HOTĂRÂREA CURȚII (Marea Cameră)

15 iunie 2021 *

„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 – Prelucrare transfrontalieră a datelor cu caracter personal – Mecanismul «ghișeului unic» – Cooperare loială și eficientă între autoritățile de supraveghere – Abilitări și competențe – Competența de a iniția proceduri judiciare”

În cauza C-645/19,

având ca obiect o cerere de decizie preliminară formulată în temeiul articolului 267 TFUE de hof van beroep te Brussel (Curtea de Apel din Bruxelles, Belgia), prin decizia din 8 mai 2019, primită de Curte la 30 august 2019, în procedura

Facebook Ireland și alții

Facebook Inc.,

Facebook Belgium BVBA,

împotriva

Gegevensbeschermingsautoriteit,

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. Ilešič și N. Wahl, președinți de cameră, domnii E. Juhász, D. Šváby, S. Rodin și F. Biltgen, doamna K. Jürimäe, domnii C. Lycourgos și P. G. Xuereb și doamna L. S. Rossi (raportoare), judecători,

avocat general: domnul M. Bobek,

grefier: doamna M. Ferreira, administrator principal,

având în vedere procedura scrisă și în urma ședinței din 5 octombrie 2020,

luând în considerare observațiile prezentate:

– pentru Facebook Ireland Ltd, Facebook Inc. și Facebook Belgium BVBA, de S. Raes, P. Lefebvre și D. Van Liedekerke, advocaten;

– pentru Gegevensbeschermingsautoriteit, de F. Debusseré și R. Roex, advocaten;

* Limba de procedură: neerlandeza.

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

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

– pentru guvernul italian, de G. Palmieri, în calitate de agent, asistată de G. Natale, avvocato dello Stato;

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

– pentru guvernul portughez, de L. Inez Fernandes, A. C. Guerra, P. Barros da Costa și L. Medeiros, în calitate de agenți;

– pentru guvernul finlandez, de A. Laine și M. Pere, în calitate de agenți;

– pentru Comisia Europeană, de H. Kranenborg, D. Nardi și P. J. O. Van Nuffel, în calitate de agenți,

după ascultarea concluziilor avocatului general în ședința din 13 ianuarie 2021,

pronunță prezenta

Hotărâre

1 Cererea de decizie preliminară privește interpretarea articolului 55 alineatul (1) și a articolelor 56-58 și 60-66 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO 2016, L 119, p. 1, rectificare în JO 2018, L 127, p. 2) coroborate cu articolele 7, 8 și 47 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”).

2 Această cerere a fost formulată în cadrul unui litigiu între Facebook Ireland Ltd, Facebook Inc. și Facebook Belgium BVBA, pe de o parte, și Gegevensbeschermingsautoriteit (Autoritatea de Protecție a Datelor, Belgia) (denumită în continuare „APD”), succesoarea Commissiter bescherming van de persoonlijke levenssfeer (Comisia pentru protecția vieții private, Belgia) (denumită în continuare „CPVP”), pe de altă parte, în legătură cu o acțiune în încetare formulată de președintele acesteia din urmă și care vizează încetarea prelucrării datelor cu caracter personal ale internauților de pe teritoriul belgian, efectuată de rețeaua socială online Facebook, prin intermediul unor cookies, al unor extensii pentru social media (*social plug-ins*) și al unor pixeli.

Cadrul juridic

Dreptul Uniunii

3 Considerentele (1), (4), (10), (11), (13), (22), (123), (141) și (145) ale Regulamentului nr. 2016/679 au următorul cuprins:

„(1) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din [cartă] și articolul 16 alineatul (1) [TFUE] prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.

[…]

(4) Prelucrarea datelor cu caracter personal ar trebui să fie în serviciul cetățenilor. Dreptul la protecția datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate și echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității. Prezentul regulament respectă toate drepturile fundamentale și libertățile și principiile recunoscute în cartă astfel cum sunt consacrate în tratate, în special respectarea vieții private și de familie, a reședinței și a comunicațiilor, a protecției datelor cu caracter personal, a libertății de gândire, de conștiință și de religie, a libertății de exprimare și de informare, a libertății de a desfășura o activitate comercială, dreptul la o cale de atac eficientă și la un proces echitabil, precum și diversitatea culturală, religioasă și lingvistică.

[…]

(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 [Europene], 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. […]

(11) Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea și stabilirea în detaliu a drepturilor persoanelor vizate și a obligațiilor celor care prelucrează și decid prelucrarea datelor cu caracter personal, ci și competențe echivalente pentru monitorizarea și asigurarea conformității cu normele de protecție a datelor cu caracter personal și sancțiuni echivalente pentru infracțiuni în statele membre.

[…]

(13) În vederea asigurării unui nivel uniform de protecție pentru persoanele fizice în întreaga Uniune și a preîntâmpinării discrepanțelor care împiedică libera circulație a datelor în cadrul pieței interne, este necesar un regulament în scopul de a furniza securitate juridică și transparență pentru operatorii economici, inclusiv microîntreprinderi și întreprinderi mici și mijlocii, precum și de a oferi persoanelor fizice în toate statele membre același nivel de drepturi, obligații și responsabilități opozabile din punct de vedere juridic pentru operatori și persoanele împuternicite de aceștia, pentru a se asigura o monitorizare coerentă a prelucrării datelor cu caracter personal, sancțiuni echivalente în toate statele membre, precum și cooperarea eficace a autorităților de supraveghere ale diferitor state membre. […]

[…]

(22) Orice prelucrare a datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune ar trebui efectuată în conformitate cu prezentul regulament, indiferent dacă procesul de prelucrare în sine are loc sau nu în cadrul Uniunii. Sediul implică exercitarea efectivă și reală a unei activități în cadrul unor înțelegeri stabile. Forma juridică a unor astfel de înțelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință.

[…]

(123) Autoritățile de supraveghere ar trebui să monitorizeze aplicarea dispozițiilor prevăzute de prezentul regulament și să contribuie la aplicarea coerentă a acestuia în întreaga Uniune, în scopul asigurării protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal și al facilitării liberei circulații a datelor cu caracter personal în interiorul pieței

interne. În acest sens, autoritățile de supraveghere ar trebui să coopereze reciproc, precum și cu Comisia [Europeană], fără să fie necesar niciun acord între statele membre cu privire la acordarea de asistență reciprocă sau cu privire la respectiva cooperare.

[…]

(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. […]

[…]

(145) În ceea ce privește acțiunile inițiate împotriva unui operator sau unei persoane împuternicite de operator, reclamantul ar trebui să aibă posibilitatea de a introduce acțiunea în fața instanțelor din statele membre în care operatorul sau persoana împuternicită de operator are un sediu sau în care persoana vizată își are reședința, cu excepția cazului în care operatorul este o autoritate publică dintr-un stat membru ce acționează în exercitarea competențelor sale publice.”

4 Articolul 3 din acest regulament, intitulat „Dreptul la opoziție”, prevede la alineatul (1):

„Prezentul regulament se aplică prelucrării datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.”

5 Articolul 4 din regulamentul menționat definește, la punctul 16 din acesta, noțiunea de „sediu principal” și, la punctul 23 din acesta, noțiunea de „tratament transfrontalier”, după cum urmează:

„16. «sediu principal» înseamnă:

a) în cazul unui operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acestuia în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competența de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal;

b) în cazul unei persoane împuternicite de operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acesteia în Uniune sau, în cazul în care persoana împuternicită de operator nu are o administrație centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activitățile principale de prelucrare, în contextul activităților unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligații specifice în temeiul prezentului regulament;

[…]

23. «prelucrare transfrontalieră» înseamnă:

a) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; […]

b) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre”.

6 Articolul 51 din același regulament, intitulat „Autoritatea de supraveghere”, prevede:

„(1) 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 […].

(2) Fiecare autoritate de supraveghere contribuie la aplicarea coerentă a prezentului regulament în întreaga Uniune. În acest scop, autoritățile de supraveghere cooperează atât între ele, cât și cu Comisia, în conformitate cu capitolul VII.

[…]”

7 Articolul 55 din Regulamentul 2016/679, intitulat „Competența”, care face parte din capitolul VI din acest regulament, intitulat, la rândul său, „Autorități de supraveghere independente”, prevede:

„(1) Fiecare 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.

(2) În cazul în care prelucrarea este efectuată de autorități publice sau de organisme private care acționează pe baza articolului 6 alineatul (1) litera (c) sau (e), autoritatea de supraveghere din statul membru respectiv are competență. În astfel de cazuri, articolul 56 nu se aplică.”

8 Articolul 56 din regulamentul menționat, intitulat „Competența autorității de supraveghere principale”, prevede:

„(1) Fără a aduce atingere articolului 55, autoritatea de supraveghere a sediului principal sau a sediului unic al operatorului sau al persoanei împuternicite de operator este competentă să acționeze în calitate de autoritate de supraveghere principală pentru prelucrarea transfrontalieră efectuată de respectivul operator sau respectiva persoană împuternicită în cauză în conformitate cu procedura prevăzută la articolul 60.

(2) Prin derogare de la alineatul (1), fiecare autoritate de supraveghere este competentă să trateze o plângere depusă în atenția sa sau o eventuală încălcare a prezentului regulament, în cazul în care obiectul acesteia se referă numai la un sediu aflat în statul său membru sau afectează în mod semnificativ persoane vizate numai în statul său membru.

(3) În cazurile menționate la alineatul (2) din prezentul articol, autoritatea de supraveghere informează fără întârziere autoritatea de supraveghere principală cu privire la această chestiune. În termen de trei săptămâni de la momentul informării, autoritatea de supraveghere principală decide dacă tratează sau nu cazul respectiv în conformitate cu procedura prevăzută la articolul 60, luând în considerare dacă există sau nu un sediu al operatorului sau al persoanei împuternicite de operator pe teritoriul statului membru a cărui autoritate de supraveghere a informat-o.

(4) În cazul în care autoritatea de supraveghere principală decide să trateze cazul, se aplică procedura prevăzută la articolul 60. Autoritatea de supraveghere care a informat autoritatea de supraveghere principală poate înainta un proiect de decizie acesteia din urmă. Autoritatea de supraveghere principală ține seama în cea mai mare măsură posibilă de proiectul respectiv atunci când pregătește proiectul de decizie prevăzut la articolul 60 alineatul (3).

(5) În cazul în care autoritatea de supraveghere principală decide să nu trateze cazul, autoritatea de supraveghere care a informat autoritatea de supraveghere principală tratează cazul în conformitate cu articolele 61 și 62.

(6) Autoritatea de supraveghere principală este singurul interlocutor al operatorului sau al persoanei împuternicite de operator în ceea ce privește prelucrarea transfrontalieră efectuată de respectivul operator sau de respectiva persoană împuternicită de operator.”

9 Articolul 57 din Regulamentul 2016/679, intitulat „Sarcini”, prevede la alineatul (1):

„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;

[…]

(g) cooperează, inclusiv prin schimb de informații, cu alte autorități de supraveghere și își oferă asistență reciprocă pentru a asigura coerența aplicării și respectării prezentului regulament;

[…]”

10 Articolul 58 din același regulament, intitulat „Competențe”, prevede la alineatele (1), (4) și (5):

„(1) Fiecare autoritate de supraveghere are toate următoarele competențe de investigare:

(a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale;

[…]

(d) de a notifica operatorul sau persoana împuternicită de operator cu privire la presupusa încălcare a prezentului regulament;

[…]

(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.

(5) Fiecare stat membru prevede, pe cale legislativă, faptul că autoritatea sa de supraveghere are competența de a aduce în fața autorităților judiciare cazurile de încălcare a prezentului regulament și, după caz, de a iniția sau de a se implica într-un alt mod în proceduri judiciare, în scopul de a asigura aplicarea dispozițiilor prezentului regulament.”

11 În capitolul VII din Regulamentul 2016/679, intitulat „Cooperare și coerență”, secțiunea I, intitulată „Cooperare”, cuprinde articolele 60-62 din acest regulament. Articolul 60, intitulat „Cooperarea dintre autoritatea de supraveghere principală și celelalte autorități de supraveghere vizate”, prevede:

„(1) Autoritatea de supraveghere principală cooperează cu celelalte autorități de supraveghere vizate, în conformitate cu prezentul articol, în încercarea de a ajunge la un consens. Autoritatea de supraveghere principală și autoritățile de supraveghere vizate își comunică reciproc toate informațiile relevante.

(2) Autoritatea de supraveghere principală poate solicita în orice moment altor autorități de supraveghere vizate să ofere asistență reciprocă în temeiul articolului 61 și poate desfășura operațiuni comune în temeiul articolului 62, în special în vederea efectuării de investigații sau a monitorizării punerii în aplicare a unei măsuri referitoare la un operator sau o persoană împuternicită de operator, stabilit(ă) în alt stat membru.

(3) Autoritatea de supraveghere principală comunică fără întârziere informațiile relevante referitoare la această chestiune celorlalte autorități de supraveghere vizate. Autoritatea de supraveghere principală transmite fără întârziere un proiect de decizie celorlalte autorități de supraveghere vizate, pentru a obține avizul lor, și ține seama în mod corespunzător de opiniile acestora.

(4) În cazul în care oricare dintre celelalte autorități de supraveghere vizate exprimă, în termen de patru săptămâni după ce a fost consultată în conformitate cu alineatul (3) din prezentul articol, o obiecție relevantă și motivată la proiectul de decizie, autoritatea de supraveghere principală, în cazul în care nu dă curs obiecției relevante și motivate sau consideră că obiecția nu este relevantă sau motivată, sesizează mecanismul pentru asigurarea coerenței menționat la articolul 63.

(5) În cazul în care intenționează să dea curs obiecției relevante și motivate formulate, autoritatea de supraveghere principală transmite celorlalte autorități de supraveghere vizate un proiect revizuit de decizie pentru a obține avizul acestora. Acest proiect revizuit de decizie face obiectul procedurii menționate la alineatul (4) pe parcursul unei perioade de două săptămâni.

(6) În cazul în care niciuna dintre celelalte autorități de supraveghere vizate nu a formulat obiecții la proiectul de decizie transmis de autoritatea de supraveghere principală în termenul menționat la alineatele (4) și (5), se consideră că autoritatea de supraveghere principală și autoritățile de supraveghere vizate sunt de acord cu proiectul de decizie respectiv, care devine obligatoriu pentru acestea.

(7) Autoritatea de supraveghere principală adoptă decizia și o notifică sediului principal sau sediului unic al operatorului sau al persoanei împuternicite de operator, după caz, și informează celelalte autorități de supraveghere vizate și [C]omitetul [european pentru protecția datelor] cu privire la decizia în cauză, incluzând un rezumat al elementelor și motivelor relevante. Autoritatea de supraveghere la care a fost depusă plângerea informează reclamantul cu privire la decizie.

(8) Prin derogare de la alineatul (7), în cazul în care o plângere este refuzată sau respinsă, autoritatea de supraveghere la care s-a depus plângerea adoptă decizia, o notifică reclamantului și informează operatorul cu privire la acest lucru.

(9) În cazul în care autoritatea de supraveghere principală și autoritățile de supraveghere vizate sunt de acord să refuze sau să respingă anumite părți ale unei plângeri și să dea curs altor părți ale plângerii respective, se adoptă o decizie separată pentru fiecare dintre aceste părți. […]

(10) În urma notificării deciziei autorității de supraveghere principale în temeiul alineatelor (7) și (9), operatorul sau persoana împuternicită de operator ia măsurile necesare pentru a se asigura că activitățile de prelucrare sunt în conformitate cu decizia în toate sediile sale din Uniune. Operatorul sau persoana împuternicită de operator notifică măsurile luate în vederea respectării deciziei autorității de supraveghere principale, care informează celelalte autorități de supraveghere vizate.

(11) În cazul în care, în circumstanțe excepționale, o autoritate de supraveghere vizată are motive să considere că există o nevoie urgentă de a acționa în vederea protejării intereselor persoanelor vizate, se aplică procedura de urgență prevăzută la articolul 66.

[…]”

12 Articolul 61 din regulamentul menționat, intitulat „Asistență reciprocă”, prevede la alineatul (1):

„Autoritățile de supraveghere își furnizează reciproc informații relevante și asistență pentru a pune în aplicare prezentul regulament în mod coerent și instituie măsuri de cooperare eficace între ele. Asistența reciprocă se referă, în special, la cereri de informații și măsuri de supraveghere, cum ar fi cereri privind autorizări și consultări prealabile, inspecții și investigații.”

13 Articolul 62 din același regulament, intitulat „Operațiuni comune ale autorităților de supraveghere”, prevede:

„(1) După caz, autoritățile de supraveghere desfășoară operațiuni comune, inclusiv investigații comune și măsuri comune de aplicare a legii, în care sunt implicați membri sau personal din autoritățile de supraveghere ale altor state membre.

(2) În cazul în care operatorul sau persoana împuternicită de operator deține sedii în mai multe state membre sau dacă un număr semnificativ de persoane vizate din mai multe state membre sunt susceptibile de a fi afectate în mod semnificativ de operațiuni de prelucrare, o autoritate de supraveghere din fiecare dintre statele membre respective are dreptul de a participa la operațiunile comune. […]

[…]”

14 Secțiunea 2, intitulată „Asigurarea coerenței”, din capitolul VII din Regulamentul 2016/679 cuprinde articolele 63-67 din acest regulament. Articolul 63, intitulat „Mecanismul pentru asigurarea coerenței”, are următorul cuprins:

„Pentru a contribui la aplicarea coerentă a prezentului regulament în întreaga Uniune, autoritățile de supraveghere cooperează între ele și, după caz, cu Comisia prin mecanismul pentru asigurarea coerenței, astfel cum se prevede în prezenta secțiune.”

15 Potrivit articolului 64 alineatul (2) din regulamentul menționat:

„Orice autoritate de supraveghere, președintele [C]omitetului [european pentru protecția datelor] 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 [C]omitet[ul] [european pentru protecția datelor] 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.”

16 Articolul 65 din același regulament, intitulat „Soluționarea litigiilor de către comitet”, prevede la alineatul (1):

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

(a) atunci când, în unul dintre cazurile menționate la articolul 60 alineatul (4), o autoritate de supraveghere vizată a formulat o obiecție relevantă și motivată la un proiect de decizie a autorității principale sau autoritatea principală a respins o astfel de obiecție ca nefiind relevantă sau motivată. Decizia obligatorie se referă la toate chestiunile vizate de obiecția relevantă și motivată, în special la chestiunea dacă prezentul regulament a fost încălcat;

(b) în cazul în care există opinii divergente cu privire la care dintre autoritățile de supraveghere vizate deține competența pentru sediul principal;

[…]”

17 Articolul 66 din Regulamentul 2016/679, intitulat „Procedura de urgență”, prevede la alineatele (1) și (2):

„(1) În circumstanțe excepționale, atunci când o autoritate de supraveghere vizată consideră că există o necesitate urgentă de a acționa în scopul protejării drepturilor și libertăților persoanelor vizate, aceasta poate, prin derogare de la mecanismul pentru asigurarea coerenței menționat la articolele 63, 64 și 65 sau de la procedura menționată la articolul 60, să adopte de îndată măsuri provizorii menite să producă efecte juridice pe propriul său teritoriu, cu o perioadă de valabilitate determinată, care să nu depășească trei luni. Autoritatea de supraveghere comunică fără întârziere aceste măsuri și motivele adoptării lor celorlalte autorități de supraveghere vizate, [C]omitetului [european pentru protecția datelor] și Comisiei.

(2) În cazul în care o autoritate de supraveghere a adoptat o măsură în temeiul alineatului (1) și consideră că este necesară adoptarea de urgență a unor măsuri definitive, aceasta poate solicita un aviz de urgență sau o decizie obligatorie urgentă din partea [C]omitetului [european pentru protecția datelor], indicând motivele pentru această solicitare.”

18 Articolul 77 din acest regulament, 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.”

19 Articolul 78 din regulamentul menționat, intitulat „Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere”, prevede:

„(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.

(3) Acțiunile introduse împotriva unei autorități de supraveghere sunt aduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

(4) În cazul în care acțiunile sunt introduse împotriva unei decizii a unei autorități de supraveghere care a fost precedată de un aviz sau o decizie a [C]omitetului [european pentru protecția datelor] în cadrul mecanismului pentru asigurarea coerenței, autoritatea de supraveghere transmite curții avizul respectiv sau decizia respectivă."

20 Articolul 79 din același regulament, intitulat „Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator", prevede:

„(1) Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în temeiul articolului 77, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta prezentul regulament.

(2) Acțiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în fața instanțelor din statul membru unde operatorul sau persoana împuternicită de operator își are un sediu. Alternativ, o astfel de acțiune poate fi prezentată în fața instanțelor din statul membru în care persoana vizată își are reședința obișnuită, cu excepția cazului în care operatorul sau persoana împuternicită de operator este o autoritate publică a unui stat membru ce acționează în exercitarea competențelor sale publice."

Dreptul belgian

21 Wet tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens (Legea privind protecția vieții private în raport cu prelucrarea datelor cu caracter personal) din 8 decembrie 1992 (*Belgisch Staatsblad* din18 martie 1993, p. 5801), astfel cum a fost modificată prin Legea din 11 decembrie 1998 (*Belgisch Staatsblad*, 3 februarie 1999, p. 3049) (denumită în continuare „Legea din 8 decembrie 1992"), a transpus în dreptul belgian 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).

22 Legea din 8 decembrie 1992 a înființat CPVP, un organism independent având ca misiune să vegheze ca datele cu caracter personal să fie prelucrate cu respectarea acestei legi, astfel încât să garanteze viața privată a cetățenilor.

23 Articolul 32 alineatul (3) din Legea din 8 decembrie 1992 prevedea următoarele:

„Fără a aduce atingere competenței instanțelor de drept comun pentru aplicarea principiilor generale de protecție a confidențialității, președintele [CPVP] poate sesiza instanța de fond cu privire la orice litigiu privind aplicarea prezentei legi și a măsurilor de punere în aplicare a acesteia."

24 Wet tot oprichting van de Gegevensbeschermingsautoriteit (Legea privind înființarea autorității de protecție a datelor) din 3 decembrie 2017 (*Belgisch Staatsblad* din 10 ianuarie 2018, p. 989, denumită în continuare „Legea din 3 decembrie 2017”), care a intrat în vigoare la 25 mai 2018, a instituit APD în calitate de autoritate de supraveghere, în sensul Regulamentului 2016/679.

25 Articolul 3 din Legea din 3 decembrie 2017 prevede:

„Se instituie pe lângă Camera Reprezentanților o «Autoritate pentru protecția datelor». Aceasta succedă [CPVP].”

26 Articolul 6 din Legea din 3 decembrie 2017 prevede:

„[APD] are competența de a sesiza autoritățile judiciare cu privire la orice încălcare a principiilor fundamentale ale protecției datelor cu caracter personal în cadrul prezentei legi și al legilor care conțin dispoziții privind protecția prelucrării datelor cu caracter personal și, dacă este cazul, de a intenta acțiuni în justiție pentru aplicarea acestor principii fundamentale.”

27 Nicio dispoziție specifică nu este prevăzută pentru procedurile jurisdicționale deja inițiate de președintele CPVP la 25 mai 2018 în temeiul articolului 32 alineatul (3) din Legea din 8 decembrie 1992. În ceea ce privește numai plângerile sau cererile depuse chiar la APD, articolul 112 din Legea din 3 decembrie 2017 prevede:

„Capitolul VI nu se aplică plângerilor sau cererilor încă pendinte la [APD] la data intrării în vigoare a prezentei legi. Plângerile sau cererile menționate în primul paragraf sunt soluționate de [APD], în calitate de succesor legal al [CPVP], în conformitate cu procedura aplicabilă înainte de intrarea în vigoare a prezentei legi.”

28 Legea din 8 decembrie 1992 a fost abrogată prin wet betreffende de bescherming van naturlijke personen met betrekking tot de verwerking van persoonsgegevens (Legea privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal) din 30 iulie 2018 (*Belgisch Staatsblad* din 5 septembrie 2018, p. 68616, denumită în continuare „Legea din 30 iulie 2018”). Această din urmă lege urmărește punerea în aplicare în dreptul belgian a dispozițiilor Regulamentului 2016/679 care impun sau permit statelor membre să adopte norme mai detaliate, în completarea acestui regulament.

Litigiul principal și întrebările preliminare

29 La 11 septembrie 2015, președintele CPVP a introdus o acțiune în încetare împotriva Facebook Ireland, a Facebook Inc. și a Facebook Belgium la Nederlandstalige rechtbank van eerste aanleg Brussel (Tribunalul de Primă Instanță neerlandofon din Bruxelles, Belgia). Întrucât CPVP nu avea personalitate juridică, îi revenea președintelui său competența de a formula acțiuni pentru a garanta respectarea legislației în materie de protecție a datelor cu caracter personal. Cu toate acestea, CPVP însăși a solicitat intervenția voluntară în procedura inițiată de președintele său.

30 Această acțiune în încetare avea ca obiect să pună capăt unei situații pe care CPVP o descrie, printre altele, ca o „încălcare gravă și pe scară largă de către Facebook a legislației în materia protecției vieții private”, care constă în colectarea de către această rețea socială online de informații cu privire la comportamentul de navigare atât al deținătorilor unui cont Facebook, cât și al neutilizatorilor serviciilor Facebook prin intermediul diferitor tehnologii, cum ar fi cookies, extensii pentru social media (de exemplu butoanele „Îmi place” sau „Distribuie”) sau pixelii. Aceste elemente permit rețelei sociale în cauză să obțină anumite date ale unui utilizator de internet care consultă o pagină a unui site internet care le conține, precum adresa acestei pagini, „adresa IP” a vizitatorului paginii respective, precum și data și ora consultării vizate.

31 Prin hotărârea din 16 februarie 2018, Nederlandstalige rechtbank van eerste aanleg Brussel (Tribunalul de Primă Instanță neerlandofon din Bruxelles) s-a declarat competent să se pronunțe cu privire la acțiunea în încetare menționată, în măsura în care privea Facebook Ireland, Facebook Inc. și Facebook Belgium, și a declarat inadmisibilă cererea de intervenție voluntară formulată de CPVP.

32 Pe fond, această instanță a statuat că rețeaua socială în cauză nu informa suficient utilizatorii de internet belgieni cu privire la colectarea informațiilor în cauză și la utilizarea acestor informații. Pe de altă parte, consimțământul dat de utilizatorii de internet pentru colectarea și prelucrarea informațiilor menționate a fost considerat nevalabil. Prin urmare, instanța respectivă a obligat Facebook Ireland, Facebook Inc. și Facebook Belgium, în primul rând, să înceteze, în privința oricărui utilizator de internet stabilit pe teritoriul belgian, să plaseze fără consimțământul său cookie-uri care rămân active timp de doi ani pe dispozitivul pe care îl utilizează atunci când navighează pe o pagină de internet a numelui de domeniu Facebook.com sau când ajunge pe site-ul unui terț, precum și să plaseze cookie-uri și să colecteze date prin intermediul unor extensii pentru social media, al unor pixeli sau al unor mijloace tehnologice similare pe site-urile internet ale unor terți, într-un mod excesiv având în vedere obiectivele astfel urmărite de rețeaua socială Facebook, în al doilea rând, să înceteze să furnizeze informații care ar putea induce în mod rezonabil în eroare persoanele vizate în ceea ce privește întinderea reală a mecanismelor puse la dispoziție de această rețea socială pentru utilizarea cookie-urilor și, în al treilea rând, să distrugă toate datele cu caracter personal obținute prin intermediul unor cookie-uri sau al unor extensii pentru social media.

33 La 2 martie 2018, Facebook Ireland, Facebook Inc. și Facebook Belgium au declarat apel împotriva acestei hotărâri în fața Hof van beroep te Brussel (Curtea de Apel din Bruxelles, Belgia). În fața acestei instanțe, APD acționează în calitate de succesor legal atât al președintelui CPVP, care intentase acțiunea în încetare, cât și al CPVP înseși.

34 Instanța de trimitere s-a declarat competentă să se pronunțe cu privire la apelul formulat doar în măsura în care privește Facebook Belgium. În schimb, s-a declarat necompetentă să soluționeze acest apel în ceea ce privește Facebook Ireland și Facebook Inc.

35 Înainte de a se pronunța pe fondul litigiului principal, instanța de trimitere ridică problema dacă APD dispune de calitatea procesuală și de interesul de a exercita acțiunea necesar. Potrivit Facebook Belgium, acțiunea în încetare introdusă ar fi inadmisibilă, în ceea ce privește faptele anterioare datei de 25 mai 2018, în măsura în care, în urma intrării în vigoare a Legii din 3 decembrie 2017 și a Regulamentului 2016/679, articolul 32 alineatul (3) din Legea din 8 decembrie 1992, care constituie temeiul juridic care permite introducerea unei astfel de acțiuni, ar fi fost abrogat. În ceea ce privește faptele ulterioare datei de 25 mai 2018, Facebook Belgium arată că APD nu ar avea competență și nu ar dispune de un drept de a intenta această acțiune ținând seama de mecanismul „ghișeului unic” prevăzut în prezent în temeiul dispozițiilor Regulamentului 2016/679. Astfel, pe baza acestor dispoziții, numai Data Protection Commissioner (Comisarul pentru protecția datelor, Irlanda) ar fi competent să introducă o acțiune în încetare împotriva Facebook Ireland, aceasta din urmă fiind singurul operator al datelor cu caracter personal ale utilizatorilor rețelei sociale în cauză în Uniune.

36 Instanța de trimitere a apreciat că APD nu justifica interesul de a exercita acțiunea necesar pentru introducerea acestei acțiuni în încetare în măsura în care aceasta din urmă privea fapte anterioare datei de 25 mai 2018. În ceea ce privește faptele ulterioare acestei date, instanța de trimitere are totuși îndoieli cu privire la incidența intrării în vigoare a Regulamentului 2016/679, în special a aplicării mecanismului „ghișeului unic” pe care îl prevede acest regulament, asupra competențelor APD, precum și asupra competenței acesteia din urmă de a introduce o astfel de acțiune în încetare.

37 Mai precis, potrivit instanței de trimitere, problema care se ridică în prezent este dacă, pentru faptele ulterioare datei de 25 mai 2018, APD poate acționa împotriva Facebook Belgium, din moment ce Facebook Ireland a fost identificată drept operator al datelor vizate. De la această dată și în temeiul principiului „ghișeului unic”, s-ar părea că, potrivit articolului 56 din Regulamentul 2016/679, numai Comisarul pentru protecția datelor ar fi competent, sub controlul exclusiv al instanțelor irlandeze.

38 Instanța de trimitere amintește că, în Hotărârea din 5 iunie 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388), Curtea a statuat că „autoritatea de supraveghere germană” era competentă să se pronunțe cu privire la un litigiu în materia protecției datelor cu caracter personal, deși operatorul datelor în cauză avea sediul în Irlanda, iar filiala acestuia care avea sediul în Germania, și anume Facebook Germany GmbH, se ocupa doar de vânzarea de spații publicitare și de alte activități de marketing pe teritoriul german.

39 Însă, în cauza în care s-a pronunțat această hotărâre, Curtea era sesizată cu o cerere de decizie preliminară privind interpretarea dispozițiilor Directivei 95/46, care a fost abrogată prin Regulamentul 2016/679. Instanța de trimitere ridică problema în ce măsură interpretarea pe care Curtea a dat-o în hotărârea menționată este încă pertinentă în ceea ce privește aplicarea Regulamentului 2016/679.

40 Instanța de trimitere menționează de asemenea o decizie a Bundeskartellamt (Autoritatea federală pentru concurență, Germania) din 6 februarie 2019 (decizie cunoscută sub numele „Facebook”), în care această autoritate pentru concurență a considerat, în esență, că întreprinderea în cauză abuza de poziția sa concentrând date provenite din diferite surse, ceea ce, de acum înainte, nu ar mai trebui să se poată face decât cu consimțământul expres al utilizatorilor, fiind de la sine înțeles că utilizatorul care nu consimte la aceasta nu poate fi exclus din serviciile Facebook. Instanța de trimitere arată că, în mod vădit, autoritatea de concurență menționată s-a considerat competentă, în pofida mecanismului „ghișeului unic”.

41 În plus, instanța de trimitere consideră că articolul 6 din Legea din 3 decembrie 2017, care permite, în principiu, APD, dacă este cazul, să acționeze în justiție, nu implică faptul că acțiunea acesteia poate fi introdusă, în orice împrejurare, în fața instanțelor belgiene, întrucât mecanismul „ghișeului unic” ar părea să impună ca o astfel de acțiune să fie introdusă în fața instanței de la locul în care este efectuată prelucrarea datelor.

42 În aceste condiții, hof van beroep te Brussel (Curtea de Apel din Bruxelles) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„1) Articolul 55 alineatul (1) și articolele 56-58 și 60-66 din [Regulamentul 2016/679] coroborate cu articolele 7, 8 și 47 din [cartă] trebuie interpretate în sensul că o autoritate de supraveghere care, în temeiul legislației naționale adoptate în aplicarea articolului 58 alineatul (5) din acest regulament, are competența de a introduce la o instanță din statul său membru o acțiune în justiție împotriva încălcărilor acestui regulament nu poate exercita această competență în ceea ce privește o prelucrare transfrontalieră dacă ea nu este autoritatea de supraveghere principală pentru această prelucrare transfrontalieră?

2) Răspunsul la prima întrebare adresată este diferit în cazul în care operatorul acestei prelucrări transfrontaliere nu are sediul principal în respectivul stat membru, însă are un alt sediu în acel stat?

3) Răspunsul la prima întrebare adresată este diferit în cazul în care autoritatea națională de supraveghere introduce acțiunea în justiție împotriva sediului principal al operatorului sau împotriva sediului său din propriul stat membru?

4) Răspunsul la prima întrebare adresată este diferit în cazul în care autoritatea națională de supraveghere a introdus deja acțiunea în justiție înainte de data la care [Regulamentul 2016/679] a intrat în vigoare (25 mai 2018)?

5) În cazul unui răspuns afirmativ la prima întrebare adresată, articolul 58 alineatul (5) din Regulamentul 2016/679 are efect direct, astfel încât o autoritate națională de supraveghere se poate baza pe articolul menționat pentru a iniția sau a continua o procedură judiciară împotriva unor părți private, chiar dacă articolul 58 alineatul (5) din Regulamentul 2016/679 nu este transpus în mod specific în legislația statelor membre, deși acest lucru este obligatoriu?

6) În cazul unui răspuns afirmativ la prima-a cincea întrebare, rezultatul acestor proceduri ar putea împiedica o constatare contrară a autorității de supraveghere principale în cazul în care autoritatea de supraveghere principală anchetează aceleași activități de prelucrare transfrontalieră sau activități similare, în conformitate cu mecanismul prevăzut la articolele 56 și 60 din Regulamentul 2016/679?”

Cu privire la întrebările preliminare

Cu privire la prima întrebare

43 Prin intermediul primei întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolul 55 alineatul (1) și articolele 56-58, precum și articolele 60-66 din Regulamentul 2016/679 coroborate cu articolele 7, 8 și 47 din cartă trebuie interpretate în sensul că o autoritate de supraveghere a unui stat membru care, în temeiul legislației naționale adoptate în aplicarea articolului 58 alineatul (5) din acest regulament, are competența de a aduce în fața unei instanțe din acest stat membru orice pretins caz de încălcare a regulamentului menționat și, după caz, de a iniția proceduri judiciare poate exercita această competență în ceea ce privește o prelucrare de date transfrontalieră, deși ea nu este autoritatea de supraveghere principală, în sensul articolului 56 alineatul (1) din același regulament, în ceea ce privește o asemenea prelucrare de date.

44 În această privință trebuie amintit, cu titlu introductiv, că, pe de o parte, spre deosebire de Directiva 95/46, care fusese adoptată în temeiul articolului 100 A din Tratatul CE, privind armonizarea pieței comune, temeiul juridic al Regulamentului 2016/679 este articolul 16 TFUE, care consacră dreptul oricărei persoane la protecția datelor cu caracter personal și autorizează Parlamentul European și Consiliul Uniunii Europene să stabilească normele privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii, precum și de către statele membre în exercitarea activităților care fac parte din domeniul de aplicare al dreptului Uniunii, precum și normele privind libera circulație a acestor date. Pe de altă parte, considerentul (1) al acestui regulament afirmă că „[p]rotecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental” și amintește că articolul 8 alineatul (1) din cartă, precum și articolul 16 alineatul (1) TFUE prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.

45 În consecință, după cum rezultă din articolul 1 alineatul (2) din Regulamentul 2016/679 coroborat cu considerentele (10), (11) și (13) ale acestui regulament, acesta din urmă impune instituțiilor, organelor, oficiilor și agențiilor Uniunii, precum și autorităților competente ale statelor membre sarcina de a asigura un nivel ridicat de protecție a drepturilor garantate la articolul 16 TFUE și la articolul 8 din cartă.

46 În plus, astfel cum enunță considerentul (4) al regulamentului menționat, acesta respectă toate drepturile fundamentale și libertățile și principiile recunoscute de cartă.

47 Acesta este contextul în care articolul 55 alineatul (1) din Regulamentul 2016/679 stabilește competența de principiu a fiecărei autorități de supraveghere de a îndeplini sarcinile și de a exercita competențele care îi sunt conferite în conformitate cu acest regulament pe teritoriul statului membru de care aparține (a se vedea în acest sens Hotărârea din 16 iulie 2020, Facebook Ireland și Schrems, C-311/18, EU:C:2020:559, punctul 147).

48 Printre sarcinile cu care sunt învestite aceste autorități de supraveghere figurează în special cea de a monitoriza aplicarea Regulamentului 2016/679 și de a asigura aplicarea acestuia, prevăzută la articolul 57 alineatul (1) litera (a) din acest regulament, precum și cea de a coopera, inclusiv prin schimb de informații, cu alte autorități de supraveghere și de a-și oferi asistență reciprocă pentru a asigura coerența aplicării și a respectării regulamentului menționat, prevăzută la articolul 57 alineatul (1) litera (g) din același regulament. Printre competențele conferite autorităților de supraveghere amintite în vederea îndeplinirii acestor sarcini figurează diverse competențe de investigare, prevăzute la articolul 58 alineatul (1) din Regulamentul 2016/679, precum și competența de a aduce în fața autorităților judiciare cazurile de încălcare a acestui regulament și, după caz, de a iniția proceduri judiciare în scopul de a asigura aplicarea dispozițiilor regulamentului menționat, prevăzută la articolul 58 alineatul (5) din acesta din urmă.

49 Îndeplinirea acestor sarcini și exercitarea acestor competențe presupun însă ca o autoritate de supraveghere să dispună de o competență în ceea ce privește o anumită prelucrare a datelor.

50 În această privință, fără a aduce atingere normei de competență enunțate la articolul 55 alineatul (1) din Regulamentul 2016/679, articolul 56 alineatul (1) din acest regulament prevede, pentru „prelucrările transfrontaliere”, în sensul articolului 4 punctul 23 din acesta, mecanismul „ghișeului unic”, întemeiat pe o repartizare a competențelor între o „autoritate de supraveghere principală” și celelalte autorități de supraveghere vizate. În temeiul acestui mecanism, autoritatea de supraveghere a sediului principal sau a sediului unic al operatorului sau al persoanei împuternicite de operator este competentă să acționeze în calitate de autoritate de supraveghere principală pentru prelucrarea transfrontalieră efectuată de respectivul operator sau respectiva persoană împuternicită în cauză în conformitate cu procedura prevăzută la articolul 60 din regulamentul menționat.

51 Acest din urmă articol stabilește procedura de cooperare dintre autoritatea de supraveghere principală și celelalte autorități de supraveghere vizate. În cadrul acestei proceduri, autoritatea de supraveghere principală este obligată, printre altele, să încerce să ajungă la un consens. În acest scop, în conformitate cu articolul 60 alineatul (3) din Regulamentul 2016/679, aceasta transmite fără întârziere un proiect de decizie celorlalte autorități de supraveghere vizate pentru a obține avizul lor și ține seama în mod corespunzător de opiniile acestora.

52 Rezultă în special din articolele 56 și 60 din Regulamentul 2016/679 că, pentru „prelucrările transfrontaliere”, în sensul articolului 4 punctul 23 din acesta, și sub rezerva articolului 56 alineatul (2) din acest regulament, diferitele autorități de supraveghere naționale vizate trebuie să coopereze, potrivit procedurii prevăzute de aceste dispoziții, pentru a ajunge la un consens și la o decizie unică ce leagă ansamblul acestor autorități și a cărei respectare trebuie asigurată de operator în ceea ce privește activitățile de prelucrare desfășurate în cadrul tuturor sediilor sale din Uniune. Pe de altă parte, articolul 61 alineatul (1) din regulamentul menționat obligă autoritățile de supraveghere, printre altele, să își furnizeze reciproc informații relevante și asistență pentru a pune în aplicare același regulament în mod coerent în ansamblul Uniunii. Articolul 63 din Regulamentul 2016/679 precizează că acesta este scopul pentru care este prevăzut mecanismul pentru asigurarea coerenței, stabilit la articolele 64 și 65 din acesta [Hotărârea din 24 septembrie 2019, Google (Întinderea teritorială a dezindexării), C-507/17, EU:C:2019:772, punctul 68].

53 Aplicarea mecanismului „ghișeului unic” impune, prin urmare, astfel cum confirmă considerentul (13) al Regulamentului 2016/679, o cooperare loială și eficientă între autoritatea de supraveghere principală și celelalte autorități de supraveghere vizate. Pentru acest motiv, după cum a arătat domnul avocat

general la punctul 111 din concluzii, autoritatea de supraveghere principală nu poate ignora punctele de vedere ale celorlalte autorități de supraveghere vizate, iar orice obiecție relevantă și motivată formulată de una dintre aceste din urmă autorități are ca efect blocarea, cel puțin temporar, a adoptării proiectului de decizie al autorității de supraveghere principale.

54 Astfel, conform articolului 60 alineatul (4) din Regulamentul 2016/679, în cazul în care oricare dintre celelalte autorități de supraveghere vizate exprimă, în termen de patru săptămâni după ce a fost consultată, o asemenea obiecție relevantă și motivată la proiectul de decizie, autoritatea de supraveghere principală, dacă nu dă curs obiecției relevante și motivate sau consideră că obiecția nu este relevantă sau motivată, sesizează mecanismul pentru asigurarea coerenței, prevăzut la articolul 63 din acest regulament, în vederea obținerii din partea Comitetului european pentru protecția datelor a unei decizii obligatorii, adoptată în temeiul articolului 65 alineatul (1) litera (a) din regulamentul menționat.

55 În schimb, potrivit articolului 60 alineatul (5) din Regulamentul 2016/679, în cazul în care intenționează să dea curs obiecției relevante și motivate formulate, autoritatea de supraveghere principală transmite celorlalte autorități de supraveghere vizate un proiect revizuit de decizie pentru a obține avizul acestora. Acest proiect revizuit de decizie face obiectul procedurii menționate la articolul 60 alineatul (4) din acest regulament în termen de două săptămâni.

56 În conformitate cu articolul 60 alineatul (7) din regulamentul menționat, autoritatea de supraveghere principală este cea care, în principiu, trebuie să adopte o decizie în ceea ce privește prelucrarea transfrontalieră vizată, să o notifice sediului principal sau sediului unic al operatorului ori al persoanei împuternicite de operator, după caz, și să informeze celelalte autorități de supraveghere vizate și Comitetul european pentru protecția datelor cu privire la decizia în cauză, incluzând un rezumat al faptelor și motivelor relevante.

57 Acestea fiind precizate, trebuie subliniat că Regulamentul 2016/679 prevede excepții de la principiul competenței decizionale a autorității de supraveghere principale în cadrul mecanismului „ghișeului unic” prevăzut la articolul 56 alineatul (1) din regulamentul menționat.

58 Printre aceste excepții figurează, în primul rând, articolul 56 alineatul (2) din Regulamentul 2016/679, care prevede că o autoritate de supraveghere care nu este autoritatea de supraveghere principală este competentă să trateze o plângere depusă în atenția sa și care privește prelucrarea transfrontalieră a datelor cu caracter personal sau o eventuală încălcare a acestui regulament în cazul în care obiectul acesteia se referă numai la un sediu aflat în statul său membru sau afectează în mod semnificativ persoane vizate numai în statul său membru.

59 În al doilea rând, articolul 66 din Regulamentul 2016/679 prevede, prin derogare de la mecanismele pentru asigurarea coerenței menționate la articolele 60 și 63-65 din acest regulament, o procedură de urgență. Această procedură de urgență permite, în circumstanțe excepționale, atunci când autoritatea de supraveghere vizată consideră că există o necesitate urgentă de a acționa în scopul protejării drepturilor și libertăților persoanelor vizate, adoptarea de îndată a unor măsuri provizorii menite să producă efecte juridice pe propriul teritoriu, cu o perioadă de valabilitate determinată, care să nu depășească trei luni, articolul 66 alineatul (2) din Regulamentul 2016/679 prevăzând, în plus, că, în cazul în care o autoritate de supraveghere a adoptat o măsură în temeiul alineatului (1) și consideră că este necesară adoptarea de urgență a unor măsuri definitive, aceasta poate solicita un aviz de urgență sau o decizie obligatorie urgentă din partea Comitetului european pentru protecția datelor, indicând motivele pentru această solicitare.

60 Această competență a autorităților de supraveghere trebuie exercitată însă cu respectarea unei cooperări loiale și eficiente cu autoritatea de supraveghere principală, în conformitate cu procedura prevăzută la articolul 56 alineatele (3)-(5) din Regulamentul 2016/679. Astfel, în această situație, în

temeiul articolului 56 alineatul (3) din acest regulament, autoritatea de supraveghere în cauză trebuie să informeze fără întârziere autoritatea de supraveghere principală, care, în termen de trei săptămâni de la momentul la care a fost informată, decide dacă va trata sau nu cazul.

61 Or, în temeiul articolului 56 alineatul (4) din Regulamentul 2016/679, în cazul în care autoritatea de supraveghere principală decide să trateze cazul, se aplică procedura de cooperare prevăzută la articolul 60 din acest regulament. În acest context, autoritatea de supraveghere care a informat autoritatea de supraveghere principală îi poate prezenta un proiect de decizie, iar aceasta din urmă trebuie să țină seama în cea mai mare măsură posibilă de acest proiect atunci când elaborează proiectul de decizie menționat la articolul 60 alineatul (3) din regulament.

62 În schimb, în temeiul articolului 56 alineatul (5) din Regulamentul 2016/679, în cazul în care autoritatea de supraveghere principală decide să nu trateze cazul, autoritatea de supraveghere care a informat autoritatea de supraveghere principală tratează cazul în conformitate cu articolele 61 și 62 din acest regulament, care impun autorităților de supraveghere respectarea unor norme de asistență reciprocă și de cooperare în cadrul operațiunilor comune în vederea asigurării unei cooperări eficiente între autoritățile vizate.

63 Din cele de mai sus rezultă că, pe de o parte, în domeniul prelucrării transfrontaliere a datelor cu caracter personal, competența autorității de supraveghere principale de a adopta o decizie prin care se constată că o astfel de prelucrare încalcă normele referitoare la protecția drepturilor persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal prevăzute în Regulamentul 2016/679 constituie regula, în timp ce competența celorlalte autorități de supraveghere vizate de a adopta o asemenea decizie, fie și cu titlu provizoriu, constituie excepția. Pe de altă parte, deși competența de principiu a autorității de supraveghere principale este confirmată la articolul 56 alineatul (6) din Regulamentul 2016/679, potrivit căruia autoritatea de supraveghere principală este „singurul interlocutor” al operatorului sau al persoanei împuternicite de operator pentru prelucrarea transfrontalieră efectuată de acest operator sau de persoana împuternicită de operator, această autoritate trebuie să exercite o astfel de competență în cadrul unei cooperări strânse cu celelalte autorități de supraveghere vizate. În special, autoritatea de supraveghere principală nu poate renunța, în exercitarea competențelor sale, după cum s-a arătat la punctul 53 din prezenta hotărâre, la un dialog indispensabil, precum și la o cooperare loială și eficace cu celelalte autorități de supraveghere vizate.

64 În această privință, reiese din considerentul (10) al Regulamentului 2016/679 că acesta din urmă urmărește, printre altele, să asigure o aplicare 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 în întreaga Uniune și să îndepărteze obstacolele din calea circulației datelor cu caracter personal în cadrul acesteia.

65 Or, un asemenea obiectiv și efectul util al mecanismului „ghișeului unic” ar putea fi compromis dacă o autoritate de supraveghere care nu este, în ceea ce privește o prelucrare transfrontalieră de date, autoritatea de supraveghere principală ar putea exercita competența prevăzută la articolul 58 alineatul (5) din Regulamentul 2016/679 în afara cazurilor în care este competentă să adopte o decizie precum cea menționată la punctul 63 din prezenta hotărâre. Astfel, exercitarea unei asemenea competențe urmărește să conducă la o decizie judecătorească obligatorie, care este la fel de susceptibilă să aducă atingere acestui obiectiv, precum și acestui mecanism ca o decizie adoptată de o autoritate de supraveghere care nu este autoritatea de supraveghere principală.

66 Contrar celor susținute de APD, împrejurarea că o autoritate de supraveghere a unui stat membru care nu este autoritatea de supraveghere principală nu poate exercita competența prevăzută la articolul 58 alineatul (5) din Regulamentul 2016/679 decât cu respectarea normelor de repartizare a competențelor decizionale prevăzute în special la articolele 55 și 56 din același regulament coroborate cu articolul 60 din acesta din urmă este conformă cu articolele 7, 8 și 47 din cartă.

67 Pe de o parte, în ceea ce privește argumentația întemeiată pe o pretinsă încălcare a articolelor 7 și 8 din cartă, trebuie amintit că articolul 7 garantează oricărei persoane dreptul la respectarea vieții sale private și de familie, a domiciliului și a secretului comunicațiilor, în timp ce articolul 8 alineatul (1) din cartă, la fel ca articolul 16 alineatul (1) TFUE, recunoaște în mod explicit oricărei persoane dreptul la protecția datelor cu caracter personal care o privesc. Or, rezultă în special din articolul 51 alineatul (1) din Regulamentul 2016/679 că autoritățile de supraveghere sunt responsabile de supravegherea aplicării acestui regulament, în special în scopul protejării drepturilor fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ale acestora. Rezultă că, în conformitate cu cele expuse la punctul 45 din prezenta hotărâre, normele de repartizare a competențelor decizionale între autoritatea de supraveghere principală și celelalte autorități de supraveghere, prevăzute în acest regulament, nu aduc atingere responsabilității care revine fiecăreia dintre aceste autorități de a contribui la un nivel ridicat de protecție a acestor drepturi, cu respectarea acestor norme, precum și a cerințelor de cooperare și de asistență reciprocă amintite la punctul 52 din prezenta hotărâre.

68 Aceasta înseamnă în special că mecanismul „ghișeului unic” nu poate conduce în niciun caz la situația în care o autoritate națională de supraveghere, în special autoritatea de supraveghere principală, nu își asumă responsabilitatea care îi revine în temeiul Regulamentului 2016/679 de a contribui la o protecție eficace a persoanelor fizice împotriva atingerilor aduse drepturilor lor fundamentale amintite la punctul anterior din prezenta hotărâre, cu riscul de a încuraja practicarea unui *forum shopping*, în special din partea operatorilor, prin care se urmărește eludarea acestor drepturi fundamentale și aplicarea efectivă a dispozițiilor acestui regulament care le implementează.

69 Pe de altă parte, în ceea ce privește argumentația întemeiată pe o pretinsă încălcare a dreptului la o cale de atac efectivă, garantat la articolul 47 din cartă, nici aceasta nu poate fi reținută. Astfel, încadrarea, expusă la punctele 64 și 65 din prezenta hotărâre, a posibilității unei alte autorități de supraveghere decât autoritatea de supraveghere principală de a exercita competența prevăzută la articolul 58 alineatul (5) din Regulamentul nr. 2016/679, în ceea ce privește o prelucrare transfrontalieră de date cu caracter personal, nu aduce atingere dreptului recunoscut oricărei persoane, prin articolul 78 alineatele (1) și (2) din acest regulament, de a formula o cale de atac jurisdicțională efectivă, printre altele împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o privește sau împotriva nesoluționării unei plângeri pe care a introdus-o de către autoritatea de supraveghere care dispune de competența decizională în temeiul articolelor 55 și 56 din regulamentul menționat coroborate cu articolul 60 din acesta din urmă.

70 Aceasta este în special situația ipotezei enunțate la articolul 56 alineatul (5) din Regulamentul 2016/679, în temeiul căreia, așa cum s-a arătat la punctul 62 din prezenta hotărâre, autoritatea de supraveghere care a transmis informația în temeiul articolului 56 alineatul (3) din acest regulament poate trata cazul în conformitate cu articolele 61 și 62 din acesta, dacă autoritatea de supraveghere principală decide, după ce a fost informată, că nu îl va trata ea însăși. În cadrul unei astfel de examinări nu se poate de altfel exclude ca autoritatea de supraveghere vizată să poată decide, dacă este cazul, să exercite competența pe care i-o conferă articolul 58 alineatul (5) din Regulamentul 2016/679.

71 Acestea fiind precizate, trebuie subliniat că exercitarea competenței unei autorități de supraveghere a unui stat membru de a se adresa instanțelor din statul său nu poate fi exclusă atunci când, după ce a solicitat asistența reciprocă a autorității de supraveghere principale, în temeiul articolului 61 din Regulamentul 2016/679, aceasta din urmă nu îi furnizează informațiile solicitate. În această situație, în temeiul articolului 61 alineatul (8) din acest regulament, autoritatea de supraveghere în cauză poate adopta o măsură provizorie pe teritoriul propriului stat membru și, în cazul în care consideră că este necesară adoptarea de urgență a unor măsuri definitive, această autoritate poate, în conformitate cu articolul 66 alineatul (2) din regulamentul menționat, să solicite un aviz de urgență sau o decizie obligatorie urgentă din partea Comitetului european pentru protecția datelor. În plus, în temeiul articolului 64 alineatul (2) din același regulament, o autoritate de supraveghere poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru să fie

examinată de Comitetul european pentru protecția datelor în vederea obținerii unui aviz, în special în cazul în care o autoritate de supraveghere competentă nu respectă obligațiile privind asistența reciprocă care îi revin conform articolului 61 din acesta. Or, în urma adoptării unui astfel de aviz sau a unei asemenea decizii și cu condiția ca, după luarea în considerare a tuturor împrejurărilor relevante, Comitetul european pentru protecția datelor să fie favorabil în acest sens, autoritatea de supraveghere în cauză trebuie să ia măsurile necesare în vederea respectării normelor referitoare la protecția drepturilor persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal care sunt prevăzute în Regulamentul 2016/679 și, în acest scop, să exercite competența care îi este conferită prin articolul 58 alineatul (5) din acest regulament.

72 Astfel, partajarea competențelor și a responsabilităților între autoritățile de supraveghere se întemeiază în mod necesar pe premisa unei cooperări loiale și eficiente între aceste autorități, precum și cu Comisia pentru a asigura aplicarea corectă și coerentă a acestui regulament, după cum confirmă articolul 51 alineatul (2) din acesta.

73 În speță, va reveni instanței de trimitere sarcina de a stabili dacă normele de repartizare a competențelor, precum și procedurile și mecanismele relevante prevăzute de Regulamentul 2016/679 au fost aplicate în mod corect în cadrul cauzei principale. Acesteia îi va reveni mai ales sarcina de a verifica dacă, deși APD nu este autoritatea de supraveghere principală în această cauză, prelucrarea în discuție, în măsura în care vizează comportamente ale rețelei sociale online Facebook ulterioare datei de 25 mai 2018, se încadrează în special în situația vizată la punctul 71 din prezenta hotărâre.

74 În această privință, Curtea observă că, în Avizul 5/2019 din 12 martie 2019, referitor la interacțiunea dintre Directiva privind viața privată și comunicațiile electronice și [Regulamentul general privind protecția datelor], în special în ceea ce privește competența, sarcinile și prerogativele autorităților pentru protecția datelor, Comitetul european pentru protecția datelor a declarat că înregistrarea și lectura datelor cu caracter personal prin intermediul unor cookie-uri țineau de domeniul de aplicare al Directivei 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO 2002, L 201, p. 37, Ediție specială, 13/vol. 36, p. 63), iar nu de mecanismul „ghișeului unic”. În schimb, toate operațiunile anterioare și activitățile ulterioare de prelucrare a acestor date cu caracter personal prin intermediul altor tehnologii intră, într-adevăr, în domeniul de aplicare al Regulamentului 2016/679 și, în consecință, al mecanismului „ghișeului unic”. Dat fiind că cererea sa de asistență reciprocă privea aceste operațiuni ulterioare de prelucrare a datelor cu caracter personal, APD a solicitat, în luna aprilie 2019, Comisarului pentru protecția datelor să dea curs cererii sale cât mai rapid posibil, cerere care nu ar fi primit niciun răspuns.

75 Având în vedere ansamblul considerațiilor care precedă, trebuie să se răspundă la prima întrebare adresată că articolul 55 alineatul (1) și articolele 56-58, precum și articolele 60-66 din Regulamentul 2016/679 coroborate cu articolele 7, 8 și 47 din cartă trebuie interpretate în sensul că o autoritate de supraveghere a unui stat membru care, în temeiul legislației naționale adoptate în aplicarea articolului 58 alineatul (5) din acest regulament, are competența de a aduce în fața unei instanțe din acest stat membru orice pretins caz de încălcare a regulamentului menționat și, după caz, de a iniția proceduri judiciare poate exercita această competență în ceea ce privește o prelucrare de date transfrontalieră, în condițiile în care ea nu este „autoritatea de supraveghere principală”, în sensul articolului 56 alineatul (1) din același regulament, în ceea ce privește această prelucrare de date, atât timp cât este vorba despre una dintre situațiile în care Regulamentul 2016/679 îi conferă acestei autorități de supraveghere competența de a adopta o decizie prin care se constată că prelucrarea menționată încalcă normele prevăzute de acesta, precum și cu respectarea procedurilor de cooperare și de asigurare a coerenței prevăzute de acest regulament.

Cu privire la a doua întrebare

76 Prin intermediul celei de a doua întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolul 58 alineatul (5) din Regulamentul nr. 2016/679 trebuie interpretat în sensul că, în cazul prelucrării datelor transfrontaliere, exercitarea competenței de către o autoritate de supraveghere a unui stat membru, alta decât autoritatea de supraveghere principală, de a iniția o procedură judiciară, în sensul acestei dispoziții, impune ca operatorul prelucrării transfrontaliere de date cu caracter personal împotriva căruia această acțiune este introdusă să dispună de un „sediu principal", în sensul articolului 4 punctul 16 din Regulamentul nr. 2016/679, pe teritoriul acestui stat membru sau de un alt sediu pe acest teritoriu.

77 În această privință trebuie amintit că, potrivit articolului 55 alineatul (1) din Regulamentul 2016/679, fiecare 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.

78 Articolul 58 alineatul (5) din Regulamentul 2016/679 prevede, în plus, competența fiecărei autorități de supraveghere de a aduce în fața unei instanțe din statul său membru orice pretins caz de încălcare a acestui regulament și, după caz, de a iniția proceduri judiciare, în scopul de a asigura aplicarea dispozițiilor regulamentului menționat.

79 Or, este necesar să se arate că articolul 58 alineatul (5) din Regulamentul 2016/679 este formulat în termeni generali și că legiuitorul Uniunii nu a subordonat exercitarea acestei competențe de către o autoritate de supraveghere a unui stat membru condiției ca acțiunea acesteia din urmă să fie intentată împotriva unui operator care dispune de un „sediu principal", în sensul articolului 4 punctul 16 din acest regulament, sau de un alt sediu pe teritoriul acestui stat membru.

80 Cu toate acestea, o autoritate de supraveghere a unui stat membru nu își poate exercita competența pe care i-o conferă articolul 58 alineatul (5) din Regulamentul 2016/679 decât dacă se stabilește că această competență intră în domeniul de aplicare teritorial al acestui regulament.

81 Articolul 3 din Regulamentul 2016/679, care reglementează domeniul de aplicare teritorial al acestui regulament, prevede în această privință, la alineatul (1), că acesta se aplică prelucrării datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.

82 În acest sens, considerentul (22) al Regulamentului nr. 2016/679 precizează că un astfel de sediu presupune exercitarea efectivă și reală a unei activități în cadrul unor înțelegeri stabile și că forma juridică a unor astfel de înțelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință.

83 Rezultă că, în conformitate cu articolul 3 alineatul (1) din Regulamentul 2016/679, domeniul de aplicare teritorial al acestui regulament este determinat, sub rezerva ipotezelor prevăzute la alineatele (2) și (3) ale acestui articol, de condiția ca operatorul sau persoana împuternicită de operator să dispună de un sediu pe teritoriul Uniunii.

84 Prin urmare, este necesar să se răspundă la a doua întrebare adresată că articolul 58 alineatul (5) din Regulamentul 2016/679 trebuie interpretat în sensul că, în cazul prelucrării datelor transfrontaliere, exercitarea competenței de către o autoritate de supraveghere a unui stat membru, alta decât autoritatea de supraveghere principală, de a iniția o procedură judiciară, în sensul acestei dispoziții, nu impune ca operatorul sau persoana împuternicită de operator în ceea ce privește prelucrarea transfrontalieră de date cu caracter personal împotriva căruia această acțiune este introdusă să dispună de un sediu principal sau de un alt sediu pe teritoriul acestui stat membru.

Cu privire la a treia întrebare

85 Prin intermediul celei de a treia întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolul 58 alineatul (5) din Regulamentul 2016/679 trebuie interpretat în sensul că, în cazul prelucrării datelor transfrontaliere, exercitarea competenței unei autorități de supraveghere a unui stat membru, alta decât autoritatea de supraveghere principală, de a aduce în fața unei instanțe din acest stat orice pretins caz de încălcare a acestui regulament și, după caz, de a iniția proceduri judiciare, în sensul acestei dispoziții, impune ca autoritatea de supraveghere vizată să își îndrepte acțiunea în justiție împotriva sediului principal al operatorului sau împotriva sediului care se află în propriul său stat membru.

86 Din decizia de trimitere reiese că această întrebare este ridicată în cadrul unei dezbateri între părți cu privire la aspectul dacă instanța de trimitere este competentă să examineze acțiunea în încetare în măsura în care este introdusă împotriva Facebook Belgium, ținând seama de faptul că, pe de o parte, în cadrul Uniunii, sediul social al grupului Facebook este situat în Irlanda, iar Facebook Ireland este operatorul exclusiv al colectării și prelucrării datelor cu caracter personal pentru întregul teritoriu al Uniunii și că, pe de altă parte, în virtutea unei repartizări interne acestui grup, sediul situat în Belgia ar fi fost creat, cu titlu principal, pentru a permite grupului menționat să întrețină relații cu instituțiile Uniunii și, cu titlu accesoriu, pentru a promova activitățile publicitare și de marketing ale aceluiași grup destinate persoanelor cu reședința în Belgia.

87 Astfel cum s-a arătat la punctul 47 din prezenta hotărâre, articolul 55 alineatul (1) din Regulamentul 2016/679 stabilește competența de principiu a fiecărei autorități de supraveghere de a îndeplini sarcinile și de a exercita competențele cu care este învestită, în conformitate cu acest regulament, pe teritoriul statului membru de care aparține.

88 În ceea ce privește competența unei autorități de supraveghere a unui stat membru de a iniția proceduri judiciare, în sensul articolului 58 alineatul (5) din Regulamentul 2016/679, trebuie amintit, după cum a arătat domnul avocat general la punctul 150 din concluzii, că această dispoziție este formulată în termeni generali și că nu precizează entitățile împotriva cărora autoritățile de supraveghere ar trebui sau ar putea îndrepta o procedură judiciară cu privire la orice încălcare a acestui regulament.

89 În consecință, dispoziția menționată nu limitează exercitarea competenței de a acționa în justiție în sensul că o astfel de acțiune ar putea fi introdusă numai împotriva unui „sediu principal” sau împotriva unui alt „sediu” al operatorului. Dimpotrivă, în temeiul aceleiași dispoziții, atunci când autoritatea de supraveghere a unui stat membru dispune de competența necesară în acest scop, în temeiul articolelor 55 și 56 din Regulamentul 2016/679, aceasta poate exercita competențele care îi sunt conferite prin acest regulament pe teritoriul său național, indiferent de statul membru în care este stabilit operatorul sau persoana împuternicită de operator.

90 Cu toate acestea, exercitarea competenței conferite fiecărei autorități de supraveghere la articolul 58 alineatul (5) din Regulamentul 2016/679 presupune ca acest regulament să fie aplicabil. În această privință și după cum s-a subliniat la punctul 81 din prezenta hotărâre, articolul 3 alineatul (1) din regulamentul menționat prevede că acesta se aplică prelucrării datelor cu caracter personal efectuate „în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii”.

91 Având în vedere obiectivul urmărit de Regulamentul 2016/679, constând în a asigura protecția eficientă a drepturilor și a libertăților fundamentale ale persoanelor fizice, în special dreptul lor la protecția vieții private și la protecția datelor cu caracter personal, condiția potrivit căreia prelucrarea datelor cu caracter personal trebuie efectuată „în cadrul activităților” sediului vizat nu poate primi o interpretare restrictivă (a se vedea prin analogie Hotărârea din 5 iunie 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, punctul 56 și jurisprudența citată).

92 În speță, din decizia de trimitere și din observațiile scrise depuse de Facebook Belgium reiese că aceasta este însărcinată, cu titlu principal, să întrețină relații cu instituțiile Uniunii și, cu titlu accesoriu, să promoveze activitățile publicitare și de marketing ale grupului său destinate persoanelor cu reședința în Belgia.

93 Prelucrarea datelor cu caracter personal în discuție în litigiul principal, care este efectuată pe teritoriul Uniunii exclusiv de Facebook Ireland și care constă în colectarea de informații cu privire la comportamentul de navigare atât al deținătorilor unui cont Facebook, cât și al neutilizatorilor serviciilor Facebook, prin intermediul diferitor tehnologii, cum ar fi în special extensiile pentru social media și pixelii, are ca obiectiv tocmai să permită rețelei sociale în cauză să își facă sistemul de publicitate mai performant prin difuzarea comunicațiilor în mod orientat.

94 Or, este necesar să se arate că, pe de o parte, o rețea socială precum Facebook generează o parte substanțială din veniturile sale în special datorită publicității care este difuzată în acest stat și că activitatea desfășurată de sediul situat în Belgia este destinată să asigure în acest stat membru, fie și numai în mod accesoriu, promovarea și vânzarea de spații publicitare care servesc la rentabilizarea serviciilor Facebook. Pe de altă parte, activitatea exercitată cu titlu principal de Facebook Belgium, care constă în întreținerea unor relații cu instituțiile Uniunii și în constituirea unui punct de contact cu acestea din urmă, urmărește în special stabilirea politicii de prelucrare a datelor cu caracter personal de către Facebook Ireland.

95 În aceste condiții, trebuie să se considere că activitățile sediului grupului Facebook situat în Belgia sunt legate în mod indisociabil de prelucrarea datelor cu caracter personal în discuție în litigiul principal, Facebook Ireland fiind operatorul în ceea ce privește teritoriul Uniunii. Prin urmare, o astfel de prelucrare trebuie privită ca fiind efectuată „în cadrul activităților unui sediu al operatorului”, în sensul articolului 3 alineatul (1) din Regulamentul 2016/679.

96 Având în vedere ansamblul considerațiilor care precedă, trebuie să se răspundă la a treia întrebare adresată că articolul 58 alineatul (5) din Regulamentul 2016/679 trebuie interpretat în sensul că competența unei autorități de supraveghere a unui stat membru, alta decât autoritatea de supraveghere principală, de a aduce în fața unei instanțe din acest stat orice pretins caz de încălcare a acestui regulament și, după caz, de a iniția proceduri judiciare, în sensul acestei dispoziții, poate fi exercitată atât în ceea ce privește sediul principal al operatorului care se află în statul membru de care aparține această autoritate, cât și în ceea ce privește un alt sediu al acestui operator, cu condiția ca acțiunea în justiție să vizeze o prelucrare a datelor efectuată în cadrul activităților acestui sediu și ca autoritatea menționată să fie competentă să exercite această competență, în conformitate cu ceea ce este expus în răspunsul la prima întrebare adresată.

Cu privire la a patra întrebare

97 Prin intermediul celei de a patra întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolul 58 alineatul (5) din Regulamentul nr. 2016/679 trebuie interpretat în sensul că, atunci când o autoritate de supraveghere a unui stat membru care nu este „autoritate de supraveghere principală”, în sensul articolului 56 alineatul (1) din acest regulament, a introdus anterior datei de 25 mai 2018 o acțiune în justiție privind o prelucrare transfrontalieră de date cu caracter personal, și anume înainte de data la care regulamentul menționat a devenit aplicabil, această împrejurare este de natură să influențeze condițiile în care această autoritate de supraveghere a unui stat membru poate exercita competența de a iniția proceduri judiciare pe care o deține în temeiul acestui articol 58 alineatul (5).

98 Astfel, în fața acestei instanțe, Facebook Ireland, Facebook Inc. și Facebook Belgium arată că aplicarea Regulamentului 2016/679 începând cu 25 mai 2018 ar avea drept consecință faptul că menținerea unei acțiuni introduse anterior acestei date este inadmisibilă sau chiar nefondată.

99 Trebuie arătat, cu titlu introductiv, că articolul 99 alineatul (1) din Regulamentul 2016/679 prevede că acesta intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*. Întrucât acest regulament a fost publicat în Jurnalul Oficial la 4 mai 2016, el a intrat, așadar, în vigoare la 25 mai. În plus, articolul 99 alineatul (2) din regulamentul menționat prevede că acesta se aplică de la 25 mai 2018.

100 În această privință trebuie amintit că o normă de drept nouă se aplică începând de la intrarea în vigoare a actului care o instituie și că, deși aceasta nu se aplică situațiilor juridice născute și care au devenit definitive sub imperiul legii vechi, ea se aplică efectelor viitoare ale acestora, precum și situațiilor juridice noi. Soluția este diferită, sub rezerva respectării principiului neretroactivității actelor juridice, numai dacă noua normă este însoțită de dispoziții speciale care stabilesc în mod specific condițiile de aplicare în timp a acesteia. În special, se consideră în general că normele de procedură se aplică de la data intrării lor în vigoare, spre deosebire de normele de drept substanțial, care sunt interpretate de regulă în sensul că nu vizează situații apărute anterior intrării lor în vigoare decât în măsura în care rezultă în mod clar din formularea, din finalitatea sau din economia acestora că trebuie să le fie atribuit un asemenea efect [Hotărârea din 25 februarie 2021, Caisse pour l'avenir des enfants (Ocuparea unui loc de muncă la naștere), C-129/20 P, EU:C:2021:140, punctul 31 și jurisprudența citată].

101 Regulamentul 2016/679 nu conține nicio normă tranzitorie și nicio altă normă care să reglementeze statutul procedurilor judiciare inițiate înainte de aplicarea acestuia și care erau în curs la data la care a devenit aplicabil. În special, nicio dispoziție din acest regulament nu prevede că acesta are ca efect încetarea tuturor procedurilor judiciare pendinte la data de 25 mai 2018 care vizează pretinse încălcări ale unor norme care reglementează prelucrarea datelor cu caracter personal prevăzute de Directiva 95/46, chiar dacă comportamentele constitutive ale unor astfel de pretinse încălcări persistă după această dată.

102 În speță, articolul 58 alineatul (5) din Regulamentul 2016/679 prevede norme care reglementează competența unei autorități de supraveghere de a aduce în fața autorităților judiciare cazurile de încălcare a acestui regulament și, după caz, de a iniția sau de a se implica într-un alt mod în proceduri judiciare în scopul de a asigura aplicarea dispozițiilor regulamentului menționat.

103 În aceste condiții, este necesar să se distingă între acțiunile introduse de o autoritate de supraveghere a unui stat membru pentru încălcări ale normelor de protecție a datelor cu caracter personal săvârșite de operatori sau de persoane împuternicite de operatori înainte de data la care Regulamentul 2016/679 a devenit aplicabil și cele introduse pentru încălcări săvârșite după această dată.

104 În prima situație, din punctul de vedere al dreptului Uniunii, o acțiune în justiție precum cea în discuție în litigiul principal poate fi menținută în temeiul dispozițiilor Directivei 95/46, care rămâne aplicabilă în ceea ce privește încălcările săvârșite până la data abrogării sale, și anume 25 mai 2018. În cea de a doua situație, o astfel de acțiune poate fi introdusă, în temeiul articolului 58 alineatul (5) din Regulamentul 2016/679, numai cu condiția ca, după cum s-a subliniat în cadrul răspunsului la prima întrebare adresată, această acțiune să intre sub incidența unei situații în care, cu titlu de excepție, acest regulament conferă unei autorități de supraveghere a unui stat membru care nu este „autoritatea de supraveghere principală" o competență de a adopta o decizie prin care să se constate că prelucrarea datelor în cauză nu respectă normele cuprinse în regulamentul menționat în ceea ce privește protecția drepturilor persoanelor fizice în raport cu prelucrarea datelor cu caracter personal, cu respectarea procedurilor prevăzute de același regulament.

105 Având în vedere ansamblul considerațiilor care precedă, este necesar să se răspundă la a patra întrebare adresată că articolul 58 alineatul (5) din Regulamentul 2016/679 trebuie interpretat în sensul că, atunci când o autoritate de supraveghere a unui stat membru care nu este „autoritatea de supraveghere principală", în sensul articolului 56 alineatul (1) din acest regulament, a introdus anterior datei de 25 mai 2018 o acțiune în justiție vizând o prelucrare transfrontalieră de date cu

caracter personal, și anume înainte de data la care regulamentul menționat a devenit aplicabil, această acțiune poate, din punctul de vedere al dreptului Uniunii, să fie menținută în temeiul dispozițiilor Directivei 95/46, care rămâne aplicabilă în ceea ce privește încălcările normelor pe care le prevede săvârșite până la data la care această directivă a fost abrogată. În plus, acțiunea menționată poate fi introdusă de această autoritate pentru încălcări săvârșite după această dată, în temeiul articolului 58 alineatul (5) din Regulamentul 2016/679, cu condiția ca aceasta să intre sub incidența uneia dintre situațiile în care, cu titlu de excepție, acest regulament conferă unei autorități de supraveghere a unui stat membru care nu este „autoritatea de supraveghere principală” o competență de a adopta o decizie prin care să se constate că prelucrarea datelor în cauză încalcă normele cuprinse în regulamentul menționat în ceea ce privește protecția drepturilor persoanelor fizice în raport cu prelucrarea datelor cu caracter personal și cu respectarea procedurilor de cooperare și de asigurare a coerenței prevăzute de același regulament, aspecte a căror verificare revine instanței de trimitere.

Cu privire la a cincea întrebare

106 Prin intermediul celei de a cincea întrebări, instanța de trimitere solicită în esență, în cazul unui răspuns afirmativ la prima întrebare adresată, să se stabilească dacă articolul 58 alineatul (5) din Regulamentul 2016/679 trebuie interpretat în sensul că această dispoziție are efect direct, astfel încât o autoritate națională de supraveghere poate invoca dispoziția menționată pentru a intenta sau a relua o acțiune împotriva unor particulari chiar dacă această dispoziție nu ar fi fost pusă în aplicare în mod specific în legislația statului membru în cauză.

107 Potrivit articolului 58 alineatul (5) din Regulamentul 2016/679, fiecare stat membru prevede, pe cale legislativă, faptul că autoritatea sa de supraveghere are competența de a aduce în fața autorităților judiciare cazurile de încălcare a acestui regulament și, după caz, de a iniția sau de a se implica într-un alt mod în proceduri judiciare, în scopul de a asigura aplicarea dispozițiilor regulamentului menționat.

108 Cu titlu introductiv, trebuie să se arate că, după cum susține guvernul belgian, articolul 58 alineatul (5) din Regulamentul 2016/679 a fost pus în aplicare în ordinea juridică belgiană prin articolul 6 din Legea din 3 decembrie 2017. Astfel, potrivit acestui articol 6, care are o formulare în esență identică cu cea a articolului 58 alineatul (5) din Regulamentul 2016/679, APD are competența de a sesiza autoritățile judiciare cu privire la orice încălcare a principiilor fundamentale ale protecției datelor cu caracter personal în cadrul acestei legi și al legilor care conțin dispoziții privind protecția prelucrării datelor cu caracter personal și, dacă este cazul, de a intenta acțiuni în justiție pentru aplicarea acestor principii fundamentale. În consecință, trebuie să se considere că APD se poate întemeia pe o dispoziție de drept național precum articolul 6 din Legea din 3 decembrie 2017, care pune în aplicare articolul 58 alineatul (5) din Regulamentul 2016/679 în dreptul belgian, pentru a iniția acțiuni în justiție în vederea asigurării respectării acestui regulament.

109 Pe de altă parte, din motive de exhaustivitate, este necesar să se arate că, în temeiul articolului 288 al doilea paragraf TFUE, un regulament este obligatoriu în toate elementele sale și este direct aplicabil în fiecare stat membru, astfel încât dispozițiile acestuia nu necesită, în principiu, nicio măsură de aplicare a statelor membre.

110 În această privință trebuie amintit că, potrivit unei jurisprudențe consacrate a Curții, în temeiul articolului 288 TFUE și având în vedere însăși natura regulamentelor și funcția lor în sistemul de izvoare ale dreptului Uniunii, dispozițiile regulamentelor menționate au în general un efect imediat în ordinile juridice naționale, fără a fi necesar ca autoritățile naționale să adopte măsuri de aplicare. Cu toate acestea, unele dintre aceste dispoziții pot necesita, pentru punerea lor în aplicare, adoptarea unor măsuri de aplicare de către statele membre (Hotărârea din 15 martie 2017, Al Chodor, C-528/15, EU:C:2017:213, punctul 27 și jurisprudența citată).

111 Or, astfel cum a arătat domnul avocat general în esență la punctul 167 din concluzii, articolul 58 alineatul (5) din Regulamentul 2016/679 prevede o normă specifică și direct aplicabilă în temeiul căreia autoritățile de supraveghere trebuie să aibă calitate procesuală activă în fața instanțelor naționale și să aibă competența de a iniția proceduri judiciare în temeiul dreptului național.

112 Din articolul 58 alineatul (5) din Regulamentul 2016/679 nu reiese că statele membre ar trebui să stabilească printr-o dispoziție explicită care sunt împrejurările în care autoritățile naționale de supraveghere pot iniția proceduri judiciare, în sensul acestei dispoziții. Este suficient ca autoritatea de supraveghere să aibă posibilitatea, în conformitate cu legislația națională, să sesizeze autoritățile judiciare în legătură cu încălcările acestui regulament și, după caz, să acționeze în justiție sau să declanșeze în alt mod o procedură prin care se urmărește aplicarea dispozițiilor regulamentului menționat.

113 Având în vedere ansamblul considerațiilor care precedă, este necesar să se răspundă la a cincea întrebare adresată că articolul 58 alineatul (5) din Regulamentul 2016/679 trebuie interpretat în sensul că această dispoziție are efect direct, astfel încât o autoritate națională de supraveghere poate invoca dispoziția menționată pentru a intenta sau a relua o acțiune împotriva unor particulari chiar dacă această dispoziție nu a fost pusă în aplicare în mod specific în legislația statului membru în cauză.

Cu privire la a șasea întrebare

114 Prin intermediul celei de a șasea întrebări, instanța de trimitere solicită în esență să se stabilească, în cazul unui răspuns afirmativ la prima-a cincea întrebare adresate, dacă rezultatul unei proceduri judiciare inițiate de o autoritate de supraveghere a unui stat membru cu privire la prelucrarea transfrontalieră de date cu caracter personal poate împiedica autoritatea de supraveghere principală să adopte o decizie în care ajunge la o constatare în sens contrar în cazul în care aceasta efectuează o anchetă cu privire la aceleași activități de prelucrare transfrontalieră sau la activități similare, în conformitate cu mecanismul prevăzut la articolele 56 și 60 din Regulamentul 2016/679.

115 În această privință trebuie amintit că, potrivit unei jurisprudențe constante, întrebările referitoare la interpretarea dreptului Uniunii beneficiază de o prezumție de pertinență. Refuzul Curții de a se pronunța asupra unei întrebări preliminare adresate de o instanță națională este posibil numai dacă este evident că interpretarea solicitată a unei norme a Uniunii nu are nicio legătură cu realitatea sau cu obiectul litigiului principal, atunci când problema este de natură ipotetică sau atunci când Curtea nu dispune de elementele de fapt și de drept necesare pentru a răspunde în mod util la întrebările care i-au fost adresate (Hotărârea din 16 iunie 2015, Gauweiler și alții, C-62/14, EU:C:2015:400, punctul 25, precum și Hotărârea din 7 februarie 2018, American Express, C-304/16, EU:C:2018:66, punctul 32).

116 În plus, în conformitate cu o jurisprudență de asemenea constantă, justificarea trimiterii preliminare nu este formularea unor opinii consultative cu privire la probleme generale sau ipotetice, ci nevoia inerentă soluționării efective a unui litigiu (Hotărârea din 10 decembrie 2018, Wightman și alții, C-621/18, EU:C:2018:999, punctul 28, precum și jurisprudența citată).

117 În speță, trebuie subliniat că, astfel cum arată guvernul belgian, a șasea întrebare adresată se întemeiază pe împrejurări despre care nu s-a stabilit nicidecum că s-ar prezenta în cadrul litigiului principal, și anume faptul că, pentru prelucrarea transfrontalieră care face obiectul acestui litigiu, ar exista o autoritate de supraveghere principală care nu numai că ar ancheta aceleași activități de prelucrare transfrontalieră de date cu caracter personal ca acelea care fac obiectul procedurii judiciare inițiate de autoritatea de supraveghere a statului membru în cauză sau activități similare, ci și ar intenționa să adopte o decizie care să ajungă la o constatare în sens contrar.

118 În aceste condiții, trebuie arătat că a șasea întrebare adresată nu are nicio legătură cu realitatea sau cu obiectul litigiului principal și privește o problemă ipotetică. În consecință, această întrebare trebuie declarată inadmisibilă.

Cu privire la cheltuielile de judecată

119 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 55 alineatul (1) și articolele 56-58, precum și articolele 60-66 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) coroborate cu articolele 7, 8 și 47 din Carta drepturilor fundamentale a Uniunii Europene trebuie interpretate în sensul că o autoritate de supraveghere a unui stat membru care, în temeiul legislației naționale adoptate în aplicarea articolului 58 alineatul (5) din acest regulament, are competența de a aduce în fața unei instanțe din acest stat membru orice pretins caz de încălcare a regulamentului menționat și, după caz, de a iniția proceduri judiciare poate exercita această competență în ceea ce privește o prelucrare de date transfrontalieră, în condițiile în care ea nu este „autoritatea de supraveghere principală”, în sensul articolului 56 alineatul (1) din același regulament, în ceea ce privește această prelucrare de date, atât timp cât este vorba despre una dintre situațiile în care Regulamentul 2016/679 îi conferă acestei autorități de supraveghere competența de a adopta o decizie prin care se constată că prelucrarea menționată încalcă normele prevăzute de acesta, precum și cu respectarea procedurilor de cooperare și de asigurare a coerenței prevăzute de acest regulament.**

2) **Articolul 58 alineatul (5) din Regulamentul 2016/679 trebuie interpretat în sensul că, în cazul prelucrării transfrontaliere a datelor, exercitarea competenței unei autorități de supraveghere a unui stat membru, alta decât autoritatea de supraveghere principală, de a iniția o procedură judiciară, în sensul acestei dispoziții, nu impune ca operatorul sau persoana împuternicită de operator în privința prelucrării transfrontaliere de date cu caracter personal împotriva căruia este intentată această acțiune să dispună de un sediu principal sau de un alt sediu pe teritoriul acestui stat membru.**

3) **Articolul 58 alineatul (5) din Regulamentul 2016/679 trebuie interpretat în sensul că competența unei autorități de supraveghere a unui stat membru, alta decât autoritatea de supraveghere principală, de a aduce în fața unei instanțe din acest stat orice pretins caz de încălcare a acestui regulament și, după caz, de a iniția proceduri judiciare, în sensul acestei dispoziții, poate fi exercitată atât în ceea ce privește sediul principal al operatorului care se află în statul membru de care aparține această autoritate, cât și în ceea ce privește un alt sediu al acestui operator, cu condiția ca acțiunea în justiție să vizeze o prelucrare a datelor efectuată în cadrul activităților acestui sediu și ca autoritatea menționată să fie competentă să exercite această competență, în conformitate cu ceea ce este expus în răspunsul la prima întrebare preliminară adresată.**

4) **Articolul 58 alineatul (5) din Regulamentul 2016/679 trebuie interpretat în sensul că, atunci când o autoritate de supraveghere a unui stat membru care nu este „autoritatea de supraveghere principală”, în sensul articolului 56 alineatul (1) din acest regulament, a**

introdus anterior datei de 25 mai 2018 o acțiune în justiție vizând o prelucrare transfrontalieră de date cu caracter personal, și anume înainte de data la care regulamentul menționat a devenit aplicabil, această acțiune poate, din punctul de vedere al dreptului Uniunii, să fie menținută în temeiul dispozițiilor Directivei 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, care rămâne aplicabilă în ceea ce privește încălcările normelor pe care le prevede săvârșite până la data la care această directivă a fost abrogată. În plus, acțiunea menționată poate fi introdusă de această autoritate pentru încălcări săvârșite după această dată, în temeiul articolului 58 alineatul (5) din Regulamentul 2016/679, cu condiția ca aceasta să intre sub incidența uneia dintre situațiile în care, cu titlu de excepție, acest regulament conferă unei autorități de supraveghere a unui stat membru care nu este „autoritatea de supraveghere principală” o competență de a adopta o decizie prin care să se constate că prelucrarea datelor în cauză încalcă normele cuprinse în regulamentul menționat în ceea ce privește protecția drepturilor persoanelor fizice în raport cu prelucrarea datelor cu caracter personal și cu respectarea procedurilor de cooperare și de asigurare a coerenței prevăzute de același regulament, aspecte a căror verificare revine instanței de trimitere.

5) **Articolul 58 alineatul (5) din Regulamentul 2016/679 trebuie interpretat în sensul că această dispoziție are efect direct, astfel încât o autoritate națională de supraveghere poate invoca dispoziția menționată pentru a intenta sau a relua o acțiune împotriva unor particulari chiar dacă această dispoziție nu a fost pusă în aplicare în mod specific în legislația statului membru în cauză.**

Semnături