Repertoriul jurisprudenței

HOTĂRÂREA CURȚII (Marea Cameră)

16 iulie 2020*

„Trimitere preliminară – Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal – Carta drepturilor fundamentale a Uniunii Europene – Articolele 7, 8 și 47 – Regulamentul (UE) 2016/679 – Articolul 2 alineatul (2) – Domeniu de aplicare – Transferuri de date cu caracter personal în scopuri comerciale către țări terțe – Articolul 45 – Decizie privind caracterul adecvat al nivelului de protecție a Comisiei – Articolul 46 – Transferuri în baza unor garanții adecvate – Articolul 58 – Competențe ale autorităților de supraveghere – Prelucrare a datelor transferate de autoritățile publice ale unei țări terțe în scopuri de securitate națională – Aprecierea caracterului adecvat al nivelului de protecție asigurat în țara terță – Decizia 2010/87/UE – Clauze standard de protecție pentru transferul de date cu caracter personal către țări terțe – Garanții adecvate oferite de operator – Validitate – Decizia de punere în aplicare (UE) 2016/1250 – Caracterul adecvat al protecției oferite de Scutul de confidențialitate Uniunea Europeană-Statele Unite – Validitate – Plângere formulată de o persoană fizică ale cărei date au fost transferate din Uniunea Europeană către Statele Unite”

În cauza C-311/18,

având ca obiect o cerere de decizie preliminară formulată în temeiul articolului 267 TFUE de High Court (Înalta Curte, Irlanda), prin decizia din 4 mai 2018, primită de Curte la 9 mai 2018, în procedura

Data Protection Commissioner

împotriva

Facebook Ireland Ltd,

Maximillian Schrems,

cu participarea:

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

* Limba de procedură: engleza.

CURTEA (Marea Cameră),

compusă din domnul K. Lenaerts, președinte, doamna R. Silva de Lapuerta, vicepreședintă, domnul A. Arabadjiev, doamna A. Prechal, domnii M. Vilaras, M. Safjan, S. Rodin și P. G. Xuereb, doamna L. S. Rossi și domnul I. Jarukaitis, președinți de cameră, și domnii M. Ilešič, T. von Danwitz (raportor) și D. Šváby, judecători,

avocat general: domnul H. Saugmandsgaard Øe,

grefier: doamna C. Strömholm, administratoare,

având în vedere procedura scrisă și în urma ședinței din 9 iulie 2019,

luând în considerare observațiile prezentate:

– pentru Data Protection Commissioner, de D. Young, solicitor, B. Murray, M. Collins, SC, și C. Donnelly, BL;

– pentru Facebook Ireland Ltd, de P. Gallagher și N. Hyland, SC, A. Mulligan și F. Kieran, BL, P. Nolan, C. Monaghan, C. O'Neill și R. Woulfe, solicitors;

– pentru domnul Schrems, de H. Hofmann, Rechtsanwalt, E. McCullough, J. Doherty și S. O'Sullivan, SC, și G. Rudden, solicitor;

– pentru The United States of America, de E. Barrington, SC, S. Kingston, BL, S. Barton și B. Walsh, solicitors;

– pentru Electronic Privacy Information Centre, de S. Lucey, solicitor, G. Gilmore și A. Butler, BL, și C. O'Dwyer, SC;

– pentru BSA Business Software Alliance Inc., de B. Van Vooren și K. Van Quathem, advocaten;

– pentru Digitaleurope, de N. Cahill, barrister, J. Cahir, solicitor, și M. Cush, SC;

– pentru Irlanda, de A. Joyce și M. Browne, în calitate de agenți, asistați de D. Fennelly, BL;

– pentru guvernul belgian, de J.-C. Halleux și P. Cottin, în calitate de agenți;

– pentru guvernul ceh, de M. Smolek, J. Vláčil, O. Serdula și A. Kasalická, în calitate de agenți;

– pentru guvernul german, de J. Möller, D. Klebs și T. Henze, în calitate de agenți;

– pentru guvernul francez, de A.-L. Desjonquères, în calitate de agent;

– pentru guvernul neerlandez, de C. S. Schillemans, K. Bulterman și M. Noort, în calitate de agenți;

– pentru guvernul austriac, de J. Schmoll și G. Kunnert, în calitate de agenți;

– pentru guvernul polonez, de B. Majczyna, în calitate de agent;

– pentru guvernul portughez, de L. Inez Fernandes, A. Pimenta și C. Vieira Guerra, în calitate de agenți;

– pentru guvernul Regatului Unit, de S. Brandon, în calitate de agent, asistat de J. Holmes, QC, și C. Knight, barrister;

– pentru Parlamentul European, de M. J. Martínez Iglesias și A. Caiola, în calitate de agenți;

– pentru Comisia Europeană, de D. Nardi, H. Krämer și H. Kranenborg, în calitate de agenți;

– pentru Comitetul European pentru Protecția Datelor (EDPB), de A. Jelinek și K. Behn, în calitate de agenți,

după ascultarea concluziilor avocatului general în ședința din 19 decembrie 2019,

pronunță prezenta

Hotărâre

1 Cererea de decizie preliminară privește în esență

– interpretarea articolului 3 alineatul (2) prima liniuță, a articolelor 25 și 26, precum și a articolului 28 alineatul (3) 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 1995, L 281, p. 31, Ediție specială, 13/vol. 17, p. 10), interpretate în lumina articolului 4 alineatul (2) TUE și a articolelor 7, 8 și 47 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”);

– interpretarea și validitatea Deciziei 2010/87/UE a Comisiei din 5 februarie 2010 privind clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele stabilite în țări terțe în temeiul Directivei 95/46 (JO 2010, L 39, p. 5), astfel cum a fost modificată prin Decizia de punere în aplicare (UE) 2016/2297 a Comisiei din 16 decembrie 2016 (JO 2016, L 344, p. 100) (denumită în continuare „Decizia Clauzele standard”), precum și

– interpretarea și validitatea Deciziei de punere în aplicare (UE) 2016/1250 a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46 privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA (JO 2016, L 207, p. 1, denumită în continuare „Decizia Scutul de confidențialitate”).

2 Această cerere a fost formulată în cadrul unui litigiu între Data Protection Commissioner (comisarul pentru protecția datelor, Irlanda) (denumit în continuare „comisarul”), pe de o parte, și Facebook Ireland Ltd și domnul Maximillian Schrems, pe de altă parte, în legătură cu o plângere formulată de acesta privind transferul datelor sale cu caracter personal de către Facebook Ireland la Facebook Inc. în Statele Unite.

Cadrul juridic

Directiva 95/46

3 Articolul 3 din Directiva 95/46, intitulat „Domeniul de aplicare”, prevedea la alineatul (2):

„Prezenta directivă nu se aplică prelucrării datelor cu caracter personal:

– puse în practică pentru exercitarea activităților din afara domeniului de aplicare al dreptului comunitar, cum ar fi cele prevăzute în titlurile V și VI din Tratatul privind Uniunea Europeană, și, în orice caz, prelucrărilor care au ca obiect siguranța publică, apărarea, securitatea statului (inclusiv bunăstarea economică a statului atunci când aceste prelucrări sunt legate de probleme de securitate a statului) și activitățile statului în domeniul dreptului penal;

[…]”

4 Articolul 25 din această directivă dispunea:

„(1) Statele membre prevăd că transferul către o țară terță a datelor cu caracter personal […] 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; […]

[…]

(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) din prezentul articol, în temeiul legislației interne sau al angajamentelor sale internaționale, luate în special la încheierea negocierilor menționate la alineatul (5), în vederea protejării vieții private și a libertăților și drepturilor fundamentale ale persoanelor.

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

5 Articolul 26 alineatele (2) și (4) din directiva menționată prevedea:

„(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.

[…]

(4) În cazul în care Comisia decide, în conformitate cu procedurile prevăzute în articolul 31 alineatul (2), că anumite clauze contractuale standard oferă garanții suficiente în sensul alineatului (2), statele membre iau măsurile necesare pentru a se conforma deciziei Comisiei.”

6 Potrivit articolului 28 alineatul (3) din aceeași directivă:

„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.

[…]”

RGPD

7 Directiva 95/46 a fost abrogată și înlocuită prin Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46 (Regulamentul general privind protecția datelor) (JO 2016, L 119, p. 1, rectificare în JO 2018, L 127, p. 2, denumit în continuare „RGPD”).

8 Considerentele (6), (10), (101), (103), (104), (107)-(109), (114), (116) și (141) ale RGPD au următorul cuprins:

„(6) Evoluțiile tehnologice rapide și globalizarea au generat noi provocări pentru protecția datelor cu caracter personal. Amploarea colectării și a schimbului de date cu caracter personal a crescut în mod semnificativ. Tehnologia permite atât societăților private, cât și autorităților publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităților lor. Din ce în ce mai mult, persoanele fizice fac publice la nivel mondial informații cu caracter personal. Tehnologia a transformat deopotrivă economia și viața socială și ar trebui să faciliteze în continuare libera circulație a datelor cu caracter personal în cadrul Uniunii și transferul către țări terțe și organizații internaționale, asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal.

[…]

(10) Pentru a se asigura un nivel consecvent și ridicat de protecție a persoanelor fizice și pentru a se îndepărta obstacolele din calea circulației datelor cu caracter personal în cadrul Uniunii, nivelul protecției drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea unor astfel de date ar trebui să fie echivalent în toate statele membre. Aplicarea consecventă și omogenă a normelor în materie de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ar trebui să fie asigurată în întreaga Uniune. În ceea ce privește prelucrarea datelor cu caracter personal în vederea respectării unei obligații legale, a îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, statelor membre ar trebui să li se permită să mențină sau să introducă dispoziții de drept intern care să clarifice într-o mai mare măsură aplicarea normelor prezentului regulament. În coroborare cu legislația generală și orizontală privind protecția datelor, prin care este pusă în aplicare Directiva 95/46/CE, statele

membre au mai multe legi sectoriale specifice în domenii care necesită dispoziții mai precise. Prezentul regulament oferă, de asemenea, statelor membre o marjă de manevră în specificarea normelor sale, inclusiv în ceea ce privește prelucrarea categoriilor speciale de date cu caracter personal («date sensibile»). În acest sens, prezentul regulament nu exclude dreptul statelor membre care stabilește circumstanțele aferente unor situații de prelucrare specifice, inclusiv stabilirea cu o mai mare precizie a condițiilor în care prelucrarea datelor cu caracter personal este legală.

[…]

(101) Fluxurile de date cu caracter personal către și dinspre țări situate în afara Uniunii și organizații internaționale sunt necesare pentru dezvoltarea comerțului internațional și a cooperării internaționale. Creșterea acestor fluxuri a generat noi provocări și preocupări cu privire la protecția datelor cu caracter personal. Cu toate acestea, în cazul în care se transferă date cu caracter personal din Uniune către operatori, persoane împuternicite de operatori sau alți destinatari din țări terțe sau organizații internaționale, nivelul de protecție a persoanelor fizice asigurat în Uniune prin prezentul regulament nu ar trebui să fie diminuat, inclusiv în cazurile de transferuri ulterioare de date cu caracter personal dinspre țara terță sau organizația internațională către operatori, persoane împuternicite de operatori din aceeași sau dintr-o altă țară terță sau organizație internațională. În orice caz, transferurile către țări terțe și organizații internaționale pot fi desfășurate numai în conformitate deplină cu prezentul regulament. Un transfer ar putea avea loc numai dacă, sub rezerva respectării celorlalte dispoziții ale prezentului regulament, operatorul sau persoana împuternicită de operator îndeplinește condițiile prevăzute de dispozițiile prezentului regulament privind transferul de date cu caracter personal către țări terțe sau organizații internaționale.

[…]

(103) Comisia poate decide, cu efect în întreaga Uniune, că o țară terță, un teritoriu sau un anumit sector dintr-o țară terță sau o organizație internațională oferă un nivel adecvat de protecție a datelor, asigurând astfel securitate juridică și uniformitate în Uniune în ceea ce privește țara terță sau organizația internațională care este considerată a furniza un astfel de nivel de protecție. În aceste cazuri, transferurile de date cu caracter personal către țara terță sau organizația internațională respectivă pot avea loc fără a fi necesar să se obțină autorizări suplimentare. De asemenea, Comisia poate să decidă, după trimiterea unei notificări și a unei justificări complete țării terțe sau organizației internaționale, să anuleze o astfel de decizie.

(104) În conformitate cu valorile fundamentale pe care se întemeiază Uniunea, în special protecția drepturilor omului, Comisia ar trebui, în evaluarea sa referitoare la țara terță sau la un teritoriu sau la un sector specificat dintr-o țară terță, să ia în considerare modul în care aceasta respectă statul de drept, accesul la justiție, precum și normele și standardele internaționale în materie de drepturi ale omului și legislația sa generală și sectorială, inclusiv legislația privind securitatea publică, apărarea și securitatea națională, precum și ordinea publică și dreptul penal. Adoptarea unei decizii privind caracterul adecvat al nivelului de protecție pentru un teritoriu sau un sector specificat dintr-o țară terță ar trebui să țină seama de criterii clare și obiective, cum ar fi activitățile specifice de prelucrare și domeniul de aplicare al standardelor legale aplicabile și legislația în vigoare în țara terță respectivă. Țara terță ar trebui să ofere garanții care să asigure un nivel adecvat de protecție, echivalent în esență cu cel asigurat în cadrul Uniunii, în special atunci când datele cu caracter personal sunt prelucrate în unul sau mai multe sectoare specifice. În special, țara terță ar trebui să asigure o supraveghere efectivă independentă în materie de protecție a datelor și să prevadă mecanisme de cooperare cu autoritățile statelor membre de protecție a datelor, iar persoanele vizate ar trebui să beneficieze de drepturi efective și opozabile și de reparații efective pe cale administrativă și judiciară.

[…]

(107) Comisia poate să recunoască faptul că o țară terță, un teritoriu sau un sector specificat dintr-o țară terță sau o organizație internațională nu mai asigură un nivel adecvat de protecție a datelor. În consecință, transferul de date cu caracter personal către țara terță sau organizația internațională respectivă ar trebui să fie interzis, cu excepția cazului în care sunt îndeplinite cerințele prevăzute în prezentul regulament privind transferurile în baza unor garanții adecvate, inclusiv regulile corporatiste obligatorii și derogările de la situațiile specifice. În acest caz, ar trebui să se prevadă dispoziții pentru consultări între Comisie și astfel de țări terțe sau organizații internaționale. Comisia ar trebui ca, în timp util, să informeze țara terță sau organizația internațională cu privire la aceste motive și să inițieze consultări cu aceasta pentru remedierea situației.

(108) În absența unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator ar trebui să adopte măsuri pentru a compensa lipsa protecției datelor într-o țară terță prin intermediul unor garanții adecvate pentru persoana vizată. Astfel de garanții adecvate pot consta în utilizarea regulilor corporatiste obligatorii, a clauzelor standard de protecție a datelor adoptate de Comisie, a clauzelor standard de protecție a datelor adoptate de o autoritate de supraveghere sau a clauzelor contractuale autorizate de o autoritate de supraveghere. Respectivele garanții ar trebui să asigure respectarea cerințelor în materie de protecție a datelor și drepturi ale persoanelor vizate corespunzătoare prelucrării în interiorul Uniunii, inclusiv disponibilitatea unor drepturi opozabile ale persoanelor vizate și a unor căi de atac eficiente, printre care dreptul de acces la reparații efective pe cale administrativă sau judiciară și dreptul de a solicita despăgubiri, în Uniune sau într-o țară terță. Acestea ar trebui să se refere în special la respectarea principiilor generale privind prelucrarea datelor cu caracter personal: principiul protecției datelor începând cu momentul conceperii și principiul protecției implicite a datelor. […]

(109) Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecție a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu ar trebui să împiedice operatorii sau persoanele împuternicite de aceștia să includă clauzele standard în materie de protecție a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator și o altă persoană împuternicită de operator, și nici să adauge alte clauze sau garanții suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciază drepturile sau libertățile fundamentale ale persoanelor vizate. Operatorii și persoanele împuternicite de operatori ar trebui să fie încurajați să ofere garanții suplimentare prin intermediul unor angajamente contractuale care să completeze clauzele standard în materie de protecție.

[…]

(114) În orice caz, atunci când Comisia nu a luat o decizie cu privire la nivelul adecvat de protecție a datelor dintr-o țară terță, operatorul sau persoana împuternicită de operator ar trebui să utilizeze soluții care să ofere persoanelor vizate drepturi opozabile și efective în ceea ce privește prelucrarea datelor lor în Uniune odată ce aceste date au fost transferate, astfel încât persoanele vizate să beneficieze în continuare de drepturi fundamentale și de garanții.

[…]

(116) Fluxul transfrontalier de date cu caracter personal în afara Uniunii poate expune unui risc sporit capacitatea persoanelor fizice de a-și exercita drepturile în materie de protecție a datelor, în special pentru a-și asigura protecția împotriva utilizării sau a divulgării ilegale a acestor informații. În același timp, autoritățile de supraveghere pot constata că se află în imposibilitatea

de a trata plângeri sau de a efectua investigații referitoare la activitățile desfășurate în afara frontierelor lor. Eforturile acestora de a conlucra în context transfrontalier pot fi, de asemenea, îngreunate de insuficiența competențelor de prevenire sau remediere, de caracterul eterogen al regimurilor juridice și de existența unor obstacole de ordin practic, cum ar fi constrângerile în materie de resurse. […]

[…]

(141) Orice persoană vizată ar trebui să aibă dreptul de a depune o plângere la o singură autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, precum și dreptul la o cale de atac eficientă în conformitate cu articolul 47 din cartă, în cazul în care persoana vizată consideră că drepturile sale în temeiul prezentului regulament sunt încălcate sau în cazul în care autoritatea de supraveghere nu reacționează la o plângere, respinge sau refuză parțial sau total o plângere sau nu acționează atunci când o astfel de acțiune este necesară pentru asigurarea protecției drepturilor persoanei vizate. […]”

9 Articolul 2 alineatele (1) și (2) din acest regulament prevede:

„(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.

(2) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:

(a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;

(b) de către statele membre atunci când desfășoară activități care intră sub incidența capitolului 2 al titlului V din Tratatul UE;

(c) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice;

(d) de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.”

10 Articolul 4 din regulamentul menționat dispune:

„În sensul prezentului regulament:

[…]

2. «prelucrare» înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

[…]

7. «operator» înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau 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 dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

8. «persoană împuternicită de operator» înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează date cu caracter personal în numele operatorului;

9. «destinatar» înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

[…]”

11 Articolul 23 din același regulament prevede:

„(1) Dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la articolele 12-22 și 34, precum și la articolul 5 în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la articolele 12-22, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura:

(a) securitatea națională;

(b) apărarea;

(c) securitatea publică;

(d) prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;

[…]

(2) În special, orice măsură legislativă menționată la alineatul (1) conține dispoziții specifice cel puțin, dacă este cazul, în ceea ce privește:

(a) scopurile prelucrării sau ale categoriilor de prelucrare;

(b) categoriile de date cu caracter personal;

(c) domeniul de aplicare al restricțiilor introduse;

(d) garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal;

(e) menționarea operatorului sau a categoriilor de operatori;

(f) perioadele de stocare și garanțiile aplicabile având în vedere natura, domeniul de aplicare și scopurile prelucrării sau ale categoriilor de prelucrare;

(g) riscurile pentru drepturile și libertățile persoanelor vizate și

(h) dreptul persoanelor vizate de a fi informate cu privire la restricție, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției.”

12 Capitolul V din RGPD, intitulat „Transferurile de date cu caracter personal către țări terțe sau organizații internaționale”, cuprinde articolele 44-50 din acest regulament. Potrivit articolului 44, intitulat „Principiul general al transferurilor”:

„Orice date cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate după ce sunt transferate într-o țară terță sau către o organizație internațională pot fi transferate doar dacă, sub rezerva celorlalte dispoziții ale prezentului regulament, condițiile prevăzute în prezentul capitol sunt respectate de operator și de persoana împuternicită de operator, inclusiv în ceea ce privește transferurile ulterioare de date cu caracter personal din țara terță sau de la organizația internațională către o altă țară terță sau către o altă organizație internațională. Toate dispozițiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice garantat prin prezentul regulament nu este subminat.”

13 Articolul 45 din acest regulament, intitulat „Transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecție”, prevede la alineatele (1)-(3):

„(1) Transferul de date cu caracter personal către o țară terță sau o organizație internațională se poate realiza atunci când Comisia a decis că țara terță, un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau organizația internațională în cauză asigură un nivel de protecție adecvat. Transferurile realizate în aceste condiții nu necesită autorizări speciale.

(2) Atunci când evaluează caracterul adecvat al nivelului de protecție, Comisia ține seama, în special, de următoarele elemente:

(a) [S]tatul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă, atât generală, cât și sectorială, inclusiv privind securitatea publică, apărarea, securitatea națională și dreptul penal, precum și accesul autorităților publice la datele cu caracter personal, precum și punerea în aplicare a acestei legislații, normele de protecție a datelor, normele profesionale și măsurile de securitate, inclusiv normele privind transferul ulterior de date cu caracter personal către o altă țară terță sau organizație internațională, care sunt respectate în țara terță respectivă sau în organizația internațională respectivă, jurisprudența, precum și existența unor drepturi efective și opozabile ale persoanelor vizate și a unor reparații efective pe cale administrativă și judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate;

(b) existența și funcționarea eficientă a uneia sau mai multor autorități de supraveghere independente în țara terță sau sub jurisdicția cărora intră o organizație internațională, cu responsabilitate pentru asigurarea și impunerea respectării normelor de protecție a datelor, incluzând competențe adecvate de asigurare a respectării aplicării, pentru acordarea de asistență și consiliere persoanelor vizate cu privire la exercitarea drepturilor acestora și pentru cooperarea cu autoritățile de supraveghere din statele membre și

(c) angajamentele internaționale la care a aderat țara terță sau organizația internațională în cauză sau alte obligații care decurg din convenții sau instrumente obligatorii din punct de vedere juridic, precum și din participarea acesteia la sisteme multilaterale sau regionale, mai ales în domeniul protecției datelor cu caracter personal.

(3) Comisia, după ce evaluează caracterul adecvat al nivelului de protecție, poate decide, printr-un act de punere în aplicare, că o țară terță, un teritoriu sau unul sau mai multe sectoare specificate dintr-o țară terță sau o organizație internațională asigură un nivel de protecție adecvat în sensul alineatului

(2) din prezentul articol. Actul de punere în aplicare prevede un mecanism de revizuire periodică, cel puțin o dată la patru ani, care ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională. Actul de punere în aplicare menționează aplicarea geografică și sectorială și, după caz, identifică autoritatea sau autoritățile de supraveghere menționate la alineatul (2) litera (b) din prezentul articol. Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2)."

14 Articolul 46 din regulamentul menționat, intitulat „Transferuri în baza unor garanții adecvate", prevede la alineatele (1)-(3):

„(1) În absența unei decizii în temeiul articolului 45 alineatul (3), operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o țară terță sau o organizație internațională numai dacă operatorul sau persoana împuternicită de operator a oferit garanții adecvate și cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate.

(2) Garanțiile adecvate menționate la alineatul (1) pot fi furnizate fără să fie nevoie de nicio autorizație specifică din partea unei autorități de supraveghere, prin:

(a) un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;

(b) reguli corporatiste obligatorii în conformitate cu articolul 47;

(c) clauze standard de protecție a datelor adoptate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2);

(d) clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2);

(e) un cod de conduită aprobat în conformitate cu articolul 40, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate, sau

(f) un mecanism de certificare aprobat în conformitate cu articolul 42, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

(3) Sub rezerva autorizării din partea autorității de supraveghere competente, garanțiile adecvate menționate la alineatul (1) pot fi furnizate de asemenea, în special, prin:

(a) clauze contractuale între operator sau persoana împuternicită de operator și operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din țara terță sau organizația internațională sau

(b) dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate."

15 Articolul 49 din același regulament, intitulat „Derogări pentru situații specifice”, prevede:

„(1) În absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 45 alineatul (3) sau a unor garanții adecvate în conformitate cu articolul 46, inclusiv a regulilor corporatiste obligatorii, un transfer sau un set de transferuri de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai în una dintre condițiile următoare:

(a) persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate;

(b) transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;

(c) transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;

(d) transferul este necesar din considerente importante de interes public;

(e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;

(f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul;

(g) transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de dreptul Uniunii sau de dreptul intern în acel caz specific.

În cazul în care un transfer nu ar putea să se întemeieze pe o dispoziție prevăzută la articolul 45 sau 46, inclusiv dispoziții privind reguli corporatiste obligatorii, și nu este aplicabilă niciuna dintre derogările pentru situații specifice prevăzute la primul paragraf din prezentul alineat, un transfer către o țară terță sau o organizație internațională poate avea loc numai în cazul în care transferul nu este repetitiv, se referă doar la un număr limitat de persoane vizate, este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează interesele sau drepturile și libertățile persoanei vizate și operatorul a evaluat toate circumstanțele aferente transferului de date și, pe baza acestei evaluări, a prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal. Operatorul informează autoritatea de supraveghere cu privire la transfer. Operatorul, în plus față de furnizarea informațiilor menționate la articolele 13 și 14, informează persoana vizată cu privire la transfer și la interesele legitime majore pe care le urmărește.

(2) Transferul în temeiul alineatului (1) primul paragraf litera (g) nu implică totalitatea datelor cu caracter personal sau ansamblul categoriilor de date cu caracter personal cuprinse în registru. Atunci când registrul urmează a fi consultat de către persoane care au un interes legitim, transferul se efectuează numai la cererea persoanelor respective sau în cazul în care acestea vor fi destinatarii.

(3) Alineatul (1) primul paragraf literele (a), (b) și (c) și paragraful al doilea nu se aplică în cazul activităților desfășurate de autoritățile publice în exercitarea competențelor lor publice.

(4) Interesul public prevăzut la alineatul (1) primul paragraf litera (d) este recunoscut în dreptul Uniunii sau în dreptul statului membru sub incidența căruia intră operatorul.

(5) În absența unei decizii privind caracterul adecvat al nivelului de protecție, dreptul Uniunii sau dreptul intern poate, din considerente importante de interes public, să stabilească în mod expres limite asupra transferului unor categorii specifice de date cu caracter personal către o țară terță sau o organizație internațională. Statele membre notifică aceste dispoziții Comisiei.

(6) Operatorul sau persoana împuternicită de operator consemnează evaluarea, precum și garanțiile adecvate prevăzute la paragraful al doilea al alineatului (1) din prezentul articol, în evidențele menționate la articolul 30."

16 Potrivit articolului 51 alineatul (1) din RGPD:

„Fiecare stat membru se asigură că una sau mai multe autorități publice independente sunt responsabile de monitorizarea aplicării prezentului regulament, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal în cadrul Uniunii («autoritatea de supraveghere»)."

17 Conform articolului 55 alineatul (1) din acest regulament, „[f]iecare autoritate de supraveghere are competența să îndeplinească sarcinile și să exercite competențele care îi sunt conferite în conformitate cu prezentul regulament pe teritoriul statului membru de care aparține".

18 Articolul 57 alineatul (1) din regulamentul menționat prevede:

„Fără a aduce atingere altor sarcini stabilite în temeiul prezentului regulament, fiecare autoritate de supraveghere, pe teritoriul său:

(a) monitorizează și asigură aplicarea prezentului regulament;

[…]

(f) tratează plângerile depuse de o persoană vizată […] și investighează într-o măsură adecvată obiectul plângerii și informează reclamantul cu privire la evoluția și rezultatul investigației, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu o altă autoritate de supraveghere;

[…]"

19 Potrivit articolului 58 alineatele (2) și (4) din același regulament:

„(2) Fiecare autoritate de supraveghere are toate următoarele competențe corective:

[…]

(f) de a impune o limitare temporară sau definitivă, inclusiv o interdicție asupra prelucrării;

[…]

(j) de a dispune suspendarea fluxurilor de date către un destinatar dintr-o țară terță sau către o organizație internațională.

[…]

(4) Exercitarea competențelor conferite autorității de supraveghere în temeiul prezentului articol face obiectul unor garanții adecvate, inclusiv căi de atac judiciare eficiente și procese echitabile, prevăzute în dreptul Uniunii și în dreptul intern în conformitate cu carta.”

20 Articolul 64 alineatul (2) din RGPD prevede:

„Orice autoritate de supraveghere, președintele [Comitetului european pentru protecția datelor (EDPB)] sau Comisia poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru să fie examinată de comitet în vederea obținerii unui aviz, în special în cazul în care o autoritate de supraveghere competentă nu respectă obligațiile privind asistența reciprocă în conformitate cu articolul 61 sau privind operațiunile comune în conformitate cu articolul 62.”

21 Potrivit articolului 65 alineatul (1) din acest regulament:

„Pentru a asigura aplicarea corectă și coerentă a prezentului regulament în cazuri individuale, comitetul adoptă o decizie obligatorie în următoarele cazuri:

[…]

(c) în cazul în care o autoritate de supraveghere competentă nu solicită avizul comitetului în cazurile menționate la articolul 64 alineatul (1) sau nu ține seama de avizul comitetului emis în temeiul articolului 64. În acest caz, orice autoritate de supraveghere vizată sau Comisia poate comunica chestiunea comitetului.”

22 Articolul 77 din regulamentul menționat, intitulat „Dreptul de a depune o plângere la o autoritate de supraveghere”, prevede:

„(1) Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezentul regulament.

(2) Autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul articolului 78.”

23 Articolul 78 din același regulament, intitulat „Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere”, prevede la alineatele (1) și (2):

„(1) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană fizică sau juridică are dreptul de a exercita o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează.

(2) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere care este competentă în temeiul articolelor 55 și 56 nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse în temeiul articolului 77.”

24 Articolul 94 din RGPD prevede:

„(1) [Directiva] [95/46] se abrogă cu efect de la 25 mai 2018.

(2) Trimiterile la directiva abrogată se interpretează ca trimiteri la prezentul regulament. Trimiterile la Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal instituit prin articolul 29 din Directiva [95/46] se interpretează ca trimiteri la Comitetul european pentru protecția datelor instituit prin prezentul regulament."

25 Potrivit articolului 99 din acest regulament:

„(1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

(2) Prezentul regulament se aplică de la 25 mai 2018."

Decizia Clauzele standard

26 Considerentul (11) al Deciziei Clauzele standard are următorul cuprins:

„Autoritățile de supraveghere din statele membre joacă un rol esențial în acest mecanism contractual, asigurând că datele cu caracter personal sunt corespunzător protejate după efectuarea transferului. În cazurile excepționale în care exportatorii de date refuză sau nu sunt în măsură să-l instruiască pe importatorul de date în mod corespunzător și există un risc iminent de prejudiciere a persoanelor vizate, clauzele contractuale tip ar trebui să permită autorităților de supraveghere să efectueze un audit la importatorii de date și la subcontractanți și, după caz, să ia decizii cu caracter obligatoriu pentru aceștia. Autoritățile de supraveghere ar trebui să aibă competența de a interzice sau suspenda un transfer sau o serie de transferuri de date pe baza clauzelor contractuale tip în acele cazuri excepționale în care s-a stabilit că transferul pe bază de contract este susceptibil să aibă efecte negative asupra garanțiilor și obligațiilor care oferă persoanelor vizate protecția adecvată."

27 Articolul 1 din această decizie prevede:

„Se consideră că clauzele contractuale tip prevăzute în anexă oferă garanții corespunzătoare în ceea ce privește protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor și cu privire la exercitarea drepturilor corespunzătoare în temeiul articolului 26 alineatul (2) din Directiva [95/46]."

28 Conform articolului 2 al doilea paragraf din această decizie, ea „se aplică transferului de date cu caracter personal de către operatorii stabiliți în Uniunea Europeană către destinatari stabiliți în afara teritoriului Uniunii Europene, care îndeplinesc în exclusivitate rolul de persoane împuternicite de către operator".

29 Articolul 3 din aceeași decizie prevede:

„În sensul prezentei decizii se aplică următoarele definiții:

[…]

(c) «exportator de date» înseamnă operatorul care transferă datele cu caracter personal;

(d) «importator de date» înseamnă persoana împuternicită de către operator stabilită într-o țară terță care este de acord să primească de la exportatorul de date datele cu caracter personal destinate prelucrării în numele exportatorului de date, în urma transferului, în conformitate cu instrucțiunile acestuia și cu condițiile prezentei decizii, și care nu este supusă unui sistem al unei țări terțe capabil să asigure o protecție adecvată, în sensul articolului 25 alineatul (1) din Directiva [95/46];

[…]

(f) «legea aplicabilă protecției datelor» înseamnă legislația care protejează drepturile și libertățile fundamentale ale particularilor și, în special, dreptul lor la viață privată cu privire la prelucrarea datelor cu caracter personal, aplicabilă operatorului de date din statul membru în care este stabilit exportatorul de date;

[…]”

30 În versiunea sa inițială, anterioară intrării în vigoare a Deciziei de punere în aplicare 2016/2297, articolul 4 din Decizia 2010/87 prevedea:

„(1) Fără a aduce atingere competențelor lor de a lua măsuri pentru a asigura respectarea dispozițiilor naționale adoptate în temeiul capitolelor II, III, V și VI din Directiva [95/46], autoritățile competente ale statelor membre își pot exercita competențele existente de interzicere sau suspendare a fluxului de date către țările terțe pentru a proteja persoanele fizice în legătură cu prelucrarea datelor cu caracter personal ale acestora, în cazurile în care:

(a) s-a stabilit că legea căreia i se supune importatorul de date sau subcontractantul îl obligă pe acesta să deroge de la legea aplicabilă protecției datelor cu caracter personal, care depășește restricțiile necesare într-o societate democratică, după cum prevede articolul 13 din Directiva [95/46], atunci când obligațiile respective sunt susceptibile de a avea efecte negative importante asupra garanțiilor oferite de legea aplicabilă protecției datelor cu caracter personal și clauzele contractuale tip;

(b) o autoritate competentă a stabilit că importatorul de date sau subcontractantul nu a respectat clauzele contractuale tip din anexă sau

(c) există o probabilitate mare de nerespectare în prezent sau în viitor a clauzelor contractuale tip din anexă și de creare a unui risc iminent de prejudiciere gravă a persoanelor vizate ca urmare a continuării transferului de date.

(2) Interzicerea sau suspendarea în temeiul alineatului (1) se ridică de îndată ce motivele care le justifică nu mai există.

(3) În cazul în care statele membre adoptă măsuri în temeiul alineatelor (1) și (2), ele informează fără întârziere Comisia, care transmite informațiile respective celorlalte state membre.”

31 Considerentul (5) al Deciziei de punere în aplicare 2016/2297, adoptată în urma pronunțării Hotărârii din 6 octombrie 2015, Schrems (C-362/14, EU:C:2015:650), are următorul cuprins:

„Prin urmare, *mutatis mutandis*, o decizie a Comisiei privind caracterul adecvat, adoptată în temeiul articolului 26 alineatul (4) din Directiva [95/46], este obligatorie pentru toate organele statelor membre cărora le este adresată, inclusiv pentru autoritățile independente de supraveghere ale statelor respective, în măsura în care are drept efect recunoașterea faptului că transferurile care au loc în baza clauzelor contractuale standard prevăzute în decizia respectivă oferă garanții suficiente, astfel cum se prevede la articolul 26 alineatul (2) din directiva menționată anterior. Acest lucru nu împiedică o autoritate națională de supraveghere să își exercite competența de supraveghere a fluxurilor de date, inclusiv competența de a suspenda sau de a interzice un transfer de date cu caracter personal în cazul în care constată că transferul în cauză are loc cu încălcarea legislației UE sau a legislației naționale în materie de protecție a datelor, de exemplu atunci când importatorul de date nu respectă clauzele contractuale standard.”

32 În versiunea sa actuală, rezultată din Decizia de punere în aplicare 2016/2297, articolul 4 din Decizia Clauzele standard prevede:

„Ori de câte ori autoritățile competente din statele membre își exercită competențele prevăzute la articolul 28 alineatul (3) din Directiva [95/46], antrenând suspendarea sau interdicția definitivă a fluxurilor de date către țări terțe în vederea asigurării protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal, statul membru în cauză informează fără întârziere Comisia, care va transmite mai departe informațiile respective celorlalte state membre."

33 Anexa la Decizia Clauzele standard, intitulată „Clauzele contractuale tip (persoanele împuternicite de către operator)", cuprinde 12 clauze-tip. Clauza 3 din aceasta, intitulată, la rândul său, „Clauza terțului beneficiar", prevede:

„(1) Persoana vizată poate invoca în fața exportatorului de date prezenta clauză, clauza 4 literele (b)-(i), clauza 5 literele (a)-(e) și (g)-(j), clauza 6 alineatele (1) și (2), clauza 7, clauza 8 alineatul (2), precum și clauzele 9-12 în calitate de terți beneficiari.

(2) Persoana vizată poate invoca în fața importatorului de date prezenta clauză, clauza 5 literele (a)-(e) și (g), clauza 6, clauza 7, clauza 8 alineatul (2) și clauzele 9-12, în situația în care exportatorul de date a dispărut în fapt sau și-a încetat existența de drept, cu excepția cazului în care vreo entitate succesoare și-a asumat toate obligațiile juridice ale exportatorului de date prin contract sau prin efectul legii și, ca rezultat, preia drepturile și obligațiile exportatorului de date, caz în care persoana vizată poate invoca clauzele menționate în fața acestei entități.

[…]"

34 Potrivit clauzei 4 din această anexă, intitulată „Obligațiile exportatorului de date":

„Exportatorul de date este de acord și garantează că:

(a) prelucrarea, inclusiv transferul în sine, a datelor cu caracter personal a fost și va continua să fie efectuată în conformitate cu dispozițiile relevante ale legii aplicabile privind protecția datelor (și, atunci când a fost cazul, a fost notificată autorităților competente din statul membru în care este stabilit exportatorul de date) și nu încalcă dispozițiile relevante din statul respectiv;

(b) a instruit și, pe toată durata serviciilor de prelucrare a datelor cu caracter personal, acesta va continua să îl instruiască pe importatorul de date să prelucreze datele cu caracter personal transferate numai în numele exportatorului de date și în conformitate cu legea aplicabilă privind protecția datelor și cu prezentele clauze;

[…]

(f) în cazul în care transferul implică categorii speciale de date, persoana vizată a fost informată sau va fi informată înainte de transferul datelor sale, sau cât de curând posibil în urma transferului, că datele sale ar putea fi transmise către o țară terță care nu oferă protecția adecvată în sensul Directivei [95/46];

(g) transmite orice notificare primită de la importatorul de date sau de la oricare dintre subcontractanți, în temeiul clauzei 5 litera (b) și al clauzei 8 alineatul (3), către autoritatea de supraveghere a protecției datelor, în cazul în care exportatorul de date decide să continue transferul sau să ridice suspendarea;

[…]"

35 Clauza 5 din anexa menționată, intitulată „Obligațiile importatorului de date […]”, prevede:

„Importatorul de date este de acord și garantează că:

(a) prelucrează datele cu caracter personal exclusiv în numele exportatorului de date și în conformitate cu instrucțiunile acestuia și cu clauzele; în cazul în care, din diverse motive, nu poate garanta conformitatea, acesta este de acord să informeze fără întârziere exportatorul de date cu privire la imposibilitatea sa de a asigura conformitatea, caz în care exportatorul de date are dreptul să suspende transferul de date și/sau să rezilieze contractul;

(b) acesta nu are niciun motiv să creadă că legislația care i se aplică îl împiedică să îndeplinească instrucțiunile primite de la exportatorul de date și obligațiile ce îi revin în temeiul contractului și că, în cazul unei modificări în legislația respectivă, susceptibilă să aibă efecte negative asupra garanțiilor și obligațiilor prevăzute de clauze, va notifica fără întârziere modificarea exportatorului de date, de îndată ce are cunoștință de aceasta, caz în care exportatorul de date are dreptul să suspende transferul de date și/sau să rezilieze contractul;

[…]

(d) acesta notifică fără întârziere exportatorului de date:
   (i) orice solicitare, obligatorie din punct de vedere juridic, de a divulga date cu caracter personal, prezentată de o autoritate de aplicare a legii, cu excepția cazului în care aceasta face obiectul altei interdicții, de exemplu interdicția, în cadrul dreptului penal, de a păstra confidențialitatea unei investigații urmărind aplicarea legii;
   (ii) orice acces accidental sau neautorizat, precum și
   (iii) orice solicitare primită direct de la persoanele vizate, fără a răspunde la aceasta, cu excepția cazului în care a fost autorizat să facă acest lucru;

[…]”

36 Nota de subsol la care face trimitere titlul acestei clauze 5 enunță:

„Cerințele imperative ale legislației naționale aplicabile importatorului de date care nu depășesc ceea ce este necesar într-o societate democratică pe baza unuia dintre interesele enumerate la articolul 13 alineatul (1) din Directiva [95/46], adică dacă reprezintă o măsură necesară salvgardării siguranței naționale, apărării, securității publice, prevenirii, cercetării, identificării și urmăririi în justiție a infracțiunilor sau a încălcării deontologiei în cazul profesiilor reglementate, unui interes economic sau financiar important al statului sau protecției persoanei vizate sau a drepturilor și libertăților celorlalți, nu sunt în contradicție cu clauzele contractuale tip. […]”

37 Clauza 6 din anexa la Decizia Clauzele standard, intitulată „Răspundere”, prevede:

„(1) Părțile convin că orice persoană vizată care a suferit un prejudiciu în urma încălcării obligațiilor prevăzute de clauza 3 sau clauza 11 de către oricare dintre părți sau de către subcontractant are dreptul de a primi despăgubiri din partea exportatorului de date pentru prejudiciul suferit.

(2) În cazul în care o persoană vizată nu poate introduce împotriva exportatorului de date o acțiune în despăgubiri menționată la alineatul (1), în urma încălcării de către importatorul de date sau subcontractantul acestuia a oricăreia dintre obligațiile prevăzute de clauza 3 sau clauza 11 din motiv că exportatorul de date a dispărut în fapt, și-a încetat existența de drept sau a devenit insolvabil, importatorul de date este de acord ca persoana vizată să poată formula o cerere de despăgubire împotriva importatorului de date, în locul exportatorului de date […]

[…]”

38 Clauza 8 din această anexă, intitulată „Cooperarea cu autoritățile de supraveghere”, prevede la alineatul (2):

„Părțile convin că autoritatea de supraveghere are dreptul să efectueze un audit la importatorul de date și la oricare dintre subcontractanți, în aceeași măsură și aceleași condiții care s-ar aplica unui audit efectuat la exportatorul de date în temeiul legii aplicabile privind protecția datelor.”

39 Clauza 9 din anexa menționată, intitulată „Legea aplicabilă”, precizează că clauzele sunt guvernate de legea statului membru în care este stabilit exportatorul de date.

40 Potrivit clauzei 11 din aceeași anexă, intitulată „Subcontractarea serviciilor de prelucrare a datelor”:

„(1) Importatorul de date nu subcontractează niciuna dintre operațiunile de prelucrare efectuate în numele exportatorului de date în temeiul clauzelor fără acordul în scris dat în prealabil de exportatorul de date. În cazul în care importatorul de date, având acordul exportatorului de date, își subcontractează obligațiile în temeiul prezentelor clauze, o face numai prin intermediul unui acord scris cu subcontractantul, care îi impune acestuia aceleași obligații ca cele impuse importatorului de date în temeiul prezentelor clauze. […]

(2) Contractul scris prealabil dintre importatorul de date și subcontractant prevede, de asemenea, o clauză a terțului beneficiar, astfel cum este menționat la clauza 3, pentru cazurile în care persoana vizată nu poate introduce acțiunea în despăgubiri prevăzută de clauza 6 alineatul (1) împotriva exportatorului de date și importatorului de date, întrucât aceștia au dispărut în fapt, și-au încetat existența de drept sau au devenit insolvabili și nicio entitate succesoare nu și-a asumat toate obligațiile juridice ale exportatorului de date și ale importatorului de date prin contract sau prin efectul legii. O astfel de răspundere civilă față de terțe părți a subcontractantului se limitează la propriile operațiuni de prelucrare în temeiul clauzelor.

[…]”

41 Clauza 12 din anexa la Decizia Clauzele standard, intitulată „Obligația după încheierea serviciilor de prelucrare a datelor cu caracter personal”, prevede la alineatul (1):

„Părțile convin că, la încheierea furnizării serviciilor de prelucrare a datelor cu caracter personal, la alegerea exportatorului de date, importatorul de date și subcontractantul returnează toate datele cu caracter personal transferate, precum și copiile acestora, sau distrug toate datele cu caracter personal, confirmând exportatorului de date că au făcut acest lucru, cu excepția cazului în care legislația aplicabilă importatorului de date îl împiedică să returneze sau să distrugă integral sau parțial datele cu caracter personal transferate. […]”

Decizia Scutul de confidențialitate

42 Prin Hotărârea din 6 octombrie 2015, Schrems (C-362/14, EU:C:2015:650), Curtea a declarat nevalidă 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. (JO 2000, L 215, p. 7, Ediție specială, 16/vol. 1, p. 64), în care Comisia constatase că această țară terță asigura un nivel de protecție adecvat.

43 În urma pronunțării hotărârii menționate, Comisia a adoptat Decizia Scutul de confidențialitate, după ce, în vederea adoptării acesteia, a efectuat o evaluare a reglementării Statelor Unite, astfel cum precizează considerentul (65) al deciziei menționate:

„Comisia a evaluat limitările și garanțiile disponibile în legislația SUA în ceea ce privește accesul și utilizarea datelor cu caracter personal transferate în temeiul Scutului de confidențialitate [Uniunea Europeană]-SUA către autoritățile publice americane pentru scopuri de securitate națională, aplicarea legii și alte scopuri de interes public. În plus, guvernul SUA, prin intermediul cabinetului Directorului Serviciului național de informații (ODNI) […], a oferit Comisiei asigurări cu declarații și angajamente detaliate, care figurează în anexa VI la prezenta decizie. Prin scrisoarea semnată de secretarul de stat prevăzută în anexa III la prezenta decizie, guvernul SUA s-a angajat, de asemenea, să instituie un nou mecanism de supraveghere pentru imixtiunea în scopul securității naționale, și anume Ombudsmanul pentru Scutul de confidențialitate, care este independent de serviciile de informații. În sfârșit, o declarație a Departamentului de Justiție al SUA, care figurează în anexa VII la prezenta decizie, descrie limitările și garanțiile aplicabile în ceea ce privește accesul și utilizarea datelor de către autoritățile publice în scopul aplicării legii sau în alte scopuri de interes public. Pentru a spori transparența și pentru a reflecta natura juridică a acestor angajamente, fiecare dintre documentele menționate și anexate la prezenta decizie vor fi publicate în Registrul federal al SUA.”

44 Analiza efectuată de Comisie cu privire la aceste limitări și garanții este rezumată în considerentele (67)-(135) ale Deciziei Scutul de confidențialitate, în timp ce concluziile instituției menționate privind nivelul adecvat de protecție în cadrul Scutului de confidențialitate Uniunea Europeană-Statele Unite figurează în cuprinsul considerentelor (136)-(141) ale acesteia.

45 În special, considerentele (68), (69), (76), (77), (109), (112)-(116), (120), (136) și (140) ale acestei decizii au următorul cuprins:

„(68) În conformitate cu Constituția Statelor Unite, asigurarea securității naționale intră sub autoritatea Președinției în calitate de comandant-șef, de șef al executivului și, în ceea ce privește serviciile de informații externe, de a conduce activitatea de afaceri externe a SUA […] Deși Congresul are competența de a impune anumite limitări, iar acest lucru s-a întâmplat în mai multe privințe, în cadrul limitelor respective, președintele poate coordona activitățile comunității serviciilor de informații americane, în special prin decrete prezidențiale sau directive prezidențiale. […] În prezent, cele două instrumente juridice esențiale în acest sens sunt Ordinul executiv nr. 12333 («O. E. 12333») […] și Directiva nr. 28 privind politica prezidențială («PPD-28»).

(69) Directiva nr. 28 privind politica prezidențială («PPD-28»), publicată la 17 ianuarie 2014, prevede o serie de limitări pentru operațiunile de «colectare de informații pe baza semnalelor electromagnetice» […] Directiva prezidențială are forță obligatorie pentru autoritățile americane de informații […] și efectul util al acesteia rămâne valabil în cazul schimbării administrației americane […] PPD-28 este deosebit de importantă pentru persoanele din afara SUA, inclusiv persoanele vizate din UE. […]

[…]

(76) Deși nu sunt formulate în termeni juridici, aceste principii [din PPD-28] reflectă esența principiilor necesității și proporționalității. […]

(77) Întrucât PPD-28 este o directivă emisă de președinte în calitate de șef al executivului, cerințele acesteia sunt obligatorii pentru întreaga comunitate a serviciilor de informații și au fost puse în aplicare în continuare prin intermediul normelor și procedurilor agenției care transpun principiile generale în instrucțiuni specifice pentru operațiunile zilnice. […]

[…]

(109) Pe de altă parte, în conformitate cu secțiunea 702 din [Foreign Intelligence Surveillance Act (FISA)], [United States Foreign Intelligence Surveillance Court (FISC) (Curtea de Supraveghere a Activităților Străine de Spionaj, Statele Unite)] nu autorizează măsuri de supraveghere individuală, ci mai degrabă programe de supraveghere (precum PRISM, UPSTREAM) pe baza unor certificări anuale întocmite de [United States Attorney General (Procurorul General)] și [Director of National Intelligence (DNI) (Directorul Serviciului național de informații)]. […] Astfel cum s-a arătat mai sus, certificările care trebuie să fie aprobate de către FISC nu conțin informații despre persoanele fizice care urmează să fie vizate, ci, mai degrabă, prezintă categoriile de informații operative străine […] Deși FISC nu evaluează – în temeiul unei suspiciuni rezonabile sau a oricărui alt criteriu – dacă persoanele sunt vizate în mod corespunzător pentru a dobândi informații operative străine […], controlul său se extinde la condiția că «un scop important al achiziției de date este de a obține informații operative străine». […]

[…]

(112) În primul rând, Legea privind supravegherea activităților străine de spionaj prevede o serie de căi de atac, care sunt disponibile, de asemenea, persoanelor care sunt cetățeni americani, pentru a contesta supravegherea electronică ilegală […] Aceasta include posibilitatea ca persoanele fizice să introducă o acțiune civilă pentru despăgubiri bănești împotriva Statelor Unite, atunci când informațiile despre acestea au fost folosite sau divulgate în mod ilegal și intenționat […]; să dea în judecată oficialii guvernului SUA în calitatea lor personală («în conformitate cu litera legii») pentru despăgubiri bănești […]; și să conteste legalitatea supravegherii (și să încerce să suprime informațiile) în cazul în care guvernul SUA intenționează să utilizeze sau să divulge orice informații obținute sau derivate din activitatea de supraveghere electronică împotriva persoanei în cadrul unei proceduri judiciare sau administrative în Statele Unite ale Americii […]

(113) În al doilea rând, guvernul SUA a transmis Comisiei o serie de căi suplimentare pe care persoanele vizate din UE le-ar putea utiliza pentru a introduce o acțiune împotriva funcționarilor guvernamentali pentru accesul ilegal la datele cu caracter personal sau utilizarea acestora, inclusiv în scopul securității naționale […]

(114) În sfârșit, Guvernul SUA a indicat [Freedom of information Act (FOIA) (Legea privind accesul liber la informații)] ca mijloc pentru persoanele care nu sunt cetățeni americani de a solicita accesul la înregistrările existente ale agențiilor federale, inclusiv în cazul în care acestea conțin date cu caracter personal ale persoanei în cauză […] Dat fiind caracterul său, FOIA nu oferă o modalitate de recurs individual împotriva ingerințelor privind datele cu caracter personal ca atare, chiar dacă aceasta ar putea, în principiu, să permită persoanelor să aibă acces la informații pertinente deținute de către agențiile naționale de informații. […]

(115) Deși persoanele fizice, inclusiv persoanele vizate din UE, au o serie de modalități de recurs în cazul în care au făcut obiectul supravegherii (electronice) ilegale în scopuri legate de securitatea națională, este la fel de clar că cel puțin anumite temeiuri juridice care pot fi utilizate de autoritățile americane de informații (de exemplu, O. E. 12333) nu sunt acoperite. În plus, inclusiv în cazul în care există, în principiu, căi de atac pentru persoanele care nu sunt cetățeni ai SUA, de exemplu pentru supravegherea în temeiul FISA, direcțiile de acțiune disponibile sunt limitate […], iar cererile prezentate de persoane (inclusiv cetățeni americani) vor fi declarate inadmisibile atunci când acestea nu pot arăta că au «calitate procesuală» […], ceea ce limitează accesul la instanțele ordinare […]

(116) Pentru a oferi o cale de atac suplimentară accesibilă tuturor persoanelor vizate din UE, Guvernul SUA a decis să creeze un nou mecanism de tip Ombudsman, după cum este prezentat în scrisoarea adresată de Secretarul de stat al SUA Comisiei, care figurează în anexa III la prezenta decizie. Acest mecanism se bazează pe desemnarea, în temeiul PPD-28, a unui coordonator principal (la nivel de subsecretar) în cadrul Departamentului de stat ca punct de contact unde administrațiile străine pot să își exprime preocuparea privind activitățile de colectare de informații electromagnetice din SUA, dar depășește în mod semnificativ acest concept inițial.

[…]

(120) [G]uvernul SUA se angajează să asigure faptul că, în exercitarea funcțiilor sale, Ombudsmanul pentru Scutul de confidențialitate se va putea baza pe cooperarea mecanismelor de supraveghere și de control al conformității existente în temeiul legislației americane. […] În cazul în care unul din aceste organisme de supraveghere a constatat o neconformitate, elementul vizat din cadrul comunității serviciilor de informații (de exemplu, o agenție de informații) va trebui să remedieze neconformitatea, întrucât doar acest lucru îi va permite Ombudsmanului să ofere persoanei un «răspuns pozitiv» (și anume, că neconformitatea a fost remediată) pe care Guvernul SUA s-a angajat să-l ofere. […]

[…]

(136) Având în vedere aceste constatări, Comisia consideră că Statele Unite garantează un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune unor organizații autocertificate din Statele Unite în temeiul Scutului de confidențialitate [Uniunea Europeană]-SUA.

[…]

(140) În cele din urmă, pe baza informațiilor disponibile cu privire la ordinea juridică americană, inclusiv declarațiile și angajamentele din partea guvernului american, Comisia consideră că orice ingerință a autorităților publice americane în drepturile fundamentale ale persoanelor ale căror date sunt transferate din Uniunea Europeană către Statele Unite ale Americii în temeiul Scutului de confidențialitate pentru securitatea națională, aplicarea legii sau alte scopuri de interes public și, prin urmare, restricțiile rezultate impuse organizațiilor autocertificate în ceea ce privește aderarea la principiile privind protecția vieții private vor fi limitate la ceea ce este strict necesar pentru atingerea obiectivului legitim în cauză și că există o protecție juridică efectivă împotriva unei astfel de ingerințe.”

46 Potrivit articolului 1 din Decizia Scutul de confidențialitate:

„(1) În sensul articolului 25 alineatul (2) din Directiva [95/46], Statele Unite garantează un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune către organizații din Statele Unite în temeiul Scutului de confidențialitate [Uniunea Europeană]-SUA.

(2) Scutul de confidențialitate [Uniunea Europeană]-SUA este constituit din principiile publicate de Departamentul Comerțului al SUA la 7 iulie 2016, prezentate în anexa II, precum și din declarațiile și angajamentele oficiale cuprinse în documentele enumerate în anexele I și III-VII.

(3) În sensul alineatului (1), datele cu caracter personal sunt transferate în temeiul Scutului de confidențialitate [Uniunea Europeană]-SUA în cazul în care acestea sunt transferate dinspre Uniune către organizații din Statele Unite ale Americii care fac parte din «lista Scutului de confidențialitate», menținută și pusă la dispoziția publicului de către Departamentul Comerțului al SUA, în conformitate cu secțiunile I și III din principiile prevăzute în anexa II.”

47 Anexa II la Decizia Scutul de confidențialitate, intitulată „Principiile cadrului privind scutul de confidențialitate [Uniunea Europeană]-SUA publicate de Departamentul Comerțului al SUA”, prevede la punctul I.5 că aderarea la principii poate fi limitată, printre altele, de „cerințele privind securitatea națională, interesul public și respectarea legislației”.

48 Anexa III la această decizie conține o scrisoare a domnului John Kerry, pe atunci Secretary of State (Secretar de Stat, Statele Unite), către Comisarul pentru Justiție, Consumatori și Egalitate de gen din 7 iulie 2016, la care este anexat, în anexa A, un memorandum intitulat „Un mecanism al Ombudsmanului pentru Scutul de confidențialitate [Uniunea Europeană]-SUA”, care conține următorul pasaj:

„În ceea ce privește activitățile de colectare de informații pe baza semnalelor electromagnetice în semn de recunoaștere a importanței cadrului privind Scutul de confidențialitate [Uniunea Europeană]-SUA, prezentul memorandum prezintă procesul de punere în aplicare a unui nou mecanism, compatibil cu Directiva nr. 28 privind politica prezidențială (PPD-28), în ceea ce privește activitățile de colectare de informații pe baza semnalelor electromagnetice.

[…] Președintele Obama a anunțat emiterea unei noi directive prezidențiale – PPD-28 – pentru a «stabili în mod clar ce facem și ce nu facem, atunci când este vorba despre activitățile noastre de supraveghere peste hotare».

Secțiunea 4 litera (d) din PPD-28 obligă secretarul de stat să desemneze «un coordonator principal pentru diplomația internațională privind tehnologia informației» (coordonator principal), «care să servească drept punct de contact pentru administrațiile străine care doresc să își exprime îngrijorarea cu privire la activitățile Statelor Unite de colectare de informații pe baza semnalelor electromagnetice».

[…]

1. [Coordonatorul principal] va servi drept Ombudsman pentru Scutul de confidențialitate și […] va colabora îndeaproape cu funcționari din alte departamente și agenții care sunt responsabili cu prelucrarea cererilor în conformitate cu legislația și politicile aplicabile în Statele Unite. Ombudsmanul este independent de serviciile de informații. Ombudsmanul se află în subordinea directă a Secretarului de Stat, care se va asigura că Ombudsmanul își îndeplinește rolul în mod obiectiv și în condiții de independență față de orice influențe neadecvate care riscă să afecteze răspunsul care urmează să fie oferit.

[…]”

49 Anexa VI la Decizia Scutul de confidențialitate conține o scrisoare a Biroului Directorului Serviciului Național de Informații (Office of the Director of National Intelligence) adresată Departamentului Comerțului al SUA, precum și Administrației Comerțului Internațional din 21 iunie 2016, în care se precizează că PPD-28 permite să se efectueze o „colectare «în masă» […] a unui volum relativ important de informații secrete obținute prin interceptarea de semnale sau a unui volum de date în condiții în care serviciile de informații nu pot utiliza un identificator asociat unei ținte specifice […] pentru a orienta colectarea”.

Litigiul principal și întrebările preliminare

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

51 Orice persoană cu reședința pe teritoriul Uniunii și care dorește să utilizeze Facebook este obligată să încheie la momentul înscrierii sale un contract cu Facebook Ireland, filială a Facebook Inc., ea însăși stabilită 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 care aparțin Facebook Inc., situate pe teritoriul Statelor Unite, unde fac obiectul unei prelucrări.

52 La 25 iunie 2013, domnul Schrems a sesizat comisarul cu o plângere prin care îi solicita acestuia în esență să interzică societății Facebook Ireland să transfere datele sale cu caracter personal către Statele Unite, susținând că dreptul și practicile în vigoare în această țară nu garantau o protecție suficientă a datelor cu caracter personal stocate pe teritoriul său împotriva activităților de supraveghere desfășurate în acest stat de autoritățile publice. Plângerea menționată a fost respinsă în special pentru motivul că în Decizia 2000/520 Comisia constatase că Statele Unite asigurau un nivel de protecție adecvat.

53 High Court (Înalta Curte, Irlanda), în fața căreia domnul Schrems introdusese o acțiune împotriva respingerii plângerii sale, a sesizat Curtea cu o cerere de decizie preliminară privind interpretarea și validitatea Deciziei 2000/520. Prin Hotărârea din 6 octombrie 2015, Schrems (C-362/14, EU:C:2015:650), Curtea a declarat această decizie ca fiind nevalidă.

54 În urma hotărârii menționate, instanța de trimitere a anulat respingerea plângerii domnului Schrems și a trimis-o comisarului spre examinare. În cadrul investigației deschise de acesta din urmă, Facebook Ireland a explicat că o mare parte dintre datele cu caracter personal era transferată Facebook Inc. în temeiul clauzelor standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard. Având în vedere aceste elemente, comisarul l-a invitat pe domnul Schrems să își reformuleze plângerea.

55 În plângerea astfel reformulată, depusă la 1 decembrie 2015, domnul Schrems a arătat în special că dreptul american impune societății Facebook Inc. să pună datele cu caracter personal care îi sunt transferate la dispoziția autorităților americane, precum National Security Agency (NSA) și Federal Bureau of Investigation (FBI). El a susținut că, întrucât aceste date sunt utilizate în cadrul diferitor programe de supraveghere într-un mod incompatibil cu articolele 7, 8 și 47 din cartă, Decizia Clauzele standard nu poate justifica transferul datelor menționate către Statele Unite. În aceste condiții, domnul Schrems a solicitat comisarului să interzică sau să suspende transferul datelor sale cu caracter personal către Facebook Inc.

56 La 24 mai 2016, comisarul a publicat un „proiect de decizie” care rezuma concluziile provizorii ale investigației sale. În acest proiect, el a considerat în mod provizoriu că datele cu caracter personal ale cetățenilor Uniunii transferate către Statele Unite riscă să fie consultate și prelucrate de autoritățile americane într-un mod incompatibil cu articolele 7 și 8 din cartă și că dreptul Statelor Unite nu oferă acestor cetățeni căi de atac compatibile cu articolul 47 din cartă. Comisarul a apreciat că clauzele standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard nu sunt de natură să remedieze această deficiență, în măsura în care ele conferă persoanelor vizate numai drepturi contractuale față de exportatorul și de importatorul datelor, fără însă a crea obligații pentru autoritățile americane.

57 Întrucât a considerat că, în aceste condiții, plângerea reformulată a domnului Schrems ridica problema validității Deciziei Clauzele standard, la 31 mai 2016, comisarul a sesizat High Court (Înalta Curte), întemeindu-se pe jurisprudența rezultată din Hotărârea din 6 octombrie 2015, Schrems (C-362/14, EU:C:2015:650, punctul 65), pentru ca aceasta din urmă să sesizeze Curtea cu privire la problema menționată. Prin decizia din 4 mai 2018, High Court (Înalta Curte) a sesizat Curtea cu prezenta trimitere preliminară.

58 High Court (Înalta Curte) a anexat la această trimitere preliminară o hotărâre pronunțată la 3 octombrie 2017, în care consemnase rezultatul examinării probelor prezentate în fața sa în cadrul procedurii naționale, procedură la care participase guvernul american.

59 În această hotărâre, la care se referă în mai multe rânduri cererea de decizie preliminară, instanța de trimitere a subliniat că în principiu ea are nu numai dreptul, ci și obligația de a examina toate faptele și argumentele invocate în fața sa pentru a decide, pe baza acestora, dacă este sau nu necesară o trimitere preliminară. În orice caz, ea ar fi obligată să ia în considerare eventualele modificări ale dreptului care intervin între introducerea căii de atac și ședința organizată în fața sa. Instanța menționată a precizat că, în cadrul procedurii principale, propria apreciere nu se limitează la motivele de nevaliditate invocate de comisar, astfel încât ea poate invoca și din oficiu alte motive de nevaliditate și, pe baza acestora, poate efectua o trimitere preliminară.

60 Potrivit constatărilor care figurează în hotărârea menționată, activitățile de informare ale autorităților americane în ceea ce privește datele cu caracter personal transferate către Statele Unite se întemeiază în special pe articolul 702 din FISA și pe O. E. 12333.

61 În ceea ce privește articolul 702 din FISA, instanța de trimitere precizează, în aceeași hotărâre, că acest articol permite Procurorului General și Directorului Serviciului Național de Informații să autorizeze de comun acord, după aprobarea FISC, pentru a dobândi „informații operative străine”, supravegherea resortisanților care nu sunt cetățeni americani care se află în afara teritoriului Statelor Unite și constituie, printre altele, temeiul pentru programele de supraveghere PRISM și UPSTREAM. În cadrul programului PRISM, furnizorii de servicii de internet sunt obligați, potrivit constatărilor acestei instanțe, să furnizeze NSA toate comunicările trimise și primite de un „selector”, o parte dintre acestea fiind de asemenea transmisă către FBI și Central Intelligence Agency (CIA) (Agenția Centrală de Informații).

62 În ceea ce privește programul UPSTREAM, instanța menționată a constatat că, în cadrul acestui program, întreprinderile de telecomunicații care exploatează „coloana vertebrală” a internetului – și anume rețeaua de cabluri, comutatoare și rutere – sunt obligate să permită NSA să copieze și să filtreze fluxurile de trafic de internet pentru a colecta comunicațiile trimise ori primite de sau cu privire la resortisantul care nu este cetățean american vizat de un „selector”. În cadrul programului respectiv, potrivit constatărilor aceleiași instanțe, NSA are acces atât la metadate, cât și la conținutul comunicațiilor în cauză.

63 În ceea ce privește O. E. 12333, instanța de trimitere constată că acesta permite NSA să aibă acces la date „aflate în tranzit” către Statele Unite, prin accesarea cablurilor submarine situate pe fundul Atlanticului, precum și să colecteze și să stocheze aceste date înainte ca ele să ajungă în Statele Unite și să fie supuse dispozițiilor FISA. Ea precizează că activitățile întemeiate pe O. E. 12333 nu sunt reglementate de lege.

64 În ceea ce privește limitele aduse activităților de informare, instanța de trimitere pune accentul pe faptul că persoanele care nu sunt cetățeni americani intră numai sub incidența PPD-28 și că aceasta se limitează la a menționa că activitățile de informare ar trebui să fie „cât mai adaptate posibil” (*as tailored as feasible*). Pe baza constatărilor sale, instanța respectivă consideră că Statele Unite efectuează o prelucrare de date în masă, fără a asigura o protecție în esență echivalentă cu cea garantată de articolele 7 și 8 din cartă.

65 În ceea ce privește protecția jurisdicțională, aceeași instanță arată că cetățenii Uniunii nu au acces la aceleași căi de atac precum cele de care dispun resortisanții americani împotriva prelucrărilor de date cu caracter personal de către autoritățile americane, din moment ce al patrulea amendament al Constitution of the United States (Constituția Statelor Unite), care constituie, în dreptul american, protecția cea mai importantă împotriva supravegherii nelegale, nu se aplică cetățenilor Uniunii. În această privință, instanța de trimitere precizează că căile de atac care rămân la dispoziția acestora din

urmă întâmpină obstacole semnificative, în special în ceea ce privește obligația – în opinia sa, excesiv de dificil de îndeplinit – de a justifica calitatea lor procesuală activă. Pe de altă parte, potrivit constatărilor instanței menționate, activitățile NSA întemeiate pe O. E. 12333 nu fac obiectul unei supravegheri judiciare și nu sunt supuse unor căi de atac jurisdicționale. În sfârșit, instanța menționată apreciază că, în măsura în care, în opinia sa, Ombudsmanul pentru Scutul de confidențialitate nu constituie o instanță judecătorească, în sensul articolului 47 din cartă, dreptul american nu asigură cetățenilor Uniunii un nivel de protecție în esență echivalent cu cel garantat de dreptul fundamental consacrat la acest articol.

66 În cererea sa de decizie preliminară, instanța de trimitere mai precizează că părțile din procedura principală au opinii divergente în special cu privire la problema aplicabilității dreptului Uniunii în cazul unor transferuri, către o țară terță, de date cu caracter personal care sunt susceptibile de a fi prelucrate de autoritățile acestei țări în special în scopuri de securitate națională, precum și cu privire la elementele care trebuie luate în considerare în vederea aprecierii nivelului de protecție adecvat asigurat de țara menționată. În special, instanța respectivă arată că, potrivit Facebook Ireland, constatările Comisiei privind caracterul adecvat al nivelului de protecție asigurat de o țară terță, precum cele care figurează în Decizia Scutul de confidențialitate, sunt obligatorii pentru autoritățile de supraveghere și în contextul unui transfer de date cu caracter personal întemeiat pe clauzele standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard.

67 În ceea ce privește aceste clauze standard de protecție a datelor, instanța menționată ridică problema dacă Decizia Clauzele standard poate fi considerată validă, chiar dacă, potrivit aceleiași instanțe, clauzele respective sunt lipsite de caracter obligatoriu în privința autorităților statale din țara terță în cauză și, prin urmare, nu sunt de natură să remedieze o eventuală lipsă a unui nivel de protecție adecvat în țara menționată. În această privință, ea consideră că posibilitatea recunoscută autorităților competente ale statelor membre prin articolul 4 alineatul (1) litera (a) din Decizia 2010/87, în versiunea sa anterioară intrării în vigoare a Deciziei de punere în aplicare 2016/2297, de a interzice transferurile de date cu caracter personal către o țară terță care impune importatorului obligații incompatibile cu garanțiile cuprinse în aceleași clauze demonstrează că stadiul dreptului țării terțe poate justifica interzicerea unui transfer de date, chiar efectuat în temeiul clauzelor standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard, și, prin urmare, evidențiază că ele pot fi insuficiente pentru a asigura o protecție adecvată. Acestea fiind spuse, instanța de trimitere ridică problema întinderii competenței comisarului de a interzice un transfer de date întemeiat pe clauzele menționate, apreciind în același timp că o putere discreționară nu poate fi suficientă pentru a asigura o protecție adecvată.

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

„1) În cazul în care datele cu caracter personal sunt transferate de o societate privată dintr-un stat membru al [Uniunii] către o societate privată dintr-o țară terță în scop comercial, în conformitate cu Decizia [Clauzele standard], și pot fi prelucrate ulterior în țara terță de către autoritățile acesteia în scopuri de securitate națională, dar și în scopul aplicării legii și al desfășurării afacerilor externe ale țării terțe, dreptul Uniunii, inclusiv carta, se aplică în cazul transferului de date sub rezerva dispozițiilor articolului 4 alineatul (2) TUE privind securitatea națională și a dispozițiilor articolului 3 alineatul (2) prima liniuță din Directiva [95/46] în ceea ce privește siguranța publică, apărarea și securitatea statului?

2) a) Pentru a se stabili dacă există o încălcare a drepturilor unei persoane fizice prin transferul de date din [Uniune] către o țară terță în temeiul Deciziei [Clauzele standard], unde pot fi prelucrate ulterior în scopuri de securitate națională, elementul de comparație relevant în sensul Directivei [95/46] este:
   i) carta, Tratatul UE, Tratatul FUE, Directiva [95/46], [Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, semnată la Roma la 4 noiembrie 1950 (denumită în continuare «CEDO»)] (sau orice alte prevederi ale dreptului [Uniunii]) sau
   ii) dreptul intern al unuia sau al mai multor state membre?
   b) Dacă elementul de comparație relevant este ii), printre elementele de comparație trebuie incluse și practicile din unul sau mai multe state membre în contextul securității naționale?

3) Pentru a se aprecia dacă o țară terță asigură nivelul de protecție impus de dreptul Uniunii pentru datele cu caracter personal transferate către respectiva țară în sensul articolului 26 din Directiva [95/46], nivelul de protecție în țara terță trebuie să fie evaluat în raport cu:
   a) normele aplicabile în țara terță, rezultate din dreptul său intern sau din acordurile internaționale și practica menită să asigure conformitatea cu aceste norme, inclusiv normele profesionale și măsurile de securitate respectate în țara terță

   sau
   b) normele menționate la punctul (a), împreună cu practicile administrative, de reglementare și de conformitate și cu garanțiile, procedurile, protocoalele, mecanismele de supraveghere și căile de atac extrajudiciare așa cum sunt în vigoare în țara terță?

4) Având în vedere faptele constatate de High Court [(Înalta Curte)] în legătură cu dreptul Statelor Unite, se încalcă drepturile persoanelor fizice prevăzute la articolul 7 sau 8 din cartă în cazul în care se transferă date cu caracter personal din [Uniune] către Statele Unite în temeiul Deciziei [Clauzele standard]?

5) Având în vedere faptele constatate de High Court [(Înalta Curte)] în legătură cu dreptul Statelor Unite, dacă datele cu caracter personal sunt transferate din [Uniune] către Statele Unite în temeiul Deciziei [Clauzele standard]:
   a) Nivelul de protecție acordat de Statele Unite respectă esența dreptului unei persoane fizice de a introduce o acțiune în justiție în cazul încălcării drepturilor sale în materie de confidențialitate a datelor garantat prin articolul 47 din cartă?

   În cazul unui răspuns afirmativ la a cincea întrebare punctul a):
   b) Limitările impuse de dreptul Statelor Unite cu privire la dreptul unei persoane fizice de a introduce o acțiune în justiție în contextul securității naționale a Statelor Unite sunt proporționale în sensul articolului 52 din cartă și nu depășesc ceea ce este necesar într-o societate democratică în scopuri de securitate națională?

6) a) Care este nivelul de protecție care se impune să fie acordat datelor cu caracter personal transferate către o țară terță în temeiul clauzelor contractuale standard adoptate în conformitate cu o decizie a Comisiei întemeiată pe articolul 26 alineatul (4) [din Directiva 95/46] în lumina prevederilor Directivei [95/46] și, în special, în temeiul articolelor 25 și 26 interpretate din perspectiva cartei?
   b) Care sunt aspectele care trebuie luate în considerare pentru a se aprecia dacă nivelul de protecție acordat datelor transferate către o țară terță în temeiul Deciziei [Clauzele standard] satisface cerințele Directivei [95/46] și ale cartei?

7) Faptul că respectivele clauze standard de protecție se aplică între exportatorul de date și importatorul de date și nu obligă autoritățile naționale ale unei țări terțe care pot solicita importatorului de date să pună la dispoziția serviciilor sale de securitate, pentru prelucrare

ulterioară, datele cu caracter personal transferate în temeiul clauzelor prevăzute de Decizia [Clauzele standard] exclude ca aceste clauze să ofere garanții suficiente, astfel cum sunt prevăzute la articolul 26 alineatul (2) din Directiva [95/46]?

8) Dacă un importator de date dintr-o țară terță face obiectul unor norme de supraveghere care, din punctul de vedere al autorității de protecție a datelor, sunt contrare prevederilor clauzelor standard de protecție sau celor ale articolului 25 și ale articolului 26 din Directiva [95/46] sau cartei, autoritatea de protecție a datelor are obligația de a utiliza competențele sale executorii în temeiul articolului 28 alineatul (3) din Directiva [95/46] pentru a suspenda transferul de date sau exercitarea unor astfel de competențe este limitată doar la cazuri excepționale, în lumina considerentului (11) al Deciziei [Clauzele standard], ori autoritatea de protecție a datelor poate face uz de marja sa de apreciere pentru a nu suspenda transferul de date?

9) a) În sensul articolului 25 alineatul (6) din Directiva [95/46], Decizia [Scutul de confidențialitate] constituie o constatare de aplicare generală pentru autoritățile de protecție a datelor și pentru instanțele statelor membre, având ca efect că Statele Unite asigură un nivel adecvat de protecție potrivit articolului 25 alineatul (2) din Directiva [95/46] în temeiul dreptului lor intern sau al acordurilor internaționale din care fac parte?
   b) În cazul unui răspuns negativ, care este relevanța, dacă există una, a Deciziei [Scutul de confidențialitate] pentru aprecierea efectuată cu privire la caracterul adecvat al garanțiilor furnizate pentru datele transferate către Statele Unite în temeiul Deciziei [Clauzele standard]?

10) Date fiind constatările High Court [(Înalta Curte)] cu privire la dreptul Statelor Unite, existența Ombudsmanului pentru Scutul de confidențialitate în temeiul anexei III A la Decizia [Scutul de confidențialitate] coroborată cu regimul existent în Statele Unite garantează că Statele Unite asigură o cale de atac persoanelor vizate ale căror date cu caracter personal sunt transferate către Statele Unite în temeiul Deciziei [Clauzele standard], care este compatibilă cu articolul 47 din cartă?

11) Decizia [Clauzele standard] încalcă articolul 7, 8 sau 47 din cartă?”

Cu privire la admisibilitatea cererii de decizie preliminară

69 Facebook Ireland, precum și guvernul german și guvernul Regatului Unit susțin că cererea de decizie preliminară este inadmisibilă.

70 În ceea ce privește excepția invocată de Facebook Ireland, această societate arată că dispozițiile Directivei 95/46 pe care se întemeiază întrebările preliminare au fost abrogate prin RGPD.

71 În această privință, deși este adevărat că Directiva 95/46 a fost, în temeiul articolului 94 alineatul (1) din RGPD, abrogată cu efect de la 25 mai 2018, această directivă era încă în vigoare la momentul formulării, la 4 mai 2018, a prezentei cereri de decizie preliminară primite de Curte la 9 mai 2018. În plus, articolul 3 alineatul (2) prima liniuță, articolele 25 și 26, precum și articolul 28 alineatul (3) din Directiva 95/46, la care se referă întrebările preliminare, au fost în esență preluate la articolul 2 alineatul (2), precum și, respectiv, la articolele 45, 46 și 58 din RGPD. Pe de altă parte, trebuie amintit că misiunea Curții este aceea de a interpreta toate dispozițiile de drept al Uniunii care sunt necesare instanțelor naționale pentru a statua în cauzele cu care sunt sesizate, chiar dacă dispozițiile respective nu sunt expres indicate în întrebările care îi sunt adresate de aceste instanțe (Hotărârea din 2 aprilie 2020, Ruska Federacija, C-897/19 PPU, EU:C:2020:262, punctul 43 și jurisprudența citată). Pentru aceste diferite motive, împrejurarea că instanța de trimitere a formulat întrebările preliminare raportându-se numai la dispozițiile Directivei 95/46 nu poate determina inadmisibilitatea prezentei cereri de decizie preliminară.

72 La rândul său, guvernul german își întemeiază excepția de inadmisibilitate pe împrejurarea, pe de o parte, că comisarul a exprimat doar îndoieli, iar nu o opinie definitivă, cu privire la problema validității Deciziei Clauzele standard și, pe de altă parte, că instanța de trimitere s-a abținut să verifice dacă domnul Schrems își dăduse în mod indubitabil consimțământul pentru transferurile de date în discuție în litigiul principal, ceea ce, dacă aceasta ar fi fost situația, ar avea ca efect să facă inutil un răspuns la această întrebare. În sfârșit, potrivit guvernului Regatului Unit, întrebările preliminare au un caracter ipotetic, din moment ce această instanță nu a constatat că datele menționate fuseseră efectiv transferate în temeiul deciziei respective.

73 Din jurisprudența constantă a Curții rezultă că numai instanțele naționale care sunt sesizate cu soluționarea litigiului și care trebuie să își asume răspunderea pentru hotărârea judecătorească ce urmează a fi pronunțată au competența să aprecieze, luând în considerare particularitățile cauzei, atât necesitatea unei decizii preliminare, pentru a fi în măsură să pronunțe propria hotărâre, cât și pertinența întrebărilor pe care le adresează Curții. În consecință, în cazul în care întrebările adresate privesc interpretarea sau validitatea unei norme a dreptului Uniunii, Curtea este, în principiu, obligată să se pronunțe. Rezultă că întrebările adresate de instanțele naționale beneficiază de o prezumție de pertinență. Curtea poate refuza să se pronunțe asupra unei întrebări preliminare adresate de o instanță națională numai dacă rezultă că interpretarea solicitată nu are nicio legătură cu realitatea sau cu obiectul litigiului principal, dacă problema este de natură ipotetică ori Curtea nu dispune de elementele de fapt și de drept necesare pentru a răspunde în mod util întrebărilor respective (Hotărârea din 16 iunie 2015, Gauweiler și alții, C-62/14, EU:C:2015:400, punctele 24 și 25, Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctul 45, precum și Hotărârea din 19 decembrie 2019, Dobersberger, C-16/18, EU:C:2019:1110, punctele 18 și 19).

74 În speță, cererea de decizie preliminară conține elemente de fapt și de drept suficiente pentru a se înțelege sensul întrebărilor preliminare. În plus și mai ales, niciun element din dosarul de care dispune Curtea nu permite să se considere că interpretarea solicitată a dreptului Uniunii nu ar avea legătură cu realitatea sau cu obiectul litigiului principal sau ar fi de natură ipotetică, în special în considerarea faptului că transferul datelor cu caracter personal în discuție în litigiul principal ar fi întemeiat pe consimțământul expres al persoanei vizate cu privire la acest transfer, iar nu pe Decizia Clauzele standard. Astfel, potrivit indicațiilor care figurează în cererea menționată, Facebook Ireland a recunoscut că transferă societății Facebook Inc. datele cu caracter personal ale abonaților săi care au reședința în Uniune și că o mare parte din aceste transferuri, a căror legalitate este contestată de domnul Schrems, este efectuată în temeiul clauzelor standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard.

75 Pe de altă parte, faptul că comisarul nu a exprimat o opinie definitivă cu privire la validitatea acestei decizii nu are nicio incidență asupra admisibilității prezentei cereri de decizie preliminară, din moment ce instanța de trimitere consideră că răspunsul la întrebările preliminare privind interpretarea și validitatea normelor dreptului Uniunii este necesar pentru soluționarea litigiului principal.

76 Rezultă că cererea de decizie preliminară este admisibilă.

Cu privire la întrebările preliminare

77 Cu titlu introductiv, trebuie amintit că prezenta cerere de decizie preliminară își are originea într-o plângere a domnului Schrems prin care solicită comisarului dispunerea suspendării sau interzicerea, pentru viitor, a transferului efectuat de Facebook Ireland a datelor sale cu caracter personal către Facebook Inc. Or, deși întrebările preliminare se referă la dispozițiile Directivei 95/46, nu se contestă că comisarul nu adoptase încă o decizie finală cu privire la această plângere atunci când directiva menționată a fost abrogată și înlocuită de RGPD, cu efect de la 25 mai 2018.

78 Această lipsă a unei decizii naționale deosebește situația în discuție în litigiul principal de cele care au condus la pronunțarea Hotărârii din 24 septembrie 2019, Google (Domeniu de aplicare teritorial al înlăturării unor linkuri) (C-507/17, EU:C:2019:772), și a Hotărârii din 1 octombrie 2019, Planet49 (C-673/17, EU:C:2019:801), în care erau în discuție decizii adoptate anterior abrogării directivei menționate.

79 Prin urmare, trebuie să se răspundă la întrebările preliminare în raport cu dispozițiile RGPD, iar nu cu cele ale Directivei 95/46.

Cu privire la prima întrebare

80 Prin intermediul primei întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolul 2 alineatul (1) și articolul 2 alineatul (2) literele (a), (b) și (d) din RGPD coroborate cu articolul 4 alineatul (2) TUE trebuie interpretate în sensul că un transfer de date cu caracter personal efectuat de un operator economic stabilit într-un stat membru către un alt operator economic stabilit într-o țară terță intră în domeniul de aplicare al acestui regulament, în cazul în care, în cursul sau în urma transferului menționat, datele respective sunt susceptibile de a fi prelucrate de autoritățile acestei țări terțe în scopuri de siguranță publică, apărare și securitate a statului.

81 În această privință, trebuie arătat de la bun început că dispoziția conținută de articolul 4 alineatul (2) TUE, potrivit căreia, în cadrul Uniunii, securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru, privește numai statele membre ale Uniunii. În consecință, dispoziția menționată nu este relevantă în speță pentru interpretarea articolului 2 alineatul (1) și a articolului 2 alineatul (2) literele (a), (b) și (d) din RGPD.

82 Potrivit articolului 2 alineatul (1), RGPD se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor. Articolul 4 punctul 2 din acest regulament definește noțiunea de „prelucrare” ca fiind „orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal, cu sau fără utilizarea de mijloace automatizate”, și citează, cu titlu de exemplu, „divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod”, fără a distinge după cum aceste operațiuni sunt realizate în interiorul Uniunii sau au legătură cu o țară terță. În plus, regulamentul menționat supune transferurile de date cu caracter personal către țări terțe unor norme speciale care figurează în capitolul V din acesta, intitulat „Transferurile de date cu caracter personal către țări terțe sau organizații internaționale”, și, de altfel, conferă autorităților de supraveghere competențe specifice în acest scop, care figurează la articolul 58 alineatul (2) litera (j) din același regulament.

83 Rezultă că operațiunea care constă în transferul datelor cu caracter personal dintr-un stat membru către o țară terță constituie, în sine, o prelucrare a datelor cu caracter personal în sensul articolului 4 punctul 2 din RGPD efectuată pe teritoriul unui stat membru, prelucrare căreia i se aplică acest regulament, în temeiul articolului 2 alineatul (1) din acesta [a se vedea prin analogie, în ceea ce privește articolul 2 litera (b) și articolul 3 alineatul (1) din Directiva 95/46, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 45 și jurisprudența citată].

84 În ceea ce privește aspectul dacă o astfel de operațiune poate fi considerată ca fiind exclusă din domeniul de aplicare al RGPD în temeiul articolului 2 alineatul (2) din acesta, trebuie amintit că dispoziția menționată prevede excepții de la domeniul de aplicare al regulamentului respectiv, astfel cum este definit la articolul 2 alineatul (1), și că aceste excepții trebuie să facă obiectul unei interpretări stricte [a se vedea prin analogie, în ceea ce privește articolul 3 alineatul (2) din Directiva 95/46, Hotărârea din 10 iulie 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, punctul 37 și jurisprudența citată].

85 În speță, întrucât transferul de date cu caracter personal în discuție în litigiul principal este efectuat de Facebook Ireland către Facebook Inc., mai precis între două persoane juridice, acest transfer nu intră sub incidența articolului 2 alineatul (2) litera (c) din RGPD, care vizează prelucrarea datelor de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice. Transferul respectiv nu intră nici sub incidența excepțiilor care figurează la articolul 2 alineatul (2) literele (a), (b) și (d) din acest regulament, din moment ce activitățile menționate cu titlu de exemplu de dispoziția respectivă sunt, în toate cazurile, activități proprii statelor sau autorităților statale, fără legătură cu domeniile de activitate ale particularilor [a se vedea prin analogie, în ceea ce privește articolul 3 alineatul (2) din Directiva 95/46, Hotărârea din 10 iulie 2018, Jehovan Todistajat, C-25/17, EU:C:2018:551, punctul 38 și jurisprudența citată].

86 Or, posibilitatea ca datele cu caracter personal transferate între doi operatori economici în scopuri comerciale să fie supuse, în cursul sau în urma transferului, unei prelucrări în scopuri de siguranță publică, apărare și securitate a statului de către autoritățile din țara terță în cauză nu poate exclude transferul menționat din domeniul de aplicare al RGPD.

87 De altfel, prin obligarea în mod explicit a Comisiei, atunci când evaluează caracterul adecvat al nivelului de protecție oferit de o țară terță, să țină seama în special de „legislația relevantă, atât generală, cât și sectorială, inclusiv privind securitatea publică, apărarea, securitatea națională și dreptul penal, precum și accesul autorităților publice la datele cu caracter personal, precum și [de] punerea în aplicare a acestei legislații”, însuși modul de redactare a articolului 45 alineatul (2) litera (a) din acest regulament pune în evidență faptul că eventuala prelucrare de către o țară terță a datelor în cauză în scopuri de siguranță publică, de apărare și de securitate a statului nu pune în discuție aplicabilitatea regulamentului menționat în cazul transferului în cauză.

88 Rezultă că un astfel de transfer nu poate fi exclus din domeniul de aplicare al RGPD pentru motivul că datele în cauză sunt susceptibile de a fi prelucrate, în cursul sau în urma acestui transfer, de către autoritățile țării terțe în cauză, în scopuri de siguranță publică, de apărare și de securitate a statului.

89 Prin urmare, este necesar să se răspundă la prima întrebare că articolul 2 alineatele (1) și (2) din RGPD trebuie interpretat în sensul că un transfer de date cu caracter personal efectuat în scopuri comerciale de un operator economic stabilit într-un stat membru către un alt operator economic stabilit într-o țară terță intră domeniul de aplicare al acestui regulament, în pofida faptului că, în cursul sau în urma transferului menționat, datele respective sunt susceptibile de a fi prelucrate de autoritățile țării terțe în cauză în scopuri de siguranță publică, de apărare și de securitate a statului.

Cu privire la a doua, a treia și a șasea întrebare

90 Prin intermediul celei de a doua, al celei de a treia și al celei de a șasea întrebări, instanța de trimitere solicită în esență Curții să se pronunțe cu privire la nivelul de protecție prevăzut la articolul 46 alineatul (1) și la articolul 46 alineatul (2) litera (c) din RGPD în cadrul unui transfer de date cu caracter personal către o țară terță întemeiat pe clauze standard de protecție a datelor. În special, această instanță solicită Curții să precizeze elementele care trebuie luate în considerare pentru a se stabili dacă nivelul de protecție menționat este asigurat în contextul unui astfel de transfer.

91 În ceea ce privește nivelul de protecție impus, din coroborarea acestor dispoziții rezultă că, în absența unei decizii privind caracterul adecvat al nivelului de protecție adoptate în temeiul articolului 45 alineatul (3) din regulamentul menționat, operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o țară terță numai dacă a oferit „garanții adecvate” și cu condiția să existe „drepturi opozabile și căi de atac eficiente” pentru persoanele vizate, respectivele garanții adecvate putând fi furnizate în special prin clauze standard de protecție a datelor adoptate de Comisie.

92 Deși articolul 46 din RGPD nu precizează natura cerințelor care decurg din această referire la „garanțiile adecvate”, la „drepturile opozabile” și la „căile de atac eficiente”, este necesar să se sublinieze că articolul menționat figurează în capitolul V din acest regulament și că, prin urmare, articolul menționat trebuie interpretat în lumina articolului 44 din regulamentul respectiv, intitulat „Principiul general al transferurilor”, care prevede că „[t]oate dispozițiile din [acest capitol] se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice garantat prin [același] regulament nu este subminat”. În consecință, acest nivel de protecție trebuie să fie garantat indiferent de dispoziția din capitolul menționat în temeiul căreia se efectuează un transfer de date cu caracter personal către o țară terță.

93 Astfel, după cum a arătat avocatul general la punctul 117 din concluziile sale, dispozițiile capitolului V din RGPD urmăresc să asigure continuitatea nivelului ridicat al acestei protecții în cazul transferului de date cu caracter personal către o țară terță, în conformitate cu obiectivul precizat în considerentul (6) al acestui regulament.

94 Articolul 45 alineatul (1) prima teză din RGPD prevede că transferul de date cu caracter personal către o țară terță poate fi autorizat printr-o decizie adoptată de Comisie, potrivit căreia această țară terță, un teritoriu ori unul sau mai multe sectoare specificate din ea asigură un nivel de protecție adecvat. În această privință, fără a impune ca țara terță în cauză să asigure un nivel de protecție identic cu cel garantat în ordinea juridică a Uniunii, expresia „nivel de protecție adecvat” trebuie înțeleasă, astfel cum confirmă considerentul (104) al regulamentului menționat, 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 regulamentului respectiv, interpretat în lumina cartei. Astfel, în lipsa unei asemenea cerințe, obiectivul menționat la punctul anterior nu ar fi respectat [a se vedea prin analogie, în ceea ce privește articolul 25 alineatul (6) din Directiva 95/46, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 73].

95 În acest context, considerentul (107) al RGPD enunță că, atunci când „o țară terță, un teritoriu sau un sector specificat dintr-o țară terță […] nu mai asigură un nivel adecvat de protecție a datelor […], transferul de date cu caracter personal către țara terță […] ar trebui să fie interzis, cu excepția cazului în care sunt îndeplinite cerințele prevăzute în [acest regulament] privind transferurile în baza unor garanții adecvate […]”. În acest scop, considerentul (108) al regulamentului menționat precizează că, în absența unei decizii privind caracterul adecvat al nivelului de protecție, garanțiile adecvate pe care operatorul sau persoana împuternicită de operator trebuie să le ofere în conformitate cu articolul 46 alineatul (1) din același regulament trebuie să „compens[eze] lipsa protecției datelor într-o țară terță” pentru a „asigur[a] respectarea cerințelor în materie de protecție a datelor și drepturi ale persoanelor vizate corespunzătoare prelucrării în interiorul Uniunii”.

96 De aici rezultă, astfel cum a arătat domnul avocat general la punctul 115 din concluziile sale, că aceste garanții adecvate trebuie să fie de natură să asigure că persoanele ale căror date cu caracter personal sunt transferate către o țară terță în temeiul unor clauze standard de protecție a datelor beneficiază, la fel ca în cadrul unui transfer întemeiat pe o decizie privind caracterul adecvat al nivelului de protecție, de un nivel de protecție în esență echivalent cu cel garantat în cadrul Uniunii.

97 Instanța de trimitere ridică de asemenea problema dacă acest nivel de protecție în esență echivalent cu cel garantat în cadrul Uniunii trebuie stabilit în raport cu dreptul Uniunii, în special cu drepturile garantate de cartă, și/sau în raport cu drepturile fundamentale consacrate de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale (denumită în continuare „CEDO”) ori în raport cu dreptul național al statelor membre.

98 În această privință, trebuie amintit că, deși, astfel cum confirmă articolul 6 alineatul (3) TUE, drepturile fundamentale consacrate de CEDO constituie principii generale ale dreptului Uniunii și deși articolul 52 alineatul (3) din cartă prevede că drepturile conținute în aceasta, corespunzătoare

drepturilor garantate de CEDO, au același înțeles și aceeași întindere cu cele pe care le conferă convenția amintită, aceasta din urmă nu constituie, atât timp cât Uniunea nu a aderat la ea, un instrument juridic integrat formal în ordinea juridică a Uniunii (Hotărârea din 26 februarie 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, punctul 44 și jurisprudența citată, precum și Hotărârea din 20 martie 2018, Menci, C-524/15, EU:C:2018:197, punctul 22).

99 În aceste condiții, Curtea a statuat că interpretarea dreptului Uniunii, precum și examinarea validității actelor Uniunii trebuie să se realizeze din perspectiva drepturilor fundamentale garantate de cartă (a se vedea prin analogie Hotărârea din 20 martie 2018, Menci, C-524/15, EU:C:2018:197, punctul 24).

100 Pe de altă parte, potrivit unei jurisprudențe constante, validitatea dispozițiilor dreptului Uniunii și, în lipsa unei trimiteri exprese la dreptul național al statelor membre, interpretarea acestora nu pot fi apreciate din perspectiva acestui drept național, chiar și de rang constituțional, în special, a drepturilor fundamentale, astfel cum au fost formulate în constituția lor națională (a se vedea în acest sens Hotărârea din 17 decembrie 1970, Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, punctul 3, Hotărârea din 13 decembrie 1979, Hauer, 44/79, EU:C:1979:290, punctul 14, precum și Hotărârea din 18 octombrie 2016, Nikiforidis, C-135/15, EU:C:2016:774, punctul 28 și jurisprudența citată).

101 Rezultă că, în condițiile în care, pe de o parte, un transfer de date cu caracter personal precum cel în discuție în litigiul principal, efectuat în scopuri comerciale de un operator economic stabilit într-un stat membru către un alt operator economic stabilit într-o țară terță, intră, astfel cum reiese din răspunsul la prima întrebare, în domeniul de aplicare al RGPD, iar pe de altă parte, acest regulament urmărește în special, astfel cum reiese din considerentul (10) al acestuia, să asigure un nivel consecvent și ridicat de protecție a persoanelor fizice în cadrul Uniunii și, în acest scop, să asigure aplicarea consecventă și omogenă a normelor în materie de protecție a drepturilor și libertăților fundamentale ale acestor persoane în ceea ce privește prelucrarea datelor cu caracter personal în întreaga Uniune, nivelul de protecție a drepturilor fundamentale prevăzut la articolul 46 alineatul (1) din regulamentul menționat trebuie să fie stabilit în temeiul dispozițiilor aceluiași regulament, interpretate în lumina drepturilor fundamentale garantate de cartă.

102 Instanța de trimitere urmărește de asemenea să afle ce elemente trebuie luate în considerare pentru a stabili caracterul adecvat al nivelului de protecție în contextul unui transfer de date cu caracter personal către o țară terță în temeiul unor clauze standard de protecție a datelor adoptate potrivit articolului 46 alineatul (2) litera (c) din RGPD.

103 În această privință, deși dispoziția menționată nu enumeră diferitele elemente de care trebuie să se țină seama pentru a aprecia caracterul adecvat al nivelului de protecție care trebuie respectat în cadrul unui astfel de transfer, articolul 46 alineatul (1) din acest regulament precizează că persoanele vizate trebuie să beneficieze de garanții adecvate și să dispună de drepturi opozabile și de căi de atac eficiente.

104 În acest scop, evaluarea impusă în contextul unui astfel de transfer trebuie în special să ia în considerare atât stipulațiile contractuale convenite între operator sau persoana împuternicită de operator stabiliți în Uniune și destinatarul transferului stabilit în țara terță în cauză, cât și, în ceea ce privește un eventual acces al autorităților publice ale țării terțe menționate la datele cu caracter personal transferate, elementele relevante ale sistemului său juridic. În această ultimă privință, elementele care trebuie luate în considerare în contextul articolului 46 din regulamentul menționat corespund celor prevăzute, în mod neexhaustiv, la articolul 45 alineatul (2) din acesta.

105 Prin urmare, este necesar să se răspundă la a doua, la a treia și la a șasea întrebare că articolul 46 alineatul (1) și articolul 46 alineatul (2) litera (c) din RGPD trebuie interpretate în sensul că garanțiile adecvate, drepturile opozabile și căile de atac eficiente prevăzute de aceste dispoziții trebuie să asigure că drepturile persoanelor ale căror date cu caracter personal sunt transferate către o țară terță în temeiul unor clauze standard de protecție a datelor beneficiază de un nivel de protecție în esență

echivalent cu cel garantat în cadrul Uniunii de regulamentul menționat, interpretat în lumina cartei. În acest scop, evaluarea nivelului de protecție asigurat în contextul unui astfel de transfer trebuie în special să ia în considerare atât stipulațiile contractuale convenite între operator sau persoana împuternicită de operator stabiliți în Uniune și destinatarul transferului stabilit în țara terță în cauză, cât și, în ceea ce privește un eventual acces al autorităților publice ale acestei țări terțe la datele cu caracter personal astfel transferate, elementele relevante ale sistemului juridic al acesteia, în special cele prevăzute la articolul 45 alineatul (2) din regulamentul menționat.

Cu privire la a opta întrebare

106 Prin intermediul celei de a opta întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolul 58 alineatul (2) literele (f) și (j) din RGPD trebuie interpretat în sensul că autoritatea de supraveghere competentă este obligată să suspende sau să interzică un transfer de date cu caracter personal către o țară terță întemeiat pe clauze standard de protecție a datelor adoptate de Comisie, atunci când această autoritate de supraveghere consideră că aceste clauze nu sunt sau nu pot fi respectate în țara terță respectivă și că protecția datelor transferate impusă de dreptul Uniunii, în special de articolele 45 și 46 din RGPD, precum și de cartă nu poate fi asigurată, sau în sensul că exercitarea acestor competențe se limitează la ipoteze excepționale.

107 Conform articolului 8 alineatul (3) din cartă, precum și conform articolului 51 alineatul (1) și articolului 57 alineatul (1) litera (a) din RGPD, autoritățile naționale de supraveghere sunt responsabile să supravegheze respectarea normelor Uniunii referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal. Prin urmare, fiecare dintre acestea este 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 regulamentul menționat (a se vedea prin analogie, în ceea ce privește articolul 28 din Directiva 95/46, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 47).

108 Din aceste dispoziții rezultă că autoritățile de supraveghere au ca primă sarcină să monitorizeze și să asigure aplicarea RGPD. Îndeplinirea acestei sarcini are o importanță deosebită în contextul unui transfer de date cu caracter personal către o țară terță, din moment ce, astfel cum reiese din însuși modul de redactare a considerentului (116) al acestui regulament, „[f]luxul transfrontalier de date cu caracter personal în afara Uniunii poate expune unui risc sporit capacitatea persoanelor fizice de a-și exercita drepturile în materie de protecție a datelor, în special pentru a-și asigura protecția împotriva utilizării sau a divulgării ilegale a acestor informații”. În această ipoteză, astfel cum se precizează în cuprinsul aceluiași considerent, „autoritățile de supraveghere pot constata că se află în imposibilitatea de a trata plângeri sau de a efectua investigații referitoare la activitățile desfășurate în afara frontierelor lor”.

109 În plus, în temeiul articolului 57 alineatul (1) litera (f) din RGPD, fiecare autoritate de supraveghere este obligată, pe teritoriul său, să trateze plângerile pe care orice persoană, conform articolului 77 alineatul (1) din acest regulament, are dreptul de a le depune în cazul în care consideră că o prelucrare a datelor cu caracter personal care o vizează încalcă regulamentul menționat și să investigheze într-o măsură adecvată obiectul acestora. Autoritatea de supraveghere trebuie să trateze o astfel de plângere cu toată diligența necesară [a se vedea prin analogie, în ceea ce privește articolul 25 alineatul (6) din Directiva 95/46, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 63].

110 Articolul 78 alineatele (1) și (2) din RGPD recunoaște fiecărei persoane dreptul de a exercita o cale de atac judiciară eficientă în special atunci când autoritatea de supraveghere omite să trateze plângerea sa. Considerentul (141) al regulamentului menționat face de asemenea referire la acest „drept la o cale de

atac eficientă în conformitate cu articolul 47 din cartă” în cazul în care această autoritate de supraveghere „nu acționează atunci când o astfel de acțiune este necesară pentru asigurarea protecției drepturilor persoanei vizate”.

111 În vederea soluționării plângerilor depuse, articolul 58 alineatul (1) din RGPD învestește fiecare autoritate de control cu competențe importante de investigare. Atunci când o astfel de autoritate consideră, la finalul investigației sale, că persoana vizată ale cărei date cu caracter personal au fost transferate către o țară terță nu beneficiază în aceasta de un nivel de protecție adecvat, ea este obligată, în temeiul dreptului Uniunii, să reacționeze în mod corespunzător pentru a remedia insuficiența constatată, indiferent de originea sau de natura insuficienței menționate. În acest scop, articolul 58 alineatul (2) din regulamentul respectiv enumeră diferitele competențe corective pe care le are autoritatea de supraveghere.

112 Deși alegerea mijlocului adecvat și necesar aparține autorității de supraveghere, iar aceasta trebuie să facă alegerea menționată luând în considerare toate împrejurările transferului de date cu caracter personal în cauză, autoritatea respectivă este totuși obligată să își îndeplinească cu toată diligența necesară sarcina care constă în a asigura respectarea deplină a RGPD.

113 În această privință și astfel cum a arătat și domnul avocat general la punctul 148 din concluziile sale, autoritatea menționată este obligată, în temeiul articolului 58 alineatul (2) literele (f) și (j) din acest regulament, să suspende sau să interzică un transfer de date cu caracter personal către o țară terță atunci când consideră, în lumina tuturor împrejurărilor proprii acestui transfer, că clauzele standard de protecție a datelor nu sunt sau nu pot fi respectate în țara terță menționată și că protecția datelor transferate impusă de dreptul Uniunii nu poate fi asigurată prin alte mijloace, în cazul în care operatorul însuși sau persoana împuternicită de el stabiliți în Uniune nu a suspendat ori nu a încetat transferul.

114 Interpretarea care figurează la punctul anterior nu este infirmată de argumentația comisarului potrivit căreia articolul 4 din Decizia 2010/87, în versiunea sa anterioară intrării în vigoare a Deciziei de punere în aplicare 2016/2297, interpretat în lumina considerentului (11) al acestei decizii, limita la anumite ipoteze excepționale competența autorităților de supraveghere de a suspenda sau de a interzice un transfer de date cu caracter personal către o țară terță. Astfel, în versiunea rezultată din Decizia de punere în aplicare 2016/2297, articolul 4 din Decizia Clauzele standard evocă competența de care dispun aceste autorități, în prezent în temeiul articolului 58 alineatul (2) literele (f) și (j) din RGPD, de a suspenda sau de a interzice un asemenea transfer, fără a limita în niciun mod exercitarea acestei competențe la împrejurări excepționale.

115 În orice caz, competența de executare recunoscută Comisiei de articolul 46 alineatul (2) litera (c) din RGPD în scopul adoptării unor clauze standard de protecție a datelor nu îi conferă competența de a restrânge competențele de care dispun autoritățile de supraveghere în temeiul articolului 58 alineatul (2) din acest regulament [a se vedea prin analogie, în ceea ce privește articolul 25 alineatul (6) și articolul 28 din Directiva 95/46, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctele 102 și 103]. De altfel, considerentul (5) al Deciziei de punere în aplicare 2016/2297 confirmă că Decizia Clauzele standard „nu împiedică o [autoritate de supraveghere] să își exercite competența de supraveghere a fluxurilor de date, inclusiv competența de a suspenda sau de a interzice un transfer de date cu caracter personal, în cazul în care constată că transferul în cauză are loc cu încălcarea legislației UE sau a legislației naționale în materie de protecție a datelor”.

116 Cu toate acestea, trebuie precizat că atribuțiile autorității de supraveghere competente sunt supuse respectării depline a deciziei prin care Comisia constată, dacă este cazul, în temeiul articolului 45 alineatul (1) prima teză din RGPD, că o țară terță specificată asigură un nivel de protecție adecvat. Astfel, într-o asemenea ipoteză, din articolul 45 alineatul (1) a doua teză din acest regulament coroborat cu considerentul (103) reiese că transferurile de date cu caracter personal către țara terță în cauză pot avea loc fără a fi necesar să se obțină autorizări speciale.

117 În temeiul articolului 288 al patrulea paragraf TFUE, o decizie privind caracterul adecvat al nivelului de protecție a Comisiei are, în toate elementele sale, un caracter obligatoriu pentru toate statele membre destinatare și este obligatorie, așadar, pentru toate organele lor, în măsura în care constată că țara terță în cauză garantează un nivel de protecție adecvat și are drept efect autorizarea transferurilor de date menționate [a se vedea prin analogie, în ceea ce privește articolul 25 alineatul (6) din Directiva 95/46, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 51 și jurisprudența citată].

118 În acest sens, atât timp cât decizia privind caracterul adecvat al nivelului de protecție 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 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 (Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 52 și jurisprudența citată) și, în consecință, să se suspende sau să se interzică transferuri de date cu caracter personal către țara terță menționată.

119 Cu toate acestea, o decizie privind caracterul adecvat al nivelului de protecție a Comisiei adoptată în temeiul articolului 45 alineatul (3) din RGPD nu poate împiedica persoanele ale căror date cu caracter personal au fost sau ar putea fi transferate către o țară terță să sesizeze, în temeiul articolului 77 alineatul (1) din RGPD, autoritatea națională de supraveghere competentă cu o plângere privind protecția drepturilor și libertăților lor în ceea ce privește prelucrarea acestor date. De asemenea, o decizie de această natură nu poate nici anula, nici reduce competențele expres recunoscute autorităților naționale de supraveghere la articolul 8 alineatul (3) din cartă, precum și la articolul 51 alineatul (1) și la articolul 57 alineatul (1) litera (a) din regulamentul menționat [a se vedea prin analogie, în ceea ce privește articolul 25 alineatul (6) și articolul 28 din Directiva 95/46, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 53].

120 Astfel, chiar în prezența unei decizii privind caracterul adecvat al nivelului de protecție a Comisiei, autoritatea națională de supraveghere competentă, sesizată de o persoană cu o plângere privind protecția drepturilor și libertăților sale în ceea ce privește o prelucrare a datelor cu caracter personal care o privesc, trebuie să poată examina în condiții de independență deplină dacă transferul acestor date respectă cerințele stabilite de RGPD și, dacă este cazul, să introducă o cale de atac în fața instanțelor naționale, astfel încât acestea din urmă să efectueze, dacă împărtășesc îndoielile acestei autorități în ceea ce privește validitatea deciziei privind caracterul adecvat al nivelului de protecție, o trimitere preliminară în vederea examinării acestei validități [a se vedea prin analogie, în ceea ce privește articolul 25 alineatul (6) și articolul 28 din Directiva 95/46, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctele 57 și 65].

121 Având în vedere considerațiile care precedă, este necesar să se răspundă la a opta întrebare că articolul 58 alineatul (2) literele (f) și (j) din RGPD trebuie interpretat în sensul că, cu excepția cazului în care există o decizie privind caracterul adecvat al nivelului de protecție adoptată în mod valabil de Comisie, autoritatea de supraveghere competentă este obligată să suspende sau să interzică un transfer de date către o țară terță întemeiat pe clauze standard de protecție a datelor adoptate de Comisie, atunci când această autoritate de supraveghere consideră, în lumina tuturor împrejurărilor proprii transferului menționat, că aceste clauze nu sunt sau nu pot fi respectate în țara terță respectivă și că protecția datelor transferate impusă de dreptul Uniunii, în special de articolele 45 și 46 din RGPD și de cartă, nu poate fi asigurată prin alte mijloace, în cazul în care operatorul însuși sau persoana împuternicită de operator stabiliți în Uniune nu a suspendat ori nu a încetat transferul.

Cu privire la a șaptea și a unsprezecea întrebare

122 Prin intermediul celei de a șaptea și al celei de a unsprezecea întrebări, care trebuie analizate împreună, instanța de trimitere solicită în esență Curții să se pronunțe cu privire la validitatea Deciziei Clauzele standard în raport cu articolele 7, 8 și 47 din cartă.

123 În special, astfel cum reiese din însăși formularea celei de a șaptea întrebări și din explicațiile aferente acesteia care figurează în cererea de decizie preliminară, instanța de trimitere ridică problema dacă Decizia Clauzele standard este în măsură să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate către țări terțe, în măsura în care clauzele standard de protecție a datelor pe care le prevede nu sunt obligatorii pentru autoritățile acestor țări terțe.

124 Articolul 1 din Decizia Clauzele standard prevede că se consideră că clauzele standard de protecție a datelor care figurează în anexa la aceasta oferă garanții corespunzătoare în ceea ce privește protecția vieții private, precum și a drepturilor și libertăților fundamentale ale persoanelor, în conformitate cu cerințele articolului 26 alineatul (2) din Directiva 95/46. Această din urmă dispoziție a fost preluată în esență la articolul 46 alineatul (1) și la articolul 46 alineatul (2) litera (c) din RGPD.

125 Cu toate acestea, deși clauzele menționate sunt obligatorii pentru operatorul stabilit în Uniune și pentru destinatarul transferului de date cu caracter personal stabilit într-o țară terță, în cazul în care au încheiat un contract raportându-se la aceste clauze, nu se contestă că respectivele clauze nu pot fi obligatorii pentru autoritățile țării terțe menționate, întrucât acestea din urmă nu sunt părți la contract.

126 Prin urmare, deși există situații în care, în funcție de stadiul dreptului și de practicile în vigoare în țara terță în cauză, destinatarul unui astfel de transfer este în măsură să garanteze protecția necesară a datelor numai pe baza clauzelor standard de protecție a datelor, există și alte situații în care stipulațiile cuprinse în aceste clauze ar putea să nu constituie un mijloc suficient care să permită asigurarea, în practică, a protecției efective a datelor cu caracter personal transferate în țara terță în cauză. Acest lucru este valabil în special atunci când legislația țării terțe menționate permite autorităților sale publice ingerințe în drepturile persoanelor vizate referitoare la datele respective.

127 Astfel, se ridică problema dacă o decizie a Comisiei privind clauze standard de protecție a datelor, adoptată în temeiul articolului 46 alineatul (2) litera (c) din RGPD, este nevalidă, în lipsa, în această decizie, a unor garanții opozabile autorităților publice ale țărilor terțe spre care sunt sau ar putea fi transferate date cu caracter personal în temeiul clauzelor menționate.

128 Articolul 46 alineatul (1) din RGPD prevede că, în absența unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o țară terță numai dacă a oferit garanții adecvate și cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate. Potrivit articolului 46 alineatul (2) litera (c) din acest regulament, garanțiile menționate pot fi furnizate prin clauze standard de protecție a datelor adoptate de Comisie. Or, aceste dispoziții nu prevăd că toate garanțiile respective trebuie să fie în mod necesar stabilite de o decizie a Comisiei, precum Decizia Clauzele standard.

129 În această privință, trebuie să se arate că o asemenea decizie se deosebește de o decizie privind caracterul adecvat al nivelului de protecție adoptată în temeiul articolului 45 alineatul (3) din RGPD, care vizează, în urma unei examinări a reglementării țării terțe în cauză care ține seama în special de legislația relevantă în materie de securitate națională și de acces al autorităților publice la datele cu caracter personal, să se constate cu efect obligatoriu că o țară terță, un teritoriu sau unul sau mai multe sectoare specificate din aceasta asigură un nivel de protecție adecvat și că, prin urmare, accesul autorităților publice ale țării terțe menționate la astfel de date nu împiedică transferurile lor către aceeași țară terță. O asemenea decizie privind caracterul adecvat al nivelului de protecție poate fi deci

adoptată de Comisie numai cu condiția ca aceasta să fi constatat că legislația țării terțe relevantă în domeniu cuprinde efectiv toate garanțiile necesare care permit să se considere că asigură un nivel de protecție adecvat.

130 În schimb, în ceea ce privește o decizie a Comisiei prin care se adoptă clauze standard de protecție a datelor, precum Decizia Clauzele standard, în măsura în care o astfel de decizie nu privește o țară terță, un teritoriu sau unul sau mai multe sectoare specificate din aceasta, din articolul 46 alineatul (1) și articolul 46 alineatul (2) litera (c) din RGPD nu se poate deduce că Comisia ar fi obligată să efectueze, înainte de adoptarea unei asemenea decizii, o evaluare a caracterului adecvat al nivelului de protecție asigurat de țările terțe către care ar putea fi transferate date cu caracter personal în temeiul unor astfel de clauze.

131 În această privință, trebuie amintit că, potrivit articolului 46 alineatul (1) din regulamentul menționat, în absența unei decizii privind caracterul adecvat al nivelului de protecție a Comisiei, revine operatorului sau persoanei împuternicite de operator stabiliți în Uniune sarcina de a oferi în special garanții adecvate. Considerentele (108) și (114) ale regulamentului respectiv confirmă că, în cazul în care Comisia nu s-a pronunțat cu privire la caracterul adecvat al nivelului de protecție a datelor într-o țară terță, operatorul sau, după caz, persoana împuternicită de operator „ar trebui să adopte măsuri pentru a compensa lipsa protecției datelor într-o țară terță prin intermediul unor garanții adecvate pentru persoana vizată” și că „[r]espectivele garanții ar trebui să asigure respectarea cerințelor în materie de protecție a datelor și drepturi ale persoanelor vizate corespunzătoare prelucrării în interiorul Uniunii, inclusiv disponibilitatea unor drepturi opozabile ale persoanelor vizate și a unor căi de atac eficiente […] în Uniune sau într-o țară terță”.

132 Din moment ce, astfel cum reiese din cuprinsul punctului 125 din prezenta hotărâre, este inerent caracterului contractual al clauzelor standard de protecție a datelor că acestea nu pot fi obligatorii pentru autoritățile publice ale țărilor terțe, însă articolul 44, articolul 46 alineatul (1) și articolul 46 alineatul (2) litera (c) din RGPD, interpretate în lumina articolelor 7, 8 și 47 din cartă, impun ca nivelul de protecție a persoanelor fizice garantat prin regulamentul menționat să nu fie subminat, se poate dovedi necesară completarea garanțiilor pe care le conțin respectivele clauze standard de protecție a datelor. În această privință, considerentul (109) al regulamentului menționat prevede că „[p]osibilitatea ca operatorul […] să utilizeze clauze standard în materie de protecție a datelor, adoptate de Comisie […] nu ar trebui să împiedice operatorii […] să adauge alte clauze sau garanții suplimentare” și precizează în special că aceștia „ar trebui să fie încurajați să ofere garanții suplimentare […] care să completeze clauzele standard în materie de protecție [a datelor]”.

133 Rezultă astfel că clauzele standard de protecție a datelor adoptate de Comisie în temeiul articolului 46 alineatul (2) litera (c) din regulamentul menționat urmăresc numai să furnizeze operatorilor sau persoanelor împuternicite de ei stabiliți în Uniune garanții contractuale care să se aplice în mod uniform în toate țările terțe și, prin urmare, independent de nivelul de protecție garantat în fiecare dintre ele. În măsura în care aceste clauze standard de protecție a datelor, având în vedere natura lor, nu pot să furnizeze garanții care să depășească o obligație contractuală de a se asigura că nivelul de protecție impus de dreptul Uniunii este respectat, ele pot necesita, în funcție de situația existentă într-o țară terță sau alta, adoptarea unor măsuri suplimentare de către operator pentru a asigura respectarea acestui nivel de protecție.

134 În această privință, astfel cum a arătat domnul avocat general la punctul 126 din concluziile sale, mecanismul contractual prevăzut la articolul 46 alineatul (2) litera (c) din RGPD se întemeiază pe responsabilizarea operatorului sau a persoanei împuternicite de operator stabiliți în Uniune, precum și, în subsidiar, a autorității de supraveghere competente. Prin urmare, revine în primul rând acestui operator sau persoanei împuternicite de operator sarcina de a verifica, de la caz la caz și, dacă este necesar, în colaborare cu destinatarul transferului, dacă dreptul țării terțe de destinație asigură o

protecție adecvată, din perspectiva dreptului Uniunii, a datelor cu caracter personal transferate în temeiul unor clauze standard de protecție a datelor, la nevoie prin furnizarea unor garanții suplimentare față de cele oferite de clauzele menționate.

135 În cazul în care operatorul sau persoana împuternicită de operator stabiliți în Uniune nu pot lua măsuri suplimentare suficiente pentru a garanta o astfel de protecție, aceștia sau, în subsidiar, autoritatea de supraveghere competentă sunt obligați să suspende sau să înceteze transferul de date cu caracter personal către țara terță în cauză. Această situație se regăsește în special atunci când dreptul țării terțe menționate impune destinatarului unui transfer de date cu caracter personal din Uniune obligații care sunt contrare clauzelor respective și, prin urmare, de natură a repune în discuție garanția contractuală a unui nivel de protecție adecvat împotriva accesului autorităților publice ale țării terțe menționate la datele respective.

136 Prin urmare, simplul fapt că clauzele standard de protecție a datelor care figurează într-o decizie a Comisiei adoptată în temeiul articolului 46 alineatul (2) litera (c) din RGPD, precum cele care figurează în anexa la Decizia Clauzele standard, nu sunt obligatorii pentru autoritățile țărilor terțe către care sunt susceptibile de a fi transferate date cu caracter personal nu poate afecta validitatea acestei decizii.

137 Validitatea menționată depinde, în schimb, de aspectul dacă, în conformitate cu cerința care rezultă din articolul 46 alineatul (1) și din articolul 46 alineatul (2) litera (c) din RGPD, interpretate în lumina articolelor 7, 8 și 47 din cartă, o asemenea decizie cuprinde mecanisme eficiente care permit, în practică, să se asigure respectarea nivelului de protecție impus de dreptul Uniunii și suspendarea sau interzicerea transferurilor de date cu caracter personal, întemeiate pe astfel de clauze, în cazul încălcării acestor clauze sau al imposibilității de a le onora.

138 În ceea ce privește garanțiile cuprinse în clauzele standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard, din clauza 4 literele (a) și (b), din clauza 5 litera (a), din clauza 9, precum și din clauza 11 alineatul (1) din aceasta reiese că operatorul stabilit în Uniune, destinatarul transferului de date cu caracter personal, precum și eventualul subcontractant al acestuia din urmă se angajează reciproc că prelucrarea datelor menționate, inclusiv transferul lor, a fost și va continua să fie efectuată în conformitate cu „leg[ea] aplicabil[ă] privind protecția datelor”, și anume, potrivit definiției care figurează la articolul 3 litera (f) din decizia respectivă, „legislația care protejează drepturile și libertățile fundamentale ale particularilor și, în special, dreptul lor la viață privată cu privire la prelucrarea datelor cu caracter personal, aplicabilă operatorului de date din statul membru în care este stabilit exportatorul de date”. Or, dispozițiile RGPD, interpretate în lumina cartei, fac parte din această legislație.

139 În plus, destinatarul transferului de date cu caracter personal stabilit într-o țară terță se angajează, în temeiul clauzei 5 litera (a), să informeze fără întârziere operatorul stabilit în Uniune cu privire la eventuala sa imposibilitate de a asigura conformitatea cu obligațiile care îi revin în temeiul contractului încheiat. În special, potrivit clauzei 5 litera (b), acest destinatar atestă că nu are niciun motiv să creadă că legislația care i se aplică îl împiedică să îndeplinească obligațiile care îi revin în conformitate cu contractul încheiat și se angajează să notifice operatorului, de îndată ce are cunoștință de aceasta, orice modificare în legislația națională, susceptibilă să aibă efecte negative asupra garanțiilor și obligațiilor oferite de clauzele standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard. Pe de altă parte, deși clauza 5 litera (d) punctul (i) permite destinatarului transferului de date cu caracter personal să nu notifice operatorului stabilit în Uniune o solicitare, obligatorie din punct de vedere juridic, de a divulga date cu caracter personal, prezentată de o autoritate de aplicare a legii, în cazul unei legislații care îi interzice acest lucru, precum interdicția, în cadrul dreptului penal, de a păstra confidențialitatea unei investigații urmărind aplicarea legii, acesta este totuși obligat, în conformitate cu clauza 5 litera (a) din anexa la Decizia Clauzele standard, să informeze operatorul cu privire la imposibilitatea sa de a asigura conformitatea cu clauzele standard de protecție a datelor.

140 În ambele ipoteze pe care le are în vedere, clauza 5 literele (a) și (b) conferă operatorului stabilit în Uniune dreptul de a suspenda transferul de date și/sau de a rezilia contractul. Având în vedere cerințele care rezultă din articolul 46 alineatul (1) și din articolul 46 alineatul (2) litera (c) din RGPD, interpretat în lumina articolelor 7 și 8 din cartă, suspendarea transferului de date și/sau rezilierea contractului au un caracter obligatoriu pentru operator, în cazul în care destinatarul transferului nu este sau nu mai este în măsură să respecte clauzele standard de protecție a datelor. În caz contrar, operatorul ar încălca cerințele care îi sunt impuse în temeiul clauzei 4 litera (a) din anexa la Decizia Clauzele standard, interpretată în lumina dispozițiilor RGPD și ale cartei.

141 Rezultă astfel că clauza 4 litera (a) și clauza 5 literele (a) și (b) din această anexă instituie în sarcina operatorului stabilit în Uniune și a destinatarului transferului de date cu caracter personal obligația de a se asigura că legislația țării terțe de destinație îi permite destinatarului respectiv să asigure conformitatea cu clauzele standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard, înainte de a efectua un transfer de date cu caracter personal către această țară terță. În ceea ce privește verificarea menționată, nota de subsol referitoare la clauza 5 precizează că cerințele imperative ale acestei legislații care nu depășesc ceea ce este necesar într-o societate democratică pentru a proteja, printre altele, siguranța națională, apărarea și securitatea publică nu sunt în contradicție cu aceste clauze standard de protecție a datelor. Dimpotrivă, astfel cum a subliniat domnul avocat general la punctul 131 din concluziile sale, faptul de a se conforma unei obligații impuse de dreptul țării terțe de destinație care depășește ceea ce este necesar în acest scop trebuie considerat o încălcare a clauzelor menționate. Aprecierea efectuată de acești operatori a caracterului necesar al unei astfel de obligații trebuie, dacă este cazul, să țină seama de constatarea caracterului adecvat al nivelului de protecție asigurat de țara terță în cauză care figurează într-o decizie privind caracterul adecvat al nivelului de protecție a Comisiei, adoptată în temeiul articolului 45 alineatul (3) din RGPD.

142 Rezultă că operatorul stabilit în Uniune și destinatarul transferului de date cu caracter personal sunt obligați să verifice, în prealabil, respectarea, în țara terță în cauză, a nivelului de protecție impus de dreptul Uniunii. Dacă este cazul, destinatarul acestui transfer are obligația, în temeiul aceleiași clauze 5 litera (b), să informeze operatorul cu privire la eventuala sa imposibilitate de a asigura conformitatea clauzelor menționate, ultimul având în acest caz sarcina de a suspenda transferul de date și/sau de a rezilia contractul.

143 Dacă destinatarul transferului datelor cu caracter personal către o țară terță comunică operatorului, în temeiul clauzei 5 litera (b) din anexa la Decizia Clauzele standard, că legislația țării terțe în cauză nu îi permite să asigure conformitatea cu clauzele standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard, din clauza 12 din anexa menționată rezultă că datele care au fost deja transferate către această țară terță și copiile trebuie să fie în integralitate returnate sau distruse. În orice caz, clauza 6 din aceeași anexă sancționează încălcarea acestor clauze standard, conferind persoanei vizate dreptul de a primi despăgubiri pentru prejudiciul suferit.

144 Trebuie adăugat că, potrivit clauzei 4 litera (f) din anexa la Decizia Clauzele standard, operatorul stabilit în Uniune se angajează, în cazul în care categorii speciale de date ar putea fi transferate către o țară terță care nu oferă un nivel de protecție adecvat, să informeze persoana vizată înainte de transfer sau cât de curând posibil în urma lui. Această informare poate oferi persoanei menționate posibilitatea de a exercita dreptul la o cale de atac recunoscut de clauza 3 alineatul (1) din această anexă împotriva operatorului, pentru ca el să suspende transferul avut în vedere, să rezilieze contractul încheiat cu destinatarul transferului de date cu caracter personal sau, dacă este cazul, să solicite acestuia din urmă returnarea sau distrugerea datelor transferate.

145 În sfârșit, în temeiul clauzei 4 litera (g) din anexa menționată, operatorul stabilit în Uniune este obligat, în cazul în care destinatarul transferului de date cu caracter personal îi notifică, în temeiul clauzei 5 litera (b) din aceasta, că legislația care i se aplică face obiectul unei modificări susceptibile să aibă efecte negative asupra garanțiilor oferite și asupra obligațiilor impuse prin clauzele standard de

protecție a datelor, să transmită această notificare către autoritatea de supraveghere competentă, în cazul în care decide, în pofida notificării menționate, să continue transferul sau să ridice suspendarea. Transmiterea unei astfel de notificări către această autoritate de supraveghere și dreptul său de a efectua un audit la destinatarul transferului de date cu caracter personal în temeiul clauzei 8 alineatul (2) din aceeași anexă permit autorității de supraveghere respective să verifice dacă este necesar să se procedeze la suspendarea sau la interzicerea transferului avut în vedere în scopul asigurării unui nivel de protecție adecvat.

146 În acest context, articolul 4 din Decizia Clauzele standard, interpretat în lumina considerentului (5) al Deciziei de punere în aplicare 2016/2297, confirmă că Decizia Clauzele standard nu împiedică nicidecum autoritatea de supraveghere competentă să suspende sau să interzică, dacă este cazul, un transfer de date cu caracter personal către o țară terță întemeiat pe clauzele standard de protecție a datelor care figurează în anexa la decizia menționată. În această privință, astfel cum rezultă din răspunsul la a opta întrebare, cu excepția cazului în care există o decizie privind caracterul adecvat al nivelului de protecție adoptată în mod valabil de Comisie, autoritatea de supraveghere competentă este obligată, în temeiul articolului 58 alineatul (2) literele (f) și (j) din RGPD, să suspende sau să interzică un asemenea transfer, atunci când consideră, în lumina tuturor împrejurărilor proprii transferului menționat, că aceste clauze nu sunt sau nu pot fi respectate în țara terță respectivă și că protecția datelor transferate impusă de dreptul Uniunii nu poate fi asigurată prin alte mijloace, în cazul în care operatorul însuși sau persoana împuternicită de operator stabiliți în Uniune nu a suspendat ori nu a încetat transferul.

147 În ceea ce privește împrejurarea, evidențiată de comisar, potrivit căreia transferurile de date cu caracter personal către o astfel de țară terță ar putea eventual să facă obiectul unor decizii divergente ale autorităților de supraveghere în diferite state membre, trebuie adăugat că astfel cum rezultă din articolul 55 alineatul (1) și din articolul 57 alineatul (1) litera (a) din RGPD, sarcina de a asigura respectarea acestui regulament este încredințată, în principiu, fiecărei autorități de supraveghere pe teritoriul statului membru de care aparține. În plus, în scopul de a evita decizii divergente, articolul 64 alineatul (2) din acest regulament prevede posibilitatea unei autorități de supraveghere care ar considera că transferurile de date către o țară terță trebuie, în general, să fie interzise, de a sesiza Comitetul european pentru protecția datelor (EDPB) în vederea obținerii unui aviz, acesta putând, în temeiul articolului 65 alineatul (1) litera (c) din același regulament, să adopte o decizie obligatorie, în special atunci când o autoritate de supraveghere nu ține seama de avizul emis.

148 Rezultă că Decizia Clauzele standard prevede mecanisme eficiente care permit, în practică, să se asigure că transferul de date cu caracter personal către o țară terță în temeiul clauzelor standard de protecție a datelor care figurează în anexa la această decizie este suspendat sau interzis, în cazul în care destinatarul transferului nu respectă clauzele menționate sau se află în imposibilitatea de a le respecta.

149 Având în vedere ansamblul considerațiilor care precedă, trebuie să se răspundă la a șaptea și la a unsprezecea întrebare că analiza Deciziei Clauzele standard în raport cu articolele 7, 8 și 47 din cartă nu a evidențiat niciun element de natură să afecteze validitatea acestei decizii.

Cu privire la a patra, a cincea, a noua și a zecea întrebare

150 Prin intermediul celei de a noua întrebări, instanța de trimitere solicită în esență să se stabilească dacă și în ce măsură o autoritate de supraveghere a unui stat membru este ținută de constatările care figurează în Decizia Scutul de confidențialitate, potrivit cărora Statele Unite asigură un nivel de protecție adecvat. Prin intermediul celei de a patra, al celei de a cincea și al celei de a zecea întrebări, această instanță solicită în esență să se stabilească dacă, având în vedere propriile constatări referitoare la dreptul Statelor Unite, transferul de date cu caracter personal către această țară terță în temeiul clauzelor standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard încalcă

drepturile garantate la articolele 7, 8 și 47 din cartă și solicită Curții, în special, să stabilească dacă instituirea Ombudsmanului menționat în anexa III la Decizia Scutul de confidențialitate este compatibilă cu respectivul articol 47.

151 Cu titlu introductiv, trebuie arătat că, deși acțiunea principală a comisarului pune la îndoială numai validitatea Deciziei Clauzele standard, această acțiune a fost introdusă la instanța de trimitere anterior adoptării Deciziei Scutul de confidențialitate. În măsura în care, prin intermediul celei de a patra și al celei de a cincea întrebări, instanța menționată solicită Curții, în general, să se pronunțe cu privire la protecția care trebuie asigurată, în temeiul articolelor 7, 8 și 47 din cartă, în contextul unui astfel de transfer, analiza Curții trebuie să ia în considerare consecințele care rezultă din adoptarea Deciziei Scutul de confidențialitate, intervenită între timp. Aceasta este situația cu atât mai mult cu cât instanța menționată solicită în mod expres, prin cea de a zecea întrebare, să se stabilească dacă protecția prevăzută la respectivul articol 47 este asigurată prin intermediul Ombudsmanului menționat în această din urmă decizie.

152 În plus, din indicațiile care figurează în cererea de decizie preliminară reiese că, în cadrul procedurii principale, Facebook Ireland a arătat că, pentru comisar, Decizia Scutul de confidențialitate producea efecte obligatorii în ceea ce privește constatarea caracterului adecvat al nivelului de protecție asigurat de Statele Unite și, în consecință, în ceea ce privește caracterul legal al unui transfer de date cu caracter personal către această țară terță întemeiat pe clauzele standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard.

153 Or, astfel cum reiese din cuprinsul punctului 59 din prezenta hotărâre, în hotărârea din 3 octombrie 2017, anexată la cererea de decizie preliminară, instanța de trimitere a subliniat că era obligată să ia în considerare modificările legale intervenite între introducerea acțiunii și ședința organizată în fața sa. Astfel, această instanță pare a fi obligată să ia în considerare, pentru soluționarea litigiului principal, schimbarea unor împrejurări care rezultă din adoptarea Deciziei Scutul de confidențialitate, precum și a eventualelor efecte obligatorii ale acesteia.

154 În special, existența efectelor obligatorii care însoțesc constatarea prin Decizia Scutul de confidențialitate a unui nivel de protecție adecvat în Statele Unite este relevantă în scopul aprecierii atât a obligațiilor, amintite la punctele 141 și 142 din prezenta hotărâre, care revin operatorului și destinatarului unui transfer de date cu caracter personal către o țară terță efectuat în temeiul clauzelor standard de protecție a datelor care figurează în anexa la Decizia Clauzele standard, cât și a obligațiilor care revin, dacă este cazul, autorității de supraveghere de a suspenda sau de a interzice un asemenea transfer.

155 Astfel, în ceea ce privește efectele obligatorii ale Deciziei Scutul de confidențialitate, articolul 1 alineatul (1) din această decizie prevede că, în sensul articolului 45 alineatul (1) din RGPD, „Statele Unite garantează un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune către organizații din Statele Unite în temeiul Scutului de confidențialitate [Uniunea Europeană]-SUA”. Conform articolului 1 alineatul (3) din decizia menționată, datele cu caracter personal sunt considerate ca fiind transferate în temeiul acestui scut în cazul în care acestea sunt transferate dinspre Uniune către organizații din Statele Unite care fac parte din „lista Scutului de confidențialitate”, menținută și pusă la dispoziția publicului de către Departamentul Comerțului al SUA, în conformitate cu secțiunile I și III din principiile enunțate în anexa II la aceeași decizie.

156 Astfel cum rezultă din jurisprudența amintită la punctele 117 și 118 din prezenta hotărâre, Decizia Scutul de confidențialitate are caracter obligatoriu pentru autoritățile de supraveghere, în măsura în care constată că Statele Unite garantează un nivel de protecție adecvat și, prin urmare, are drept efect autorizarea transferurilor de date cu caracter personal efectuate în temeiul Scutului de confidențialitate Uniunea Europeană-Statele Unite. Prin urmare, atât timp cât această decizie nu a fost declarată nevalidă de către Curte, autoritatea de supraveghere competentă nu poate suspenda sau interzice un transfer de date cu caracter personal către o organizație care aderă la acest scut, pentru motivul că ea

consideră, contrar aprecierii reținute de Comisie în decizia menționată, că legislația Statelor Unite care reglementează accesul la datele cu caracter personal transferate în temeiul scutului respectiv și utilizarea acestor date de către autoritățile publice ale acestei țări terțe în scopuri de securitate națională, de aplicare a legii sau de interes public, nu asigură un nivel de protecție adecvat.

157 Nu este mai puțin adevărat că, în conformitate cu jurisprudența amintită la punctele 119 și 120 din prezenta hotărâre, atunci când este sesizată de o persoană cu o plângere, autoritatea de supraveghere competentă trebuie să examineze, în condiții de independență deplină, dacă transferul de date cu caracter personal în cauză respectă cerințele stabilite de RGPD și, în ipoteza în care consideră întemeiate motivele invocate de această persoană pentru a contesta validitatea unei decizii privind caracterul adecvat al nivelului de protecție, să introducă o acțiune în fața instanțelor naționale, astfel încât acestea din urmă să sesizeze Curtea cu o trimitere preliminară în aprecierea validității deciziei menționate.

158 Astfel, o plângere depusă în temeiul articolului 77 alineatul (1) din RGPD, prin care o persoană ale cărei date cu caracter personal au fost sau ar putea fi transferate către o țară terță invocă faptul că dreptul și practicile acestei țări nu asigură, în pofida celor constatate de Comisie într-o decizie adoptată în temeiul articolului 45 alineatul (3) din acest regulament, un nivel de protecție adecvat, trebuie înțeleasă în sensul că privește în esență compatibilitatea acestei decizii cu protecția vieții private, precum și a drepturilor și libertăților fundamentale ale persoanelor [a se vedea prin analogie, în ceea ce privește articolul 25 alineatul (6) și articolul 28 alineatul (4) din Directiva 95/46, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 59].

159 În speță, domnul Schrems a solicitat în esență comisarului să interzică sau să suspende transferul datelor sale cu caracter personal efectuat de Facebook Ireland către Facebook Inc., stabilită în Statele Unite, pentru motivul că această țară terță nu asigura un nivel de protecție adecvat. Întrucât, în urma unei investigații cu privire la susținerile domnului Schrems, comisarul a sesizat instanța de trimitere, aceasta din urmă, având în vedere probele prezentate și dezbaterea contradictorie desfășurată în fața sa, pare să ridice problema temeiniciei îndoielilor domnului Schrems cu privire la caracterul adecvat al nivelului de protecție asigurat în țara terță menționată, în pofida constatărilor efectuate între timp de Comisie în Decizia Scutul de confidențialitate, ceea ce a determinat respectiva instanță să adreseze Curții a patra, a cincea și a zecea întrebare preliminară.

160 Astfel cum a arătat domnul avocat general la punctul 175 din concluziile sale, aceste întrebări preliminare trebuie astfel interpretate în sensul că, în esență, pun în discuție constatarea Comisiei, care figurează în Decizia Scutul de confidențialitate, potrivit căreia Statele Unite asigură un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune către țara terță menționată și, prin urmare, validitatea deciziei respective.

161 Având în vedere constatările efectuate în cuprinsul punctelor 121 și 157-160 din prezenta hotărâre și pentru a oferi un răspuns complet instanței de trimitere, trebuie, așadar, să se analizeze dacă Decizia Scutul de confidențialitate este conformă cu cerințele care decurg din RGPD, interpretat în lumina cartei (a se vedea prin analogie Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 67).

162 Adoptarea de către Comisie a unei decizii privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 alineatul (3) din RGPD 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 [a se vedea prin analogie, în ceea ce privește articolul 25 alineatul (6) din Directiva 95/46, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 96].

Cu privire la conținutul Deciziei Scutul de confidențialitate

163 Comisia a constatat, la articolul 1 alineatul (1) din Decizia Scutul de confidențialitate, că Statele Unite garantează un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune către organizații din Statele Unite în temeiul Scutului de confidențialitate Uniunea Europeană-SUA, acesta fiind constituit, în temeiul articolului 1 alineatul (2) din decizia menționată, în special din principiile publicate de Departamentul Comerțului al SUA la 7 iulie 2016, prezentate în anexa II la decizia menționată, precum și din declarațiile și angajamentele oficiale cuprinse în documentele enumerate în anexele I și III-VII la aceeași decizie.

164 Cu toate acestea, Decizia Scutul de confidențialitate precizează de asemenea, la punctul I.5 din anexa II, intitulată „Principiile cadrului privind Scutul de confidențialitate [Uniunea Europeană]-SUA publicate de Departamentul Comerțului al SUA”, că aderarea la principii poate fi limitată, printre altele, de „cerințele privind securitatea națională, interesul public și respectarea legilor Statelor Unite ale Americii”. Astfel, această decizie consacră, asemenea Deciziei 2000/520, supremația cerințelor menționate asupra principiilor respective, supremație în temeiul căreia organizațiile americane autocertificate care primesc date cu caracter personal din Uniune sunt obligate să înlăture, fără limitare, aceleași principii atunci când acestea din urmă intră în conflict cu cerințele menționate și se dovedesc, așadar, incompatibile cu ele (a se vedea prin analogie, în ceea ce privește Decizia 2000/520, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 86).

165 Având în vedere caracterul său general, derogarea care figurează la punctul I.5 din anexa II la Decizia Scutul de confidențialitate 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 (a se vedea prin analogie, în ceea ce privește Decizia 2000/520, Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 87). Mai precis și astfel cum se constată în Decizia Scutul de confidențialitate, asemenea ingerințe pot rezulta din accesul la datele cu caracter personal transferate din Uniune către Statele Unite și din utilizarea acestor date de către autoritățile publice americane, în cadrul programelor de supraveghere PRISM și UPSTREAM întemeiate pe articolul 702 din FISA, precum și în temeiul O. E. 12333.

166 În acest context, Comisia a evaluat, în considerentele (67)-(135) ale Deciziei Scutul de confidențialitate, limitările și garanțiile disponibile în legislația SUA, în special la articolul 702 din FISA, în O. E. 12333 și în PPD-28, în ceea ce privește accesul și utilizarea datelor cu caracter personal transferate în temeiul Scutului de confidențialitate Uniunea Europeană-Statele Unite de către autoritățile publice americane pentru scopuri de securitate națională, aplicarea legii și alte scopuri de interes public.

167 La finalul acestei evaluări, Comisia a constatat, în cuprinsul considerentului (136) al deciziei menționate, că „Statele Unite garantează un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune unor organizații autocertificate din Statele Unite” și a apreciat, în cuprinsul considerentului (140) al deciziei respective, că, „pe baza informațiilor disponibile cu privire la ordinea juridică americană, […] orice ingerință a autorităților publice americane în drepturile fundamentale ale persoanelor ale căror date sunt transferate din Uniunea Europeană către Statele Unite ale Americii în temeiul Scutului de confidențialitate pentru securitatea națională, aplicarea legii sau alte scopuri de interes public și, prin urmare, restricțiile rezultate impuse organizațiilor autocertificate în ceea ce privește aderarea la principiile privind protecția vieții private vor fi limitate la ceea ce este strict necesar pentru atingerea obiectivului legitim în cauză și că există o protecție juridică efectivă împotriva unei astfel de ingerințe”.

Cu privire la constatarea referitoare la nivelul de protecție adecvat

168 Având în vedere elementele menționate de Comisie în Decizia Scutul de confidențialitate, precum și pe cele stabilite de instanța de trimitere în cadrul procedurii principale, această instanță are îndoieli cu privire la aspectul dacă dreptul Statelor Unite asigură în mod efectiv nivelul de protecție adecvat prevăzut la articolul 45 din RGPD, interpretat în lumina drepturilor fundamentale garantate la articolele 7, 8 și 47 din cartă. În special, instanța menționată consideră că dreptul acestei țări terțe nu prevede limitările și garanțiile necesare în privința ingerințelor autorizate de reglementarea sa națională și nici nu asigură o protecție jurisdicțională efectivă împotriva unor astfel de ingerințe. În această din urmă privință, ea adaugă că instituirea Ombudsmanului pentru Scutul de confidențialitate nu poate, în opinia sa, să remedieze lacunele respective din moment ce acest Ombudsman nu poate fi asimilat unei instanțe judecătorești în sensul articolului 47 din cartă.

169 În ceea ce privește, în primul rând, articolele 7 și 8 din cartă, care participă la nivelul de protecție impus în cadrul Uniunii, a cărui respectare trebuie să fie constatată de Comisie înainte ca aceasta să adopte o decizie privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 alineatul (1) din RGPD, trebuie amintit că articolul 7 din cartă garantează oricărei persoane dreptul la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor sale. În ceea ce privește articolul 8 alineatul (1) din cartă, acesta recunoaște în mod expres oricărei persoane dreptul la protecția datelor cu caracter personal care o privesc.

170 Astfel, accesul la datele cu caracter personal ale unei persoane fizice în vederea stocării sau a utilizării lor afectează dreptul fundamental al acestei persoane la respectarea vieții private, garantat la articolul 7 din cartă, dreptul menționat raportându-se la orice informație privind o persoană fizică identificată sau identificabilă. Prelucrarea datelor respectivă se încadrează și la articolul 8 din cartă ca urmare a faptului că reprezintă o prelucrare de date cu caracter personal în sensul acestui articol și trebuie, în consecință, să îndeplinească în mod necesar cerințele de protecție a datelor prevăzute de respectivul articol [a se vedea în acest sens Hotărârea din 9 noiembrie 2010, Volker und Markus Schecke și Eifert, C-92/09 și C-93/09, EU:C:2010:662, punctele 49 și 52, și Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctul 29, precum și Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctele 122 și 123].

171 Curtea a statuat deja că comunicarea de date cu caracter personal unui terț, precum o autoritate publică, constituie o ingerință în drepturile fundamentale consacrate la articolele 7 și 8 din cartă, indiferent de utilizarea ulterioară a informațiilor comunicate. Aceeași situație se regăsește în privința stocării de date cu caracter personal, precum și a accesului la respectivele date în vederea utilizării lor de către autoritățile publice, independent de aspectul dacă informațiile vizate referitoare la viața privată prezintă sau nu un caracter sensibil sau dacă persoanele interesate au suferit sau nu eventuale inconveniente ca urmare a acestei ingerințe [a se vedea în acest sens Hotărârea din 20 mai 2003, Österreichischer Rundfunk și alții, C-465/00, C-138/01 și C-139/01, EU:C:2003:294, punctele 74 și 75, Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctele 33-36, precum și Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctele 124 și 126].

172 Cu toate acestea, drepturile consacrate la articolele 7 și 8 din cartă nu sunt prerogative absolute, ci trebuie să fie luate în considerare în raport cu funcția lor în societate [a se vedea în acest sens Hotărârea din 9 noiembrie 2010, Volker und Markus Schecke și Eifert, C-92/09 și C-93/09, EU:C:2010:662, punctul 48 și jurisprudența citată, Hotărârea din 17 octombrie 2013, Schwarz, C-291/12, EU:C:2013:670, punctul 33 și jurisprudența citată, precum și Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 136].

173 În această privință, trebuie de asemenea arătat că, potrivit articolului 8 alineatul (2) din cartă, datele cu caracter personal trebuie, în special, să fie prelucrate „în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege”.

174 În plus, conform articolului 52 alineatul (1) prima teză din cartă, orice restrângere a exercițiului drepturilor și libertăților recunoscute prin aceasta trebuie să fie prevăzută de lege și să respecte substanța acestor drepturi și libertăți. Potrivit articolului 52 alineatul (1) a doua teză din cartă, prin respectarea principiului proporționalității, pot fi impuse restrângeri privind aceste drepturi și libertăți numai în cazul în care sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

175 Trebuie adăugat, în această din urmă privință, că cerința potrivit căreia orice restrângere a exercitării drepturilor fundamentale trebuie să fie prevăzută de lege presupune ca temeiul juridic care permite ingerința în aceste drepturi să definească el însuși întinderea restrângerii exercitării dreptului vizat [a se vedea Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 139 și jurisprudența citată].

176 În sfârșit, pentru a îndeplini cerința proporționalității potrivit căreia derogările de la protecția datelor cu caracter personal și restrângerile acesteia trebuie să fie efectuate în limitele strictului necesar, reglementarea în cauză care presupune o ingerință trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime, astfel încât persoanele ale căror date au fost transferate să dispună de garanții suficiente care să permită protejarea în mod eficient a datelor lor cu caracter personal împotriva riscurilor de abuz. Această reglementare trebuie în special să indice în ce împrejurări și în ce condiții poate fi luată o măsură care prevede prelucrarea unor asemenea date, garantând în acest mod că o ingerință este limitată la strictul necesar. Necesitatea de a dispune de astfel de garanții este cu atât mai importantă atunci când datele cu caracter personal sunt supuse unei prelucrări automatizate [a se vedea în acest sens Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctele 140 și 141, precum și jurisprudența citată].

177 În acest scop, articolul 45 alineatul (2) litera (a) din RGPD precizează că, în cadrul evaluării caracterului adecvat al nivelului de protecție asigurat de o țară terță, Comisia ține seama în special de „existența unor drepturi efective și opozabile ale persoanelor vizate” ale căror date cu caracter personal sunt transferate.

178 În speță, constatarea efectuată de Comisie în Decizia Scutul de confidențialitate, potrivit căreia Statele Unite asigură un nivel de protecție în esență echivalent cu cel garantat în cadrul Uniunii de RGPD, interpretat în lumina articolelor 7 și 8 din cartă, a fost repusă în discuție, printre altele, pentru motivul că ingerințele care rezultă din programele de supraveghere întemeiate pe articolul 702 din FISA și pe O. E. 12333 nu ar fi supuse unor cerințe care să asigure, cu respectarea principiului proporționalității, un nivel de protecție în esență echivalent cu cel garantat de articolul 52 alineatul (1) a doua teză din cartă. Este, așadar, necesar să se analizeze dacă aceste programe de supraveghere sunt puse în aplicare cu respectarea unor astfel de cerințe, fără a fi necesar să se verifice în prealabil respectarea de către această țară terță a unor condiții în esență echivalente cu cele prevăzute la articolul 52 alineatul (1) prima teză din cartă.

179 În această privință, în ceea ce privește programele de supraveghere întemeiate pe articolul 702 din FISA, Comisia a constatat, în cuprinsul considerentului (109) al Deciziei Scutul de confidențialitate, că, în conformitate cu articolul respectiv, „FISC nu autorizează măsuri individuale de supraveghere; dimpotrivă, acesta autorizează programe de supraveghere (precum PRISM, UPSTREAM) pe baza unor certificări anuale întocmite de procurorul general și directorul Serviciului național de informații”. Astfel cum reiese din cuprinsul aceluiași considerent, controlul exercitat de FISC urmărește astfel să verifice dacă programele de supraveghere menționate corespund obiectivului de a obține informații operative străine, însă nu se referă la aspectul „dacă persoanele sunt vizate în mod corespunzător pentru a dobândi informații operative străine”.

180 Rezultă astfel că articolul 702 din FISA nu evidențiază în niciun mod existența unor limitări ale abilitării pe care o presupune pentru punerea în aplicare a programelor de supraveghere în scopul informării externe și nici existența unor garanții pentru persoane care nu sunt cetățeni americani potențial vizate de programele menționate. În aceste condiții și astfel cum a arătat domnul avocat general în esență la punctele 291, 292 și 297 din concluziile sale, articolul respectiv nu este susceptibil de a asigura un nivel de protecție în esență echivalent cu cel garantat de cartă, astfel cum a fost interpretată prin jurisprudența amintită la punctele 175 și 176 din prezenta hotărâre, potrivit căreia un temei juridic care permite ingerințe în drepturile fundamentale trebuie, pentru a respecta principiul proporționalității, să definească el însuși întinderea restrângerii exercitării dreptului vizat și să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună cerințe minime.

181 Potrivit constatărilor care figurează în Decizia Scutul de confidențialitate, programele de supraveghere întemeiate pe articolul 702 din FISA trebuie, desigur, să fie puse în aplicare cu respectarea cerințelor care rezultă din PPD-28. Cu toate acestea, deși Comisia a subliniat, în cuprinsul considerentelor (69) și (77) ale Deciziei Scutul de confidențialitate, că cerințele care rezultă din PPD-28 au un caracter obligatoriu pentru serviciile de informații americane, guvernul american a admis, ca răspuns la o întrebare a Curții, că PPD-28 nu conferă persoanelor în cauză drepturi opozabile autorităților americane în fața instanțelor judecătorești. Prin urmare, ea nu este susceptibilă de a asigura un nivel de protecție în esență echivalent cu cel care rezultă din cartă, contrar cerințelor prevăzute la articolul 45 alineatul (2) litera (a) din RGPD, potrivit căruia constatarea acestui nivel depinde în special de existența unor drepturi efective și opozabile ale persoanelor ale căror date au fost transferate către țara terță în cauză.

182 În ceea ce privește programele de supraveghere întemeiate pe O. E. 12333, din dosarul de care dispune Curtea reiese că nici acest decret nu conferă drepturi opozabile autorităților americane în fața instanțelor judecătorești.

183 Trebuie adăugat că PPD-28, care trebuie respectată în cadrul aplicării programelor vizate la cele două puncte precedente, permite să se efectueze o „colectare «în masă» […] a unui volum relativ important de informații secrete obținute prin interceptarea de semnale sau a unui volum de date în condiții în care serviciile de informații nu pot utiliza un identificator asociat unei ținte specifice […] pentru a orienta colectarea”, astfel cum se precizează într-o scrisoare din 21 iunie 2016 a Biroului Directorului Serviciului Național de Informații (Office of the Director of National Intelligence) către Departamentul Comerțului al SUA, precum și către Administrația Comerțului Internațional, care figurează în anexa VI la Decizia Scutul de confidențialitate. Or, această posibilitate, care permite, în cadrul programelor de supraveghere întemeiate pe O. E. 12333, accesul la date aflate în tranzit către Statele Unite fără ca accesul menționat să facă obiectul vreunui control jurisdicțional, nu delimitează, indiferent de situație, în mod suficient de clar și de precis conținutul unei astfel de colectări în masă a datelor cu caracter personal.

184 Prin urmare, rezultă că nici articolul 702 din FISA, nici O. E. 12333 coroborate cu PPD-28 nu corespund cerințelor minime aferente, în dreptul Uniunii, principiului proporționalității, astfel încât nu se poate considera că programele de supraveghere întemeiate pe aceste dispoziții sunt limitate la strictul necesar.

185 În aceste condiții, limitările protecției datelor cu caracter personal care decurg din reglementarea internă a Statelor Unite privind accesul și utilizarea de către autoritățile publice americane a unor astfel de date transferate din Uniune către Statele Unite și pe care Comisia le-a evaluat în Decizia Scutul de confidențialitate nu sunt circumscrise astfel încât să îndeplinească cerințe în esență echivalente cu cele prevăzute, în dreptul Uniunii, la articolul 52 alineatul (1) a doua teză din cartă.

186 În ceea ce privește, în al doilea rând, articolul 47 din cartă, care participă de asemenea la nivelul de protecție impus în cadrul Uniunii și a cărui respectare trebuie să fie constatată de Comisie înainte ca aceasta să adopte o decizie privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 alineatul (1) din RGPD, trebuie amintit că primul paragraf al acestui articol 47 impune ca orice persoană ale cărei drepturi și libertăți garantate de dreptul Uniunii sunt încălcate să aibă dreptul la o cale de atac eficientă în fața unei instanțe judecătorești, în conformitate cu condițiile stabilite de acest articol. Potrivit celui de al doilea paragraf al articolului menționat, orice persoană are dreptul la un proces în fața unei instanțe judecătorești independente și imparțiale.

187 Potrivit unei jurisprudențe constante, existența însăși a unui control jurisdicțional efectiv destinat să asigure respectarea dispozițiilor dreptului Uniunii este inerentă existenței unui stat de drept. Astfel, 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 substanța dreptului fundamental la o protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din cartă (Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 95 și jurisprudența citată).

188 În acest scop, articolul 45 alineatul (2) litera (a) din RGPD impune Comisiei, în cadrul evaluării sale privind caracterul adecvat al nivelului de protecție asigurat de o țară terță, să țină seama în special „[de] reparații[le] efective pe cale administrativă și judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate”. Considerentul (104) al RGPD subliniază în această privință că țara terță „ar trebui să asigure o supraveghere efectivă independentă în materie de protecție a datelor și să prevadă mecanisme de cooperare cu autoritățile statelor membre de protecție a datelor” și precizează că „persoanele vizate ar trebui să beneficieze de drepturi efective și opozabile și de reparații efective pe cale administrativă și judiciară”.

189 Existența unor astfel de posibilități efective de exercitare a unei căi de atac în țara terță în cauză prezintă o importanță deosebită în contextul unui transfer de date cu caracter personal către această țară terță, în măsura în care, astfel cum reiese din considerentul (116) al RGPD, persoanele în cauză se pot confrunta cu insuficiența competențelor și a mijloacelor autorităților administrative și judiciare ale statelor membre de a soluționa în mod util plângerile lor întemeiate pe o prelucrare pretins nelegală, în această țară terță, a datelor lor astfel transferate, ceea ce este de natură să le oblige să se adreseze autorităților și instanțelor naționale ale aceleiași țări terțe.

190 În speță, constatarea efectuată de Comisie în Decizia Scutul de confidențialitate, potrivit căreia Statele Unite asigură un nivel de protecție în esență echivalent cu cel garantat la articolul 47 din cartă, a fost repusă în discuție în special pentru motivul că instituirea Ombudsmanului pentru Scutul de confidențialitate nu poate acoperi lacunele constatate de Comisia însăși în ceea ce privește protecția jurisdicțională a persoanelor ale căror date cu caracter personal sunt transferate către țara terță menționată.

191 În această privință, în considerentul (115) al Deciziei Scutul de confidențialitate, Comisia a arătat că, deși „persoanele fizice, inclusiv persoanele vizate din [Uniune], au o serie de modalități de recurs în cazul în care au făcut obiectul supravegherii (electronice) ilegale în scopuri legate de securitatea națională, este la fel de clar că cel puțin anumite temeiuri juridice care pot fi utilizate de autoritățile americane de informații (de exemplu, O. E. 12333) nu sunt acoperite”. Astfel, în ceea ce privește O. E. 12333, ea a pus accentul, în respectivul considerent (115), pe lipsa oricărei căi de atac. Or, potrivit jurisprudenței amintite la punctul 187 din prezenta hotărâre, o asemenea lacună în protecția jurisdicțională față de ingerințele legate de programele de informații întemeiate pe acest decret prezidențial se opune să se rețină, astfel cum a procedat Comisia în Decizia Scutul de confidențialitate, că dreptul Statelor Unite asigură un nivel de protecție în esență echivalent cu cel garantat la articolul 47 din cartă.

192 Pe de altă parte, în ceea ce privește atât programele de supraveghere întemeiate pe articolul 702 din FISA, cât și cele întemeiate pe O. E. 12333, la punctele 181 și 182 din prezenta hotărâre s-a arătat că nici PPD-28, nici O. E. 12333 nu conferă persoanelor vizate drepturi opozabile autorităților americane în fața instanțelor judecătorești, astfel încât aceste persoane nu dispun de un drept la o cale de atac eficientă.

193 În cuprinsul considerentelor (115) și (116) ale Deciziei Scutul de confidențialitate, Comisia a constatat însă că, din cauza existenței mecanismului de tip Ombudsman instituit de autoritățile americane, astfel cum este prezentat în scrisoarea adresată la 7 iulie 2016 de Secretarul de Stat al SUA Comisarului European pentru Justiție, Consumatori și Egalitate de gen, care figurează în anexa III la această decizie, și a naturii sarcinii încredințate Ombudsmanului, în speță un „coordonator principal pentru diplomația internațională privind tehnologia informației”, se putea considera că Statele Unite asigurau un nivel de protecție în esență echivalent cu cel garantat la articolul 47 din cartă.

194 Analiza aspectului dacă mecanismul de tip Ombudsman prevăzut de Decizia Scutul de confidențialitate este efectiv de natură să compenseze limitările dreptului la o protecție jurisdicțională constatate de Comisie trebuie, în conformitate cu cerințele care decurg din articolul 47 din cartă și din jurisprudența amintită la punctul 187 din prezenta hotărâre, să pornească de la principiul că justițiabilii trebuie să dispună de posibilitatea de a exercita căi legale în fața unei instanțe judecătorești independente și imparțiale pentru a avea acces la date cu caracter personal care îi privesc sau de a obține rectificarea sau ștergerea unor astfel de date.

195 Or, în scrisoarea amintită la punctul 193 din prezenta hotărâre, Ombudsmanul pentru Scutul de confidențialitate, deși este descris ca fiind „independent de serviciile de informații”, a fost prezentat ca „[aflându-se] în subordinea directă a Secretarului de Stat, care se va asigura că Ombudsmanul își îndeplinește rolul în mod obiectiv și în condiții de independență față de orice influențe neadecvate care riscă să afecteze răspunsul care urmează să fie oferit”. Pe de altă parte, pe lângă faptul că, astfel cum a constatat Comisia în considerentul (116) al acestei decizii, Ombudsmanul este desemnat de Secretarul de Stat și face parte integrantă din Departamentul de Stat al Statelor Unite, în decizia menționată nu există, astfel cum a arătat domnul avocat general la punctul 337 din concluziile sale, nicio mențiune potrivit căreia revocarea Ombudsmanului sau anularea numirii sale ar fi însoțite de garanții specifice, ceea ce este de natură să pună în discuție independența Ombudsmanului în raport cu puterea executivă (a se vedea în acest sens Hotărârea din 21 ianuarie 2020, Banco de Santander, C-274/14, EU:C:2020:17, punctele 60 și 63, precum și jurisprudența citată).

196 De asemenea, astfel cum a subliniat domnul avocat general la punctul 338 din concluziile sale, deși considerentul (120) al Deciziei Scutul de confidențialitate menționează un angajament al guvernului american ca respectiva componentă a serviciilor de informații să fie obligată să remedieze orice încălcare a normelor aplicabile detectată de Ombudsmanul pentru Scutul de confidențialitate, decizia menționată nu conține nicio indicație potrivit căreia acest Ombudsman ar fi abilitat să adopte decizii obligatorii în privința respectivelor servicii și nici nu menționează garanțiile legale care ar însoți acest angajament și de care s-ar putea prevala persoanele vizate.

197 În consecință, mecanismul de tip Ombudsman prevăzut de Decizia Scutul de confidențialitate nu furnizează o cale de atac în fața unui organ care oferă persoanelor ale căror date sunt transferate către Statele Unite garanții în esență echivalente cu cele prevăzute la articolul 47 din cartă.

198 Prin urmare, prin faptul că a constatat, la articolul 1 alineatul (1) din Decizia Scutul de confidențialitate, că Statele Unite garantează un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune către organizații din această țară terță în temeiul Scutului de confidențialitate Uniunea Europeană-Statele Unite, Comisia a încălcat cerințele care rezultă din articolul 45 alineatul (1) din RGPD, interpretat în lumina articolelor 7, 8 și 47 din cartă.

199 Rezultă că articolul 1 din Decizia Scutul de confidențialitate este incompatibil cu articolul 45 alineatul (1) din RGPD, interpretat în lumina articolelor 7, 8 și 47 din cartă, și că, pentru acest motiv, este nevalid.

200 Întrucât articolul 1 din Decizia Scutul de confidențialitate este indisociabil de articolele 2-6 și de anexele la aceasta, nevaliditatea sa are drept efect afectarea validității deciziei menționate în ansamblul său.

201 Având în vedere toate considerațiile care precedă, trebuie să se concluzioneze că Decizia Scutul de confidențialitate este nevalidă.

202 În ceea ce privește aspectul dacă efectele acestei decizii trebuie menținute în scopul de a evita crearea unui vid juridic (a se vedea în acest sens Hotărârea din 28 aprilie 2016, Borealis Polyolefine și alții, C-191/14, C-192/14, C-295/14, C-389/14 și C-391/14-C-393/14, EU:C:2016:311, punctul 106), trebuie să se observe că, indiferent de situație, având în vedere articolul 49 din RGPD, anularea unei decizii privind caracterul adecvat al nivelului de protecție precum Decizia Scutul de confidențialitate nu este susceptibilă de a crea un asemenea vid juridic. Astfel, articolul menționat stabilește în mod precis condițiile în care pot avea loc transferuri de date cu caracter personal către țări terțe în absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 45 alineatul (3) din regulamentul respectiv sau a unor garanții adecvate în conformitate cu articolul 46 din același regulament.

Cu privire la cheltuielile de judecată

203 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 2 alineatele (1) și (2) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) trebuie interpretat în sensul că un transfer de date cu caracter personal efectuat în scopuri comerciale de un operator economic stabilit într-un stat membru către un alt operator economic stabilit într-o țară terță intră în domeniul de aplicare al acestui regulament, în pofida faptului că, în cursul sau în urma transferului menționat, datele respective sunt susceptibile de a fi prelucrate de autoritățile țării terțe în cauză în scopuri de siguranță publică, de apărare și de securitate a statului.**

2) **Articolul 46 alineatul (1) și articolul 46 alineatul (2) litera (c) din Regulamentul 2016/679 trebuie interpretate în sensul că garanțiile adecvate, drepturile opozabile și căile de atac eficiente prevăzute de aceste dispoziții trebuie să asigure că drepturile persoanelor ale căror date cu caracter personal sunt transferate către o țară terță în temeiul unor clauze standard de protecție a datelor beneficiază de un nivel de protecție în esență echivalent cu cel garantat în cadrul Uniunii Europene de regulamentul menționat, interpretat în lumina cartei. În acest scop, evaluarea nivelului de protecție asigurat în contextul unui astfel de transfer trebuie în special să ia în considerare atât stipulațiile contractuale convenite între operator sau persoana împuternicită de operator stabiliți în Uniunea Europeană și destinatarul transferului stabilit în țara terță în cauză, cât și, în ceea ce privește un eventual**

acces al autorităților publice ale acestei țări terțe la datele cu caracter personal astfel transferate, elementele relevante ale sistemului juridic al acesteia, în special cele prevăzute la articolul 45 alineatul (2) din regulamentul menționat.

3) **Articolul 58 alineatul (2) literele (f) și (j) din Regulamentul 2016/679 trebuie interpretat în sensul că, cu excepția cazului în care există o decizie privind caracterul adecvat al nivelului de protecție adoptată în mod valabil de Comisia Europeană, autoritatea de supraveghere competentă este obligată să suspende sau să interzică un transfer de date către o țară terță întemeiat pe clauze standard de protecție a datelor adoptate de Comisie, atunci când această autoritate de supraveghere consideră, în lumina tuturor împrejurărilor proprii transferului menționat, că aceste clauze nu sunt sau nu pot fi respectate în țara terță respectivă și că protecția datelor transferate impusă de dreptul Uniunii, în special de articolele 45 și 46 din acest regulament și de Carta drepturilor fundamentale, nu poate fi asigurată prin alte mijloace, în cazul în care operatorul însuși sau persoana împuternicită de operator stabiliți în Uniune nu a suspendat ori nu a încetat transferul.**

4) **Analiza Deciziei 2010/87/UE a Comisiei din 5 februarie 2010 privind clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele stabilite în țări terțe în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului, astfel cum a fost modificată prin Decizia de punere în aplicare (UE) 2016/2297 a Comisiei din 16 decembrie 2016, în raport cu articolele 7, 8 și 47 din Carta drepturilor fundamentale, nu a evidențiat niciun element de natură să afecteze validitatea acestei decizii.**

5) **Decizia de punere în aplicare (UE) 2016/1250 a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA este nevalidă.**

Semnături