HOTĂRÂREA CURȚII (Marea Cameră)

6 octombrie 2015 *

„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 — Articolele 25 și 28 — Transfer de date cu caracter personal către țări terțe — Decizia 2000/520/CE — Transfer de date cu caracter personal către Statele Unite — Nivel de protecție neadecvat — Validitate — Plângere a unei persoane fizice ale cărei date au fost transferate din Uniunea Europeană către Statele Unite — Competențele autorităților naționale de supraveghere”

În cauza C-362/14,

având ca obiect o cerere de decizie preliminară formulată în temeiul articolului 267 TFUE de High Court (Înalta Curte de Justiție, Irlanda), prin decizia din 17 iulie 2014, primită de Curte la 25 iulie 2014, în procedura

Maximillian Schrems

împotriva

Data Protection Commissioner,

cu participarea:

Digital Rights Ireland Ltd,

CURTEA (Marea Cameră),

compusă din domnul V. Skouris, președinte, domnul K. Lenaerts, vicepreședinte, domnul A. Tizzano, doamna R. Silva de Lapuerta, domnii T. von Danwitz (raportor) și S. Rodin și doamna K. Jürimäe, președinți de cameră, domnii A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský și D. Šváby, doamna M. Berger și domnii F. Biltgen și C. Lycourgos, judecători,

avocat general: domnul Y. Bot,

grefier: doamna L. Hewlett, administrator principal,

având în vedere procedura scrisă și în urma ședinței din 24 martie 2015,

luând în considerare observațiile prezentate:

— pentru domnul Schrems, de N. Travers, SC, de P. O’Shea, BL, și de G. Rudden, solicitor, precum și de H. Hofmann, Rechtsanwalt;

* Limba de procedură: engleza.

— pentru Data Protection Commissioner, de P. McDermott, BL, de S. More O'Ferrall și de D. Young, solicitors;

— pentru Digital Rights Ireland Ltd, de F. Crehan, BL, precum și de S. McGarr și de E. McGarr, solicitors;

— pentru Irlanda, de A. Joyce, de B. Counihan și de E. Creedon, în calitate de agenți, asistați de D. Fennelly, BL;

— pentru guvernul belgian, de J.-C. Halleux și de C. Pochet, în calitate de agenți;

— pentru guvernul ceh, de M. Smolek și de J. Vláčil, în calitate de agenți;

— pentru guvernul italian, de G. Palmieri, în calitate de agent, asistată de P. Gentili, avvocato dello Stato;

— pentru guvernul austriac, de G. Hesse și de G. Kunnert, în calitate de agenți;

— pentru guvernul polonez, de M. Kamejsza, de M. Pawlicka și de B. Majczyna, în calitate de agenți;

— pentru guvernul sloven, de A. Grum și de V. Klemenc, în calitate de agenți;

— pentru guvernul Regatului Unit, de L. Christie și de J. Beeko, în calitate de agenți, asistați de J. Holmes, barrister;

— pentru Parlamentul European, de D. Moore, de A. Caiola și de M. Pencheva, în calitate de agenți;

— pentru Comisia Europeană, de B. Schima, de B. Martenczuk, de B. Smulders și de J. Vondung, în calitate de agenți;

— pentru Autoritatea Europeană pentru Protecția Datelor (AEPD), de C. Docksey, de A. Buchta și de V. Pérez Asinari, în calitate de agenți,

după ascultarea concluziilor avocatului general în ședința din 23 septembrie 2015,

pronunță prezenta

Hotărâre

1 Cererea de decizie preliminară privește interpretarea, în raport cu articolele 7, 8 și 47 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta"), a articolului 25 alineatul (6) și a articolului 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 (JO L 281, p. 31, Ediție specială, 13/vol. 17, p. 10), 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, Ediție specială, 01/vol. 4, p. 213, denumită în continuare „Directiva 95/46"), precum și, în esență, validitatea Deciziei 2000/520/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46 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 S.U.A. (JO L 215, p. 7, Ediție specială, 16/vol. 1, p. 64).

2 Această cerere a fost formulată în cadrul unui litigiu între domnul Schrems, pe de o parte, și Data Protection Commissioner (Comisarul pentru protecția datelor, denumit în continuare „Comisarul”), pe de altă parte, în legătură cu refuzul acestuia din urmă de a investiga o plângere depusă de domnul Schrems ca urmare a faptului că Facebook Ireland Ltd (denumită în continuare „Facebook Ireland”) transferă către Statele Unite datele cu caracter personal ale utilizatorilor săi și le stochează pe servere situate în această țară.

Cadrul juridic

Directiva 95/46

3 Considerentele (2), (10), (56), (57), (60), (62) și (63) ale Directivei 95/46 sunt redactate după cum urmează:

„(2) […] sistemele de prelucrare a datelor sunt în serviciul omului; […] acestea trebuie, indiferent de naționalitatea sau reședința persoanelor fizice, să le respecte drepturile și libertățile fundamentale, în special dreptul la viață privată, și să contribuie la […] bunăstarea persoanelor;

[…]

(10) […] obiectivul legislației interne privind prelucrarea datelor cu caracter personal este de a proteja drepturile și libertățile fundamentale, inclusiv dreptul la viață privată care este recunoscut atât prin articolul 8 din Convenția Europeană pentru apărarea drepturilor omului și a libertăților fundamentale[, semnată la Roma la 4 noiembrie 1950,] cât și în principiile generale ale dreptului comunitar; […] din acest motiv, apropierea acestor legislații nu trebuie să aibă ca rezultat scăderea protecției pe care o oferă, ci trebuie, dimpotrivă, să încerce să asigure un nivel înalt de protecție în Comunitate;

[…]

(56) […] pentru dezvoltarea comerțului internațional sunt necesare fluxuri transfrontaliere de date cu caracter personal; […] protecția persoanei garantată în Comunitate prin prezenta directivă nu se opune transferului datelor cu caracter personal în țări terțe, asigurând un nivel de protecție adecvat; […] caracterul adecvat al nivelului de protecție oferit de o țară terță trebuie apreciat având în vedere toate circumstanțele referitoare la un transfer sau o categorie de transferuri;

(57) […] pe de altă parte, trebuie interzis transferul datelor cu caracter personal către o țară terță care nu asigură un nivel de protecție adecvat;

[…]

(60) […] în orice caz, transferurile către țările terțe se efectuează numai cu respectarea deplină a dispozițiilor adoptate de statele membre în temeiul prezentei directive, în special articolul 8;

[…]

(62) […] instituirea în statele membre a unor autorități de supraveghere care să-și exercite atribuțiile în deplină independență este un element esențial al protecției persoanelor în ceea ce privește prelucrarea datelor cu caracter personal;

(63) […] aceste autorități trebuie să dispună de mijloacele necesare pentru a-și îndeplini sarcinile, indiferent dacă acestea sunt puteri de investigare sau de intervenție, în special atunci când autoritățile primesc plângeri, sau competențe de a acționa în justiție; […]”

4 Articolele 1, 2, 25, 26, 28 și 31 din Directiva 95/46 prevăd:

„*Articolul 1*

Obiectul directivei

(1) Statele membre asigură, în conformitate cu prezenta directivă, protejarea drepturilor și libertăților fundamentale ale persoanei și în special a dreptului la viața privată în ceea ce privește prelucrarea datelor cu caracter personal.

[…]

Articolul 2

Definiții

În sensul prezentei directive:

(a) «date cu caracter personal» înseamnă orice informație referitoare la o persoană fizică identificată sau identificabilă (persoana vizată); o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

(b) «prelucrarea datelor cu caracter personal» (prelucrare) înseamnă orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

[…]

(d) «operator» înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin acte cu putere de lege sau norme administrative interne sau comunitare, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi stabilite prin dreptul intern sau comunitar;

[…]

Articolul 25

Principii

(1) Statele membre prevăd ca transferul către o țară terță a datelor cu caracter personal care fac obiectul prelucrării sau sunt destinate prelucrării după transfer nu poate avea loc decât dacă, sub rezerva respectării dispozițiilor de drept intern adoptate în temeiul celorlalte dispoziții ale prezentei directive, țara terță în cauză asigură un nivel de protecție adecvat.

(2) Caracterul 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.

(3) Statele 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).

(4) Atunci 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) al prezentului articol, statele membre iau măsurile necesare pentru a preveni orice transfer de date de același tip către țara terță în cauză.

(5) La momentul oportun, Comisia intră în negocieri în vederea remedierii situației apărute în urma constatărilor făcute în temeiul alineatului (4).

(6) 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) al prezentului 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.

Statele membre iau măsurile necesare pentru a se conforma deciziei Comisiei.

Articolul 26

Derogări

(1) Prin derogare de la articolul 25 și sub rezerva dispozițiilor contrare din dreptul intern care reglementează cazuri particulare, statele membre prevăd ca un transfer de date cu caracter personal către o țară terță care nu asigură un nivel de protecție adecvat în sensul articolului 25 alineatul (2) să poată avea loc cu condiția ca:

(a) persoana vizată să își dea consimțământul ferm la transferul avut în vedere sau

(b) transferul să fie necesar pentru executarea unui contract între persoana vizată și operator sau pentru aducerea la îndeplinire a măsurilor precontractuale luate ca răspuns la cererea persoanei vizate sau

(c) transferul să fie necesar pentru încheierea sau executarea unui contract încheiat sau care urmează să fie încheiat în interesul persoanei vizate între operator și un terț sau

(d) transferul să fie necesar sau impus prin lege pentru apărarea unui interes public important sau pentru constatarea, exercitarea sau apărarea unui drept în justiție sau

(e) transferul să fie necesar apărării interesului vital al persoanei vizate sau

(f) transferul să fie făcut dintr-un registru public care, în conformitate cu dispozițiile legale sau de reglementare, este destinat informării publicului și este deschis spre consultare publicului sau oricărei persoane care demonstrează un interes legitim, în măsura în care se îndeplinesc condițiile prevăzute prin lege pentru consultări în cazurile particulare.

(2) Fără a aduce atingere alineatului (1), un stat membru poate autoriza un transfer sau o serie de transferuri de date cu caracter personal către o țară terță care nu asigură un nivel de protecție adecvat în sensul articolului 25 alineatul (2) atunci când operatorul oferă garanții suficiente privind atât protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor, cât și exercitarea drepturilor corespunzătoare; aceste garanții pot rezulta în special din clauze contractuale adecvate.

(3) Statul membru informează Comisia și alte state membre despre autorizațiile pe care le acordă în temeiul alineatului (2).

În cazul în care un stat membru sau Comisia își exprimă opoziția din motive justificate care implică protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor, Comisia adoptă măsurile adecvate, în conformitate cu procedurile prevăzute în articolul 31 alineatul (2).

Statele membre iau măsurile necesare pentru a se conforma deciziei Comisiei.

[…]

Articolul 28

Autoritatea de supraveghere

(1) Fiecare 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.

Aceste autorități acționează în condiții de independență deplină în exercitarea atribuțiilor cu care sunt învestite.

(2) Fiecare stat membru prevede ca autoritățile de supraveghere să fie consultate la elaborarea normelor și actelor administrative referitoare la protecția drepturilor și libertăților persoanelor în ceea ce privește prelucrarea datelor cu caracter personal.

(3) Fiecare autoritate este, în special, învestită cu:

— competențe de investigare, cum ar fi cea de acces la datele care fac obiectul unei prelucrări și cea de a colecta toate informațiile necesare pentru îndeplinirea îndatoririlor de supraveghere;

— competențe efective de intervenție, cum ar fi, de exemplu, competența de a emite avize înainte de începerea prelucrării, în conformitate cu articolul 20, și de a asigura publicarea adecvată a acestor avize sau de a ordona blocarea, ștergerea sau distrugerea datelor, de a impune interdicția temporară sau definitivă de prelucrare, de a avertiza sau de a admonesta operatorul sau de a sesiza parlamentele naționale sau alte instituții politice;

— competența de a acționa în justiție, în cazul încălcării dispozițiilor de drept intern adoptate în temeiul prezentei directive sau de a sesiza autoritățile judecătorești asupra acestor încălcări.

Deciziile autorităților de supraveghere care dau naștere unor plângeri pot face obiectul unei acțiuni în justiție.

(4) Fiecare autoritate de supraveghere poate fi sesizată de orice persoană sau de orice asociație care o reprezintă printr-o cerere de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal. Persoana vizată este informată despre soluția dată plângerii sale.

Fiecare 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. Persoana este informată, în orice caz, că s-a efectuat o verificare.

[…]

(6) Fiecare autoritate de supraveghere are competența, indiferent de dreptul intern aplicabil prelucrării în cauză, să exercite pe teritoriul statului membru din care provine competențele conferite în conformitate cu alineatul (3). Fiecare autoritate este chemată să își exercite competențele la cererea unei autorități a unui alt stat membru.

[…]

Articolul 31

[…]

(2) Atunci când se face trimitere la prezentul articol, se aplică articolele 4 și 7 din Decizia 1999/468/CE [a Consiliului din 28 iunie 1999 de stabilire a normelor privind exercitarea competențelor de executare conferite Comisiei (JO L 184, p. 23, Ediție specială, 01/vol. 2, p. 159)], cu respectarea dispozițiilor articolului 8.

[…]”

Decizia 2000/520

5 Decizia 2000/520 a fost adoptată de Comisie în temeiul articolului 25 alineatul (6) din Directiva 95/46.

6 Considerentele (2), (5) și (8) ale acestei decizii au următorul cuprins:

„(2) Comisia poate constata că o țară terță asigură un nivel adecvat de protecție. În acest caz, datele cu caracter personal pot fi transferate din statele membre fără a mai fi necesare garanții suplimentare.

[…]

(5) Nivelul adecvat de protecție pentru transferul de date din Comunitate către Statele Unite ale Americii, recunoscut prin prezenta decizie, ar trebui obținut în cazul în care organizațiile respectă principiile «sferei de siguranță» privind protecția vieții private pentru protecția datelor cu caracter personal transferate dintr-un stat membru în Statele Unite ale Americii (denumite în continuare «principiile») și întrebările de bază, «frequently asked questions» (denumite în continuare «FAQ»), care oferă indicații pentru punerea în aplicare a principiilor publicate de Guvernul Statelor Unite ale Americii la 21 iulie 2000. Mai mult, organizațiile ar trebui să-și facă publice politicile de confidențialitate și să se supună jurisdicției Comisiei Federale pentru Comerț [Federal Trade Commission (FTC)] în temeiul articolului 5 din Federal Trade Commission Act, care interzice actele sau practicile neloiale sau frauduloase în comerț sau care afectează comerțul, sau altui organism oficial care asigură punerea în aplicare cu eficacitate a principiilor în conformitate cu FAQ.

[…]

(8) În 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."

7 Potrivit articolelor 1-4 din Decizia 2000/520:

„Articolul 1

(1) În sensul articolului 25 alineatul (2) din Directiva 95/46/CE, pentru toate activitățile care intră în domeniul de aplicare al acelei directive, principiile «sferei de siguranță» privind protecția vieții private (denumite în continuare «principiile»), cuprinse în anexa I la prezenta decizie, puse în aplicare în conformitate cu orientările furnizate de întrebările de bază («frequently asked questions» – denumite în continuare «FAQ») publicate de Departamentul Comerțului al Statelor Unite ale Americii la 21 iulie 2000, cuprinse în anexa II la prezenta decizie, asigură un nivel adecvat de protecție a datelor personale transferate din Comunitate către organizații stabilite în Statele Unite ale Americii, ținând seama de următoarele documente emise de Departamentul Comerțului al Statelor Unite ale Americii:

(a) studiul privind punerea în aplicare a principiilor «sferei de siguranță» menționat la anexa III;

(b) un memorandum privind despăgubirile pentru încălcarea vieții private și autorizațiile exprese prevăzute de legislația Statelor Unite ale Americii, menționat la anexa IV;

(c) o scrisoare din partea Comisiei Federale pentru Comerț, menționată la anexa V;

(d) o scrisoare din partea Departamentului Transporturilor al Statelor Unite ale Americii, menționată la anexa VI.

(2) În ceea ce privește fiecare transfer de date, trebuie respectate următoarele condiții:

(a) organizația care primește datele își declară în mod public și clar angajamentul de a respecta principiile puse în aplicare în conformitate cu FAQ și

(b) organizația intră sub jurisdicția unui organism administrativ din Statele Unite ale Americii menționat la anexa VII la prezenta decizie care este împuternicit să ancheteze plângerile și să obțină măsuri de reparare împotriva practicilor neloiale sau frauduloase, precum și despăgubirea persoanelor în cauză, indiferent de țara de reședință sau de cetățenia acestora, în cazul nerespectării principiilor puse în aplicare în conformitate cu FAQ.

(3) Se consideră că sunt îndeplinite condițiile prevăzute la alineatul (2) de fiecare organizație care își declară adeziunea la principiile puse în aplicare în conformitate cu FAQ, de la data la care organizația notifică Departamentului Comerțului al Statelor Unite ale Americii (sau reprezentantului acestuia) declararea publică a angajamentului menționat la alineatul (2) litera (a) și identitatea organismului administrativ menționat la alineatul (2) litera (b).

Articolul 2

Prezenta decizie se referă numai la caracterul adecvat al protecției oferite în Statele Unite ale Americii de principiile puse în aplicare în conformitate cu FAQ în vederea respectării cerințelor prevăzute la articolul 25 alineatul (1) din Directiva 95/46/CE și nu afectează aplicarea altor dispoziții din directiva menționată care privesc prelucrarea de date cu caracter personal în statele membre, în special articolul 4.

Articolul 3

(1) Fără a aduce atingere competențelor lor de a lua măsuri în vederea asigurării respectării dispozițiilor naționale adoptate în temeiul unor dispoziții altele decât cele prevăzute la articolul 25 din Directiva 95/46/CE, autoritățile competente din statele membre își pot exercita competențele de care dispun pentru a suspenda fluxurile de date către o organizație care și-a declarat adeziunea la principiile puse în aplicare în conformitate cu FAQ în vederea protejării persoanelor cu privire la prelucrarea datelor cu caracter personal ale acestora în cazurile în care:

(a) organismul administrativ din Statele Unite ale Americii menționat la anexa VII la prezenta decizie sau o instanță de recurs independentă în sensul literei (a) din principiul de punere în aplicare menționat la anexa I la prezenta decizie a constatat că organizația încalcă principiile puse în aplicare în conformitate cu FAQ sau

(b) este foarte probabil 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-i oferi posibilitatea de a răspunde.

Suspendarea încetează de îndată ce se asigură respectarea principiilor puse în aplicare în conformitate cu FAQ, iar autoritățile competente în cauză din Comunitate sunt informate în consecință.

(2) Statele membre informează fără întârziere Comisia atunci când sunt adoptate măsuri în temeiul alineatului (1).

(3) De asemenea, statele membre și Comisia se informează reciproc asupra cazurilor în care măsurile luate de organismele însărcinate cu asigurarea respectării principiilor puse în aplicare în conformitate cu FAQ în Statele Unite ale Americii nu asigură această respectare.

(4) În 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 conformitate cu procedura menționată la articolul 31 din Directiva 95/46/CE în vederea abrogării sau suspendării prezentei decizii ori a limitării domeniului de aplicare al acesteia.

Articolul 4

(1) Prezenta decizie 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/CE 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/CE și orice dovadă care indică faptul că prezenta decizie este aplicată în mod discriminatoriu.

(2) În cazul în care este necesar, Comisia prezintă un proiect de măsuri în conformitate cu procedura menționată la articolul 31 din Directiva 95/46/CE.”

8 Anexa I la Decizia 2000/520 are următorul cuprins:

„Principiile «sferei de siguranță» privind protecția vieții private publicate de Departamentul Comerțului al Statelor Unite ale Americii la 21 iulie 2000 […] […] Departamentul Comerțului publică prezentul document («principiile»), precum și «întrebările de bază» («FAQ») în calitate de autoritate competentă cu scopul de a stimula, promova și dezvolta comerțul internațional. Principiile au fost elaborate prin consultări cu întreprinderile și publicul larg în scopul facilitării comerțului și relațiilor de afaceri dintre Statele Unite ale Americii și Uniunea Europeană. Ele sunt destinate exclusiv organizațiilor din Statele Unite ale Americii care primesc date cu caracter personal din Uniunea Europeană 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. Deoarece principiile au fost concepute pentru a servi exclusiv acestui scop, adoptarea lor în alte scopuri ar putea fi inadecvată. […] Îndeplinirea sau nu a condițiilor privind «sfera de siguranță» rămâne la latitudinea organizațiilor, care dispun de diferite mijloace pentru a se conforma acestor condiții. […] Aderarea la aceste principii 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; (c) excepțiile sau derogările prevăzute de directivă sau de legislația statului membru, cu condiția ca aceste excepții sau derogări să fie aplicate în contexte comparabile. În conformitate cu obiectivul de a consolida protecția vieții private, organizațiile trebuie să facă eforturi să aplice aceste principii integral și transparent, inclusiv să indice în codurile lor de protejare a vieții private domeniile în care excepțiile menționate la litera (b) de mai sus se vor aplica cu regularitate. Din același motiv, atunci când principiile și/sau legile Statelor Unite ale Americii permit organizațiilor să aleagă, acestea sunt invitate să opteze, în limita posibilului, pentru nivelul cel mai înalt de protecție. […]”

9 Anexa II la Decizia 2000/520 are următorul cuprins:

„Întrebări de bază (FAQ)

[…] FAQ 6 – Autocertificarea

Î: *Cum autocertifică o organizație faptul că aderă la principiile «sferei de siguranță»*?

R: Avantajele «sferei de siguranță» sunt asigurate de la data la care o organizație autocertifică Departamentului Comerțului (sau reprezentantului acestuia) că aderă la principii în conformitate cu normele de mai jos.

Pentru autocertificarea aderării la «sfera de siguranță», organizațiile pot adresa Departamentului Comerțului (sau reprezentantului acestuia) o scrisoare semnată de un funcționar al organizației care trebuie să conțină cel puțin următoarele informații:

1. numele organizației, adresa poștală, adresa electronică, numerele de telefon și de fax ale acesteia;

2. descrierea activităților organizației cu privire la informațiile cu caracter personal primite din Uniunea Europeană;

3. descrierea dispozițiilor organizației cu privire la protecția vieții private în cazul informațiilor menționate anterior, precizând: (a) locul în care textul acestor dispoziții poate fi consultat de către public; (b) data punerii în aplicare a acestor dispoziții; (c) serviciul care poate fi

contactat pentru rezolvarea plângerilor, pentru cererile de acces sau pentru orice altă problemă legată de «sfera de siguranță»; (d) denumirea instanței de reglementare specifice care este însărcinată să hotărască în privința plângerilor depuse, după caz, împotriva organizației pentru practici neloiale sau frauduloase și pentru încălcări ale legilor sau reglementărilor privind protecția vieții private (și care este menționată în anexa la principii); (e) numele oricărui program privind protecția vieții private la care participă organizația; (f) metoda de verificare (de exemplu internă sau printr-un terț) […] și (g) instanța independentă de recurs care poate ancheta plângerile nesoluționate.

O organizație poate extinde avantajele «sferei sale de siguranță» la informații de tip «resurse umane» transferate din UE pentru a fi utilizate în cadrul raporturilor de muncă, atunci când una dintre instanțele de reglementare menționată în anexa la principii are competența de a ancheta plângerile depuse, după caz, împotriva organizației menționate în domeniul informațiilor de tip «resurse umane». […]

Departamentul (sau reprezentantul acestuia) va păstra o listă a tuturor organizațiilor care urmează această procedură, garantând astfel avantajele «sferei de siguranță», și va actualiza această listă pe baza scrisorilor și notificărilor anuale primite în conformitate cu FAQ 11. […]

[…] FAQ 11 – Soluționarea litigiilor și punerea în aplicare a deciziilor

Î: *Cum trebuie puse în aplicare cerințele privind soluționarea litigiilor formulate în principiul punerii în aplicare și ce măsuri vor fi luate în cazul nerespectării repetate a principiilor de către o organizație*?

R: Principiul punerii în aplicare stabilește cerințele pentru punerea în aplicare a «sferei de siguranță». Modul în care sunt îndeplinite cerințele de la litera (b) a principiului este prezentat în FAQ privind verificarea (FAQ 7). Prezenta FAQ 11 vizează literele (a) și (c), ambele necesitând instanțe de recurs independente. Aceste instanțe pot lua forme diferite, dar trebuie să îndeplinească cerințele principiului punerii în aplicare. Organizațiile care participă la «sfera de siguranță» pot satisface aceste cerințe în următoarele moduri: (1) participând la programele organizate de sectorul privat cu privire la protecția vieții private care integrează principiile «sferei de siguranță» în normele lor și care includ mecanisme de punere în aplicare eficiente de tipul celor descrise în principiul punerii în aplicare; (2) conformându-se instrucțiunilor organelor de supraveghere sau de reglementare legale care asigură prelucrarea plângerilor persoanelor și soluționarea litigiilor; (3) luându-și angajamentul de a coopera cu autoritățile însărcinate cu protecția datelor în cadrul Uniunii Europene sau cu reprezentanții autorizați ale acestora. Prezenta listă are valoare ilustrativă și nu este restrictivă. Sectorul privat poate elabora alte mecanisme de punere în aplicare, cu condiția ca acestea să întrunească cerințele principiului punerii în aplicare și ale FAQ. Trebuie remarcat faptul că cerințele principiului punerii în aplicare vin în completarea cerinței stabilite la paragraful al treilea din introducerea la principii, în conformitate cu care inițiativele de autoreglementare trebuie să fie aplicate în conformitate cu articolul 5 din Federal Trade Commission Act sau cu o lege similară.

Instanțe de recurs

Consumatorii ar trebui să fie încurajați să adreseze eventualele plângeri organizației în cauză înainte de a face apel la instanțe de recurs independente. […]

[…]

Acțiunea FTC

FTC s-a angajat să acorde prioritate analizării sesizărilor prezentate de organizațiile de autoreglementare, precum BBBOnline și TRUSTe, precum și de statele membre ale Uniunii Europene în ceea ce privește nerespectarea principiilor «sferei de siguranță», pentru a stabili dacă a fost încălcat articolul 5 din Federal Trade Commission Act, care interzice actele sau practicile comerciale neloiale sau frauduloase. […] […]”

10 Potrivit anexei IV la Decizia 2000/520:

„Daune interese pentru nerespectarea protecției vieții private, autorizații legale, fuziuni și absorbții în conformitate cu legislația Statelor Unite ale Americii

Prezentul document răspunde cererii formulate de Comisia Europeană privind clarificarea legislației Statelor Unite ale Americii cu privire la (a) cererile de despăgubiri pentru nerespectarea protecției vieții private, (b) «autorizațiile exprese» prevăzute în legislația Statelor Unite ale Americii pentru utilizarea informațiilor cu caracter personal într-un mod care contravine principiilor «sferei de siguranță» și (c) efectul fuziunilor și absorbțiilor asupra obligațiilor asumate în conformitate cu principiile «sferei de siguranță».

[…]

B. Autorizări legale exprese Principiile «sferei de siguranță» conțin o excepție atunci când legile, reglementările sau jurisprudența instituie «obligații contradictorii sau autorizări exprese, cu condiția ca, la data acestor autorizări, o organizație să poată demonstra că nerespectarea principiilor este limitată în măsura necesară satisfacerii intereselor legitime principale stabilite de această autorizație». În 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. 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. Excepția limitată de la respectarea strictă a principiilor «sferei de siguranță» încearcă să stabilească un echilibru pentru a ține seama de interesele legitime ale fiecărei părți. Excepția se limitează la cazurile în care există o autorizație expresă. În consecință, ca situație limită, legislația, reglementarea sau decizia judecătorească pertinentă trebuie să autorizeze în mod afirmativ [a se citi «expres»] o anumită conduită a organizațiilor care aderă la «sfera de siguranță». Cu alte cuvinte, această excepție nu se va aplica atunci când legea nu dispune. Pe lângă aceasta, excepția nu se va aplica decât în cazul în care autorizația expresă vine în conflict cu respectarea principiilor «sferei de siguranță». Chiar și în aceste condiții, excepția «este limitată în măsura necesară satisfacerii intereselor legitime principale stabilite de această autorizație». De exemplu, în cazul în care legea autorizează în mod simplu [a se citi «pur și simplu»] o societate comercială să furnizeze informații cu caracter personal organismelor guvernamentale, excepția nu se aplică. Pe de altă parte, atunci când legea autorizează în mod expres societatea comercială să furnizeze informații cu caracter personal organismelor guvernamentale fără acordul persoanei, aceasta ar constitui o «autorizație expresă» de a acționa într-un mod care contravine principiilor «sferei de siguranță». De altfel, excepțiile specifice de la cerințele privind notificarea și consimțământul s-ar încadra în domeniul de aplicare al excepției (echivalând cu o autorizație specifică de divulgare a informației fără notificare și consimțământ). De exemplu, o lege care îi autorizează pe medici să furnizeze dosarele medicale cu privire la pacienții lor autorităților sanitare fără acordul prealabil al acestor pacienți ar putea permite o excepție de la principiul notificării și principul opțiunii. Această autorizație nu ar permite unui doctor să furnizeze aceleași dosare medicale organizațiilor de protecție a sănătății sau laboratoarelor de cercetare farmaceutică, acesta nefiind unul din scopurile autorizate de lege și prin urmare nefăcând parte din domeniul de aplicare a excepției. […] Autorizația în cauză poate

fi o autorizație «autonomă» de a face anumite lucruri cu informațiile cu caracter personal, dar, după cum ilustrează exemplele de mai jos, este mai probabil ca ea să fie o excepție de la o lege mai vastă care interzice colectarea, utilizarea sau divulgarea informațiilor cu caracter personal. […]”

Comunicarea COM(2013) 846 final

11 La 27 noiembrie 2013, Comisia a adoptat Comunicarea către Parlamentul European și Consiliu intitulată „Restabilirea încrederii în fluxurile de date dintre UE și SUA” [COM(2013) 846 final, denumită în continuare „Comunicarea COM(2013) 846 final”]. Această comunicare era însoțită de un raport, de asemenea din data de 27 noiembrie 2013, care conținea „Constatările copreședinților europeni ai Grupului de lucru *ad hoc* Uniunea Europeană-Statele Unite ale Americii pentru protecția datelor” („Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection”). Acest raport fusese elaborat, astfel cum se menționează la punctul 1 din acesta, în cooperare cu Statele Unite ale Americii, în urma dezvăluirii existenței în această țară a mai multor programe de supraveghere care includ colectarea și prelucrarea pe scară largă de date cu caracter personal. Raportul menționat conținea printre altele o analiză detaliată a ordinii juridice a Statelor Unite în ceea ce privește în special temeiurile legale de autorizare a existenței unor programe de supraveghere, precum și colectarea și prelucrarea datelor cu caracter personal de către autorități americane.

12 La punctul 1 din Comunicarea COM(2013) 846 final, Comisia a precizat că „[s]chimburile comerciale sunt reglementate prin Decizia [2000/520]”, adăugând că „[a]ceastă decizie prevede un temei juridic pentru transferurile de date cu caracter personal din UE către întreprinderi cu sediul în SUA care au aderat la principiile sferei de siguranță privind protecția vieții private”. În plus, la același punct 1, Comisia a subliniat importanța din ce în ce mai mare a fluxurilor de date cu caracter personal, legată în special de dezvoltarea economiei digitale, întrucât aceasta „a condus [astfel] la creșterea exponențială a cantității, calității, diversității și naturii activităților de prelucrare a datelor”.

13 La punctul 2 din această comunicare, Comisia a observat că „a crescut îngrijorarea cu privire la nivelul de protecție a datelor cu caracter personal ale cetățenilor [Uniunii] transferate către SUA în cadrul sistemului privind sfera de siguranță”, iar „[c]aracterul voluntar și declarativ al sistemului a atras o atenție sporită asupra transparenței și punerii sale în aplicare.”

14 În plus, aceasta a indicat, la același punct 2, că „[d]atele cu caracter personal ale cetățenilor [Uniunii] trimise către SUA în cadrul sferei de siguranță pot fi accesate și prelucrate ulterior de către autoritățile SUA într-un mod incompatibil cu motivele pentru care datele au fost inițial colectate în [Uniune] și cu scopul pentru care au fost transferate către SUA” și că „[m]ajoritatea furnizorilor de servicii de internet din SUA care par a fi mai direct vizați de [programele de supraveghere] sunt certificați în cadrul sistemului privind sfera de siguranță”.

15 La punctul 3.2 din Comunicarea COM(2013) 846 final, Comisia a subliniat existența unei serii de deficiențe privind punerea în aplicare a Deciziei 2000/520. Aceasta a menționat, pe de o parte, faptul că unele societăți americane certificate nu respectau principiile prevăzute la articolul 1 alineatul (1) din Decizia 2000/520 (denumite în continuare „principiile sferei de siguranță”), și că trebuiau aduse îmbunătățiri acestei decizii, care să aibă în vedere „deficiențele structurale legate de transparență și controlul punerii în aplicare, principiile materiale privind sfera de siguranță și aplicarea excepției pe motivul securității naționale”. Pe de altă parte, aceasta a precizat că „[s]fera de siguranță servește, de asemenea, ca interfață pentru transferul de date cu caracter personal ale cetățenilor Uniunii din [Uniune] către SUA de către societățile care au obligația de a transmite date către agențiile de informații americane în cadrul programelor SUA de colectare de informații”.

16 Comisia a concluzionat, la același punct 3.2, că, deși, „[a]vând în vedere deficiențele identificate, nu pot fi menținute modalitățile actuale de aplicare a sferei de siguranță[,] [c]u toate acestea, revocarea sa ar afecta în mod negativ interesele societăților membre atât din [Uniune], cât și din SUA”. În sfârșit, tot la punctul 3.2 menționat, Comisia a adăugat că „[î]n cel mai scurt timp, […] va iniția un dialog cu autoritățile SUA pentru a discuta deficiențele identificate”.

Comunicarea COM(2013) 847 final

17 La aceeași dată de 27 noiembrie 2013, Comisia a adoptat Comunicarea 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, denumită în continuare „Comunicarea COM(2013) 847 final”]. Astfel cum reiese din cuprinsul punctului 1 din comunicare, aceasta se baza, printre altele, pe informațiile primite în cadrul Grupului de lucru ad-hoc Uniunea Europeană-Statele Unite și fusese precedată de două rapoarte de evaluare ale Comisiei, publicate în 2002 și, respectiv, în 2004.

18 Punctul 1 din această comunicare precizează că funcționarea Deciziei 2000/520 „se bazează pe angajamentele și pe autocertificarea societăților care aderă” și adaugă că „[s]emnarea acestor acorduri este voluntară, dar regulile sunt obligatorii pentru cei care aderă”.

19 În plus, din cuprinsul punctului 2.2 din Comunicarea COM(2013) 847 final reiese că, la data de 26 septembrie 2013, 3 246 de întreprinderi, care făceau parte dintr-un număr mare de sectoare industriale și de servicii, erau certificate. Aceste întreprinderi furnizau în principal servicii pe piața internă a Uniunii, printre altele în domeniul internetului, iar o parte dintre ele erau întreprinderi din Uniune care au filiale în Statele Unite. Unele dintre aceste întreprinderi prelucrau datele persoanelor angajate de acestea în Europa, care erau transferate către această țară din motive legate de resursele umane.

20 La același punct 2.2, Comisia a subliniat că „[o]rice deficiențe ale SUA în ceea ce privește transparența sau asigurarea respectării [determinau] transferul responsabilității către autoritățile europene pentru protecția datelor și către societățile care utilizează sistemul”.

21 Reiese în special din cuprinsul punctelor 3-5 și 8 din Comunicarea COM(2013) 847 final că, în practică, un număr important de întreprinderi certificate nu respectau sau nu respectau integral principiile sferei de siguranță.

22 În plus, la punctul 7 din această comunicare, Comisia a menționat că „toate societățile implicate în programul PRISM [program de colectare de informații pe scară largă] și care oferă autorităților din SUA acces la datele stocate și prelucrate în SUA au statutul de societăți certificate în sistemul sferei de siguranță” și că „[d]in acest motiv, sfera de siguranță a constituit unul dintre canalele prin care s-a permis serviciilor de informații din SUA să colecteze date personale prelucrate inițial în [Uniune]”. În această privință, Comisia a constatat, la punctul 7.1. din comunicarea menționată, că „o serie de temeiuri juridice din legislația SUA permit colectarea și prelucrarea pe scară largă a datelor cu caracter personal care sunt stocate sau prelucrate de societățile cu sediul în SUA” și că „[s]cara largă a acestor programe poate permite ca datele transferate să fie accesate și prelucrate ulterior de către autoritățile SUA depășind ceea ce este strict necesar și proporțional cu protecția securității naționale, conform derogării prevăzute de Decizia [2000/520]”.

23 La punctul 7.2 din Comunicarea COM(2013) 847 final, intitulat „Limitări și posibilități de remediere”, Comisia a subliniat că „garanțiile prevăzute de legislația SUA sunt valabile în principal pentru cetățenii SUA sau persoanele care își au reședința legală în această țară” și că „[î]n plus, nu există posibilități

pentru persoanele vizate, din [Uniune] sau din SUA, să obțină [accesarea], 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 ale SUA”.

24 Potrivit punctului 8 din Comunicarea COM(2013) 847 final, figurau printre societățile certificate „[f]urnizorii de servicii internet precum Google, Facebook, Microsoft, Apple sau Yahoo”, acestea având „sute de milioane de clienți în Europa” și transferând date personale în Statele Unite în vederea prelucrării lor.

25 Comisia a concluzionat, la același punct 8, că „accesul pe scară largă al serviciilor de informații la datele transferate către SUA de societățile certificate în sistemul sferei de siguranță ridică întrebări suplimentare importante cu privire la continuitatea respectării drepturilor în materie de protecție a datelor ale cetățenilor europeni atunci când datele lor sunt transferate către SUA”.

Litigiul principal și întrebările preliminare

26 Domnul Schrems, resortisant austriac având reședința în Austria, este utilizator al rețelei sociale Facebook (denumită în continuare „Facebook”) din anul 2008.

27 Orice persoană care are reședința pe teritoriul Uniunii și care dorește să utilizeze Facebook trebuie să încheie, la momentul înscrierii sale, un contract cu Facebook Ireland, filială a Facebook Inc., stabilită ea însăși în Statele Unite. Datele cu caracter personal ale utilizatorilor Facebook care au reședința pe teritoriul Uniunii sunt, în tot sau în parte, transferate către servere aparținând Facebook Inc., situate pe teritoriul Statelor Unite, unde fac obiectul unei prelucrări.

28 La 25 iunie 2013, domnul Schrems a sesizat Comisarul cu o plângere prin care îi solicita în esență acestuia să își exercite competențele statutare interzicând Facebook Ireland să transfere datele sale cu caracter personal către Statele Unite. În cadrul plângerii, invoca faptul că dreptul și practicile în vigoare în țara menționată nu garantau o protecție suficientă a datelor cu caracter personal stocate pe teritoriul său împotriva activităților de supraveghere practicate de autoritățile publice în această țară. Domnul Schrems se referea în această privință la dezvăluirile făcute de domnul Edward Snowden cu privire la activitățile serviciilor de informații din Statele Unite, în special cele ale National Security Agency (denumită în continuare „NSA”).

29 Considerând că nu era obligat să deschidă o investigație cu privire la faptele denunțate de domnul Schrems în plângerea sa, Comisarul a respins plângerea menționată ca fiind nefondată. Acesta a estimat astfel că nu existau dovezi că NSA ar fi avut acces la datele cu caracter personal ale persoanei interesate. Comisarul a adăugat că motivele formulate de domnul Schrems în plângerea sa nu puteau fi invocate în mod util, dat fiind că orice problemă referitoare la caracterul adecvat al protecției datelor cu caracter personal în Statele Unite trebuia să fie soluționată în conformitate cu Decizia 2000/520 și că, în această decizie, Comisia constatase că Statele Unite ale Americii asigurau un nivel adecvat de protecție.

30 Domnul Schrems a introdus o acțiune la High Court (Înalta Curte de Justiție) împotriva deciziei în discuție în litigiul principal. După ce a examinat probele prezentate de părțile din litigiul principal, această instanță a constatat că supravegherea electronică și interceptarea datelor cu caracter personal transferate din Uniune către Statele Unite răspundeau unor scopuri necesare și indispensabile pentru interesul public. Instanța menționată a adăugat însă că dezvăluirile făcute de domnul Snowden demonstraseră că NSA și alte organe federale săvârșiseră „excese considerabile”.

31 Or, potrivit aceleiași instanțe, cetățenii Uniunii nu ar dispune de niciun drept efectiv de a fi ascultați. Supravegherea acțiunilor serviciilor de informații ar fi efectuată în cadrul unei proceduri secrete și necontradictorii. Odată ce datele cu caracter personal sunt transferate către Statele Unite, NSA și alte organe federale, cum ar fi Federal Bureau of Investigation (FBI), ar putea avea acces la aceste date în cadrul supravegherii și interceptărilor nediferențiate pe care aceștia le practică pe scară largă.

32 High Court (Înalta Curte de Justiție) a constatat că dreptul irlandez interzice transferul datelor cu caracter personal în afara teritoriului național, cu excepția cazurilor în care țările terțe în discuție asigură un nivel adecvat de protecție a vieții private, precum și a drepturilor și libertăților fundamentale. Importanța dreptului la respectarea vieții private și a dreptului la inviolabilitatea domiciliului, garantate de Constituția irlandeză, ar impune ca orice ingerință în aceste drepturi să fie proporțională și conformă cu cerințele prevăzute de lege.

33 Or, accesul în masă și nediferențiat la date cu caracter personal ar fi în mod vădit contrar principiului proporționalității și valorilor fundamentale protejate de Constituția irlandeză. Pentru ca interceptări de comunicații electronice să poată fi considerate conforme acestei Constituții, ar trebui să se facă dovada că aceste interceptări prezintă un caracter particularizat, că supravegherea anumitor persoane sau a anumitor grupuri de persoane este justificată în mod obiectiv în interesul securității naționale sau al combaterii criminalității și că există garanții adecvate și verificabile. Astfel, potrivit High Court (Înalta Curte de Justiție), în cazul în care cauza principală ar fi soluționată doar în temeiul dreptului irlandez, ar trebui să se constate că, având în vedere existența unei îndoieli serioase în ceea ce privește aspectul dacă Statele Unite ale Americii asigură un nivel adecvat de protecție a datelor cu caracter personal, Comisarul ar fi trebuit să deschidă o investigație cu privire la faptele denunțate de domnul Schrems în plângerea sa și că în mod eronat acesta a respins plângerea.

34 High Court (Înalta Curte de Justiție) consideră însă că această cauză privește punerea în aplicare a dreptului Uniunii în sensul articolului 51 din cartă, astfel încât legalitatea deciziei în discuție în litigiul principal trebuie apreciată în raport cu dreptul Uniunii. Or, potrivit acestei instanțe, Decizia 2000/520 nu îndeplinește cerințele care decurg atât din articolele 7 și 8 din cartă, cât și din principiile enunțate de Curte în Hotărârea Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238). Dreptul la respectarea vieții private, garantat de articolul 7 din cartă și de valorile esențiale comune tradițiilor statelor membre, ar fi lipsit de orice conținut în cazul în care s-ar permite autorităților publice să aibă acces la comunicațiile electronice în mod aleatoriu și generalizat, fără nicio justificare obiectivă întemeiată pe motive de securitate națională sau de prevenire a criminalității, legate în mod specific de persoanele vizate și fără ca aceste practici să fie însoțite de garanții adecvate și verificabile.

35 High Court (Înalta Curte de Justiție) observă, în plus, că domnul Schrems, cu ocazia acțiunii sale, denunță în realitate legalitatea sistemului „sferei de siguranță” instituit prin Decizia 2000/520 și din care decurge decizia în discuție în litigiul principal. Astfel, chiar dacă domnul Schrems nu a contestat formal nici validitatea Directivei 95/46, nici pe cea a Deciziei 2000/520, se pune întrebarea, potrivit acestei instanțe, dacă, în temeiul articolului 25 alineatul (6) din această directivă, Comisarul era ținut să respecte constatarea efectuată de Comisie în această decizie, potrivit căreia Statele Unite ale Americii asigură un nivel de protecție adecvat, sau dacă articolul 8 din cartă autoriza Comisarul să se distanțeze eventual de o astfel de constatare.

36 În aceste condiții, High Court (Înalta Curte de Justiție) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„1) În cursul analizei unei plângeri adresate unui funcționar independent învestit prin lege cu funcții de administrare și de aplicare a legislației privind protecția datelor, 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, acest funcționar,

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]?

2) Sau, dimpotrivă, funcționarul poate și/sau trebuie să desfășoare o investigație proprie asupra problemei în lumina evoluțiilor factuale ulterioare datei la care decizia Comisiei a fost publicată pentru prima dată?"

Cu privire la întrebările preliminare

37 Prin intermediul întrebărilor preliminare formulate, care trebuie analizate împreună, instanța de trimitere solicită, în esență, să se stabilească dacă și în ce măsură articolul 25 alineatul (6) din Directiva 95/46, interpretat în lumina articolelor 7, 8 și 47 din cartă, trebuie interpretat în sensul că o decizie adoptată în temeiul acestei dispoziții, precum Decizia 2000/520, prin care Comisia constată că o țară terță asigură un nivel de protecție adecvat, se opune ca o autoritate de supraveghere dintr-un stat membru, în sensul articolului 28 din această directivă, să poată examina cererea unei persoane de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal care o privesc care au fost transferate dintr-un stat membru către această țară terță, atunci când această persoană invocă faptul că dreptul și practicile în vigoare în țara menționată nu asigură un nivel de protecție adecvat.

Cu privire la competențele autorităților naționale de supraveghere, în sensul articolului 28 din Directiva 95/46, în prezența unei decizii a Comisiei adoptate în temeiul articolului 25 alineatul (6) din această directivă

38 Trebuie amintit, cu titlu introductiv, 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 respectarea vieții private, trebuie interpretate în mod necesar în lumina drepturilor fundamentale garantate de cartă (a se vedea Hotărârea Österreichischer Rundfunk și alții, C-465/00, C-138/01 și C-139/01, EU:C:2003:294, punctul 68, Hotărârea Google Spain și Google, C-131/12, EU:C:2014:317, punctul 68, precum și Hotărârea Ryneš, C-212/13, EU:C:2014:2428, punctul 29).

39 Din cuprinsul articolului 1, precum și din considerentele (2) și (10) ale Directivei 95/46 rezultă că aceasta urmărește să garanteze nu numai protejarea eficientă și completă a drepturilor și libertăților fundamentale ale persoanei, în special a dreptului fundamental la respectarea vieții private în ceea ce privește prelucrarea datelor cu caracter personal, ci și un nivel înalt de protecție a acestor drepturi și libertăți fundamentale. Importanța atât a dreptului fundamental la respectarea vieții private, garantat la articolul 7 din cartă, cât și a dreptului fundamental la protecția datelor cu caracter personal, garantat la articolul 8 din aceasta, este în plus subliniată în jurisprudența Curții (a se vedea Hotărârea Rijkeboer, C-553/07, EU:C:2009:293, punctul 47, Hotărârea Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctul 53, precum și Hotărârea Google Spain și Google, C-131/12, EU:C:2014:317, punctele 53, 66 și 74 și jurisprudența citată).

40 În ceea ce privește competențele de care dispun autoritățile de supraveghere naționale în ceea ce privește transferurile de date cu caracter personal către țări terțe, trebuie arătat că articolul 28 alineatul (1) din Directiva 95/46 impune statelor membre să instituie una sau mai multe autorități publice responsabile de supravegherea, în condiții de independență deplină, a respectării normelor Uniunii referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea unor astfel de date. Această cerință 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 (a se vedea în acest sens Hotărârea Comisia/Austria, C-614/10, EU:C:2012:631, punctul 36, și Hotărârea Comisia/Ungaria C-288/12, EU:C:2014:237, punctul 47).

41 Garanția de independență a autorităților naționale de supraveghere urmărește să asigure eficiența și fiabilitatea supravegherii respectării dispozițiilor în domeniul protecției persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și trebuie să fie interpretată în lumina acestui obiectiv. Aceasta a fost instituită în vederea consolidării protecției persoanelor și a organismelor vizate de deciziile acestor autorități. Instituirea în statele membre a unor autorități de supraveghere independente constituie, așadar, astfel cum arată considerentul (62) al Directivei 95/46, un element esențial al respectării protecției persoanelor în ceea ce privește prelucrarea datelor cu caracter personal (a se vedea Hotărârea Comisia/Germania, C-518/07, EU:C:2010:125, punctul 25, precum și Comisia/Ungaria C-288/12, EU:C:2014:237, punctul 48 și jurisprudența citată).

42 Pentru a garanta această protecție, autoritățile naționale de supraveghere trebuie, printre altele, să asigure un just echilibru între, pe de o parte, respectarea dreptului fundamental la viață privată și, pe de altă parte, interesele care impun o liberă circulație a datelor cu caracter personal (a se vedea în acest sens Hotărârea Comisia/Germania, C-518/07, EU:C:2010:125, punctul 24, și Hotărârea Comisia/Ungaria, C-288/12, EU:C:2014:237, punctul 51).

43 În acest scop, autoritățile respective dispun de o gamă largă de competențe, iar acestea, enumerate în mod neexhaustiv la articolul 28 alineatul (3) din Directiva 95/46, constituie tot atâtea mijloace necesare pentru a-și îndeplini sarcinile, după cum subliniază considerentul (63) al acestei directive. Astfel, autoritățile menționate beneficiază, printre altele, de competențe de investigare, cum ar fi aceea de a colecta toate informațiile necesare pentru îndeplinirea îndatoririlor de supraveghere, de competențe efective de intervenție, cum ar fi aceea de a impune interdicția temporară sau definitivă de prelucrare a datelor, sau de competența de a acționa în justiție.

44 Desigur, din cuprinsul articolului 28 alineatele (1) și (6) din Directiva 95/46 reiese că competențele autorităților naționale de supraveghere privesc prelucrările datelor cu caracter personal efectuate pe teritoriul statului membru din care aceste autorități provin, astfel încât ele nu dispun de competențe, în temeiul acestui articol 28, în ceea ce privește prelucrările unor astfel de date efectuate pe teritoriul unei țări terțe.

45 Cu toate acestea, operațiunea care constă în transferarea de date cu caracter personal dintr-un stat membru către o țară terță constituie, în sine, o prelucrare a datelor cu caracter personal în sensul articolului 2 litera (b) din Directiva 95/46 (a se vedea în acest sens Hotărârea Parlamentul/Consiliul și Comisia, C-317/04 și C-318/04, EU:C:2006:346, punctul 56) efectuată pe teritoriul unui stat membru. Astfel, această dispoziție definește „prelucrarea datelor cu caracter personal” ca fiind „orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate” și citează, cu titlu de exemplu, „dezvăluirea prin transmitere, diseminare sau în orice alt mod”.

46 Considerentul (60) al Directivei 95/46 precizează că transferurile de date cu caracter personal către țările terțe se efectuează numai cu respectarea deplină a dispozițiilor adoptate de statele membre în temeiul acestei directive. În această privință, capitolul IV din directiva menționată, în care figurează articolele 25 și 26, a instituit un regim prin care se urmărește asigurarea unei supravegheri de către statele membre a transferurilor de date cu caracter personal către țările terțe. Acest regim este complementar față de regimul general instituit în capitolul II din aceeași directivă, care prevede condițiile generale de legalitate a prelucrării datelor cu caracter personal (a se vedea în acest sens Hotărârea Lindqvist, C-101/01, EU:C:2003:596, punctul 63).

47 Autoritățile naționale de supraveghere fiind, conform articolului 8 alineatul (3) din cartă și articolului 28 din Directiva 95/46, responsabile de supravegherea respectării normelor Uniunii referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, fiecare dintre acestea este, așadar, învestită cu competența de a verifica dacă un transfer de date cu caracter personal din statul membru din care provine către o țară terță respectă cerințele stabilite de Directiva 95/46.

48 Recunoscând, în considerentul (56), că pentru dezvoltarea comerțului internațional sunt necesare transferuri de date cu caracter personal din statele membre către țările terțe, Directiva 95/46 stabilește drept principiu, la articolul 25 alineatul (1), că astfel de transferuri nu pot avea loc decât dacă aceste țări terțe asigură un nivel de protecție adecvat.

49 În plus, considerentul (57) al directivei menționate precizează că trebuie interzis transferul datelor cu caracter personal către o țară terță care nu asigură un nivel de protecție adecvat.

50 În scopul de a supraveghea transferul de date cu caracter personal către țările terțe în funcție de nivelul de protecție acordat acestora în fiecare dintre aceste țări, articolul 25 din Directiva 95/46 impune o serie de obligații statelor membre și Comisiei. Din cuprinsul acestui articol reiese printre altele că constatarea că o țară terță asigură sau nu asigură un nivel de protecție adecvat poate să fie efectuată, astfel cum a arătat avocatul general la punctul 86 din concluzii, fie de către statele membre, fie de către Comisie.

51 Comisia poate adopta, în temeiul articolului 25 alineatul (6) din Directiva 95/46, o decizie prin care să constate că o țară terță asigură un nivel de protecție adecvat. O astfel de decizie are drept destinatari, în conformitate cu cel de al doilea paragraf al dispoziției menționate, statele membre, care trebuie să ia măsurile necesare pentru a se conforma acesteia. În temeiul articolului 288 al patrulea paragraf TFUE, aceasta are un caracter obligatoriu pentru toate statele membre destinatare și este obligatorie, așadar, pentru toate organele lor (a se vedea în acest sens Hotărârea Albako Margarinefabrik, 249/85, EU:C:1987:245, punctul 17, și Hotărârea Mediaset, C-69/13, EU:C:2014:71, punctul 23), în măsura în care are drept efect autorizarea transferurilor de date cu caracter personal din statele membre către țările terțe vizate de aceasta.

52 În acest sens, atât timp cât decizia Comisiei nu a fost declarată nevalidă de către Curte, statele membre și organele lor, printre care se numără și autoritățile lor de supraveghere independente, nu pot, desigur, să adopte măsuri contrare acestei decizii, cum ar fi acte prin care se urmărește să se constate cu efect obligatoriu că țara terță vizată de decizia menționată nu asigură un nivel de protecție adecvat. Astfel, actele instituțiilor Uniunii beneficiază, în principiu, de o prezumție de legalitate și produc, prin urmare, efecte juridice atât timp cât nu au fost revocate, anulate în cadrul unei acțiuni în anulare sau declarate ca fiind nevalide în urma unei trimiteri preliminare sau a unei excepții de nelegalitate (Hotărârea Comisia/Grecia, C-475/01, EU:C:2004:585, punctul 18 și jurisprudența citată).

53 Cu toate acestea, o decizie a Comisiei adoptată în temeiul articolului 25 alineatul (6) din Directiva 95/46, precum Decizia 2000/520, nu poate împiedica persoanele ale căror date cu caracter personal au fost sau ar putea fi transferate către o țară terță să sesizeze autoritățile naționale de supraveghere cu o cerere, în sensul articolului 28 alineatul (4) din această directivă, de protecție a drepturilor și libertăților lor în ceea ce privește prelucrarea acestor date. O decizie de această natură nu poate, astfel cum a subliniat avocatul general în special la punctele 61, 93 și 116 din concluzii, nici anula, nici reduce competențele expres recunoscute autorităților naționale de supraveghere la articolul 8 alineatul (3) din cartă, precum și la articolul 28 din directiva menționată.

54 Nici articolul 8 alineatul (3) din cartă, nici articolul 28 din Directiva 95/46 nu exclud din domeniul de competență al autorităților naționale de supraveghere supravegherea transferurilor de date cu caracter personal către țări terțe care au făcut obiectul unei decizii a Comisiei în temeiul articolului 25 alineatul (6) din această directivă.

55 În special, articolul 28 alineatul (4) primul paragraf din Directiva 95/46, care prevede că autoritățile naționale de supraveghere pot fi sesizate de „orice persoană […] printr-o cerere de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal”, nu prevede nicio excepție în această privință în ipoteza în care Comisia ar fi adoptat o decizie în temeiul articolului 25 alineatul (6) din această directivă.

56 În plus, ar fi contrar sistemului instituit de Directiva 95/46, precum și scopului articolelor 25 și 28 din aceasta ca o decizie adoptată de Comisie în temeiul articolului 25 alineatul (6) din directiva menționată să aibă drept efect să împiedice investigarea de către o autoritate națională de supraveghere a cererii unei persoane de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal care au fost sau ar putea fi transferate dintr-un stat membru către o țară terță vizată de această decizie.

57 Dimpotrivă, articolul 28 din Directiva 95/46 se aplică, prin însăși natura sa, oricărei prelucrări a datelor cu caracter personal. Astfel, chiar în prezența unei decizii a Comisiei adoptate în temeiul articolului 25 alineatul (6) din această directivă, autoritățile naționale de supraveghere, sesizate de o persoană cu o cerere de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal care o privesc, trebuie să poată examina, în condiții de independență deplină, dacă transferul acestor date respectă cerințele stabilite de directiva menționată.

58 În caz contrar, persoanele ale căror date cu caracter personal au fost sau ar putea fi transferate către țara terță respectivă ar fi private de dreptul, garantat la articolul 8 alineatele (1) și (3) din cartă, de a sesiza autoritățile naționale de supraveghere cu o cerere în vederea protecției drepturilor lor fundamentale (a se vedea prin analogie Hotărârea Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctul 68).

59 O cerere, în sensul articolului 28 alineatul (4) din Directiva 95/46, prin care o persoană ale cărei date cu caracter personal au fost sau ar putea fi transferate către o țară terță invocă, precum în cauza principală, faptul că dreptul și practicile acestei țări nu asigură, în pofida celor constatate de Comisie într-o decizie adoptată în temeiul articolului 25 alineatul (6) din această directivă, un nivel de protecție adecvat trebuie înțeleasă în sensul că privește, în esență, compatibilitatea acestei decizii cu protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor.

60 În această privință, trebuie amintită jurisprudența constantă a Curții potrivit căreia Uniunea este o uniune de drept în care orice act al instituțiilor sale este supus controlului conformității în special cu tratatele, cu principiile generale ale dreptului, precum și cu drepturile fundamentale (a se vedea în acest sens Hotărârea Comisia și alții/Kadi, C-584/10 P, C-593/10 P și C-595/10 P, EU:C:2013:518, punctul 66, Hotărârea Inuit Tapiriit Kanatami și alții/Parlamentul și Consiliul, C-583/11 P, EU:C:2013:625, punctul 91, precum și Hotărârea Telefónica/Comisia, C-274/12 P, EU:C:2013:852, punctul 56). Deciziile Comisiei adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46 nu se pot sustrage, așadar, unui astfel de control.

61 În aceste condiții, Curtea este singura competentă să constate nevaliditatea unui act al Uniunii, cum ar fi o decizie a Comisiei adoptată în temeiul articolului 25 alineatul (6) din Directiva 95/46, caracterul exclusiv al acestei competențe având ca obiectiv garantarea securității juridice prin asigurarea aplicării uniforme a dreptului Uniunii (a se vedea Hotărârea Melki și Abdeli, C-188/10 și C-189/10, EU:C:2010:363, punctul 54, precum și Hotărârea CIVAD, C-533/10, EU:C:2012:347, punctul 40).

62 Deși instanțele naționale sunt, desigur, competente să examineze validitatea unui act al Uniunii precum o decizie a Comisiei adoptată în temeiul articolului 25 alineatul (6) din Directiva 95/46, acestea nu dispun însă de competența de a constata ele însele nevaliditatea unui astfel de act (a se vedea în acest sens Hotărârea Foto-Frost, 314/85, EU:C:1987:452, punctele 15-20, precum și Hotărârea IATA și ELFAA, C-344/04, EU:C:2006:10, punctul 27). *A fortiori*, cu ocazia examinării unei cereri, în sensul articolului 28 alineatul (4) din această directivă, privind compatibilitatea unei decizii a Comisiei adoptate în temeiul articolului 25 alineatul (6) din directiva menționată cu protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor, autoritățile naționale de supraveghere nu sunt abilitate să constate ele însele nevaliditatea unei astfel de decizii.

63 Având în vedere aceste considerații, atunci când o persoană ale cărei date cu caracter personal au fost sau ar putea să fie transferate către o țară terță care a făcut obiectul unei decizii a Comisiei în temeiul articolului 25 alineatul (6) din Directiva 95/46 sesizează o autoritate națională de supraveghere cu o cerere de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea acestor date și contestă, cu ocazia acestei cereri, precum în cauza principală, compatibilitatea acestei decizii cu protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor, revine acestei autorități sarcina de a examina cererea menționată cu toată diligența necesară.

64 În ipoteza în care autoritatea menționată ajunge la concluzia că elementele invocate în susținerea unei astfel de cereri sunt nefondate și respinge, prin urmare, această cerere, persoana care a introdus cererea menționată trebuie, astfel cum rezultă din cuprinsul articolului 28 alineatul (3) al doilea paragraf din Directiva 95/46 interpretat în lumina articolului 47 din cartă, să aibă acces la căi de atac jurisdicționale care să îi permită să conteste o astfel de decizie cauzatoare de prejudicii la instanțele naționale. Având în vedere jurisprudența citată la punctele 61 și 62 din prezenta hotărâre, aceste instanțe sunt obligate să suspende judecarea cauzei și să sesizeze Curtea cu o procedură de trimitere preliminară în aprecierea validității atunci când consideră că unul sau mai multe motive de nevaliditate formulate de părți sau, dacă este cazul, invocate din oficiu sunt întemeiate (a se vedea în acest sens Hotărârea T & L Sugars și Sidul Açúcares/Comisia, C-456/13 P, EU:C:2015:284, punctul 48 și jurisprudența citată).

65 În ipoteza contrară, în care autoritatea menționată consideră întemeiate motivele invocate de persoana care a sesizat-o cu o cerere de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal, aceeași autoritate trebuie, conform articolului 28 alineatul (3) primul paragraf a treia liniuță din Directiva 95/46 interpretat în lumina în special a articolului 8 alineatul (3) din cartă, să aibă competența de a acționa în justiție. În această privință, revine legiuitorului național sarcina de a prevedea căi de atac care să permită autorității naționale de supraveghere în cauză să invoce motivele pe care le consideră întemeiate în fața instanțelor naționale, astfel încât acestea din urmă să efectueze, dacă împărtășesc îndoielile acestei autorități în ceea ce privește validitatea deciziei Comisiei, o trimitere preliminară în vederea examinării validității acestei decizii.

66 Având în vedere considerațiile care precedă, trebuie să se răspundă la întrebările adresate că articolul 25 alineatul (6) din Directiva 95/46, înțeles în lumina articolelor 7, 8 și 47 din cartă, trebuie interpretat în sensul că o decizie adoptată în temeiul acestei dispoziții, precum Decizia 2000/520, prin care Comisia constată că o țară terță asigură un nivel de protecție adecvat, nu se opune ca o autoritate de supraveghere dintr-un stat membru, în sensul articolului 28 din această directivă, să examineze cererea unei persoane de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal care o privesc, care au fost transferate dintr-un stat membru către această țară terță, atunci când această persoană invocă faptul că dreptul și practicile în vigoare în țara terță menționată nu asigură un nivel de protecție adecvat.

Cu privire la validitatea Deciziei 2000/520

67 Astfel cum reiese din explicațiile instanței de trimitere referitoare la întrebările adresate, domnul Schrems invocă în procedura principală faptul că dreptul și practicile din Statele Unite nu asigură un nivel de protecție adecvat, în sensul articolului 25 din Directiva 95/46. După cum a arătat avocatul general la punctele 123 și 124 din concluzii, domnul Schrems exprimă îndoieli, pe care această instanță pare de altfel să le împărtășească în esență, cu privire la validitatea Deciziei 2000/520. În astfel de circumstanțe, având în vedere constatările făcute la punctele 60-63 din prezenta hotărâre și pentru a oferi un răspuns complet instanței menționate, trebuie să se analizeze dacă această decizie este conformă cu cerințele care decurg din directiva menționată, interpretată în lumina cartei.

Cu privire la cerințele care decurg din cuprinsul articolului 25 alineatul (6) din Directiva 95/46

68 Astfel cum s-a subliniat deja la punctele 48 și 49 din prezenta hotărâre, articolul 25 alineatul (1) din Directiva 95/46 interzice transferul datelor cu caracter personal către o țară terță care nu asigură un nivel de protecție adecvat.

69 Cu toate acestea, în scopul supravegherii unui asemenea transfer, articolul 25 alineatul (6) primul paragraf din această directivă prevede că Comisia „poate constata […] că o țară terță asigură un nivel de protecție adecvat în sensul alineatului (2) din [acest] articol, în temeiul legislației interne sau al angajamentelor sale internaționale […], în vederea protejării vieții private și a libertăților și drepturilor fundamentale ale persoanelor”.

70 Este adevărat că nici articolul 25 alineatul (2) din Directiva 95/46, nici vreo altă dispoziție a acesteia nu conțin o definiție a noțiunii de nivel de protecție adecvat. În special, articolul 25 alineatul (2) din directiva menționată se limitează să enunțe că respectivul caracter 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” și enumeră, în mod neexhaustiv, circumstanțele care trebuie luate în considerare în cadrul unei astfel de aprecieri.

71 Cu toate acestea, pe de o parte, așa cum reiese din însăși formularea articolului 25 alineatul (6) din Directiva 95/46, această dispoziție impune ca o țară terță să „asigure” un nivel de protecție adecvat, în temeiul legislației interne sau al angajamentelor sale internaționale. Pe de altă parte, tot potrivit acestei dispoziții, caracterul adecvat al protecției asigurate de țara terță se apreciază „în vederea protejării vieții private și a libertăților și drepturilor fundamentale ale persoanelor”.

72 Astfel, articolul 25 alineatul (6) din Directiva 95/46 pune în aplicare obligația explicită de protecție a datelor cu caracter personal prevăzută la articolul 8 alineatul (1) din cartă și urmărește să asigure, după cum a arătat avocatul general la punctul 139 din concluzii, continuitatea nivelului ridicat al acestei protecții în cazul transferului de date cu caracter personal către o țară terță.

73 Desigur, termenul „adecvat” care figurează la articolul 25 alineatul (6) din Directiva 95/46 implică faptul că nu se poate impune ca o țară terță să asigure un nivel de protecție identic cu cel garantat în ordinea juridică a Uniunii. Cu toate acestea, așa cum a arătat avocatul general la punctul 141 din concluzii, expresia „nivel de protecție adecvat” trebuie înțeleasă în sensul că impune ca această țară terță să asigure efectiv, în temeiul legislației interne sau al angajamentelor sale internaționale, un nivel de protecție a drepturilor și libertăților fundamentale în esență echivalent cu cel garantat în cadrul Uniunii în temeiul Directivei 95/46, interpretată în lumina cartei. Astfel, în lipsa unei asemenea cerințe, obiectivul menționat la punctul anterior din prezenta hotărâre nu ar fi respectat. În plus, nivelul ridicat de protecție garantat de Directiva 95/46, interpretată în lumina cartei, ar putea fi eludat cu ușurință prin transferuri de date cu caracter personal din Uniune către țări terțe în scopul prelucrării lor în aceste țări.

74 Reiese din formularea expresă a articolului 25 alineatul (6) din Directiva 95/46 că ordinea juridică a țării terțe vizate de decizia Comisiei este cea care trebuie să asigure un nivel de protecție adecvat. Chiar dacă mijloacele la care această țară terță a recurs, în această privință, pentru a asigura un astfel de nivel de protecție pot fi diferite de cele puse în aplicare în cadrul Uniunii pentru a garanta respectarea cerințelor care decurg din această directivă, interpretată în lumina cartei, aceste mijloace trebuie totuși să se dovedească în practică efective în scopul de a asigura o protecție în esență echivalentă cu cea garantată în cadrul Uniunii.

75 În aceste condiții, în cadrul examinării nivelului de protecție oferit de o țară terță, Comisia este obligată să evalueze conținutul normelor aplicabile în această țară care rezultă din legislația internă sau din angajamentele sale internaționale, precum și practica ce vizează asigurarea respectării acestor norme,

această instituție trebuind, conform articolului 25 alineatul (2) din Directiva 95/46, să ia în considerare toate circumstanțele referitoare la un transfer de date cu caracter personal către o țară terță.

76 De asemenea, având în vedere că nivelul de protecție asigurat de o țară terță este susceptibil să evolueze, revine Comisiei, după adoptarea unei decizii în temeiul articolului 25 alineatul (6) din Directiva 95/46, sarcina de a verifica în mod periodic dacă constatarea referitoare la nivelul de protecție adecvat asigurat de țara terță în cauză este în continuare justificată în fapt și în drept. O astfel de verificare se impune, în orice caz, atunci când există indicii care dau naștere unei îndoieli în această privință.

77 În plus, după cum a arătat avocatul general la punctele 134 și 135 din concluzii, în cadrul examinării validității unei decizii a Comisiei adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46, trebuie să se țină seama și de circumstanțele intervenite ulterior adoptării acestei decizii.

78 În această privință, trebuie să se constate 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 numărul important de persoane ale căror drepturi fundamentale sunt susceptibile să fie încălcate în caz de transfer al datelor cu caracter personal către o țară terță care nu asigură un nivel de protecție adecvat, puterea de apreciere a Comisiei cu privire la caracterul adecvat al nivelului de protecție asigurat de o țară terță se dovedește redusă, astfel încât este necesară efectuarea unei supravegheri stricte a cerințelor care decurg din cuprinsul articolului 25 din Directiva 95/46, interpretat în lumina cartei (a se vedea prin analogie Hotărârea Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctele 47 și 48).

Cu privire la articolul 1 din Decizia 2000/520

79 Comisia a considerat, la articolul 1 alineatul (1) din Decizia 2000/520, că principiile cuprinse în anexa I la aceasta, puse în aplicare în conformitate cu orientările furnizate de FAQ cuprinse în anexa II la decizia menționată, asigură un nivel adecvat de protecție a datelor personale transferate din Uniune către organizații stabilite în Statele Unite ale Americii. Reiese din această dispoziție că atât aceste principii, cât și FAQ au fost publicate de Departamentul Comerțului al Statelor Unite ale Americii.

80 Aderarea unei organizații la principiile sferei de siguranță se efectuează pe baza unui sistem de autocertificare, astfel cum reiese din cuprinsul articolului 1 alineatele (2) și (3) din această decizie coroborat cu FAQ 6, care figurează în anexa II la decizia menționată.

81 Deși recurgerea de către o țară terță la un sistem de autocertificare nu este, prin ea însăși, contrară cerinței prevăzute la articolul 25 alineatul (6) din Directiva 95/46, potrivit căreia țara terță în cauză trebuie să asigure un nivel de protecție adecvat „în temeiul legislației interne sau al angajamentelor […] internaționale” ale acestei țări, fiabilitatea unui astfel de sistem, din punctul de vedere al acestei cerințe, se bazează în esență pe instituirea unor mecanisme eficace de detectare și de supraveghere care să permită identificarea și sancționarea în practică a eventualelor încălcări ale normelor care asigură protecția drepturilor fundamentale, în special a dreptului la respectarea vieții private, precum și a dreptului la protecția datelor cu caracter personal.

82 În speță, principiile sferei de siguranță sunt, în temeiul celui de al doilea paragraf al anexei I la Decizia 2000/520, „destinate exclusiv organizațiilor din Statele Unite ale Americii care primesc date cu caracter personal din Uniunea Europeană 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”. Aceste principii sunt, așadar, aplicabile numai organizațiilor americane autocertificate care primesc date cu caracter personal din Uniune, fără a se impune ca autoritățile publice americane să fie supuse respectării principiilor menționate.

83 În plus, în temeiul articolului 2 din Decizia 2000/520, aceasta din urmă „se referă numai la caracterul adecvat al protecției oferite în Statele Unite ale Americii de principiile [sferei de siguranță] puse în aplicare în conformitate cu FAQ în vederea respectării cerințelor prevăzute la articolul 25 alineatul (1) din Directiva [95/46]”, fără a conține însă constatări suficiente cu privire la măsurile prin care Statele Unite ale Americii asigură un nivel de protecție adecvat, în sensul articolului 25 alineatul (6) din această directivă, în temeiul legislației interne sau al angajamentelor lor internaționale.

84 La aceasta se adaugă faptul că, în conformitate cu al patrulea paragraf al anexei I la Decizia 2000/520, aplicabilitatea principiilor menționate poate fi limitată printre altele de „cerințele privind securitatea națională, interesul public și respectarea legilor Statelor Unite ale Americii”, precum 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”.

85 În această privință, în titlul B din anexa IV la Decizia 2000/520 se subliniază, în ceea ce privește limitele cărora le este supusă aplicabilitatea principiilor sferei de siguranță, că, „[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”.

86 Astfel, Decizia 2000/520 consacră supremația „cerințelor privind securitatea națională, interesul public și respectarea legilor Statelor Unite ale Americii” asupra principiilor sferei de siguranță, supremație în temeiul căreia organizațiile americane autocertificate care primesc date cu caracter personal din Uniune sunt obligate să înlăture, fără limitare, aceste principii atunci când acestea din urmă intră în conflict cu aceste cerințe și se dovedesc, așadar, incompatibile cu ele.

87 Având în vedere caracterul general al derogării care figurează la al patrulea paragraf din anexa I la Decizia 2000/520, aceasta face astfel posibile unele ingerințe, întemeiate pe cerințe privind securitatea națională și interesul public sau pe legislația internă a Statelor Unite, în drepturile fundamentale ale persoanelor ale căror date cu caracter personal sunt sau ar putea fi transferate din Uniune către Statele Unite. În această privință, pentru a stabili existența unei ingerințe în dreptul fundamental la respectarea vieții private, este irelevant dacă informațiile vizate referitoare la viața privată prezintă sau nu prezintă un caracter sensibil sau dacă persoanele interesate au suferit sau nu au suferit eventuale inconveniente ca urmare a acestei ingerințe (Hotărârea Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctul 33 și jurisprudența citată).

88 În plus, Decizia 2000/520 nu cuprinde nicio constatare în privința existenței în Statele Unite a unor norme cu caracter statal destinate să limiteze eventualele ingerințe în drepturile fundamentale ale persoanelor ale căror date sunt transferate din Uniune către Statele Unite, ingerințe pe care entități de stat din această țară ar fi autorizate să le practice atunci când urmăresc scopuri legitime precum securitatea națională.

89 La aceasta se adaugă faptul că Decizia 2000/520 nu menționează existența unei protecții juridice eficiente împotriva unor ingerințe de această natură. Astfel cum a arătat avocatul general la punctele 204-206 din concluzii, mecanismele de arbitraj privat și procedurile în fața Comisiei Federale pentru Comerț, ale cărei competențe, descrise în special în FAQ 11, care figurează în anexa II la această decizie, sunt limitate la litigiile de natură comercială, privesc respectarea de către întreprinderile americane a principiilor sferei de siguranță și nu pot fi puse în aplicare în cadrul litigiilor privind legalitatea ingerințelor în drepturile fundamentale care rezultă din măsuri de origine statală.

90 Pe de altă parte, analiza Deciziei 2000/520 care precedă este confirmată de aprecierea pe care Comisia însăși a făcut-o cu privire la situația care rezultă din punerea în aplicare a acestei decizii. Astfel, în special la punctele 2 și 3.2 din Comunicarea COM(2013) 846 final, precum și la punctele 7.1, 7.2 și 8

din Comunicarea COM(2013) 847 final, al căror conținut este expus la punctele 13-16 și, respectiv, la punctele 22, 23 și 25 din prezenta hotărâre, această instituție a constatat că autoritățile americane puteau să aibă acces la datele cu caracter personal transferate din statele membre către Statele Unite și să le prelucreze într-un mod incompatibil în special cu scopul pentru care au fost transferate și depășind ceea ce era strict necesar și proporțional cu protecția securității naționale. De asemenea, Comisia a constatat că nu existau pentru persoanele respective măsuri reparatorii administrative sau judiciare care să permită printre altele accesul la datele care le privesc și, dacă este cazul, obținerea rectificării sau ștergerii lor.

91 Referitor la nivelul de protecție a libertăților și a drepturilor fundamentale garantat în cadrul Uniunii, o reglementare a acesteia care implică o ingerință în drepturile fundamentale garantate la articolele 7 și 8 din cartă trebuie, potrivit jurisprudenței constante a Curții, să prevadă norme clare și precise care să reglementeze conținutul și aplicarea unei măsuri și care să impună o serie de cerințe minime, astfel încât persoanele ale căror date cu caracter personal sunt vizate să dispună de garanții suficiente care să permită protejarea în mod eficient a datelor lor împotriva riscurilor de abuz, precum și împotriva oricărei accesări și a oricărei utilizări ilicite a acestor date. Necesitatea 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 de acces ilicit la aceste date (Hotărârea Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctele 54 și 55, precum și jurisprudența citată).

92 În plus și mai ales, protecția dreptului fundamental la respectarea vieții private la nivelul Uniunii impune ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele strictului necesar (Hotărârea Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctul 52 și jurisprudența citată).

93 Astfel, nu este limitată la strictul necesar o reglementare care autorizează în mod generalizat stocarea integralității datelor cu caracter personal ale tuturor persoanelor ale căror date au fost transferate din Uniune către Statele Unite, fără a se face vreo diferențiere, limitare sau excepție în funcție de obiectivul urmărit și fără a se prevedea un criteriu obiectiv care să permită delimitarea accesului autorităților publice la date și utilizarea lor ulterioară în scopuri precise, strict restrânse și susceptibile să justifice ingerința pe care o implică atât accesarea, cât și utilizarea acestor date [a se vedea în acest sens, în ceea ce privește Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE (JO L 105, p. 54, Ediție specială, 13/vol. 53, p. 51), Hotărârea Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctele 57-61].

94 În special, trebuie să se considere că o reglementare care permite autorităților publice să acceadă în mod generalizat la conținutul comunicărilor electronice aduce atingere substanței dreptului fundamental la respectarea vieții private, astfel cum este garantat la articolul 7 din cartă (a se vedea în acest sens Hotărârea Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctul 39).

95 O reglementare care nu prevede nicio posibilitate a justițiabilului de a exercita căi legale pentru a avea acces la date cu caracter personal care îl privesc sau pentru a obține rectificarea sau ștergerea unor astfel de date nu respectă nici substanța dreptului fundamental la o protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din cartă. Astfel, articolul 47 primul paragraf din cartă impune ca orice persoană ale cărei drepturi și libertăți garantate de dreptul Uniunii sunt încălcate să aibă dreptul la o cale de atac efectivă în fața unei instanțe judecătorești, în conformitate cu condițiile stabilite de acest articol. În această privință, existența însăși a unui control jurisdicțional efectiv destinat să asigure respectarea dispozițiilor dreptului Uniunii este inerentă existenței unui stat de drept (a se vedea în acest sens Hotărârea Les Verts/Parlamentul, 294/83, EU:C:1986:166, punctul 23,

Hotărârea Johnston, 222/84, EU:C:1986:206, punctele 18 și 19, Hotărârea Heylens și alții, 222/86, EU:C:1987:442, punctul 14, precum și Hotărârea UGT-Rioja și alții, C-428/06-C-434/06, EU:C:2008:488, punctul 80).

96 După cum s-a constatat în special la punctele 71, 73 și 74 din prezenta hotărâre, adoptarea de către Comisie a unei decizii în temeiul articolului 25 alineatul (6) din Directiva 95/46 necesită constatarea, motivată corespunzător de către această instituție, că țara terță respectivă asigură efectiv, în temeiul legislației interne sau al angajamentelor sale internaționale, un nivel de protecție a drepturilor fundamentale în esență echivalent cu cel garantat în ordinea juridică a Uniunii, astfel cum reiese între altele din cuprinsul punctelor precedente din prezenta hotărâre.

97 Or, este necesar să se arate că Comisia nu a afirmat în Decizia 2000/520 că Statele Unite ale Americii „asigură” efectiv un nivel de protecție adecvat în temeiul legislației interne sau al angajamentelor lor internaționale.

98 Prin urmare, și fără a fi nevoie să se examineze principiile sferei de siguranță din punctul de vedere al conținutului lor, trebuie să se concluzioneze că articolul 1 din această decizie nu respectă cerințele stabilite la articolul 25 alineatul (6) din Directiva 95/46, interpretat în lumina cartei, și că, din acest motiv, este nevalid.

Cu privire la articolul 3 din Decizia 2000/520

99 Din considerațiile expuse la punctele 53, 57 și 63 din prezenta hotărâre reiese că, având în vedere articolul 28 din Directiva 95/46, interpretat în special în lumina articolului 8 din cartă, autoritățile naționale de supraveghere trebuie să poată examina, în condiții de independență deplină, orice cerere de protecție a drepturilor și a libertăților unei persoane în ceea ce privește prelucrarea datelor cu caracter personal care o privesc. Aceasta este situația în special atunci când, cu ocazia unei astfel de cereri, această persoană ridică întrebări cu privire la compatibilitatea unei decizii a Comisiei adoptate în temeiul articolului 25 alineatul (6) din această directivă cu protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor.

100 Cu toate acestea, articolul 3 alineatul (1) primul paragraf din Decizia 2000/520 prevede o reglementare specifică în ceea ce privește competențele de care dispun autoritățile naționale de supraveghere în raport cu o constatare efectuată de Comisie referitoare la nivelul de protecție adecvat, în sensul articolului 25 din Directiva 95/46.

101 Astfel, potrivit acestei dispoziții, aceste autorități pot, „[f]ără a aduce atingere competențelor lor de a lua măsuri în vederea asigurării respectării dispozițiilor naționale adoptate în temeiul [altor] dispoziții decât cele prevăzute la articolul 25 din Directiva [95/46], [să suspende] fluxurile de date către o organizație care și-a declarat adeziunea la principiile [Deciziei 2000/520]”, în condiții restrictive care stabilesc un prag înalt de intervenție. Chiar dacă această dispoziție nu aduce atingere competențelor respectivelor autorități de a lua măsuri în vederea asigurării respectării dispozițiilor naționale adoptate în temeiul acestei directive, ea exclude, în schimb, posibilitatea autorităților menționate de a lua măsuri în vederea asigurării respectării articolului 25 din aceeași directivă.

102 Articolul 3 alineatul (1) primul paragraf din Decizia 2000/520 trebuie, așadar, înțeles în sensul că privează autoritățile naționale de supraveghere de competențele întemeiate pe articolul 28 din Directiva 95/46 în cazul în care o persoană invocă, cu ocazia unei cereri în temeiul acestei dispoziții, elemente susceptibile să repună în discuție compatibilitatea cu protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor a unei decizii a Comisiei care a constatat, în temeiul articolului 25 alineatul (6) din această directivă, că o țară terță asigură un nivel de protecție adecvat.

103 Or, competența de executare acordată Comisiei de legiuitorul Uniunii la articolul 25 alineatul (6) din Directiva 95/46 nu conferă acestei instituții competența de a restrânge competențele autorităților naționale de supraveghere vizate la punctul anterior din prezenta hotărâre.

104 În aceste condiții, este necesar să se constate că, prin adoptarea articolului 3 din Decizia 2000/520, Comisia și-a depășit competența care îi este atribuită la articolul 25 alineatul (6) din Directiva 95/46, interpretat în lumina cartei, și că, din acest motiv, articolul 3 menționat este nevalid.

105 Întrucât articolele 1 și 3 din Decizia 2000/520 nu pot fi disociate de articolele 2 și 4 și nici de anexele la această directivă, nevaliditatea lor are drept efect afectarea validității acestei decizii în ansamblul său.

106 Având în vedere toate considerațiile care precedă, trebuie să se concluzioneze că Decizia 2000/520 este nevalidă.

Cu privire la cheltuielile de judecată

107 Întrucât, în privința părților din litigiul principal, procedura are caracterul unui incident survenit la instanța de trimitere, este de competența acesteia să se pronunțe cu privire la cheltuielile de judecată. Cheltuielile efectuate pentru a prezenta observații Curții, altele decât cele ale părților menționate, nu pot face obiectul unei rambursări.

Pentru aceste motive, Curtea (Marea Cameră) declară:

1) **Articolul 25 alineatul (6) 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, astfel cum a fost modificată prin Regulamentul (CE) nr. 1882/2003 al Parlamentului European și al Consiliului din 29 septembrie 2003, interpretat în lumina articolelor 7, 8 și 47 din Carta drepturilor fundamentale a Uniunii Europene, trebuie interpretat în sensul că o decizie adoptată în temeiul acestei dispoziții, precum Decizia 2000/520/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46 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 S.U.A., prin care Comisia Europeană constată că o țară terță asigură un nivel de protecție adecvat, nu se opune ca o autoritate de supraveghere dintr-un stat membru, în sensul articolului 28 din această directivă, cu modificările ulterioare, să examineze cererea unei persoane de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal care o privesc, care au fost transferate dintr-un stat membru către această țară terță, atunci când respectiva persoană invocă faptul că dreptul și practicile în vigoare în țara terță menționată nu asigură un nivel de protecție adecvat.**

2) **Decizia 2000/520 este nevalidă.**

Semnături