterul adecvat al nivelului de protecție oferit de o țară terță. Dimpotrivă, prezumția care stă la baza acestei dispoziții, potrivit căreia transferul de date către o țară terță respectă drepturile fundamentale, trebuie considerată refragabilă [42]. În consecință, dispoziția menționată nu ar trebui interpretată în sensul că repune în discuție garanțiile care figurează în special la articolul 28 alineatul (3) din Directiva 95/46 și la articolul 8 alineatul (3) din cartă, privind protecția și respectarea dreptului la protecția datelor cu caracter personal.

105. Prin urmare, deducem din hotărârea amintită că, în cazul unor deficiențe sistemice constatate în țara terță către care sunt transferate date cu caracter personal, statele membre trebuie să poată lua măsurile necesare pentru apărarea drepturilor fundamentale protejate prin articolele 7 și 8 din cartă.

34 — C-411/10 și C-493/10, EU:C:2011:865.

35 — Regulamentul Consiliului din 18 februarie 2003 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe (JO L 50, p. 1, Ediție specială, 19/vol. 6, p. 56).

36 — Punctul 99 din această hotărâre.

37 — *Recueil des traités des Nations unies*, vol. 189, p. 150, nr. 2545 (1954).

38 — A se vedea Hotărârea N. S. și alții (C-411/10 și C-493/10, EU:C:2011:865, punctul 80).

39 — *Ibidem* (punctul 81).

40 — *Ibidem* (punctul 94).

41 — C-411/10 și C-493/10, EU:C:2011:865.

42 — Punctul 104 din această hotărâre.

106. Pe de altă parte, astfel cum a arătat guvernul italian în observații, adoptarea de către Comisie a unei decizii de adecvare nu poate avea drept efect reducerea protecției cetățenilor Uniunii în privința prelucrării datelor lor atunci când acestea sunt transferate către o țară terță, în raport cu nivelul de protecție de care ar beneficia aceste persoane în cazul în care datele lor ar face obiectul unei prelucrări în cadrul Uniunii. În consecință, autoritățile naționale de supraveghere trebuie să fie în măsură să intervină și să își exercite competențele în privința transferurilor de date către țări terțe care fac obiectul unei decizii de adecvare. În caz contrar, cetățenii Uniunii ar fi mai puțin protejați decât în ipoteza prelucrării datelor lor în cadrul Uniunii.

107. Astfel, adoptarea de către Comisie a unei decizii în temeiul articolului 25 alineatul (6) din Directiva 95/46 are drept efect doar eliminarea interdicției generale de exportare a datelor cu caracter personal către țări terțe care garantează un nivel de protecție comparabil cu cel asigurat de această directivă. Cu alte cuvinte, nu se pune în discuție crearea unui regim de excepție special și mai puțin protector pentru cetățenii Uniunii în raport cu regimul general prevăzut de directiva menționată pentru prelucrarea datelor care se realizează în cadrul Uniunii.

108. Desigur, Curtea a indicat, la punctul 63 din Hotărârea Lindqvist [43], că „[c]apitolul IV din Directiva 95/46, în care figurează articolul 25, instituie un regim special”. Totuși, aceasta nu înseamnă, în opinia noastră, că un astfel de regim trebuie să fie mai puțin protector. Dimpotrivă, în vederea atingerii obiectivului de protecție a datelor stabilit la articolul 1 alineatul (1) din Directiva 95/46, articolul 25 din aceasta impune o serie de obligații statelor membre și Comisiei [44], iar acest articol 25 prevede principiul potrivit căruia, atunci când o țară terță nu oferă un nivel de protecție adecvat, transferul datelor cu caracter personal către această țară trebuie interzis [45].

109. În ceea ce privește în special sistemul sferei de siguranță, Comisia are în vedere intervenția autorităților naționale de supraveghere și suspendarea de către acestea a fluxurilor de date doar în cadrul delimitat de articolul 3 alineatul (1) litera (b) din Decizia 2000/520.

110. Potrivit considerentului (8) al acestei decizii, „[î]n scopul transparenței și pentru a permite autorităților competente din statele membre să asigure protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, este necesar ca în prezenta decizie să se indice circumstanțele excepționale în care suspendarea anumitor fluxuri de date ar fi justificată în ciuda constatării unei protecții adecvate”.

111. În cadrul prezentei cauze, a fost discutată în mod special aplicarea articolului 3 alineatul (1) litera (b) din decizia menționată. Astfel, în temeiul acestei dispoziții, suspendarea fluxurilor de date poate fi decisă de autoritățile naționale de supraveghere în cazurile în care „este foarte improbabil ca principiile să fie încălcate; există motive serioase pentru a crede că organismul de aplicare în cauză nu ia sau nu va lua din timp măsuri adecvate pentru a soluționa cauza respectivă; continuarea transferului ar crea pentru persoanele în cauză un risc iminent de a suferi prejudicii grave; iar autoritățile competente din statul membru au depus eforturi rezonabile, ținând seama de circumstanțe, de a avertiza organizația și a îi oferi posibilitatea de a răspunde”.

43 — C-101/01, EU:C:2003:596.

44 — Punctul 65.

45 — Punctul 64.

112. Dispoziția menționată prevede mai multe condiții care au făcut obiectul a diverse interpretări de către părți în cursul prezentei proceduri [46]. Fără a detalia aceste interpretări, reiese de aici că aceste condiții delimitează în sens strict competența autorităților naționale de supraveghere de suspendare a fluxurilor de date.

113. Or, contrar susținerilor Comisiei, articolul 3 alineatul (1) litera (b) din Decizia 2000/520 trebuie interpretat în conformitate cu obiectivul de protecție a datelor cu caracter personal urmărit de Directiva 95/46, precum și în lumina articolului 8 din cartă. Imperativul interpretării conforme cu drepturile fundamentale pledează în favoarea unei interpretări largi a acestei dispoziții.

114. În consecință, condițiile care sunt prevăzute la articolul 3 alineatul (1) litera (b) din Decizia 2000/520 nu pot împiedica, în opinia noastră, o autoritate națională de supraveghere să exercite, în condiții de independență deplină, competențele cu care este învestită în temeiul articolului 28 alineatul (3) din Directiva 95/46.

115. Astfel cum au arătat, în esență, guvernele belgian și austriac în ședință, soluția salvatoare reprezentată de articolul 3 alineatul (1) litera (b) din Decizia 2000/520 este atât de restrânsă încât este dificil să fie pusă în practică. Aceasta prevede criterii cumulative și este mult prea exigentă. Or, în lumina articolului 8 alineatul (3) din cartă, este imposibil ca marja de manevră a autorităților naționale de supraveghere cu privire la prerogativele care rezultă din articolul 28 alineatul (3) din Directiva 95/46 să fie limitată în așa mod încât acestea nu ar mai putea fi exercitate.

116. În această privință, Parlamentul European a observat, în mod întemeiat, că legiuitorul Uniunii a decis care erau competențele care trebuiau să revină autorităților naționale de supraveghere. Or, competența de executare acordată Comisiei de legiuitorul Uniunii la articolul 25 alineatul (6) din Directiva 95/46 nu afectează competențele conferite de același legiuitor autorităților naționale de supraveghere la articolul 28 alineatul (3) din această directivă. Cu alte cuvinte, Comisia nu dispune de competența de a restrânge atribuțiile autorităților naționale de supraveghere.

117. În consecință, pentru a asigura o protecție adecvată a drepturilor fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, autoritățile naționale de supraveghere trebuie să fie abilitate, în cazul unor susțineri referitoare la încălcări ale acestor drepturi, să efectueze investigații. În cazul în care, în urma unor asemenea investigații, aceste autorități consideră că există într-o țară terță acoperită de o decizie de adecvare indicii serioase privind o atingere adusă dreptului cetățenilor Uniunii la protecția datelor cu caracter personal, acestea trebuie să poată suspenda transferul de date către destinatarul stabilit în această țară terță.

118. Cu alte cuvinte, autoritățile naționale de supraveghere trebuie să poată efectua propriile investigații și, dacă este cazul, să suspende un transfer de date, independent de condițiile restrictive stabilite la articolul 3 alineatul (1) litera (b) din Decizia 2000/520.

119. Pe de altă parte, în temeiul competenței lor de a acționa în justiție în cazul încălcării dispozițiilor de drept intern adoptate în temeiul Directivei 95/46 sau de a sesiza autoritățile judecătorești asupra acestor încălcări, prevăzută la articolul 28 alineatul (3) din această directivă, autoritățile naționale de supraveghere ar trebui să poată, atunci când au cunoștință de fapte care demonstrează că o țară terță nu asigură un nivel de protecție adecvat, să sesizeze o instanță națională care va putea decide ea însăși, dacă este cazul, să adreseze Curții o trimitere preliminară în vederea aprecierii validității unei decizii de adecvare a Comisiei.

46 — Conform domnului Schrems, prima condiție, potrivit căreia „este foarte improbabil ca principiile să fie încălcate”, nu ar fi îndeplinită. Or, nu se susține că Facebook USA, în calitate de organism autocertificat căruia i se transferă datele, ar fi încălcat ea însăși principiile sferei de siguranță ca urmare a accesului de masă și nediferențiat al autorităților americane la datele pe care le deține. Astfel, principiile sferei de siguranță sunt limitate în mod expres de dreptul american pe care al patrulea paragraf din anexa I la Decizia 2000/520 le definește printr-o trimitere la textele legislative, reglementările administrative sau jurisprudență.

120. Din ansamblul acestor elemente reiese că articolul 28 din Directiva 95/46 coroborat cu articolele 7 și 8 din cartă trebuie interpretat în sensul că existența unei decizii adoptate de Comisie în temeiul articolului 25 alineatul (6) din această directivă nu are drept efect să împiedice o autoritate națională de supraveghere să investigheze o plângere prin care se susține că o țară terță nu asigură un nivel adecvat de protecție a datelor cu caracter personal și, dacă este cazul, să suspende transferul acestor date.

121. Chiar dacă High Court subliniază, în decizia de trimitere, că domnul Schrems nu a contestat în mod formal în acțiunea din litigiul principal nici validitatea Directivei 95/46, nici pe cea a Deciziei 2000/520, reiese din această decizie de trimitere că critica principală formulată de domnul Schrems urmărește să repună în discuție constatarea potrivit căreia Statele Unite asigură, în cadrul sistemului sferei de siguranță, un nivel adecvat de protecție a datelor cu caracter personal transferate.

122. Reiese de asemenea din observațiile formulate de Comisar că plângerea domnului Schrems urmărește să pună în discuție în mod direct Decizia 2000/520. Prin depunerea plângerii respective, acesta din urmă a dorit să conteste termenii și funcționarea sistemului sferei de siguranță ca atare, pentru motivul că supravegherea de masă a datelor cu caracter personal transferate Statelor Unite ar demonstra că nu există o protecție reală a acestor date în dreptul și în practicile în vigoare în această țară terță.

123. În plus, însăși instanța de trimitere observă că garanția oferită de articolul 7 din cartă și de valorile esențiale comune tradițiilor constituționale ale statelor membre ar fi compromisă în cazul în care s-ar permite autorităților publice să aibă acces la comunicațiile electronice în mod aleatoriu și generalizat fără a trebui să furnizeze o motivare obiectivă întemeiată pe considerente de securitate națională sau de prevenire a criminalității legate în mod specific de persoanele vizate și fără nicio garanție adecvată și verificabilă[47]. Instanța de trimitere exprimă astfel indirect îndoieli cu privire la validitatea Deciziei 2000/520.

124. Aprecierea aspectului dacă Statele Unite, în cadrul sistemului sferei de siguranță, garantează un nivel adecvat de protecție a datelor cu caracter personal transferate conduce, așadar, în mod necesar, la analizarea validității acestei decizii.

125. În această privință, trebuie arătat că, în cadrul instrumentului de cooperare dintre Curte și instanțele naționale instituit prin articolul 267 TFUE, Curtea, chiar și sesizată în mod exclusiv cu titlu preliminar cu privire la o problemă de interpretare a dreptului Uniunii, poate fi chemată, în anumite circumstanțe speciale, să examineze validitatea dispozițiilor de drept derivat.

126. Prin urmare, Curtea a declarat în mai multe rânduri, din oficiu, ca fiind nevalid un act cu privire la care i se solicita numai interpretarea[48]. Aceasta a statuat de asemenea că, „atunci când se constată că adevăratul obiect al întrebărilor adresate de o instanță națională privește mai mult examinarea validității decât interpretarea actelor [Uniunii], Curtea trebuie să ofere imediat un răspuns instanței în cauză, fără a o obliga la un formalism pur dilatoriu, incompatibil cu natura specifică a mecanismelor instituite prin articolul [267 TFUE]”[49]. Pe de altă parte, Curtea a considerat deja că îndoielile exprimate de o instanță de trimitere cu privire la compatibilitatea unui act de drept derivat cu normele referitoare protecția drepturilor fundamentale trebuiau interpretate în sensul că pun în discuție validitatea acestui act în raport cu dreptul Uniunii[50].

47 — Punctul 24 din decizia de trimitere.

48 — A se vedea în special Hotărârile Strehl (62/76, EU:C:1977:18, punctele 10-17), Roquette Frères (145/79, EU:C:1980:234, punctul 6), precum și Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, punctele 32-39).

49 — Hotărârea Schwarze (16/65, EU:C:1965:117, p. 1094).

50 — A se vedea Hotărârea Hauer (44/79, EU:C:1979:290, punctul 16).

127. Reamintim de asemenea că rezultă din jurisprudența Curții că actele instituțiilor, organelor, oficiilor și agențiilor Uniunii beneficiază de o prezumție de validitate, ceea ce implică faptul că acestea produc efecte juridice atât timp cât nu au fost revocate, anulate în cadrul unei acțiuni în anulare sau declarate nevalide în urma unei trimiteri preliminare sau a unei excepții de nelegalitate. Curtea este singura competentă să constate nevaliditatea unui act al Uniunii, competență care are ca obiectiv garantarea securității juridice prin asigurarea aplicării uniforme a dreptului Uniunii. În lipsa constatării nevalidității, a modificării sau a abrogării de către Comisie, decizia rămâne obligatorie în toate elementele sale și direct aplicabilă în orice stat membru [51].

128. Pentru a furniza un răspuns complet instanței de trimitere și pentru a înlătura îndoielile exprimate în cursul prezentei proceduri privind validitatea Deciziei 2000/520, considerăm că Curtea ar trebui să procedeze, așadar, la o apreciere a validității acestei decizii.

129. În aceste condiții, trebuie să se precizeze de asemenea că examinarea aspectului dacă Decizia 2000/520 este sau nu este validă trebuie limitată la criticile care au făcut obiectul unei dezbateri în cadrul prezentei proceduri. Astfel, nu toate aspectele referitoare la funcționarea sistemului sferei de siguranță au fost discutate în acest cadru și acesta este motivul pentru care nu ne pare posibil să efectuăm în cauză o examinare exhaustivă a insuficiențelor acestui sistem.

130. În schimb, problema dacă accesul generalizat și neparticularizat al serviciilor americane de informații la datele transferate poate afecta legalitatea Deciziei 2000/520 a făcut obiectul unei dezbateri în fața Curții în cadrul prezentei proceduri. Prin urmare, validitatea acestei decizii poate fi apreciată din această perspectivă.

B – *Cu privire la validitatea Deciziei 2000/520*

1. Cu privire la elementele care trebuie luate în considerare pentru aprecierea validității Deciziei 2000/520

131. Trebuie amintită jurisprudența potrivit căreia, „în cadrul unei acțiuni în anulare, legalitatea unui act trebuie apreciată în funcție de elemente de fapt și de drept existente la data la care actul a fost adoptat, aprecierea Comisiei neputând fi cenzurată decât în cazul în care este în mod vădit eronată având în vedere elementele de care dispunea la momentul adoptării actului în discuție” [52].

132. În Hotărârea Gaz de France – Berliner Investissement [53], Curtea a amintit principiul potrivit căruia „aprecierea validității unui act, care este de competența Curții în cadrul unei trimiteri preliminare, trebuie în mod normal să fie întemeiată pe situația care există la momentul adoptării actului” [54]. Aceasta a părut însă să admită că „validitatea unui act poate, în anumite cazuri, să fie apreciată în funcție de elemente noi intervenite ulterior adoptării sale” [55].

133. Această deschidere astfel prezentată de către Curte ne pare deosebit de pertinentă în cadrul prezentei cauze.

51 — A se vedea în special Hotărârea CIVAD (C-533/10, EU:C:2012:347, punctele 39-41 și jurisprudența citată).

52 — A se vedea în special Hotărârea BVGD/Comisia (T-104/07 și T-339/08, EU:T:2013:366, punctul 291), care se referă la Hotărârea IECC/Comisia (C-449/98 P, EU:C:2001:275, punctul 87).

53 — C-247/08, EU:C:2009:600.

54 — Punctul 49 și jurisprudența citată.

55 — Punctul 50 și jurisprudența citată. A se vedea în acest sens Lenaerts, K., Maselis, I., și Gutman, K., *EU Procedural Law*, Oxford University Press, 2014, care enunță că, „in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court” (punctul 10.16, p. 471).

134. Astfel, deciziile adoptate de Comisie în temeiul articolului 25 alineatul (6) din Directiva 95/46 prezintă caracteristici speciale. Acestea sunt destinate să evalueze dacă nivelul de protecție a datelor cu caracter personal care este oferit de o țară terță prezintă sau nu prezintă un caracter adecvat. Este vorba despre o apreciere destinată să evolueze în funcție de contextul de fapt și de drept care prevalează în țara terță.

135. Având în vedere că decizia de adecvare constituie un tip special de decizie, regula potrivit căreia aprecierea validității acesteia ar putea fi efectuată numai în funcție de elemente care existau în momentul adoptării sale trebuie nuanțată în speță. O astfel de regulă ar conduce în caz contrar la situația că, după mai mulți ani de la adoptarea unei decizii de adecvare, aprecierea validității pe care trebuie să o efectueze Curtea nu poate ține seama de evenimente care s-au produs ulterior, chiar dacă o trimitere preliminară în aprecierea validității nu este limitată în timp, iar declanșarea acesteia poate fi tocmai consecința faptelor ulterioare care evidențiază insuficiențele actului în cauză.

136. În speță, menținerea în vigoare a Deciziei 2000/520 de aproximativ 15 ani constituie dovada confirmării implicite de către Comisie a evaluării sale efectuate în anul 2000. Atunci când, în cadrul unei trimiteri preliminare, Curtea este chemată să aprecieze validitatea unei evaluări menținute în timp de Comisie, este, în consecință, nu numai posibil, dar și adecvat, ca aceasta să poată confrunta această evaluare cu circumstanțele noi care au intervenit de la adoptarea deciziei de adecvare.

137. Ținând seama de natura specială a deciziei de adecvare, aceasta trebuie să facă obiectul unei reexaminări regulate de către Comisie. În cazul în care, în urma unor elemente noi intervenite între timp, Comisia nu își modifică decizia, înseamnă că aceasta confirmă în mod implicit, dar necesar, aprecierea efectuată inițial. Comisia reiterează astfel constatarea sa potrivit căreia țara terță în cauză asigură un nivel adecvat de protecție a datelor cu caracter personal transferate. Revine Curții sarcina de a examina dacă această constatare continuă să fie valabilă în pofida circumstanțelor intervenite ulterior.

138. Pentru a se asigura un control jurisdicțional efectiv al acestui tip de decizie, aprecierea validității sale trebuie efectuată, așadar, în opinia noastră, în funcție de contextul de fapt și de drept actual.

2. Cu privire la noțiunea de nivel de protecție adecvat

139. Articolul 25 din Directiva 95/46 se întemeiază în întregime pe principiul potrivit căruia transferul de date cu caracter personal către o țară terță poate avea loc numai sub rezerva garantării de către această țară terță a unui nivel adecvat de protecție a unor asemenea date. Astfel, obiectivul acestui articol este de a asigura continuitatea protecției acordate de această directivă în cazul transferului de date cu caracter personal către o țară terță. Trebuie amintit, în această privință, că directiva menționată oferă un nivel ridicat de protecție a cetățenilor Uniunii în privința prelucrării datelor lor cu caracter personal.

140. Ținând seama de rolul important pe care îl are protecția datelor cu caracter personal în raport cu dreptul fundamental la respectarea vieții private, un asemenea nivel ridicat de protecție trebuie garantat, în consecință, inclusiv în cazul transferului de date cu caracter personal către o țară terță.

141. Acesta este motivul pentru care considerăm că Comisia nu poate constata, în temeiul articolului 25 alineatul (6) din Directiva 95/46, că o țară terță asigură un nivel de protecție adecvat doar atunci când, la încheierea unei evaluări de ansamblu a dreptului și a practicii în țara terță în discuție, este în măsură să stabilească faptul că această țară terță oferă un nivel de protecție în esență echivalent cu cel oferit de directiva menționată, chiar dacă modalitățile acestei protecții pot fi diferite de cele aplicate în general în cadrul Uniunii.

142. Deși termenul englez „adequate” poate fi interpretat, din punct de vedere lingvistic, în sensul că desemnează un nivel de protecție doar satisfăcător sau suficient și are astfel un câmp semantic diferit de termenul francez „adéquat”, trebuie să se observe că singurul criteriu care trebuie să orienteze interpretarea acestui termen este obiectivul de a atinge un nivel ridicat de protecție a drepturilor fundamentale, astfel cum prevede Directiva 95/46.

143. Examinarea nivelului de protecție oferit de o țară terță trebuie să implice două elemente fundamentale, și anume conținutul normelor aplicabile și mijloacele de asigurare a respectării acestor norme [56].

144. În opinia noastră, pentru a atinge un nivel de protecție în esență echivalent cu cel în vigoare în cadrul Uniunii, sistemul sferei de siguranță, care se întemeiază în mare parte pe autocertificarea și pe autoevaluarea efectuate de întreprinderile care participă în mod voluntar la acest sistem, ar trebui însoțit de garanții adecvate și de un mecanism de control suficient. Astfel, transferurile de date cu caracter personal către țări terțe nu ar trebui să beneficieze de o protecție mai redusă decât prelucrările efectuate în cadrul Uniunii.

145. În această privință, subliniem de la bun început că, în cadrul Uniunii, prevalează concepția potrivit căreia un dispozitiv de control extern sub forma unei autorități independente constituie un element necesar al oricărui sistem prin care se urmărește asigurarea respectării normelor referitoare la protecția datelor cu caracter personal.

146. Pe de altă parte, pentru a asigura efectul util al articolului 25 alineatele (1)-(3) din Directiva 95/46, trebuie să se țină seama de faptul că caracterul adecvat al nivelului de protecție oferit de o țară terță este o situație evolutivă care se poate schimba de-a lungul timpului în funcție de o serie de factori. În consecință, statele membre și Comisia trebuie să fie atente în mod constant la orice schimbare a circumstanțelor susceptibilă să facă necesară o reevaluare a caracterului adecvat al nivelului de protecție oferit de o țară terță. O evaluare a caracterului adecvat al acestui nivel de protecție nu poate nicidecum să fie stabilită la un moment dat și, în continuare, să fie menținută pe termen nelimitat, independent de orice schimbare a circumstanțelor care demonstrează că, în realitate, nivelul de protecție oferit nu mai este adecvat.

147. Obligația țării terțe de a asigura un nivel de protecție adecvat constituie astfel o obligație continuă. În cazul în care evaluarea este efectuată la un moment dat, menținerea deciziei de adecvare presupune ca nicio circumstanță intervenită ulterior să nu fie de natură să repună în discuție evaluarea inițială efectuată de Comisie.

148. Astfel, nu trebuie să se omită că obiectivul prevăzut la articolul 25 din Directiva 95/46 este de a evita întotdeauna ca datele cu caracter personal să fie transferate către o țară terță care nu asigură un nivel de protecție adecvat, cu încălcarea dreptului fundamental la protecția datelor cu caracter personal garantat de articolul 8 din cartă.

149. Trebuie să se sublinieze că puterea conferită Comisiei de legiuitorul Uniunii, la articolul 25 alineatul (6) din această Directiva 95/46, de a constata că o țară terță asigură un nivel de protecție adecvat este condiționată în mod expres de cerința ca această țară terță să asigure un astfel de nivel, în sensul alineatului (2) al acestui articol. În cazul în care circumstanțe noi ar fi de natură să repună în discuție evaluarea inițială a Comisiei, aceasta ar trebui să își adapteze decizia în consecință.

56 — A se vedea p. 5 din Documentul de lucru WP 12 al Comisiei, intitulat „Transferuri de date cu caracter personal către țări terțe: Aplicarea articolelor 25 și 26 din Directiva privind protecția datelor”, adoptat de grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal la 24 iulie 1998.

3. Aprecierea noastră

150. Reamintim că, în temeiul articolului 25 alineatul (6) din Directiva 95/46, „Comisia poate constata, în conformitate cu procedura prevăzută în articolul 31 alineatul (2), că o țară terță asigură un nivel de protecție adecvat în sensul alineatului (2) din prezentul articol, în temeiul legislației interne sau al angajamentelor sale internaționale, luate în special la încheierea negocierilor menționate la alineatul (5), în vederea protejării vieții private și a libertăților și drepturilor fundamentale ale persoanelor”. Coroborat cu articolul 25 alineatul (2) din această directivă, articolul 25 alineatul (6) presupune că, pentru a constata că o țară terță asigură un nivel de protecție adecvat, Comisia trebuie să efectueze o evaluare de ansamblu a normelor de drept în vigoare în această țară terță, precum și a aplicării acestora.

151. Am constatat că menținerea de către Comisie a Deciziei 2000/520, în pofida survenirii unor elemente de fapt și de drept noi, trebuie interpretată ca o intenție din partea sa de a confirma evaluarea sa inițială.

152. Curtea nu are competența, în cadrul unei trimiteri preliminare, de a se pronunța asupra situației de fapt aflate la originea litigiului care a determinat instanța națională să efectueze această trimitere [57].

153. Prin urmare, ne vom întemeia pe faptele indicate de instanța de trimitere în cererea de decizie preliminară, fapte care, de altfel, sunt admise în sens larg chiar de către Comisie ca fiind stabilite [58].

154. Elementele care au fost invocate în fața Curții pentru a contesta evaluarea Comisiei potrivit căreia sistemul referitor la sfera de siguranță asigură un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune către Statele Unite pot fi descrise astfel.

155. În cererea de decizie preliminară, instanța de trimitere pornește de la următoarele două constatări de fapt. Pe de o parte, datele cu caracter personal transferate de întreprinderi precum Facebook Ireland către societatea-mamă stabilită în Statele Unite pot fi consultate ulterior de NSA, precum și de alte agenții de securitate americane în cadrul activităților de supraveghere și de interceptare în masă și neparticularizate. Astfel, ca urmare a dezvăluirilor făcute de domnul Snowden, nicio altă concluzie plauzibilă nu poate fi dedusă, la ora actuală, pe baza elementelor de probă disponibile [59]. Pe de altă parte, cetățenii Uniunii nu ar avea niciun drept efectiv de a fi ascultați cu privire la problema supravegherii și interceptării datelor lor de către NSA și de către alte agenții de securitate americane [60].

156. Constatările de fapt efectuate astfel de High Court se întemeiază pe constatările efectuate chiar de Comisie.

157. Astfel, în Comunicarea privind funcționarea sferei de siguranță din punctul de vedere al cetățenilor UE și al întreprinderilor stabilite pe teritoriul său, menționată mai sus, Comisia a pornit de la constatarea că, în cursul anului 2013, informațiile privind amploarea programelor de supraveghere americane au ridicat semne de întrebare cu privire la continuitatea protecției datelor personale transferate în mod legal către Statele Unite în cadrul sistemului sferei de siguranță. Aceasta a arătat că toate societățile implicate în programul PRISM și care oferă autorităților din Statele Unite acces la

57 — A se vedea în special Hotărârea Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, punctul 22 și jurisprudența citată).

58 — A se vedea Comunicarea Comisiei menționată la nota de subsol 2 și Comunicarea Comisiei către Parlamentul European și Consiliu privind funcționarea sferei de siguranță din punctul de vedere al cetățenilor UE și al întreprinderilor stabilite în UE [COM(2013) 847 final].

59 — Punctul 7 litera (c) din decizia de trimitere.

60 — Punctul 7 litera (b) din decizia de trimitere.

datele stocate și prelucrate în Statele Unite au statutul de societăți certificate în sistemul sferei de siguranță. În opinia sa, din acest motiv, sfera de siguranță a constituit unul dintre canalele prin care s-a permis serviciilor de informații din Statele Unite să colecteze date personale prelucrate inițial în cadrul Uniunii [61].

158. Reiese din aceste elemente că dreptul și practica Statelor Unite permit colectarea, la scară largă, a datelor cu caracter personal ale cetățenilor Uniunii care sunt transferate în cadrul sistemului sferei de siguranță, fără ca aceștia din urmă să beneficieze de o protecție jurisdicțională efectivă.

159. Aceste constatări de fapt demonstrează, în opinia noastră, că Decizia 2000/520 nu conține suficiente garanții. Ca urmare a lipsei garanțiilor, această decizie a fost pusă în aplicare într-un mod care nu respectă cerințele impuse atât de cartă, cât și de Directiva 95/46.

160. Or, o decizie adoptată de Comisie în temeiul articolului 25 alineatul (6) din Directiva 95/46 are drept obiect constatarea că o țară terță „asigură” un nivel de protecție adecvat. Termenul „asigură”, conjugat la timpul prezent, presupune că, pentru a putea fi menținută, o asemenea decizie trebuie să privească o țară terță care continuă, după adoptarea deciziei menționate, să garanteze un nivel de protecție adecvat.

161. În realitate, dezvăluirile menționate cu privire la acțiunile NSA care ar utiliza date transferate în cadrul sistemului sferei de siguranță au evidențiat deficiențele temeiului legal reprezentat de Decizia 2000/520.

162. Insuficiențele care au fost subliniate în cursul prezentei proceduri figurează în special la al patrulea paragraf din anexa I la această decizie.

163. Reamintim că, potrivit acestei dispoziții, „[a]derarea la […] principii[le sferei de siguranță] poate fi limitată de: (a) cerințele privind securitatea națională, interesul public și respectarea legilor Statelor Unite ale Americii; (b) textele legislative, regulamentele administrative sau jurisprudența care creează obligații contradictorii sau prevăd autorizații exprese, cu condiția ca organizația care a recurs la o asemenea autorizație să poată demonstra că nerespectarea principiilor se limitează la măsurile necesare pentru garantarea intereselor legitime superioare pe care această autorizație urmărește să le servească”.

164. Problema se referă, în esență, la utilizarea dată de autoritățile americane derogărilor prevăzute de dispoziția menționată. Ca urmare a formulării lor prea generale, punerea în aplicare a acestor derogări de către respectivele autorități nu este limitată la ceea ce este strict necesar.

165. La această formulare prea generală se adaugă împrejurarea că cetățenii Uniunii nu dispun de o cale de atac adaptată împotriva prelucrării datelor lor cu caracter personal în alte scopuri decât cele pentru care au fost inițial colectate, ulterior transferate către Statele Unite.

166. Derogările prevăzute de Decizia 2000/520 de la aplicarea principiilor sferei de siguranță, în special pentru cerințe privind securitatea națională, ar fi trebuit să fie însoțite de instituirea unui mecanism de control independent de natură să evite atingerile constatate aduse dreptului la viață privată.

167. Astfel, dezvăluirile cu privire la practicile serviciilor de informații americane în ceea ce privește supravegherea generalizată a datelor transferate în cadrul sferei de siguranță au evidențiat anumite insuficiențe specifice Deciziei 2000/520.

61 — Pagina 19 din comunicarea acesteia.

168. Afirmațiile menționate în cadrul prezentei cauze nu constituie o încălcare de către Facebook a principiilor sferei de siguranță. În cazul în care o întreprindere certificată, precum Facebook USA, oferă autorităților americane accesul la date care i-au fost transferate dintr-un stat membru, se poate considera că aceasta procedează astfel pentru a se conforma legislației americane. Având în vedere faptul că o asemenea situație este admisă în mod expres prin Decizia 2000/520, ca urmare a formulării largi a derogărilor prevăzute de aceasta, în realitate, problema care se ridică în cadrul prezentei cauze este cea a compatibilității unor astfel de derogări cu dreptul primar al Uniunii.

169. În această privință, trebuie să se sublinieze că, potrivit unei jurisprudențe constante a Curții, respectarea drepturilor omului constituie o condiție a legalității actelor Uniunii și nu pot fi admise în Uniune măsuri incompatibile cu respectarea acestora [62].

170. Pe de altă parte, rezultă din jurisprudența Curții că comunicarea datelor cu caracter personal colectate către persoane terțe, publice sau private, constituie o ingerință în dreptul la respectarea vieții private „indiferent de utilizarea ulterioară a informațiilor astfel comunicate” [63]. În plus, în Hotărârea Digital Rights Ireland și alții [64], Curtea a confirmat că faptul de a permite autorităților naționale competente să aibă acces la astfel de date constituie o atingere suplimentară adusă acestui drept fundamental [65]. Mai mult, orice formă de prelucrare a datelor cu caracter personal este prevăzută la articolul 8 din cartă și constituie o ingerință în dreptul la protecția unor astfel de date [66]. Prin urmare, accesul de care dispun serviciile de informații americane la datele transferate constituie și o ingerință în dreptul fundamental la protecția datelor cu caracter personal garantat de articolul 8 din cartă, întrucât un astfel de acces constituie o prelucrare a acestor date.

171. În mod similar constatărilor efectuate de Curte în această hotărâre, ingerința astfel identificată are o vastă amploare și trebuie considerată deosebit de gravă, având în vedere numărul considerabil al utilizatorilor în cauză și cantitățile de date transferate. Aceste elemente, asociate cu caracterul secret al accesului autorităților americane la datele cu caracter personal transferate către întreprinderile stabilite în Statele Unite, fac ca ingerința să fie extrem de serioasă.

172. La aceasta se adaugă împrejurarea că cetățenii Uniunii, utilizatori ai Facebook, nu sunt informați cu privire la faptul că datele lor cu caracter personal vor fi accesibile în general agențiilor de securitate americane.

173. Trebuie să se pună accentul și pe faptul că instanța de trimitere a constatat că, în Statele Unite, cetățenii Uniunii nu au niciun drept efectiv de a fi ascultați cu privire la problema supravegherii și interceptării datelor lor. Cu toate că există o supraveghere din partea FISC, această procedură este secretă și necontradictorie [67]. Considerăm că este vorba în acest caz despre o ingerință în dreptul cetățenilor Uniunii la o cale de atac efectivă protejat prin articolul 47 din cartă.

174. Ingerința permisă de derogările de la principiile sferei de siguranță care figurează la al patrulea paragraf din anexa I la Decizia 2000/520 în drepturile fundamentale protejate prin articolele 7, 8 și 47 din cartă este, așadar, constituită.

175. Este necesar, la acest moment, să se verifice dacă această ingerință este sau nu este justificată.

62 — A se vedea în special Hotărârea Kadi și Al Barakaat International Foundation/Consiliul și Comisia (C-402/05 P și C-415/05 P, EU:C:2008:461, punctul 284, precum și jurisprudența citată).

63 — Hotărârea Österreichischer Rundfunk și alții (C-465/00, C-138/01 și C-139/01, EU:C:2003:294, punctul 74).

64 — C-293/12 și C-594/12, EU:C:2014:238.

65 — Punctul 35.

66 — Punctul 36.

67 — Punctul 7 litera (b) din decizia de trimitere.

176. Potrivit articolului 52 alineatul (1) din cartă, orice restrângere a exercițiului drepturilor și libertăților recunoscute prin cartă trebuie să fie prevăzută de lege și să respecte substanța acestor drepturi și libertăți. Prin respectarea principiului proporționalității, pot fi impuse restrângeri drepturilor și libertăților menționate numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

177. Având în vedere condițiile astfel prevăzute pentru a putea admite restrângeri impuse exercițiului drepturilor și libertăților protejate de cartă, avem îndoieli serioase că se poate considera că restrângerile în discuție în prezenta cauză respectă substanța articolelor 7 și 8 din cartă. Astfel, accesul serviciilor de informații americane la datele transferate pare să se extindă la conținutul comunicațiilor electronice, ceea ce ar aduce atingere substanței dreptului fundamental la respectarea vieții private și a celorlalte drepturi consacrate la articolul 7 din cartă. În plus, în măsura în care formularea largă a restrângerilor prevăzute al patrulea paragraf din anexa I la Decizia 2000/520 permite în mod potențial înlăturarea aplicării tuturor principiilor sferei de siguranță, s-ar putea considera că aceste restrângeri aduc atingere substanței dreptului fundamental la protecția datelor cu caracter personal [68].

178. În ceea ce privește problema dacă ingerința constatată răspunde unui obiectiv de interes general, amintim mai întâi că, potrivit celui de al patrulea paragraf litera (b) din anexa I la Decizia 2000/520, aderarea la principiile sferei de siguranță poate fi limitată de „textele legislative, regulamentele administrative sau jurisprudența care creează obligații contradictorii sau prevăd autorizații exprese, cu condiția ca organizația care a recurs la o asemenea autorizație să poată demonstra că nerespectarea principiilor se limitează la măsurile necesare pentru garantarea intereselor legitime superioare pe care această autorizație urmărește să le servească”.

179. Se impune constatarea că „interesele legitime” menționate în această dispoziție nu sunt precizate. Rezultă de aici o incertitudine în ceea ce privește domeniul de aplicare, potențial extrem de larg, al acestei derogări de la aplicarea principiilor sferei de siguranță de către întreprinderile aderente.

180. Interpretarea explicațiilor conținute în secțiunea B din anexa IV la Decizia 2000/520, intitulată „Autorizări legale exprese”, confirmă această impresie, în special afirmația potrivit căreia, „[î]n mod evident, în cazurile în care legislația Statelor Unite ale Americii impune o obligație conflictuală, organizațiile din Statele Unite ale Americii care fac parte sau nu din «sfera de siguranță» trebuie să se conformeze acestei legislații”. Pe de altă parte, se arată că, în ceea ce privește autorizațiile exprese, „deși principiile «sferei de siguranță» sunt destinate să restrângă diferențele dintre sistemul din Statele Unite ale Americii și cel european cu privire la protecția vieții private, trebuie să respectăm prerogativele legislative ale legislatorilor pe care i-am ales”.

181. Rezultă că, în opinia noastră, această derogare este contrară articolelor 7, 8 și articolului 52 alineatul (1) din cartă deoarece nu urmărește un obiectiv de interes general definit într-un mod suficient de precis.

182. În orice caz, facilitatea și caracterul general cu care Decizia 2000/520 însăși, la al patrulea paragraf litera (b) din anexa I, precum și în secțiunea B din anexa IV, prevede că principiile sferei de siguranță pot fi înlăturate în temeiul normelor dreptului american sunt incompatibile cu condiția potrivit căreia derogările de la normele referitoare la protecția datelor cu caracter personal trebuie limitate la ceea ce este strict necesar. Se menționează, desigur, condiția necesității, însă, pe lângă faptul că demonstrarea acestei condiții revine întreprinderii în cauză, nu înțelegem cum ar putea să se sustragă o asemenea întreprindere de la obligația de a înlătura principiile sferei de siguranță care decurge din normele de drept pe care este ținută să le aplice.

68 — A se vedea în această privință Hotărârea Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238, punctele 39 și 40).

183. În consecință, considerăm că Decizia 2000/520 trebuie declarată nevalidă, întrucât existența unei derogări care permite cu titlu atât de general și de imprecis să se înlăture principiile sistemului sferei de siguranță împiedică prin ea însăși să se considere că acest sistem asigură un nivel adecvat de protecție a datelor cu caracter personal care sunt transferate în Statele Unite din Uniune.

184. În ceea ce privește, acum, prima categorie de limite prevăzute la al patrulea paragraf litera (a) din anexa I la Decizia 2000/520 ca urmare a cerințelor privind securitatea națională, a interesului public și respectarea legilor americane, numai primul obiectiv ne pare a fi suficient de precis pentru a fi considerat un obiectiv de interes general recunoscut de Uniune în sensul articolului 52 alineatul (1) din cartă.

185. Este necesar să se verifice, în acest moment, proporționalitatea ingerinței constatate.

186. În această privință, trebuie amintit că „principiul proporționalității impune, potrivit unei jurisprudențe constante a Curții, ca actele instituțiilor Uniunii să fie de natură să atingă obiectivele legitime urmărite de reglementarea în cauză și să nu depășească limitele a ceea ce este adecvat și necesar pentru realizarea acestor obiective” [69].

187. În ceea ce privește controlul jurisdicțional al respectării acestor condiții, „întrucât sunt în discuție ingerințe în drepturile fundamentale, întinderea puterii de apreciere a legiuitorului Uniunii poate fi limitată în funcție de un anumit număr de elemente, printre care figurează în special domeniul vizat, natura dreptului în cauză garantat de cartă, natura și gravitatea ingerinței, precum și finalitatea acesteia” [70].

188. Considerăm că deciziile pe care Comisia le adoptă în temeiul articolului 25 alineatul (6) din Directiva 95/46 sunt supuse controlului complet al Curții în ceea ce privește proporționalitatea evaluării efectuate de această instituție referitoare la caracterul adecvat al nivelului de protecție oferit de o țară terță „în temeiul legislației interne sau al angajamentelor sale internaționale”.

189. Trebuie să se observe în această privință că, în Hotărârea Digital Rights Ireland și alții [71], Curtea a decis că, „ținând seama, pe de o parte, de rolul important pe care îl are protecția datelor cu caracter personal în lumina dreptului fundamental la respectarea vieții private și, pe de altă parte, de amploarea și de gravitatea ingerinței în acest drept cauzate de [directiva în cauză], puterea de apreciere a legiuitorului Uniunii este redusă, astfel încât este necesară efectuarea unui control strict” [72].

190. O asemenea ingerință trebuie să fie de natură să realizeze obiectivul urmărit de actul Uniunii în discuție și să fie necesară pentru atingerea acestui obiectiv.

191. În această privință, „[î]n ceea ce privește dreptul la respectarea vieții private, potrivit unei jurisprudențe constante a Curții, protecția acestui drept fundamental impune […] ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele strictului necesar” [73].

192. În cadrul controlului său, Curtea ține seama și de circumstanța că „protecția datelor cu caracter personal, care rezultă din obligația explicită prevăzută la articolul 8 alineatul (1) din cartă, prezintă o importanță deosebită pentru dreptul la respectarea vieții private consacrat la articolul 7 din aceasta” [74].

69 — Hotărârea Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238, punctul 46 și jurisprudența citată).

70 — *Ibidem* (punctul 47 și jurisprudența citată).

71 — C-293/12 și C-594/12, EU:C:2014:238.

72 — Punctul 48.

73 — Hotărârea Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238, punctul 52 și jurisprudența citată).

74 — *Ibidem* (punctul 53).

193. Potrivit Curții, care se referă, în această privință, la jurisprudența Curții Europene a Drepturilor Omului, „reglementarea Uniunii în cauză trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime astfel încât persoanele ale căror date au fost păstrate să dispună 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”[75]. Curtea arată că „[n]ecesitatea de a dispune de asemenea garanții este cu atât mai importantă în cazul în care […] datele cu caracter personal sunt supuse unei prelucrări automate și există un risc important privind un acces ilicit la aceste date”[76].

194. Există, în opinia noastră, o analogie între al patrulea paragraf litera (a) din anexa I la Decizia 2000/520 și articolul 13 alineatul (1) din Directiva 95/46. În cuprinsul primei dispoziții, se arată că aderarea la principiile sferei de siguranță poate fi limitată de „cerințele privind securitatea națională, interesul public și respectarea legilor Statelor Unite ale Americii”. În cuprinsul celei de a doua dispoziții, se prevede că statele membre pot adopta măsuri legislative pentru a restrânge domeniul obligațiilor și drepturilor prevăzute la articolul 6 alineatul (1), la articolul 10, la articolul 11 alineatul (1) și la articolele 12 și 21 din această directivă, dacă o astfel de restricție constituie o măsură necesară pentru a proteja printre altele securitatea statului, apărarea, siguranța publică, precum și prevenirea, investigarea, detectarea și punerea sub urmărire a infracțiunilor.

195. Astfel cum a arătat Curtea în Hotărârea IPI[77], rezultă din modul de redactare a articolului 13 alineatul (1) din Directiva 95/46 că statele membre pot să prevadă măsurile vizate de această dispoziție doar dacă acestea sunt necesare. Caracterul „necesar” al măsurilor condiționează astfel posibilitatea acordată statelor membre de dispoziția menționată[78]. Pentru prelucrarea datelor cu caracter personal în cadrul Uniunii, restricțiile prevăzute la articolul 13 din această directivă trebuie interpretate în sensul că se limitează la ceea ce este strict necesar pentru atingerea obiectivului urmărit. În opinia noastră, situația trebuie să fie aceeași și în ceea ce privește restrângerile principiilor sferei de siguranță care sunt prevăzute la al patrulea paragraf din anexa I la Decizia 2000/520.

196. Or, se impune constatarea că nu toate versiunile lingvistice menționează criteriul necesității în textul celui de al patrulea paragraf litera (a) din anexa I la Decizia 2000/520. Acest lucru este valabil în special în cazul versiunii în limba franceză, care arată că „[l]’adhésion aux principes peut être limitée par […] les exigences relatives à la sécurité nationale, l’intérêt public et le respect des lois des États-Unis”, în condițiile în care, de exemplu, versiunile în limbile spaniolă, germană și engleză arată că restrângerile instituite trebuie să fie necesare pentru atingerea obiectivelor menționate mai sus.

197. În orice caz, elementele de fapt care sunt invocate de instanța de trimitere, precum și de Comisie în comunicările menționate mai sus demonstrează cu claritate că, în practică, punerea în aplicare a acestor restrângeri nu se limitează la ceea ce este strict necesar pentru atingerea obiectivelor urmărite.

198. Observăm, în această privință, că accesul la datele cu caracter personal transferate de care dispun serviciile de informații americane acoperă în mod generalizat toate persoanele și toate mijloacele de comunicare electronică, precum și ansamblul datelor transferate, inclusiv conținutul comunicărilor, fără a se realiza nicio diferențiere, limitare sau excepție în funcție de obiectivul de interes general urmărit[79].

75 — *Ibidem* (punctul 54 și jurisprudența citată).

76 — *Ibidem* (punctul 55 și jurisprudența citată).

77 — C-473/12, EU:C:2013:715.

78 — Punctul 32.

79 — A se vedea prin analogie Hotărârea Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238, punctul 57 și jurisprudența citată).

199. Astfel, accesul serviciilor de informații americane la datele transferate privește în mod global ansamblul persoanelor care utilizează servicii de comunicații electronice, fără a fi necesar ca persoanele în cauză să prezinte o amenințare pentru securitatea națională [80].

200. O asemenea supraveghere în masă și neparticularizată este disproporționată prin natura sa și constituie o ingerință nejustificată în drepturile garantate la articolele 7 și 8 din cartă.

201. Astfel cum a arătat, în mod întemeiat, Parlamentul European în observații, întrucât este imposibil pentru legiuitorul Uniunii sau pentru statele membre să adopte dispoziții legislative care, cu încălcarea cartei, ar prevedea o supraveghere în masă și neparticularizată, rezultă în mod necesar că, *a fortiori*, nu se poate considera că țări terțe asigură un nivel adecvat de protecție a datelor cu caracter personal ale cetățenilor Uniunii în cazul în care reglementarea lor autorizează efectiv supravegherea și interceptarea în masă și neparticularizate ale acestui tip de date.

202. În plus, trebuie să se sublinieze că sistemul sferei de siguranță, astfel cum este definit prin Decizia 2000/520, nu conține garanții de natură să evite un acces în masă și generalizat la datele transferate.

203. Observăm în această privință că, în Hotărârea Digital Rights Ireland și alții [81], Curtea a subliniat importanța de a prevedea „norme clare și precise care reglementează întinderea ingerinței în drepturile fundamentale consacrate la articolele 7 și 8 din cartă” [82]. O asemenea ingerință trebuie să fie, în opinia Curții, „încadrată în mod precis de dispoziții care să permită garantarea faptului că ea este limitată efectiv la strictul necesar” [83]. În această hotărâre, Curtea a pus accentul și pe necesitatea de a prevedea „garanții suficiente, astfel cum sunt impuse de articolul 8 din cartă, care să permită asigurarea unei protecții eficiente a datelor [cu caracter personal] păstrate împotriva riscurilor de abuz, precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date” [84].

204. Or, se impune constatarea că mecanismele de arbitraj privat și FTC, ca urmare a rolului său limitat la litigiile de natură comercială, nu constituie mijloace de contestare a accesului serviciilor de informații americane la datele cu caracter personal transferate din Uniune.

205. Competența FTC acoperă actele și practicile neloiale sau frauduloase din domeniul comerțului și nu acoperă colectarea și utilizarea de informații cu caracter personal în scopuri necomerciale [85]. Domeniul de competență limitat al FTC restrânge dreptul particularilor la protecția datelor lor cu caracter personal. FTC a fost instituită nu pentru a asigura, astfel cum este cazul în cadrul Uniunii pentru autoritățile naționale de supraveghere, protecția dreptului individual la viața privată, ci pentru a garanta un comerț loial și fiabil pentru consumatori, ceea ce limitează, *de facto*, capacitățile sale de intervenție în sfera referitoare la protecția datelor cu caracter personal. Prin urmare, FTC nu are un rol comparabil cu cel al autorităților naționale de supraveghere prevăzute la articolul 28 din Directiva 95/46.

80 — *Ibidem* (punctele 58 și 59).

81 — C-293/12 și C-594/12, EU:C:2014:238.

82 — Punctul 65.

83 — *Idem.*

84 — *Ibidem* (punctul 66).

85 — A se vedea în această privință FAQ 11 din anexa II la Decizia 2000/520, în cadrul secțiunii „Acțiunea FTC”, și anexele III, V și VII la aceasta.

206. Cetățenii Uniunii ale căror date au fost transferate se pot adresa unor organisme de arbitraj specializate stabilite în Statele Unite precum TRUSTe și BBBOnline pentru a solicita precizări cu privire la aspectul dacă întreprinderea care deține datele lor cu caracter personal încalcă condițiile sistemului de autocertificare. Arbitrajul privat asigurat de organisme precum TRUSTe nu poate examina încălcările dreptului la protecția datelor cu caracter personal care sunt săvârșite de alte organisme sau autorități decât întreprinderile autocertificate. Aceste organisme de arbitraj nu au nicio competență să se pronunțe cu privire la legalitatea activităților agențiilor de securitate americane.

207. Prin urmare, nici FTC, nici organismele de arbitraj private nu au competența să controleze posibilele încălcări ale principiilor de protecție a datelor cu caracter personal săvârșite de actorii publici precum agențiile de securitate americane. O asemenea competență ar fi esențială însă pentru a garanta pe deplin dreptul la protecția efectivă a acestor date. În consecință, Comisia nu putea constata, prin adoptarea Deciziei 2000/520 și menținerea acesteia în vigoare, că ar exista pentru toate datele cu caracter personal care ar fi transferate către Statele Unite o protecție adecvată a dreptului acordat de articolul 8 alineatul (3) din cartă, cu alte cuvinte că o autoritate independentă ar exercita un control efectiv al respectării cerințelor de protecție și de securitate a acestor date.

208. În consecință, este necesar să se constate absența în cadrul sistemului sferei de siguranță prevăzut de Decizia 2000/520 a unei autorități independente care ar putea controla ca punerea în aplicare a derogărilor de la principiile sferei de siguranță să se limiteze la ceea ce este strict necesar. Or, am constatat că un astfel de control efectuat de o autoritate independentă constituie, din punctul de vedere al dreptului Uniunii, un element esențial al respectării protecției persoanelor în ceea ce privește prelucrarea datelor cu caracter personal [86].

209. În această privință, trebuie să se sublinieze rolul pe care îl ocupă, în sistemul de protecție a datelor cu caracter personal în vigoare în cadrul Uniunii, autoritățile naționale de supraveghere în controlul restricțiilor prevăzute la articolul 13 din Directiva 95/46. Potrivit articolului 28 alineatul (4) al doilea paragraf din această directivă, „[f]iecare autoritate de supraveghere poate fi sesizată printr-o plângere depusă de orice persoană cu privire la legalitatea prelucrării datelor, atunci când se aplică dispozițiile de drept intern adoptate în temeiul articolului 13 din prezenta directivă”. Prin analogie, considerăm că menționarea restrângerilor aplicării principiilor sferei de siguranță la al patrulea paragraf din anexa I la Decizia 2000/520 ar fi trebuit să fie însoțită de instituirea unui mecanism de control asigurat de o autoritate independentă specializată în domeniul protecției datelor cu caracter personal.

210. Astfel, intervenția autorităților de supraveghere independente reprezintă aspectul central al sistemului european de protecție a datelor cu caracter personal. Prin urmare, existența unor asemenea autorități a fost considerată în mod firesc, de la bun început, una dintre condițiile necesare pentru constatarea adecvării nivelului de protecție oferit de țările terțe. Este vorba despre o condiție pentru ca fluxurile de date de pe teritoriul statelor membre către cel al țărilor terțe să nu fie interzise conform articolului 25 din Directiva 95/46 [87]. Astfel cum prevede documentul de dezbatere adoptat de grupul de lucru instituit prin articolul 29 din această directivă, există în Europa un larg consens potrivit căruia „un dispozitiv de «control extern», sub forma unei autorități independente, constituie un element necesar al oricărui sistem prin care se urmărește să se asigure respectarea normelor cu privire la protecția datelor” [88].

86 — A se vedea Hotărârea Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238, punctul 68, precum și jurisprudența citată).

87 — A se vedea Poullet, Y., „L'autorité de contrôle: «vues» de Bruxelles”, *Revue française d'administration publique*, nr. 89, ianuarie-martie 1999, p. 69, în special p. 71.

88 — A se vedea p. 7 din Documentul de lucru WP 12 al Comisiei, menționat la nota de subsol 56.

211. Subliniem, în plus, că FISC nu oferă o cale de atac efectivă cetățenilor Uniunii ale căror date cu caracter personal sunt transferate către Statele Unite. Astfel, protecția împotriva supravegherii exercitate de serviciile guvernamentale în cadrul articolului 702 din Legea din 1978 privind supravegherea serviciilor de informații străine se aplică doar cetățenilor americani, precum și cetățenilor străini care au reședința legală și permanentă în Statele Unite. Astfel cum a arătat Comisia însăși, supravegherea programelor SUA de colectare de informații ar fi îmbunătățită prin consolidarea rolului FISC și prin introducerea unor căi de atac pentru particulari. Aceste mecanisme ar putea reduce volumul prelucrării datelor cu caracter personal ale cetățenilor Uniunii care nu sunt relevante în scopul protecției securității naționale [89].

212. Pe de altă parte, Comisia însăși a indicat că nu există posibilități pentru cetățenii Uniunii să obțină accesul, rectificarea sau ștergerea datelor și nici măsuri reparatorii administrative sau judiciare, în ceea ce privește colectarea și prelucrarea ulterioară a datelor lor personale în cadrul programelor de supraveghere americane [90].

213. În sfârșit, trebuie să se menționeze că normele americane referitoare la protecția vieții private pot face obiectul unei aplicări diferențiate între cetățenii americani și cetățenii străini [91].

214. Din considerațiile de mai sus rezultă că Decizia 2000/520 nu prevede norme clare și precise care să reglementeze întinderea ingerinței în drepturile fundamentale consacrate la articolele 7 și 8 din cartă. Prin urmare, se impune constatarea că această decizie și aplicarea sa implică o ingerință în drepturile fundamentale amintite de o vastă amploare și de o gravitate deosebită fără ca o astfel de ingerință să fie delimitată în mod precis de dispoziții care să permită să se garanteze că aceasta este limitată efectiv la ceea ce este strict necesar.

215. Prin adoptarea Deciziei 2000/520, apoi prin menținerea acesteia în vigoare, Comisia a depășit, așadar, limitele impuse de respectarea principiului proporționalității în raport cu articolele 7, 8 și cu articolul 52 alineatul (1) din cartă. La aceasta se adaugă constatarea unei ingerințe nejustificate în dreptul cetățenilor Uniunii la o cale de atac efectivă protejat prin articolul 47 din cartă.

216. În consecință, trebuie să se constate nevaliditatea acestei decizii întrucât, ca urmare a încălcării drepturilor fundamentale descrise anterior, nu se poate considera că sistemul sferei de siguranță pe care îl instituie asigură un nivel adecvat de protecție a datelor cu caracter personal care sunt transferate din Uniune către Statele Unite în cadrul acestui sistem.

217. În fața unei asemenea constatări a încălcării drepturilor fundamentale ale cetățenilor Uniunii, considerăm că Comisia ar fi trebuit să suspende aplicarea Deciziei 2000/520.

218. Această decizie are o durată nedeterminată. Or, prezenta cauză demonstrează că caracterul adecvat al nivelului de protecție oferit de o țară terță poate evolua în timp în funcție de schimbarea atât a circumstanțelor de fapt, cât și de drept care au constituit temeiul deciziei menționate.

219. Subliniem că Decizia 2000/520 însăși conține dispoziții care prevăd posibilitatea Comisiei de a o adapta în funcție de circumstanțe.

89 — Paginile 10 și 11 din comunicarea Comisiei menționată la nota de subsol 2.

90 — A se vedea punctul 7.2, p. 20, din comunicarea Comisiei menționată la nota de subsol 58.

91 — A se vedea, cu privire la această chestiune, Kuner, C., „Foreign Nationals and Data Protection Law: A Transatlantic Analysis”, *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Cambridge, 2014, p. 213, în special p. 216 și următoarele.

220. Astfel, rezultă din considerentul (9) al acestei decizii că „[a]r putea fi necesar ca «sfera de siguranță» creată de principii și de FAQ să fie revizuită în lumina experienței, a evoluției protecției vieții private în circumstanțe în care tehnologia facilitează din ce în ce mai mult transferul și prelucrarea datelor cu caracter personal și în lumina rapoartelor privind punerea în aplicare elaborate de autoritățile competente”.

221. De asemenea, potrivit articolului 3 alineatul (4) din decizia menționată, „[î]n cazul în care informațiile strânse în aplicarea alineatelor (1), (2) și (3) demonstrează că un organism însărcinat cu asigurarea respectării principiilor puse în aplicare în conformitate cu FAQ în Statele Unite ale Americii nu își îndeplinește eficient rolul, Comisia informează Departamentul Comerțului al Statelor Unite ale Americii și, în cazul în care este necesar, prezintă un proiect de măsuri […] în vederea abrogării sau suspendării prezentei decizii ori a limitării domeniului de aplicare al acesteia”.

222. În plus, potrivit articolului 4 alineatul (1) din Decizia 2000/520, aceasta „poate fi oricând adaptată în lumina experienței dobândite în timpul punerii ei în aplicare și/sau în cazul în care nivelul de protecție oferit de principii și FAQ este depășit de exigențele legislației SUA. În orice caz, Comisia evaluează punerea în aplicare a prezentei decizii pe baza informațiilor disponibile la trei ani de la notificarea ei statelor membre și raportează comitetului înființat în temeiul articolului 31 din Directiva 95/46[…] orice constatare pertinentă, inclusiv orice dovadă care ar putea afecta evaluarea conform căreia dispozițiile de la articolul 1 din prezenta decizie asigură un nivel adecvat de protecție în sensul articolului 25 din Directiva 95/46”. Potrivit articolului 4 alineatul (2) din Decizia 2000/520, „[î]n cazul în care este necesar, Comisia prezintă un proiect de măsuri în conformitate cu procedura menționată la articolul 31 din Directiva 95/46”.

223. Comisia a constatat în observațiile formulate că există „o probabilitate ridicată […] ca aderarea la principiile sferei de siguranță să fi fost limitată într-un mod care nu mai corespunde condițiilor strict delimitate ale excepției prevăzute în domeniul securității naționale” [92]. În această privință, Comisia observă că „[d]ezvăluirile în discuție dovedesc un grad de supraveghere nediferențiat la scară largă care nu este compatibil cu criteriul necesității prevăzut în această excepție și nici, în general, cu dreptul la protecția datelor cu caracter personal consacrat la articolul 8 din cartă” [93]. Pe de altă parte, Comisia însăși a constatat că „[a]mploarea […] programe[lor] de supraveghere, combinată cu tratamentul inegal al cetățenilor [Uniunii], pune sub semnul întrebării nivelul de protecție asigurat de înțelegerea privind sfera de siguranță” [94].

224. În plus, Comisia a recunoscut în mod expres în ședință că, în cadrul Deciziei 2000/520, astfel cum se aplică în prezent, nu există nicio garanție că dreptul cetățenilor Uniunii la protecția datelor lor va fi asigurat. Această constatare nu este totuși, în opinia sa, de natură să lipsească de validitate această decizie. Deși Comisia este de acord cu afirmația potrivit căreia trebuie să reacționeze în fața unor circumstanțe noi, aceasta consideră că a luat măsuri adecvate și proporționate prin inițierea negocierilor cu Statele Unite pentru a reforma sistemul sferei de siguranță.

225. Nu suntem de acord cu această opinie. Astfel, între timp, transferul datelor cu caracter personal către Statele Unite trebuie să poată fi suspendat la inițiativa autorităților naționale de supraveghere sau ca urmare a plângerilor depuse la acestea.

226. Pe de altă parte, considerăm că, în fața unor asemenea constatări, Comisia ar fi trebuit să suspende aplicarea Deciziei 2000/520. Astfel, obiectivul protecției datelor cu caracter personal urmărit de Directiva 95/46, precum și de articolul 8 din cartă impune obligații nu numai statelor membre, ci și instituțiilor Uniunii, astfel cum rezultă din articolul 51 alineatul (1) din cartă.

92 — Punctul 44.

93 — *Idem.*

94 — A se vedea p. 5 din comunicarea Comisiei menționată la nota de subsol 2.

227. La evaluarea nivelului de protecție oferit de o țară terță, Comisia trebuie să examineze nu numai legislația internă și angajamentele internaționale ale acestei țări terțe, ci și modalitatea în care protecția datelor cu caracter personal este asigurată în practică. În cazul în care examinarea practicii dezvăluie disfuncționalități, Comisia trebuie să reacționeze și, dacă este cazul, să suspende și/sau să își adapteze fără întârziere decizia.

228. Astfel cum am constatat în considerațiile anterioare, obligația care revine statelor membre constă în principal în a se asigura, prin acțiunea autorităților naționale de supraveghere, respectarea normelor prevăzute de Directiva 95/46.

229. Obligația care revine Comisiei constă în suspendarea aplicării unei decizii pe care a adoptat-o în temeiul articolului 25 alineatul (6) din această directivă în cazul unor încălcări dovedite din partea țării terțe în cauză în timp ce poartă negocieri cu țara terță respectivă pentru a pune capăt acestor încălcări.

230. Amintim că o decizie adoptată de Comisie în temeiul acestei dispoziții are drept obiect constatarea că o țară terță „asigură” un nivel adecvat de protecție a datelor cu caracter personal care fac obiectul unui transfer către această țară terță. Termenul „asigură” conjugat la timpul prezent presupune că, pentru a putea fi menținută, o astfel de decizie trebuie să vizeze o țară terță care continuă, după adoptarea deciziei menționate, să garanteze un astfel de nivel de protecție adecvat.

231. Potrivit considerentului (57) al Directivei 95/46, „trebuie interzis transferul datelor cu caracter personal către o țară terță care nu asigură un nivel de protecție adecvat”.

232. Potrivit articolului 25 alineatul (4) din această directivă, „[a]tunci când Comisia constată, în conformitate cu procedura prevăzută în articolul 31 alineatul (2), că o țară terță nu asigură un nivel de protecție adecvat în sensul alineatului (2) din prezentul articol, statele membre iau măsurile necesare pentru a preveni orice transfer de date de același tip către țara terță în cauză”. Pe de altă parte, articolul 25 alineatul (5) din directiva menționată prevede că, „[l]a momentul oportun, Comisia intră în negocieri în vederea remedierii situației apărute în urma constatărilor făcute în temeiul alineatului (4)”.

233. Rezultă din această ultimă dispoziție că, în sistemul instituit prin articolul 25 din Directiva 95/46, negocierile inițiate cu o țară terță au drept scop remedierea lipsei nivelului de protecție adecvat, constatată în conformitate cu procedura prevăzută la articolul 31 alineatul (2) din această directivă. În cazul care ne preocupă, Comisia nu a constatat în mod formal, în conformitate cu această procedură, că sistemul sferei de siguranță nu ar mai asigura un nivel de protecție adecvat. În aceste condiții, dacă Comisia a decis să inițieze negocieri cu Statele Unite, aceasta este tocmai urmarea faptului că a considerat, în prealabil, că nivelul de protecție asigurat de această țară terță nu mai era adecvat.

234. În condițiile în care avea cunoștință de anumite disfuncționalități în aplicarea Deciziei 2000/520, Comisia nu a suspendat-o și nici nu a adaptat-o, determinând astfel continuarea încălcării drepturilor fundamentale ale persoanelor ale căror date cu caracter personal au fost și continuă să fie transferate în cadrul sistemului sferei de siguranță.

235. Or, Curtea a statuat deja, desigur în alt context, că revine Comisiei obligația de a asigura adaptarea reglementării la noile date [95].

95 — A se vedea în acest sens Hotărârea Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, punctul 40).

236. O asemenea omisiune a Comisiei de a acționa, care aduce în mod direct atingere drepturilor fundamentale protejate de articolele 7, 8 și 47 din cartă, constituie, în opinia noastră, un motiv suplimentar de constatare a nevalidității Deciziei 2000/520 în cadrul prezentei trimiteri preliminare [96].

III – **Concluzie**

237. Având în vedere considerațiile anterioare, propunem Curții să răspundă la întrebările adresate de High Court după cum urmează:

„Articolul 28 din Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date coroborat cu articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene trebuie interpretat în sensul că existența unei decizii adoptate de Comisia Europeană în temeiul articolului 25 alineatul (6) din Directiva 95/46 nu are drept efect să se împiedice o autoritate națională de supraveghere să investigheze o plângere prin care se susține că o țară terță nu asigură un nivel adecvat de protecție a datelor cu caracter personal transferate și, dacă este cazul, să suspende transferul aceste date.

Decizia 2000/520/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de principiile «sferei de siguranță» privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al SUA, este nevalidă.”

96 — Deși Curtea a statuat în Hotărârea T. Port (C-68/95, EU:C:1996:452) că „tratatul nu a prevăzut posibilitatea unei trimiteri prin care o instanță națională ar solicita Curții să constate cu titlu preliminar carența unei instituții” (punctul 53), se pare că aceasta a adoptat o poziție mai favorabilă acestei posibilități în Hotărârea Ten Kate Holding Musselkanaal și alții (C-511/03, EU:C:2005:625, punctul 29).