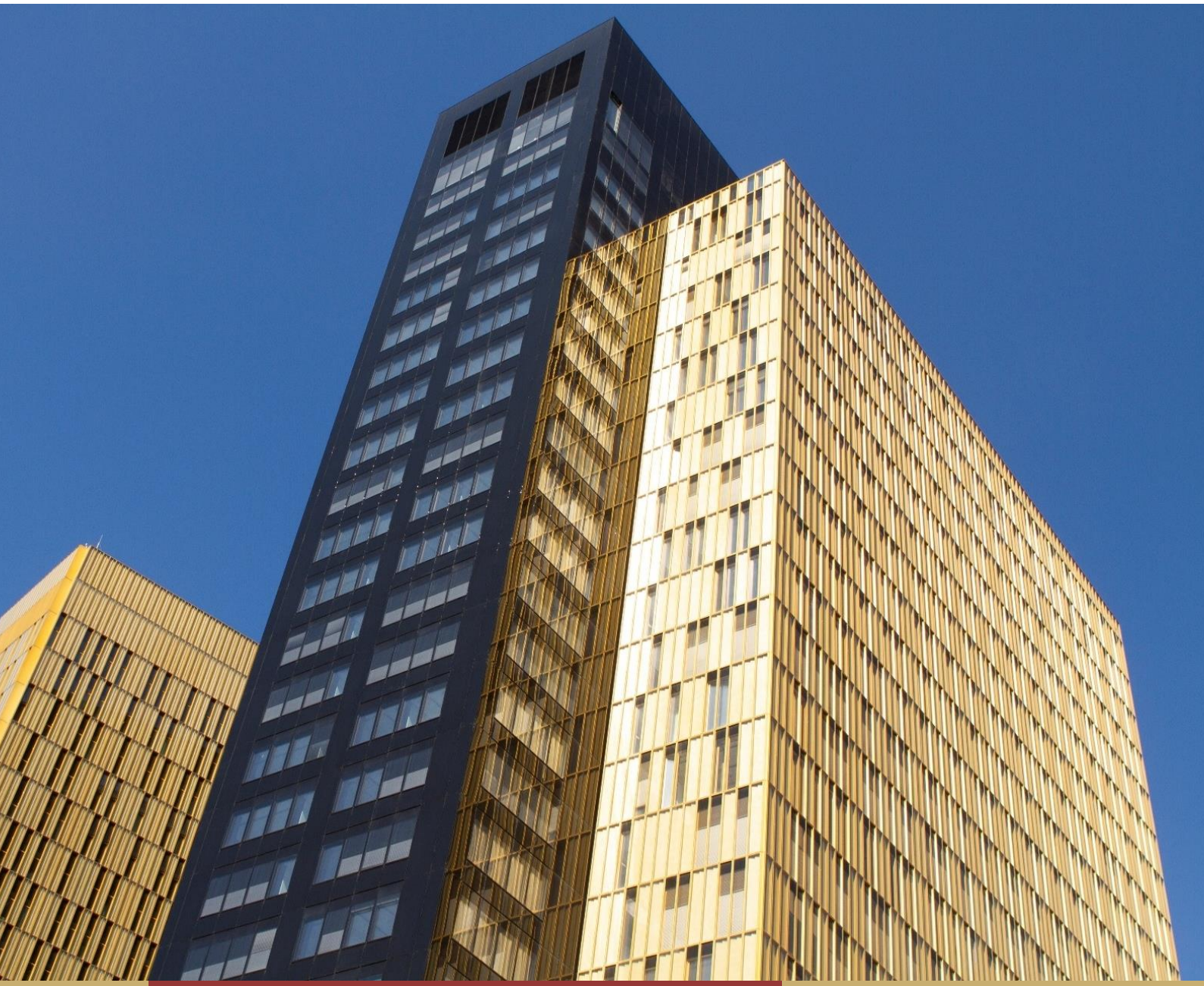
CURTEA DE JUSTIȚIE
A UNIUNII EUROPENE

RO



Fișă tematică

Protecția datelor cu caracter personal

Direcția cercetare și documentare

curia.europa.eu

Cuvânt-înainte

Dreptul la protecția datelor cu caracter personal este un drept fundamental, a cărui respectare reprezintă un obiectiv important pentru Uniunea Europeană.

El este consacrat în dreptul primar, în special la articolul 8 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”), precum și la articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE). În plus, acest drept fundamental este strâns legat de dreptul la respectarea vieții private și de familie, consacrat la articolul 7 din cartă.

În ceea ce privește dreptul derivat, începând cu mijlocul anilor ’90, Comunitatea Europeană a instituit o serie de instrumente menite să asigure protecția datelor cu caracter personal. Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date[1], abrogată din anul 2018, a constituit în această privință principalul act juridic al Uniunii în domeniu.

Directiva 2002/58/CE[2] a completat ulterior Directiva 95/46 prin armonizarea dispozițiilor legislației statelor membre referitoare la protecția dreptului la viață privată, în special în ceea ce privește prelucrarea datelor cu caracter personal în sectorul comunicațiilor electronice[3]. Trebuie menționat că, pentru a ține seama de noile evoluții tehnologice și comerciale, legiuitorul Uniunii a început din anul 2017 revizuirea acestei directive[4], aceasta aflându-se încă în curs[5].

În anul 2016, Uniunea Europeană a reformat cadrul juridic global în acest domeniu. În acest scop, ea a adoptat Regulamentul (UE) 2016/679[6] privind protecția datelor cu

---

1 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), versiune consolidată la 20 noiembrie, abrogată începând de la 25 mai 2018 (a se vedea nota de subsol 6).

2 Directiva 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), versiune consolidată la 19 decembrie 2009.

3 Directiva 2002/58 a fost modificată prin Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE (JO 2006, L 105, p. 54, Ediție specială, 13/vol. 53, p. 51). Această directivă a fost declarată nevalidă de Curte prin Hotărârea din 8 aprilie 2014, Digital Rights Ireland și Seitlinger și alții (C-293/12 și C-594/12, EU:C:2014:238), pentru motivul că încălca în mod grav drepturile la respectarea vieții private și la protecția datelor cu caracter personal (a se vedea secțiunea I.1., intitulată „Conformitatea dreptului derivat al Uniunii cu dreptul la protecția datelor cu caracter personal”, din prezenta fișă).

4 Comisia a prezentat la 10 ianuarie 2017 o propunere de înlocuire a acestei directive printr-un regulament referitor la viața privată și la comunicațiile electronice.

5 La 10 februarie 2021, Consiliul Uniunii Europene a aprobat un mandat de negociere pentru revizuirea normelor în materie de protecție a vieții private și a confidențialității în utilizarea serviciilor de comunicații electronice, care permite începerea negocierilor cu Parlamentul European. Textul propunerii de regulament privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice și de abrogare a Directivei 2002/58/CE (Regulamentul privind viața privată și comunicațiile electronice) este disponibil pe acest link: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*

6 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 (JO 2016, L 119, p. 1).

caracter personal (denumit în continuare „RGPD”), care abrogă Directiva 95/46 și care este aplicabil începând de la 25 mai 2018, precum și Directiva (UE) 2016/680[7] privind protecția respectivelor date în materie penală, ale cărei dispoziții sunt aplicabile începând de la 6 mai 2018.

În ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile și organele Uniunii Europene, protecția lor este asigurată, începând de la 11 decembrie 2018, în special de Regulamentul (UE) 2018/1725[8]. În interesul unei abordări coerente a protecției datelor cu caracter personal în întreaga Uniune, acest regulament vizează alinierea cât mai mult posibil a normelor din domeniu cu regimul instituit prin RGPD.

În sfârșit, pentru a face față provocărilor ridicate de noile tehnologii, legiuitorul Uniunii a inițiat, începând cu anul 2020, adoptarea unor noi măsuri legislative[9] care se corelează cu dispozițiile de drept al Uniunii privind protecția datelor cu caracter personal.

Având în vedere jurisprudența bogată a Curții de Justiție în materie de protecție a datelor cu caracter personal, prezenta fișă tematică urmărește să prezinte o selecție de hotărâri fondatoare în materie, precum și de hotărâri care au contribuit în mod semnificativ la dezvoltarea acestei jurisprudențe, un interes deosebit fiind acordat hotărârilor pronunțate de Marea Cameră a Curții. Mai precis, această fișă are vocația de a acoperi atât jurisprudența referitoare la reglementarea generală în materie de protecție a datelor cu caracter personal, rezultată din interpretarea Directivei 95/46 și a RGPD, cât și pe cea privind reglementarea sectorială care vizează, printre altele, sectorul comunicațiilor electronice și dreptul penal. Pe de altă parte, ea vizează să prezinte o selecție de hotărâri privind reglementări care se aplică în mod transversal, subliniind totodată de la bun început rolul determinant al cartei în dezvoltarea jurisprudenței.

---

7 Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO 2016, L 119, p. 89).

8 Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO 2018, L 295, p. 39).

9 În acest cadru, trebuie să se menționeze în special trei inițiative legislative: *i)* Regulamentul (UE) 2022/868 al Parlamentului European și al Consiliului din 30 mai 2022 privind guvernanța datelor la nivel european și de modificare a Regulamentului (UE) 2018/1724 (Regulamentul privind guvernanța datelor) (JO 2022, L 152, p 1) și Regulamentul (UE) 2023/2854 al Parlamentului European și al Consiliului din 13 decembrie 2023 privind norme armonizate pentru un acces echitabil la date și o utilizare corectă a acestora și de modificare a Regulamentului (UE) 2017/2394 și a Directivei (UE) 2020/1828 (Regulamentul privind datele) (JO 2023, L 2854, p. 1); *ii)* un pachet legislativ privind serviciile și piețele digitale, compus din Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale) (JO 2022, L 277, p. 1) și din Regulamentul 2022/1925 al Parlamentului European și al Consiliului din 14 septembrie 2022 privind piețe contestabile și echitabile în sectorul digital și de modificare a Directivelor (UE) 2019/1937 și (UE) 2020/1828 (Regulamentul privind piețele digitale) (JO 2022, L 265, p. 1), și *iii)* prima propunere legislativă care vizează crearea unui cadru normativ în materie de inteligență artificială, care s-a concretizat printr-un regulament privind inteligența artificială (*JO 2024, L, 1689*).

Cuprins

I. Dreptul la protecția datelor cu caracter personal recunoscut de Carta drepturilor fundamentale a Uniunii Europene

1. Conformitatea dreptului derivat al Uniunii cu dreptul la protecția datelor cu caracter personal

Hotărârea din 9 noiembrie 2010 (Marea Cameră), Volker und Markus Schecke și Eifert (C-92/09 și C-93/09, EU:C:2010:662)

În această cauză, litigiile principale aveau ca părți producători agricoli și Land Hessen, în legătură cu publicarea pe site-ul internet al Bundesanstalt für Landwirtschaft und Ernährung (Oficiul Federal pentru Agricultură și Alimentație) a datelor cu caracter personal care îi privesc în calitate de beneficiari de fonduri provenite din Fondul european de garantare agricolă (FEGA) și din Fondul european agricol pentru dezvoltare rurală (FEADR). Producătorii agricoli se opuneau acestei publicări susținând în special că aceasta nu era justificată de un interes public preponderent. Land Hessen considera că publicarea acestor date se baza pe Regulamentele (CE) nr. 1290/2005[10] și 259/2008[11], care privesc finanțarea politicii agricole comune și care impun publicarea unor informații referitoare la persoanele fizice care beneficiază de FEGA și de FEADR.

În acest context, Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden, Germania) a adresat Curții o serie de întrebări privind validitatea anumitor dispoziții ale Regulamentului nr. 1290/2005 și a Regulamentului nr. 259/2008, care prevăd punerea unor astfel de informații la dispoziția publicului, în special prin intermediul unor site-uri internet administrate de oficiile naționale.

Curtea a arătat, în ceea ce privește corelarea dintre dreptul la protecția datelor cu caracter personal recunoscut de cartă și obligația de transparență în materie de fonduri europene, că publicarea pe un site internet a datelor nominale ale beneficiarilor fondurilor și a sumelor primite de aceștia constituie, din cauza liberului acces la site al terților, o atingere adusă dreptului beneficiarilor respectivi la respectarea vieții lor private în general și protecției datelor lor cu caracter personal în special.

Pentru a fi justificată, o astfel de atingere trebuie să fie prevăzută de lege, să respecte substanța acestor drepturi și, în aplicarea principiului proporționalității, să fie necesară

---

10 Regulamentul (CE) nr. 1290/2005 al Consiliului din 21 iunie 2005 privind finanțarea politicii agricole comune (JO 2005, L 209, p. 1, Ediție specială, 14/vol. 1, p. 193), abrogat prin Regulamentul (UE) nr. 1306/2013 al Parlamentului European și al Consiliului din 17 decembrie 2013 privind finanțarea, gestionarea și monitorizarea politicii agricole comune (JO 2013, L 347, p. 549).

11 Regulamentul (CE) nr. 259/2008 al Comisiei din 18 martie 2008 de stabilire a normelor de aplicare a Regulamentului (CE) nr. 1290/2005 al Consiliului în ceea ce privește publicarea informațiilor referitoare la beneficiarii fondurilor provenite din Fondul european de garantare agricolă (FEGA) și din Fondul european agricol pentru dezvoltare rurală (FEADR) (JO 2008, L 76, p. 28), abrogat prin Regulamentul de punere în aplicare (UE) nr. 908/2014 al Comisiei din 6 august 2014 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 1306/2013 al Parlamentului European și al Consiliului în ceea ce privește agențiile de plăți și alte organisme, gestiunea financiară, verificarea conturilor, normele referitoare la controale, valorile mobiliare și transparența (JO 2014, L 255, p. 59).

și să răspundă efectiv unor obiective de interes general recunoscute de Uniune, derogările sau restrângerile acestor drepturi trebuind a fi efectuate în limitele strictului necesar. În acest context, Curtea a apreciat că, deși într-o societate democratică contribuabilii au dreptul de a fi informați cu privire la utilizarea fondurilor publice, Consiliul și Comisia erau totuși obligate să realizeze un just echilibru între diferitele interese în cauză, ceea ce impunea, înainte de adoptarea dispozițiilor în litigiu, verificarea aspectului dacă publicarea acestor date de către statul membru prin intermediul unui site internet unic nu depășea ceea ce era necesar pentru realizarea obiectivelor legitime urmărite.

Astfel, Curtea a declarat nevalide anumite dispoziții ale Regulamentului nr. 1290/2005, precum și Regulamentul nr. 259/2008 în ansamblul său, în măsura în care, în ceea ce privește persoanele fizice beneficiare ale fondurilor din FEGA și din FEADR, aceste dispoziții impun publicarea datelor cu caracter personal referitoare la fiecare beneficiar fără a face distincție în funcție de criterii relevante, precum perioadele în care acestea au primit astfel de fonduri, frecvența sau tipul și valoarea acestora. Cu toate acestea, Curtea nu a repus în discuție efectele publicării listelor de beneficiari ai unor astfel de fonduri de către autoritățile naționale în perioada anterioară datei pronunțării hotărârii.

Hotărârea din 8 aprilie 2014 (Marea Cameră), Digital Rights Ireland și Seitlinger ș.a. (cauzele conexate C-293/12 și C-594/12,* EU:C:2014:238*)

Prezenta hotărâre își găsește originea în cererile de apreciere a validității Directivei 2006/24/CE privind păstrarea datelor din perspectiva drepturilor fundamentale la respectarea vieții private și la protecția datelor cu caracter personal, formulate în cadrul unor litigii naționale în fața instanțelor irlandeze și austriece. În cauza C-293/12, High Court (Înalta Curte, Irlanda) era sesizată cu un litigiu între societatea Digital Rights și autoritățile irlandeze cu privire la legalitatea măsurilor naționale privind păstrarea datelor referitoare la comunicațiile electronice. În cauza C-594/12, Verfassungsgerichtshof (Curtea Constituțională, Austria) era sesizată cu mai multe acțiuni în materie constituțională având ca obiect anularea dispoziției naționale de transpunere a Directivei 2006/24 în dreptul austriac.

Prin intermediul cererilor de decizie preliminară, instanțele irlandeză și austriacă au adresat întrebări Curții cu privire la validitatea Directivei 2006/24 în lumina articolelor 7, 8 și 11 din cartă. Mai precis, aceste instanțe au solicitat Curții să stabilească dacă obligația care revine în temeiul acestei directive furnizorilor de servicii de comunicații electronice accesibile publicului sau de rețele de comunicații publice de a păstra pentru o anumită perioadă date referitoare la viața privată a unei persoane și la comunicațiile sale și de a oferi acces autorităților naționale competente reprezenta o ingerință nejustificată în drepturile fundamentale respective. Tipurile de date în cauză includ în special datele necesare pentru trasarea și identificarea sursei unei comunicații și destinația acesteia, stabilirea datei, a orei, a duratei și a tipului unei comunicații, dispozitivele de comunicații ale utilizatorilor, precum și identificarea situării

echipamentului de comunicație mobilă, date care includ printre altele numele și adresa abonatului sau ale utilizatorului înregistrat, numărul de telefon al apelantului și numărul apelat, precum și o adresă IP pentru serviciile de internet. Aceste date permit în special stabilirea persoanei cu care a comunicat un abonat sau un utilizator înregistrat și prin ce mijloace, precum și stabilirea duratei comunicației și a locului de unde a fost inițiată aceasta. În plus, cu ajutorul datelor în cauză se poate cunoaște frecvența comunicațiilor abonatului sau ale utilizatorului înregistrat cu anumite persoane într-o perioadă determinată.

Curtea a statuat mai întâi că, întrucât impun astfel de obligații furnizorilor, dispozițiile Directivei 2006/24 constituie o ingerință deosebit de gravă în drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal garantate de articolele 7 și 8 din cartă. În acest context, Curtea a stabilit că, desigur, această ingerință putea fi justificată de urmărirea unui obiectiv de interes general, precum combaterea criminalității organizate. În această privință, Curtea a subliniat, în primul rând, că păstrarea datelor prevăzută de directivă nu era de natură să afecteze conținutul esențial al drepturilor fundamentale la respectarea vieții private și la protecția datelor cu caracter personal, în măsura în care aceasta nu permitea să se ia cunoștință de conținutul comunicațiilor electronice ca atare și prevedea că furnizorii de servicii sau de rețele trebuie să respecte anumite principii de protecție și de securitate a datelor. În al doilea rând, Curtea a observat că păstrarea datelor pentru posibila transmitere către autoritățile naționale competente răspunde efectiv unui obiectiv de interes general, și anume combaterea criminalității grave și astfel, în definitiv, siguranța publică.

Cu toate acestea, Curtea a apreciat că, prin adoptarea directivei privind păstrarea datelor, legiuitorul Uniunii a depășit limitele impuse de respectarea principiului proporționalității. În consecință, aceasta a declarat directiva nevalidă, considerând că ingerința de o mare amploare și de o gravitate deosebită în drepturile fundamentale pe care o implica nu era suficient încadrată de dispoziții care să garanteze că această ingerință este limitată la strictul necesar. Astfel, Directiva 2006/24 acoperea în mod generalizat orice persoană și orice mijloc de comunicare electronică, precum și ansamblul datelor de trafic, fără a face nicio diferențiere, limitare sau excepție în funcție de obiectivul combaterii infracțiunilor grave. De altfel, directiva nu prevedea niciun criteriu obiectiv care să permită garantarea faptului că autoritățile naționale competente au acces la date și le pot utiliza numai în scopul prevenirii, al detectării sau al urmăririi penale în legătură cu infracțiuni care ar putea fi considerate suficient de grave pentru a justifica o asemenea ingerință și nici condițiile materiale și procedurale ale unui astfel de acces sau de utilizare. În ceea ce privește durata de păstrare a datelor, directiva impunea păstrarea acestora pentru o perioadă de cel puțin șase luni, fără a se face vreo distincție între categoriile de date în funcție de persoanele vizate sau utilitatea lor eventuală în scopul realizării obiectivului urmărit.

Pe de altă parte, în ceea ce privește cerințele care decurg din articolul 8 alineatul (3) din cartă, Curtea a constatat că Directiva 2006/24 nu prevede garanții suficiente pentru

asigurarea unei protecții eficiente a datelor împotriva riscurilor de abuz, precum și împotriva accesului și a utilizării neautorizate a datelor și nici nu impune păstrarea datelor pe teritoriul Uniunii.

În consecință, această directivă nu garanta pe deplin verificarea respectării cerințelor de protecție și de securitate de către o autoritate independentă, așa cum impune totuși în mod explicit carta.

Hotărârea din 21 iunie 2022 (Marea Cameră), Ligue des droits humains (C-817/19, EU:C:2022:491)

Datele din PNR (Passenger Name Record) sunt informații de rezervare stocate de transportatorii aerieni în sistemele lor de rezervare și de control al plecărilor. Directiva PNR[12] obligă acești transportatori să transfere datele oricărui pasager care efectuează un zbor extra-UE, operat între o țară terță și Uniunea Europeană, către unitatea de informații despre pasageri (denumită în continuare „UIP") a statului membru de destinație sau de plecare a zborului în cauză pentru a combate terorismul și infracțiunile grave. De fapt, datele din PNR astfel transferate fac obiectul unei evaluări prealabile de către UIP[13] și sunt apoi păstrate în vederea unei eventuale evaluări ulterioare de către autoritățile competente ale statului membru în cauză sau de către cele ale unui alt stat membru. Statele membre pot decide să aplice directiva și în cazul zborurilor intra-UE[14].

Cour constitutionnelle (Curtea Constituțională, Belgia) a fost sesizată de Ligue des droits humains cu o acțiune în anulare împotriva legii belgiene care transpune în dreptul național atât Directiva PNR, cât și Directiva API[15]. Potrivit reclamantei, această lege încalcă dreptul la respectarea vieții private și la protecția datelor cu caracter personal. Reclamanta critică, pe de o parte, caracterul prea larg al datelor din PNR și, pe de altă parte, caracterul general al colectării, al transferului și al prelucrării acestor date. Legea ar aduce atingere și liberei circulații a persoanelor prin faptul că ar restabili în mod indirect controale la frontiere prin extinderea sistemului PNR în cazul zborurilor intra-UE și în cazul transporturilor efectuate cu alte mijloace în interiorul Uniunii.

---

12 Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave (JO 2016, L 119, p. 132) (denumită în continuare „Directiva PNR").

13 Această evaluare prealabilă vizează identificarea persoanelor pentru care este necesară o examinare mai aprofundată de către autoritățile competente, ținând seama de faptul că aceste persoane pot fi implicate într-o infracțiune de terorism sau într-o infracțiune gravă. Ea se efectuează în mod sistematic și prin mijloace automatizate, prin compararea datelor din PNR cu baze de date „utile" sau prin prelucrarea acestora în raport cu criterii prestabilite la articolul 6 alineatul (2) litera (a) și alineatul (3) din Directiva PNR.

14 Prin utilizarea posibilității prevăzute la articolul 2 din Directiva PNR.

15 Directiva 2004/82/CE a Consiliului din 29 aprilie 2004 privind obligația operatorilor de transport de a comunica datele privind pasagerii (JO 2004, L 261, p. 24, Ediție specială, 19/vol. 7, p. 40) (denumită în continuare „Directiva API"). Această directivă reglementează transmiterea către autoritățile naționale competente de către operatorii de transport aerian a unor informații prealabile referitoare la pasageri (cum ar fi numărul și tipul documentului de călătorie utilizat, precum și cetățenia) în vederea îmbunătățirii controalelor la frontieră și a combaterii imigrației ilegale.

În acest context, Cour constitutionnelle (Curtea Constituțională) belgiană a sesizat Curtea cu titlu preliminar, adresându-i întrebări referitoare în special la validitatea Directivei PNR.

Prin hotărârea pronunțată în Marea Cameră, Curtea confirmă validitatea Directivei PNR în măsura în care aceasta poate fi interpretată în conformitate cu carta.

În această privință, Curtea statuează că, din moment ce interpretarea dedusă de Curte din dispozițiile Directivei PNR în lumina drepturilor fundamentale garantate de articolele 7, 8 și 21, precum și de articolul 52 alineatul (1) din cartă[16] asigură conformitatea acestei directive cu aceste articole, analiza întrebărilor adresate nu a scos la iveală niciun element de natură să afecteze validitatea directivei menționate.

Cu titlu prealabil, Curtea amintește că un act al Uniunii trebuie interpretat, în măsura posibilului, într-un mod care să nu repună în discuție validitatea acestuia și în conformitate cu dreptul primar în ansamblul său și în special cu dispozițiile cartei, statele membre fiind obligate astfel să se asigure că nu se întemeiază pe o interpretare a acestuia care ar intra în conflict cu drepturile fundamentale protejate de ordinea juridică a Uniunii sau cu celelalte principii generale recunoscute de această ordine juridică. Referitor la Directiva PNR, Curtea precizează că un număr important de considerente ale acesteia și de dispoziții din aceasta impun o asemenea interpretare conformă, punând accentul pe importanța pe care legiuitorul Uniunii o acordă, prin trimiterea făcută la un nivel ridicat de protecție a datelor, respectării depline a drepturilor fundamentale consacrate de cartă.

Curtea constată că Directiva PNR conține ingerințe de o gravitate certă în drepturile garantate de articolele 7 și 8 din cartă, mai ales în măsura în care aceasta urmărește să instituie un regim de supraveghere continuu, nedirecționat și sistematic, care include evaluarea automatizată a datelor cu caracter personal ale tuturor persoanelor care recurg la servicii de transport aerian. Ea amintește că posibilitatea statelor membre de a justifica o astfel de ingerință trebuie apreciată cântărind gravitatea sa și verificând că importanța obiectivului de interes general urmărit este în raport cu această gravitate.

Curtea concluzionează că transferul, prelucrarea și păstrarea datelor din PNR prevăzute de această directivă pot fi considerate limitate la strictul necesar pentru combaterea infracțiunilor de terorism și a infracțiunilor grave cu condiția ca respectivele competențe prevăzute de Directiva PNR să facă obiectul unei interpretări stricte. În această privință, hotărârea pronunțată în această zi precizează printre altele că:

- sistemul instituit de Directiva PNR nu trebuie să privească decât informațiile care pot fi identificate în mod clar și care se circumscriu rubricilor care se regăsesc în

[16] Potrivit acestei dispoziții, orice restrângere a exercițiului drepturilor și libertăților recunoscute prin cartă trebuie să fie prevăzută de lege și să respecte substanța lor. În plus, pot fi impuse restrângeri privind aceste drepturi și libertăți numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

anexa I la aceasta, care sunt în legătură cu un zbor efectuat și cu pasagerul avut în vedere, ceea ce implică, pentru anumite rubrici din această anexă, că numai informațiile vizate în mod expres fac obiectul directivei[17];

- aplicarea sistemului instituit de Directiva PNR trebuie să se limiteze la infracțiunile de terorism și doar la infracțiunile grave care au o legătură obiectivă, cel puțin indirectă, cu transportul aerian de pasageri. Referitor la aceste forme, aplicarea sistemului menționat nu poate fi extinsă la infracțiuni care, deși îndeplinesc criteriul prevăzut de această directivă privind nivelul de gravitate și sunt în special menționate în anexa II la aceasta, se încadrează în rândul infracțiunilor de drept comun, având în vedere particularitățile sistemului de drept penal național;

- eventuala extindere a aplicării Directivei PNR la toate sau la o parte din zborurile intra-UE pe care un stat membru o poate decide făcând uz de posibilitatea prevăzută de această directivă trebuie să fie limitată la strictul necesar. În acest scop, ea trebuie să poată face obiectul unui control efectiv al unei instanțe sau al unei entități administrative independente a cărei decizie să aibă efect obligatoriu. În această privință, Curtea precizează că:

  - numai în situația în care respectivul stat membru constată existența unor împrejurări suficient de concrete pentru a aprecia că se confruntă cu o amenințare teroristă care se dovedește reală și actuală sau previzibilă, aplicarea acestei directive în cazul tuturor zborurilor intra-UE dinspre sau către statul membru menționat, pentru o durată limitată la strictul necesar, dar care poate fi prelungită, nu depășește limitele strictului necesar[18];

  - în lipsa unei astfel de amenințări teroriste, aplicarea directivei menționate nu se poate extinde la toate zborurile intra-UE, ci trebuie să se limiteze la zborurile intra-UE care vizează în special anumite legături aeriene sau scheme de zbor sau chiar anumite aeroporturi pentru care există, potrivit aprecierii statului membru interesat, indicii de natură să justifice această aplicare. Caracterul strict necesar al acestei aplicări în cazul zborurilor intra-UE astfel selectate trebuie să fie în mod regulat reexaminat în funcție de evoluția condițiilor care au justificat selectarea lor;

- pentru evaluarea prealabilă a datelor din PNR, care are ca obiectiv identificarea persoanelor pentru care este necesară o examinare mai aprofundată înainte de

[17] Astfel, printre altele, „informațiile privind forma de plată” (rubrica 6 din anexă) trebuie să se limiteze la modalitățile de plată și la facturarea biletului de avion, cu excluderea oricărei alte informații care nu are o legătură directă cu zborul, iar „mențiuni[le] cu caracter general” (rubrica 12) nu pot privi decât informațiile enumerate expres în această rubrică, referitoare la pasagerii minori.

[18] Într-adevăr, existența unei asemenea amenințări este de natură prin ea însăși să stabilească o relație între transferul și prelucrarea datelor vizate și combaterea terorismului. Prin urmare, a prevedea aplicarea directivei PNR în cazul tuturor zborurilor intra-UE dinspre sau către statul membru în cauză, pentru o perioadă limitată, nu depășește limitele strictului necesar, decizia prevăzând că această aplicare trebuie să poată face obiectul unui control exercitat de o instanță sau de o entitate administrativă independentă.

sosirea sau de plecarea lor și care este, într-o primă fază, efectuată prin prelucrări automatizate, UIP nu poate, pe de o parte, să compare aceste date decât cu bazele de date care privesc persoanele sau obiectele căutate sau care fac obiectul unei alerte[19]. Aceste baze de date trebuie să fie nediscriminatorii și exploatate de autoritățile competente în relație cu combaterea terorismului și a infracțiunilor grave care au o legătură obiectivă, cel puțin indirectă, cu transportul aerian de pasageri. În ceea ce privește, pe de altă parte, evaluarea prealabilă în raport cu criteriile prestabilite, UIP nu poate utiliza tehnologii de inteligență artificială în cadrul sistemului de autoinstruire (*machine learning*), de natură să modifice, fără intervenție și control umane, procesul de evaluare și în special criteriile de evaluare pe care se întemeiază rezultatul aplicării acestui proces, precum și evaluarea comparativă a acestor criterii. Criteriile menționate trebuie să fie stabilite într-un mod în care aplicarea lor să vizeze în mod specific particularii față de care ar putea să existe o suspiciune rezonabilă de participare la infracțiuni de terorism sau la infracțiuni grave și în care să se țină cont atât de elemente „incriminatorii", cât și de elemente „dezincriminatorii", fără a da naștere unor discriminări directe sau indirecte[20];

- ținând cont de marja de eroare inerentă unor asemenea prelucrări automatizate a datelor din PNR și de numărul destul de consecvent de rezultate „fals pozitive" obținute în urma aplicării lor în cursul anilor 2018 și 2019, capacitatea sistemului instituit prin Directiva PNR de a atinge obiectivele urmărite depinde esențialmente de buna funcționare a verificării rezultatelor pozitive obținute în temeiul acestor prelucrări, pe care UIP le efectuează, într-o a doua fază, prin mijloace neautomatizate. În această privință, statele membre trebuie să prevadă norme clare și precise de natură să ghideze și să încadreze analiza efectuată de agenții UIP însărcinați cu această reexaminare individuală pentru a asigura respectarea deplină a drepturilor fundamentale consacrate la articolele 7, 8 și 21 din cartă și în special pentru a garanta o practică administrativă coerentă în cadrul UIP, ce respectă principiul nediscriminării. În special, acestea trebuie să se asigure că UIP stabilește criterii de reexaminare obiective care permit agenților săi să verifice, pe de o parte, dacă și în ce măsură un rezultat pozitiv (*hit*) privește efectiv o persoană susceptibilă de a fi implicată în săvârșirea de infracțiuni de terorism sau de infracțiuni grave, precum și, pe de altă parte, caracterul nediscriminatoriu al prelucrărilor automatizate. În acest context, Curtea subliniază în plus că autoritățile competente trebuie să se asigure că persoana

[19] Și anume bazele de date privind persoanele sau obiectele căutate sau care fac obiectul unei alerte în sensul articolului 6 alineatul (3) litera (a) din Directiva PNR. În schimb, analize pornind de la baze de date diverse ar putea lua forma unei explorări de date (*data mining*) și ar fi susceptibile să conducă la o utilizare disproporționată a acestor date, furnizând mijloacele de a stabili profilul precis al persoanelor vizate pentru simplul motiv că acestea au intenția de a călători cu avionul.

[20] Criteriile prestabilite trebuie să fie personalizate, proporționale și specifice și să fie revizuite periodic [articolul 6 alineatul (4) din Directiva PNR]. Evaluarea prealabilă pe baza unor criterii prestabilite trebuie să se realizeze în mod nediscriminatoriu. Potrivit articolului 6 alineatul (4) a patra teză din Directiva PNR, criteriile nu se întemeiază în niciun caz pe rasa sau originea etnică a unei persoane, opiniile sale politice, religia sau convingerile sale filozofice, apartenența la un sindicat, starea sa de sănătate, viața sexuală sau orientarea sexuală.

interesată poate înțelege funcționarea criteriilor de evaluare prestabilite și a programelor care aplică aceste criterii, așa încât să poată decide în deplină cunoștință de cauză dacă își exercită sau nu dreptul la o cale de atac jurisdicțională. De asemenea, în cadrul unei astfel de căi de atac, instanța însărcinată cu controlul legalității deciziei adoptate de autoritățile competente, precum și, mai puțin în cazurile de amenințări la adresa siguranței statului, persoana interesată însăși trebuie să poată lua cunoștință atât de ansamblul motivelor, cât și de elementele de probă pe baza cărora a fost adoptată această decizie, inclusiv de criteriile de evaluare prestabilite și de funcționarea programelor care aplică aceste criterii;

- comunicarea și evaluarea ulterioare ale datelor din PNR, altfel spus, după sosirea sau plecarea persoanei avute în vedere, nu se pot efectua decât pe baza unor împrejurări noi și a unor elemente obiective care fie sunt de natură să fundamenteze suspiciunea rezonabilă de implicare a acestei persoane în săvârșirea de infracțiuni grave care au o legătură obiectivă, cel puțin indirectă, cu transportul aerian de pasageri, fie permit să se aprecieze că aceste date ar putea, într-un caz concret, să aducă o contribuție efectivă în combaterea infracțiunilor de terorism care au o atare legătură. Comunicarea datelor din PNR în vederea unei asemenea evaluări ulterioare trebuie să fie în principiu, mai puțin în caz de urgență justificată în mod corespunzător, subordonată unui control prealabil efectuat fie de o instanță, fie de o autoritate administrativă independentă, la cererea motivată a autorităților competente, indiferent dacă această cerere a fost formulată înainte sau după expirarea termenului de șase luni ulterior transferului acestor date către UIP[21].

Hotărârea din 22 noiembrie 2022 (Marea Cameră), Luxembourg Business Registers (C-37/20 și C-601/20, EU:C:2022:912)

În scopul combaterii și al prevenirii spălării banilor și a finanțării terorismului, Directiva împotriva spălării banilor[22] impune statelor membre să țină un registru care să conțină informații cu privire la beneficiarii reali[23] ai unor entități corporative și ai altor entități juridice înregistrate pe teritoriul lor. În urma unei modificări a acestei directive prin

[21] Potrivit articolului 12 alineatele (1) și (3) din Directiva PNR, un astfel de control este prevăzut în mod expres numai pentru cererile de dezvăluire a datelor din PNR depuse după termenul de șase luni de la transferul acestor date către UIP.

[22] Directiva (UE) 2015/849 a Parlamentului European și a Consiliului din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, de modificare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului și de abrogare a Directivei 2005/60/CE a Parlamentului European și a Consiliului și a Directivei 2006/70/CE a Comisiei (JO 2015, L 141, p. 73, denumită în continuare „Directiva împotriva spălării banilor”).

[23] În conformitate cu articolul 3 punctul 6 din Directiva împotriva spălării banilor, beneficiarii reali sunt persoanele fizice care dețin sau controlează în ultimă instanță clientul și/sau persoana fizică (persoanele fizice) în numele căreia (cărora) se realizează o tranzacție sau o activitate.

Directiva 2018/843[24], unele dintre aceste informații trebuie să fie făcute accesibile în toate cazurile oricărui membru al publicului larg. În conformitate cu Directiva împotriva spălării banilor astfel modificată (denumită în continuare „Directiva împotriva spălării banilor modificată”), legislația luxemburgheză a instituit un Registru al beneficiarilor reali (denumit în continuare „RBR”), destinat să dețină și să pună la dispoziție o serie de informații cu privire la beneficiarii reali ai entităților înregistrate, la care accesul este deschis oricărei persoane.

În acest context, tribunal d’arrondissement de Luxembourg (Tribunalul Districtual din Luxemburg) a fost sesizat cu două cauze, introduse de WM și, respectiv, de Sovim SA, care contestă respingerea de către Luxembourg Business Registers, gestionară a RBR, a cererilor lor de împiedicare a accesului publicului larg la informațiile referitoare, în prima cauză, la WM în calitate de beneficiar real al unei societăți civile imobiliare și, în a doua cauză, la beneficiarul real al Sovim SA. În cadrul acestor două cauze, având îndoieli în special cu privire la validitatea dispozițiilor dreptului Uniunii care instituie sistemul de acces public la informațiile referitoare la beneficiarii reali, tribunal d’arrondissement de Luxembourg (Tribunalul Districtual din Luxemburg) a sesizat Curtea cu o întrebare preliminară în aprecierea validității.

Prin hotărârea sa, Curtea, reunită în Marea Cameră, declară nevalidă Directiva 2018/843 în măsura în care a modificat Directiva împotriva spălării banilor în sensul că statele membre trebuie să se asigure că informațiile cu privire la beneficiarii reali ai entităților corporative și ale altor entități juridice constituite pe teritoriul lor sunt accesibile în toate cazurile oricărui membru al publicului larg[25].

În primul rând, Curtea constată că accesul publicului larg la informațiile cu privire la beneficiarii reali, prevăzut de Directiva împotriva spălării banilor modificată, constituie o ingerință gravă în drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal, consacrate la articolele 7 și, respectiv, 8 din cartă.

În această privință, Curtea observă că, din moment ce datele vizate conțin informații despre persoane fizice identificate, și anume beneficiarii reali ai entităților corporative și ai altor entități juridice înregistrate pe teritoriul statelor membre, accesul oricărui membru al publicului larg la acestea afectează dreptul fundamental la respectarea vieții private. În plus, punerea lor la dispoziția publicului larg constituie o prelucrare a datelor cu caracter personal. Aceasta adaugă că o astfel de punere la dispoziția publicului larg constituie o ingerință în cele două drepturi fundamentale menționate anterior, indiferent de utilizarea ulterioară a informațiilor comunicate.

---

[24] Directiva (UE) 2018/843 a Parlamentului European și a Consiliului din 30 mai 2018 de modificare a Directivei (UE) 2015/849 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, precum și de modificare a Directivelor 2009/138/CE și 2013/36/UE (JO 2018, L 156, p. 43).

[25] Nevaliditatea articolului 1 punctul 15 litera (c) din Directiva 2018/843 de modificare a articolului 30 alineatul (5) primul paragraf litera (c) din Directiva împotriva spălării banilor.

În ceea ce privește gravitatea acestei ingerințe, Curtea arată că, în măsura în care informațiile puse la dispoziția publicului larg se referă la identitatea beneficiarului real, precum și la natura și amploarea interesului generator de beneficii deținut în entități corporative sau în alte entități juridice, ele pot permite stabilirea unui profil privind anumite date personale de identificare, situația financiară a persoanei interesate, precum și sectoarele economice, țările și întreprinderile specifice în care aceasta a investit. În plus, aceste informații devin accesibile unui număr potențial nelimitat de persoane, așa încât o astfel de prelucrare de date cu caracter personal poate permite de asemenea accesul liber la aceste informații unor persoane care, din motive străine obiectivului vizat de această măsură, urmăresc să se informeze cu privire la situația în special materială și financiară a unui beneficiar real. Această posibilitate se dovedește cu atât mai ușoară atunci când datele pot fi consultate pe internet. Pe de altă parte, consecințele potențiale pentru persoanele vizate care rezultă dintr-o eventuală utilizare abuzivă a datelor lor cu caracter personal sunt agravate de faptul că, odată puse la dispoziția marelui public, aceste date pot nu numai să fie consultate în mod liber, ci și să fie păstrate și difuzate și devine, în cazul unor asemenea prelucrări succesive, cu atât mai dificil, chiar iluzoriu, pentru aceste persoane să se apere în mod eficace împotriva abuzurilor.

În al doilea rând, în cadrul examinării justificării ingerinței în cauză, *primo*, Curtea observă că, în speță, principiul legalității este respectat. Astfel, restrângerea exercițiului drepturilor fundamentale menționate mai sus care rezultă din accesul publicului larg la informațiile cu privire la beneficiarii reali este prevăzută de un act legislativ, și anume Directiva împotriva spălării banilor modificată. În plus, pe de o parte, această directivă precizează că informațiile respective trebuie să fie adecvate, exacte și actuale și enumeră în mod expres unele dintre datele la care trebuie acordat accesul public. Pe de altă parte, aceasta stabilește condițiile în care statele membre pot prevedea derogări de la un astfel de acces.

Secundo, ea precizează că ingerința în cauză nu aduce atingere substanței drepturilor fundamentale garantate la articolele 7 și 8 din cartă. Deși este adevărat că Directiva împotriva spălării banilor modificată nu conține o enumerare exhaustivă a datelor la care orice membru al publicului larg trebuie să fie autorizat să aibă acces și că statele membre sunt abilitate să prevadă accesul la informații suplimentare, nu este mai puțin adevărat că numai informațiile adecvate cu privire la beneficiarii reali și la interesele generatoare de beneficii deținute pot fi obținute, deținute și, prin urmare, în mod potențial făcute publice, ceea ce exclude printre altele informații care nu au un raport adecvat cu finalitățile Directivei împotriva spălării banilor modificate. Or, nu rezultă că punerea la dispoziția publicului larg a informațiilor care au un astfel de raport ar aduce în vreun fel atingere substanței drepturilor fundamentale.

Tertio, Curtea subliniază că, prevăzând accesul publicului larg la informațiile privind beneficiarii reali, legiuitorul Uniunii urmărește prevenirea spălării banilor și a finanțării terorismului prin instituirea, prin intermediul unei transparențe sporite, a unui mediu

mai puțin susceptibil să fie utilizat în acest scop, ceea ce constituie un obiectiv de interes general care poate justifica ingerințe, chiar grave, în drepturile fundamentale consacrate la articolele 7 și 8 din cartă.

Quarto, în cadrul examinării caracterului apt, necesar și proporțional al ingerinței în cauză, Curtea constată că, desigur, accesul publicului larg la informațiile cu privire la beneficiarii reali este apt să contribuie la realizarea acestui obiectiv.

Ea apreciază însă că această ingerință nu poate fi considerată ca fiind limitată la strictul necesar. Pe de o parte, stricta necesitate a ingerinței menționate nu poate fi demonstrată în temeiul faptului că criteriul „interesului legitim” de care, potrivit Directivei împotriva spălării banilor în versiunea anterioară modificării sale prin Directiva 2018/843, trebuia să dispună orice persoană care dorea să aibă acces la informațiile cu privire la beneficiarii reali era dificil de pus în aplicare și că aplicarea sa putea conduce la decizii arbitrare. Astfel, eventuala existență a unor dificultăți de a defini cu precizie ipotezele și condițiile în care publicul poate avea acces la informațiile referitoare la beneficiarii reali nu poate justifica faptul că legiuitorul Uniunii prevede accesul publicului larg la aceste informații.

Pe de altă parte, nici explicațiile care figurează în Directiva 2018/843 nu pot dovedi stricta necesitate a ingerinței în cauză[26]. În măsura în care, potrivit acestor explicații, accesul publicului larg la informațiile privind beneficiarii reali se presupune că permite un control sporit al informațiilor de către societatea civilă, în special presa sau organizațiile societății civile, Curtea arată că atât presa, cât și organizațiile societății civile care au legătură cu prevenirea și combaterea spălării banilor și a finanțării terorismului au un interes legitim să acceadă la informațiile în cauză. Aceeași este situația persoanelor care doresc să cunoască identitatea beneficiarilor reali ai unei entități corporative sau ai unei alte entități juridice ca urmare a faptului că pot încheia tranzacții cu acestea sau chiar a instituțiilor financiare și a autorităților implicate în combaterea infracțiunilor în materie de spălare a banilor sau de finanțare a terorismului.

În plus, ingerința în cauză nu prezintă nici un caracter proporțional. În această privință, Curtea constată că normele materiale care reglementează această ingerință nu răspund cerinței de claritate și de precizie. Astfel, Directiva împotriva spălării banilor modificată prevede accesul oricărui membru al publicului larg „cel puțin” la datele vizate de aceasta și conferă statelor membre posibilitatea de a acorda acces la informații suplimentare, care includ „cel puțin” data nașterii sau datele de contact ale beneficiarului real în cauză. Or, din utilizarea expresiei „cel puțin” reiese că aceste prevederi autorizează punerea la dispoziția publicului a unor date care nu sunt suficient definite și nici identificabile.

Pe de altă parte, în ceea ce privește evaluarea comparativă a gravității acestei ingerințe cu importanța obiectivului de interes general urmărit, Curtea recunoaște că, ținând

[26] Sunt vizate explicațiile care figurează în considerentul (30) al Directivei 2018/843.

seama de importanța sa, acest obiectiv este susceptibil să justifice ingerințe, chiar grave, în drepturile fundamentale consacrate la articolele 7 și 8 din cartă.

Cu toate acestea, pe de o parte, combaterea spălării banilor și a finanțării terorismului intră cu prioritate în sarcina autorităților publice, precum și a entităților, cum sunt instituțiile de credit sau instituțiile financiare, cărora, din cauza activităților lor, le sunt impuse obligații specifice în materie. Acesta este motivul pentru care Directiva împotriva spălării banilor modificată prevede că informațiile privind beneficiarii reali trebuie să fie accesibile în toate cazurile autorităților competente și unităților de informații financiare, fără nicio restricție, precum și entităților obligate, în cadrul aplicării măsurilor de precauție privind clientela[27].

Pe de altă parte, în comparație cu regimul anterior, care prevedea, pe lângă accesul autorităților competente și al anumitor entități la informațiile privind beneficiarii reali, pe cel al oricăror persoane sau organizații care pot demonstra un interes legitim, regimul introdus de Directiva 2018/843 reprezintă o atingere considerabil mai gravă adusă drepturilor fundamentale garantate la articolele 7 și 8 din cartă, fără ca această agravare să poată fi compensată de eventualele beneficii care ar putea rezulta din acest din urmă regim în raport cu primul în ceea ce privește combaterea spălării banilor și a finanțării terorismului.

2. Respectarea dreptului la protecția datelor cu caracter personal în cadrul punerii în aplicare a dreptului Uniunii

Hotărârea din 21 decembrie 2016 (Marea Cameră), Tele2 Sverige (cauzele conexate C-203/15 și C-698/15, EU:C:2016:970)

Ca urmare a Hotărârii Digital Rights Ireland și Seitlinger ș.a., prin care Directiva 2006/24 a fost declarată nevalidă (a se vedea mai sus), Curtea a fost sesizată cu două cauze privind obligația generală impusă în Suedia și în Regatul Unit furnizorilor de servicii de comunicații electronice să păstreze datele referitoare la astfel de comunicări, păstrare prevăzută în directiva declarată nevalidă.

A doua zi după pronunțarea Hotărârii Digital Rights Ireland și Seitlinger ș.a., operatorul de telecomunicații Tele2 Sverige a notificat autoritatea suedeză de supraveghere a poștei și telecomunicațiilor cu privire la decizia sa de a înceta păstrarea datelor și la intenția sa de a șterge datele care au fost deja înregistrate (cauza C-203/15). Dreptul suedez obliga într-adevăr furnizorii de servicii de comunicații electronice să păstreze în mod sistematic și continuu, fără nicio excepție, toate datele privind traficul și datele de

[27] Articolul 30 alineatul (5) primul paragraf literele (a) și (b) din Directiva împotriva spălării banilor modificată.

localizare ale tuturor abonaților și utilizatorilor înregistrați, în cazul tuturor mijloacelor de comunicații electronice. În cauza C-698/15, trei persoane au introdus acțiuni împotriva regimului britanic de păstrare a datelor care permitea ministrului de interne să impună operatorilor de telecomunicații publice să păstreze toate datele privind comunicațiile pentru o perioadă maximă de 12 luni, păstrarea conținutului acestor comunicări fiind totuși exclusă.

Sesizată de Kammarrätten i Stockholm (Curtea de Apel Administrativă din Stockholm, Suedia) și de Court of Appeal (England and Wales) (Civil Division)] [Curtea de Apel (Anglia și Țara Galilor) (Secția civilă), Regatul Unit], Curtea a fost invitată să se pronunțe cu privire la interpretarea articolului 15 alineatul (1) din Directiva 2002/58, denumită „asupra confidențialității și comunicațiilor electronice”, care permite statelor membre să introducă anumite excepții de la obligația, prevăzută de această directivă, de a asigura confidențialitatea comunicațiilor electronice și a traficului de date aferent.

În hotărârea sa, Curtea a statuat mai întâi că articolul 15 alineatul (1) din Directiva 2002/58 coroborat cu articolele 7, 8 și 11, precum și cu articolul 52 alineatul (1) din cartă se opune unei reglementări naționale, precum cea a Suediei, care prevede, în scopul combaterii criminalității, păstrarea generalizată și nediferențiată a tuturor datelor legate de trafic și de localizare ale tuturor abonaților și utilizatorilor înregistrați, în cazul tuturor mijloacelor de comunicații electronice. În opinia Curții, o asemenea reglementare depășește limitele strictului necesar și nu poate fi considerată justificată într-o societate democratică, astfel cum impune articolul 15 alineatul (1) interpretat în lumina articolelor citate anterior din cartă.

Aceeași dispoziție, interpretată în lumina acelorași articole din cartă, se opune deopotrivă unei reglementări naționale care guvernează protecția și securitatea datelor de transfer și a datelor de localizare, în special accesul autorităților naționale competente la datele păstrate, fără a limita acest acces, în cadrul combaterii infracționalității, numai la combaterea infracționalității grave, fără a supune respectivul acces unui control prealabil din partea unei instanțe sau a unei autorități administrative independente și fără a impune ca datele în cauză să fie păstrate pe teritoriul Uniunii.

În schimb, Curtea a considerat că articolul 15 alineatul (1) din Directiva 2002/58 nu se opune unei reglementări care permite, cu titlu preventiv, păstrarea direcționată a datelor de această natură în scopul combaterii infracționalității grave, cu condiția ca păstrarea datelor să fie limitată la strictul necesar în ceea ce privește categoriile de date vizate, mijloacele de comunicare vizate, persoanele în cauză, precum și durata de păstrare reținută. Pentru a îndeplini aceste cerințe, reglementarea națională menționată trebuie, în primul rând, să prevadă norme clare și precise care să protejeze datele în mod eficient împotriva riscurilor de abuz. Aceasta trebuie să indice în special împrejurările și condițiile în care poate fi luată, cu titlu preventiv, o măsură de păstrare a datelor, garantând astfel că o asemenea măsură este limitată la strictul necesar. În al doilea rând, în ceea ce privește condițiile materiale pe care trebuie să le îndeplinească reglementarea națională pentru a se asigura faptul că aceasta se limitează la ceea ce

este strict necesar, păstrarea datelor trebuie să răspundă întotdeauna unor criterii obiective, care să stabilească un raport între datele care trebuie păstrate și obiectivul urmărit. În special, astfel de condiții trebuie să se dovedească în practică de natură să delimiteze în mod efectiv amploarea măsurii și, în consecință, publicul în cauză. Referitor la această delimitare, reglementarea națională trebuie să se întemeieze pe elemente obiective care să permită să fie vizat un public ale cărui date pot prezenta o legătură, cel puțin indirectă, cu acte de infracționalitate gravă, să contribuie într-un mod sau altul la combaterea infracționalității grave sau să prevină un risc grav pentru siguranța publică.

II. Prelucrarea datelor cu caracter personal în sensul reglementării generale în materie

1. Domeniul de aplicare al reglementării generale

Hotărârea din 30 mai 2006 (Marea Cameră), Parlamentul/Consiliul (C-317/04 și C-318/04, EU:C:2006:346)

În urma atacurilor teroriste de la 11 septembrie 2001, Statele Unite au adoptat o legislație care prevede că transportatorii aerieni care operează zboruri către, dinspre sau prin Statele Unite au obligația să furnizeze autorităților americane accesul electronic la datele conținute în sistemele lor de rezervare și de control al plecărilor, denumite Passenger Name Records (PNR).

Întrucât a considerat că aceste dispoziții ar putea intra în conflict cu legislația europeană și cu cea a statelor membre în materie de protecție a datelor, Comisia a început negocieri cu autoritățile americane. În urma acestor negocieri, Comisia a adoptat, la 14 mai 2004, Decizia 2004/535/CE[28] prin care s-a constatat că Biroul Vamal și de Protecție la Frontieră al Statelor Unite (United States Bureau of Customs and Border Protection, denumit în continuare „CBP”) asigură un nivel adecvat de protecție a datelor PNR transferate din Comunitate (denumită în continuare „decizia de adecvare”). În continuare, la 17 mai 2004, Consiliul a adoptat Decizia 2004/496/CE[29] de aprobare a încheierii unui acord între Comunitatea Europeană și Statele Unite privind prelucrarea și transferul către CBP al datelor PNR de către transportatori aerieni stabiliți pe teritoriul statelor membre ale Comunității.

[28] Decizia 2004/535/CE a Comisiei din 14 mai 2004 privind protecția adecvată a datelor cu caracter personal din registrele nominale ale pasagerilor aerieni transferate către Biroul Vamal și de Protecție la Frontieră al Statelor Unite ale Americii (JO 2004, L 235, p. 11).

[29] Decizia 2004/496/CE a Consiliului din 17 mai 2004 privind încheierea unui acord între Comunitatea Europeană și Statele Unite ale Americii cu privire la prelucrarea și la transferul datelor PNR de către transportatorii aerieni către Biroul Vamal și de Protecție la Frontieră din cadrul Ministerului american pentru Securitate Internă (JO 2004, L 183, p. 83, rectificare în JO 2005, L 255, p. 168).

Parlamentul European a solicitat Curții să anuleze cele două decizii menționate anterior, susținând printre altele că decizia de adecvare a fost adoptată *ultra vires*, că articolul 95 CE (în prezent articolul 114 TFUE) nu constituie un temei juridic adecvat pentru decizia de aprobare a încheierii acordului și, în ambele cazuri, că a existat o încălcare a drepturilor fundamentale.

În ceea ce privește decizia de adecvare, Curtea a examinat mai întâi dacă Comisia putea să adopte în mod valabil decizia în temeiul Directivei 95/46. În acest context, Curtea a constatat că din decizia de adecvare reieșea că transferul de date PNR către CBP constituie o prelucrare având ca obiect siguranța publică și activitățile statului în domenii ale dreptului penal. Potrivit Curții, deși datele PNR erau inițial colectate de companiile aeriene în cadrul unei activități care intră în domeniul de aplicare al dreptului Uniunii, și anume vânzarea unui bilet de avion care conferă dreptul la o prestare de servicii, prelucrarea datelor care era luată în considerare în cadrul deciziei de adecvare avea o natură cu totul diferită. Astfel, această decizie nu viza o prelucrare de date care era necesară pentru realizarea unei prestări de servicii, ci o prelucrare de date considerată necesară pentru garantarea siguranței publice și în scopuri represive.

În această privință, Curtea a precizat că împrejurarea că datele PNR au fost colectate de operatori privați în scopuri comerciale și că aceștia din urmă sunt cei care organizează transferul lor către un stat terț nu se opune ca acest transfer să fie considerat o prelucrare a datelor exclusă din domeniul de aplicare al directivei. Într-adevăr, acest transfer era efectuat într-un cadru instituit de autoritățile publice și care viza siguranța publică. În consecință, Curtea a considerat că decizia de adecvare nu intră în domeniul de aplicare al directivei întrucât era vorba despre o prelucrare a datelor cu caracter personal care este exclusă din acesta. Prin urmare, Curtea a anulat decizia de adecvare.

În ceea ce privește decizia Consiliului, Curtea a apreciat că articolul 95 CE coroborat cu articolul 25 din Directiva 95/46 nu poate să constituie temeiul competenței Comunității de a încheia acordul în cauză cu Statele Unite. Astfel, acest acord viza același transfer de date ca decizia de adecvare și, prin urmare, prelucrări ale datelor care sunt excluse din domeniul de aplicare al directivei. În consecință, Curtea a anulat decizia Consiliului de aprobare a încheierii acordului.

Hotărârea din 13 mai 2014 (Marea Cameră), Google Spain și Google (C-131/12, EU:C:2014:317)

În anul 2010, un cetățean spaniol a formulat o reclamație la Agencia Española de Protección de Datos (Agenția Spaniolă de Protecție a Datelor, denumită în continuare „AEPD”) împotriva La Vanguardia Ediciones SL, care publică un cotidian cu difuzare largă în Spania, precum și împotriva Google Spain și a Google. Această persoană arăta că, atunci când un utilizator de internet introducea numele său în motorul de căutare al grupului Google, se afișau linkuri către două pagini ale cotidianului *La Vanguardia*, din 1998, pe care figura un anunț în care se menționa o vânzare la licitație a unor imobile asociată unei proceduri de executare silită desfășurate în vederea recuperării datoriilor

sale. Prin reclamație, această persoană a solicitat, pe de o parte, să se dispună ca *La Vanguardia* fie să elimine sau să modifice paginile menționate, fie să utilizeze anumite instrumente puse la dispoziție de motoarele de căutare pentru a proteja aceste date. Pe de altă parte, a solicitat să se dispună ca Google Spain sau Google să elimine sau să oculteze datele sale cu caracter personal astfel încât acestea să nu mai apară printre rezultatele căutării și să nu mai figureze în linkurile *La Vanguardia*.

AEPD a respins reclamația în ceea ce privea *La Vanguardia*, apreciind că publicarea de către aceasta a informațiilor în cauză era legală, dar, în schimb, a admis-o în ceea ce privea Google Spain și Google și a cerut acestor societăți să ia măsurile necesare pentru a retrage datele din indexul lor și pentru a face imposibil accesul pe viitor. Întrucât aceste societăți au formulat două acțiuni la Audiencia Nacional (Curtea Națională, Spania) pentru a obține anularea deciziei AEPD, instanța spaniolă a adresat o serie de întrebări Curții.

În această hotărâre, Curtea s-a pronunțat de asemenea cu privire la domeniul de aplicare teritorial al Directivei 95/46.

Astfel, Curtea a statuat că o prelucrare a datelor cu caracter personal este efectuată în cadrul activităților unui sediu al operatorului pe teritoriul unui stat membru, în sensul Directivei 95/46, în cazul în care operatorul unui motor de căutare, deși are sediul într-un stat terț, înființează într-un stat membru o sucursală sau o filială destinată promovării și vânzării spațiului publicitar de pe pagina acestui motor, a cărei activitate este orientată către locuitorii acelui stat membru.

Într-adevăr, în asemenea împrejurări, activitățile operatorului motorului de căutare și cele ale sediului său situat în statul membru în cauză, deși distincte, sunt indisociabil legate, întrucât activitățile referitoare la spațiile publicitare constituie mijlocul de a face motorul de căutare în cauză rentabil din punct de vedere economic, iar acest motor este în același timp mijlocul care permite realizarea activităților menționate.

Hotărârea din 11 decembrie 2014, Ryneš (C-212/13, EU:C:2014:2428)

Ca răspuns la agresiuni repetate, domnul Ryneš a instalat pe casa sa o cameră de supraveghere. În urma unui nou atac asupra casei sale, înregistrările efectuate cu această cameră au ajutat la identificarea a doi suspecți, împotriva cărora au fost inițiate proceduri penale. Întrucât legalitatea prelucrării datelor înregistrate de camera de supraveghere a fost contestată de unul dintre suspecți în fața Oficiului pentru Protecția Datelor cu Caracter Personal ceh, acesta din urmă a constatat că domnul Ryneš a încălcat normele privind protecția datelor cu caracter personal și i-a aplicat acestuia o amendă.

Sesizată cu recursul declarat de domnul Ryneš împotriva unei decizii a Městský soud v Praze (Tribunalul Municipal din Praga, Republica Cehă), care confirmase decizia Oficiului, Nejvyšší správní soud (Curtea Administrativă Supremă, Republica Cehă) a întrebat

Curtea dacă înregistrarea efectuată de domnul Ryneš cu scopul de a proteja viața, sănătatea și proprietatea sa constituia o prelucrare de date care nu este prevăzută de Directiva 95/46, pentru motivul că această înregistrare a fost efectuată de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice, în sensul articolului 3 alineatul (2) a doua liniuță din această directivă.

Curtea a statuat că operarea unui sistem de supraveghere video care determină o înregistrare video a unor persoane stocată pe un echipament de înregistrare în mod continuu, cum ar fi un hard disk, instalat de o persoană fizică pe locuința sa de familie în vederea protejării proprietății, a sănătății și a vieții proprietarilor locuinței, acest sistem supraveghind de asemenea spațiul public, nu constituie o prelucrare a datelor efectuată în cursul unei activități exclusiv personale sau domestice.

În această privință, Curtea a amintit că protecția dreptului fundamental la viață privată, garantat de articolul 7 din cartă, impune ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele strictului necesar. Întrucât dispozițiile Directivei 95/46, în măsura în care reglementează prelucrarea unor date cu caracter personal care poate aduce atingere libertăților fundamentale și în special dreptului la viață privată, trebuie interpretate în mod necesar în lumina drepturilor fundamentale care sunt înscrise în carta menționată, derogarea prevăzută la articolul 3 alineatul (2) a doua liniuță din această directivă trebuie să primească o interpretare strictă. În plus, însuși modul de redactare a acestei dispoziții exclude de la aplicarea Directivei 95/46 prelucrarea datelor efectuată pentru exercitarea unor activități „exclusiv” personale sau domestice. Or, în măsura în care o supraveghere video se extinde, fie și parțial, la spațiul public și, în consecință, este îndreptată în afara sferei private a persoanei care efectuează prelucrarea datelor prin acest mijloc, aceasta nu poate fi considerată drept o activitate exclusiv „personală sau domestică” în sensul dispoziției menționate.

Hotărârea din 16 ianuarie 2024 (Marea Cameră), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Pentru a examina o eventuală influență politică asupra Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Oficiul Federal pentru Protecția Constituției și pentru Combaterea Terorismului, Austria)[30], Nationalrat (Adunarea Națională, Austria) a constituit o comisie de anchetă (denumită în continuare „comisia de anchetă BVT”). Această comisie l-a audiat pe WK în calitate de martor. În pofida cererii sale de anonimizare, procesul-verbal al audierii acestuia, în care se menționau numele și prenumele sale complete, a fost publicat pe site-ul internet al Parlament Österreich (parlamentul austriac). Susținând că o astfel de divulgare a identității sale era contrară

[30] La 1 decembrie 2021, această entitate a devenit „Direktion Staatsschutz und Nachrichtendienst” (Direcția pentru Siguranța Statului și a Serviciilor de Informații, Austria).

RGPD și legislației austriece, WK a introdus o plângere la Österreichische Datenschutzbehörde (Autoritatea pentru Protecția Datelor, Austria) (denumită în continuare „Datenschutzbehörde”). Prin decizia din 18 septembrie 2019, Datenschutzbehörde s-a declarat necompetentă să se pronunțe cu privire la plângere, explicând că principiul separării puterilor excludea ca, în calitate de organ al puterii executive, ea să poată controla comisia de anchetă BVT, care face parte din puterea legislativă.

În urma deciziei Bundesverwaltungsgericht (Tribunalul Administrativ Federal, Austria), care a admis acțiunea formulată de WK și a anulat decizia Datenschutzbehörde, aceasta din urmă a sesizat Curtea Administrativă cu un recurs împotriva deciziei Tribunalului Administrativ Federal.

În acest context, instanța de trimitere a solicitat Curții să stabilească dacă activitățile unei comisii de anchetă instituite de parlamentul unui stat membru intră în domeniul de aplicare al RGPD și dacă regulamentul menționat se aplică atunci când aceste activități privesc protecția securității naționale.

În primul rând, Curtea amintește că articolul 2 alineatul (2) litera (a) din RGPD, care prevede că acest regulament nu se aplică prelucrării datelor cu caracter personal efectuate în cadrul unei activități care nu intră sub incidența dreptului Uniunii, are ca unic obiectiv excluderea din domeniul său de aplicare a prelucrărilor de date cu caracter personal efectuate de autoritățile de stat în cadrul unei activități care urmărește să apere securitatea națională sau care se încadrează în aceeași categorie. Astfel, simplul fapt că o activitate este proprie statului sau unei autorități publice nu este suficient pentru a exclude în mod automat aplicarea RGPD în privința unei asemenea activități.

Această interpretare, care decurge din lipsa unei distincții în funcție de identitatea autorului prelucrării în cauză, este confirmată de articolul 4 punctul 7 din RGPD[31].

Curtea precizează că natura parlamentară a comisiei de anchetă BVT nu implică excluderea activităților sale din domeniul de aplicare al RGPD. Astfel, excepția prevăzută la articolul 2 alineatul (2) litera (a) din acest regulament se referă numai la categorii de activități care, prin natura lor, nu intră în domeniul de aplicare al dreptului Uniunii, iar nu la categorii de persoane. Prin urmare, împrejurarea că prelucrarea datelor cu caracter personal este efectuată de o comisie de anchetă instituită de parlamentul unui stat membru în exercitarea competenței sale de control asupra puterii executive nu permite, ca atare, să se stabilească faptul că această prelucrare este efectuată în cadrul unei activități care nu intră sub incidența dreptului Uniunii.

În al doilea rând, Curtea arată că, deși este de competența statelor membre să își definească interesele esențiale de securitate și să adopte măsurile apte să o asigure[32],

[31] Acesta definește noțiunea de „operator” ca referindu-se la „persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal”.

simplul fapt că o măsură națională a fost adoptată în vederea protejării securității naționale nu poate să determine inaplicabilitatea dreptului Uniunii și nici să absolve statele membre de necesitatea de a respecta acest drept. Or, excepția prevăzută la articolul 2 alineatul (2) litera (a) din RGPD se referă numai la categorii de activități care, prin natura lor, nu intră în domeniul de aplicare al dreptului Uniunii. În această privință, împrejurarea că operatorul este o autoritate publică a cărei activitate principală este de a asigura securitatea națională nu poate fi suficientă, ca atare, pentru a exclude din domeniul de aplicare al RGPD prelucrările de date cu caracter personal pe care le efectuează în cadrul celorlalte activități desfășurate de ea.

În speță, controlul politic efectuat de comisia de anchetă BVT nu pare să constituie în sine o activitate care urmărește să apere securitatea națională sau care se încadrează în aceeași categorie. Prin urmare, sub rezerva verificării de către instanța de trimitere, această activitate nu este exclusă din domeniul de aplicare al RGPD.

Astfel fiind, o comisie parlamentară de anchetă poate avea acces la date cu caracter personal care, din motive de securitate națională, trebuie să beneficieze de o protecție specială. În această privință, pot fi stabilite restricții, prin intermediul unor măsuri legislative, privind drepturile și obligațiile care decurg din RGPD pentru a garanta printre altele securitatea națională[33]. Ar putea fi astfel justificate, în acest temei, restricții privind colectarea datelor cu caracter personal, informarea persoanelor vizate și accesul lor la respectivele date sau divulgarea acestora, fără consimțământul persoanelor vizate, altor persoane decât operatorul, cu condiția ca astfel de restricții să respecte esența drepturilor și libertăților fundamentale ale persoanelor vizate și să constituie o măsură necesară și proporțională într-o societate democratică.

Curtea observă însă că din informațiile puse la dispoziția sa nu reiese că comisia de anchetă BVT ar fi susținut că divulgarea datelor cu caracter personal ale persoanei în cauză era necesară pentru protejarea securității naționale și întemeiată pe o măsură legislativă națională prevăzută în acest scop, aspect a cărui verificare rămâne, dacă este cazul, în sarcina instanței de trimitere.

2. Noțiunea de „date cu caracter personal”

Hotărârea din 19 octombrie 2016, Breyer (C-582/14, EU:C:2016:779)

Domnul Breyer a introdus la instanțele civile germane o acțiune având ca obiect obligarea Republicii Federale Germania să înceteze să stocheze sau să permită stocarea

[32] Potrivit articolului 4 alineatul (2) TUE.
[33] Potrivit articolului 23 din RGPD.

de către terți a datelor informatice care erau transmise la fiecare accesare a site-urilor internet ale organismelor federale germane. Astfel, pentru a preveni atacurile și a face posibilă urmărirea penală a „piraților”, furnizorul de servicii de comunicații electronice al organismelor federale germane înregistra date care constau într-o adresă IP „dinamică” – o adresă IP care se schimbă cu ocazia fiecărei noi conectări la internet –, precum și în data și ora la care a avut loc consultarea site-ului. Spre deosebire de adresele IP statice, adresele IP dinamice nu permit, *a priori*, să se facă legătura, prin intermediul unor fișiere accesibile publicului, între un anumit calculator și conexiunea fizică la rețea utilizată de furnizorul de acces la internet. Datele înregistrate nu ofereau, în sine, furnizorului de servicii de comunicații electronice posibilitatea de a identifica utilizatorul. În schimb, furnizorul de servicii de acces la internet dispunea de informații suplimentare care, în combinație cu adresa IP, permiteau identificarea utilizatorului respectiv.

În acest context, Bundesgerichtshof (Curtea Federală de Justiție, Germania), sesizată cu un recurs, a solicitat Curții să stabilească dacă o adresă IP care este înregistrată de un furnizor de servicii de comunicații electronice cu ocazia accesului la site-ul său internet reprezintă pentru acesta o dată cu caracter personal.

Curtea a arătat mai întâi că, pentru ca o dată să poată fi calificată drept „dată cu caracter personal” în sensul articolului 2 litera (a) din Directiva 95/46, nu este necesar ca toate informațiile care permit identificarea persoanei vizate să se afle în posesia unei singure persoane. Faptul că informațiile suplimentare necesare pentru a identifica utilizatorul unui site internet sunt deținute nu de furnizorul de servicii de comunicații electronice, ci de furnizorul de acces la internet al acestui utilizator nu pare astfel de natură să excludă că adresele IP dinamice înregistrate de furnizorul de servicii de comunicații electronice constituie pentru acesta date cu caracter personal în sensul articolului 2 litera (a) din Directiva 95/46.

În consecință, Curtea a constatat că o adresă IP dinamică înregistrată de un furnizor de servicii de comunicații electronice cu ocazia consultării de către o persoană a unui site internet pe care acest furnizor îl pune la dispoziția publicului constituie pentru furnizorul respectiv o dată cu caracter personal în sensul articolului 2 litera (a) din Directiva 95/46 în cazul în care acesta dispune de mijloace legale care îi permit să identifice persoana vizată cu ajutorul informațiilor suplimentare ale acestei persoane de care dispune furnizorul de acces la internet al persoanei respective.

Hotărârea din 20 decembrie 2017, Nowak (C-434/16, EU:C:2017:994)

Domnul Nowak, un expert contabil stagiar, nu a promovat examenul organizat de ordinul irlandez al experților contabili autorizați. El a formulat, în temeiul articolului 4 din Legea privind protecția datelor, o cerere de acces care viza ansamblul datelor cu caracter personal care îl privesc, deținute de ordinul experților contabili. Acesta din urmă i-a comunicat domnului Nowak anumite documente, însă a refuzat să îi transmită

foaia sa de examinare, pentru motivul că aceasta nu conținea date cu caracter personal care îl privesc, în sensul Legii privind protecția datelor.

Întrucât comisarul pentru protecția datelor nu a dat curs cererii sale de acces pentru aceleași motive, domnul Nowak a introdus o acțiune în fața instanțelor naționale. Supreme Court (Curtea Supremă, Irlanda), sesizată cu un recurs formulat de domnul Nowak, a solicitat Curții să se pronunțe asupra chestiunii dacă articolul 2 litera (a) din Directiva 95/46 trebuie interpretat în sensul că, în împrejurări precum cele în discuție în litigiul principal, răspunsurile scrise oferite de un candidat în timpul unei examinări profesionale și eventualele comentarii ale examinatorului cu privire la acestea constituie date cu caracter personal referitoare la solicitant, în sensul acestei dispoziții.

În primul rând, Curtea a arătat că, pentru ca o dată să poată fi considerată „dată cu caracter personal”, în sensul articolului 2 litera (a) din Directiva 95/46, nu este necesar ca toate informațiile care permit identificarea persoanei vizate să se afle în posesia unei singure persoane. Pe de altă parte, în ipoteza în care examinatorul nu cunoaște identitatea candidatului cu ocazia notării răspunsurilor furnizate de acesta în cadrul unui examen, entitatea care organizează examenul, în speță ordinul experților contabili, dispune, în schimb, de informațiile necesare care îi permit să identifice acest candidat fără dificultăți sau îndoieli, pe baza numărului său de identificare, consemnat pe foaia de examinare sau pe pagina de gardă a acestei foi, și astfel să îi atribuie răspunsurile furnizate.

În al doilea rând, Curtea a constatat că răspunsurile scrise oferite de un candidat la un examen profesional reprezintă informații referitoare la acesta. Astfel, conținutul acestor răspunsuri reflectă nivelul cunoștințelor și al competențelor candidatului într-un anumit domeniu, precum și, după caz, procesul de gândire, raționamentul și spiritul său critic. Mai mult, colectarea răspunsurilor respective are ca finalitate evaluarea capacităților profesionale ale candidatului și a capacității acestuia de a exercita profesia în cauză. În plus, utilizarea acestor informații, care se reflectă în special în succesul sau eșecul candidatului la examenul respectiv, poate avea impact asupra drepturilor și intereselor acestuia, în măsura în care poate determina sau influența, de exemplu, șansele de acces la exercitarea profesiei sau la locul de muncă dorit. Constatarea că răspunsurile scrise furnizate de un candidat la un examen profesional constituie informații referitoare la acest candidat ca urmare a conținutului, a finalității și a efectului lor este valabilă, pe de altă parte, și atunci când este vorba, precum în speță, despre un examen cu cărțile deschise.

În al treilea rând, în ceea ce privește observațiile examinatorului cu privire la răspunsurile candidatului, Curtea a considerat că acestea constituie, împreună cu răspunsurile formulate de către candidat la momentul examenului, informații referitoare la respectivul candidat, întrucât ele reflectă opinia sau aprecierea examinatorului cu privire la performanțele individuale ale candidatului în timpul examenului, în special cu privire la cunoștințele și la competențele sale în domeniul vizat. Pe de altă parte, observațiile menționate au ca finalitate tocmai să documenteze

evaluarea de către examinator a performanțelor candidatului și sunt susceptibile să aibă efecte asupra acestuia din urmă.

În al patrulea rând, Curtea a considerat că răspunsurile scrise furnizate de un candidat în cadrul unui examen profesional și eventualele observații ale examinatorului care se referă la acestea sunt susceptibile să fie supuse unei verificări, în special în ceea ce privește exactitatea și necesitatea păstrării lor, în sensul articolului 6 alineatul (1) literele (d) și (e) din Directiva 95/46, și pot face obiectul unei rectificări sau al unei ștergeri, în temeiul articolului 12 litera (b) din aceasta. Faptul de a acorda candidatului un drept de acces la aceste răspunsuri și observații, în temeiul articolului 12 litera (a) din respectiva directivă, servește la realizarea obiectivului acesteia din urmă care constă în asigurarea protecției dreptului la viață privată al candidatului menționat referitor la prelucrarea datelor care îl privesc, iar aceasta independent de aspectul dacă respectivul candidat dispune sau nu dispune de un asemenea drept de acces și în temeiul reglementării naționale aplicabile procedurii de examinare. Cu toate acestea, Curtea a subliniat că drepturile de acces și de rectificare, în temeiul articolului 12 literele (a) și (b) din Directiva 95/46, nu se extind la întrebările din examen, care nu constituie, ca atare, date cu caracter personal ale candidatului.

Având în vedere aceste elemente, Curtea a concluzionat că, în împrejurări precum cele în discuție în litigiul principal, răspunsurile scrise furnizate de un candidat în cadrul unui examen profesional și eventualele observații ale examinatorului referitoare la aceste răspunsuri constituie date cu caracter personal în sensul articolului 2 litera (a) din Directiva 95/46.

3. Noțiunea de „prelucrare a datelor cu caracter personal”

Hotărârea din 6 noiembrie 2003 (Marea Cameră), Lindqvist (C-101/01, EU:C:2003:596)

Doamna Lindqvist, care efectua muncă voluntară într-o parohie a Bisericii Protestante din Suedia, a creat pe calculatorul personal pagini de internet pe care a publicat date cu caracter personal cu privire la mai multe persoane care lucrau, ca și ea, în mod voluntar în cadrul parohiei respective. Doamna Lindqvist a fost obligată să plătească o amendă pe motiv că a utilizat date cu caracter personal în cadrul unei prelucrări automate fără a depune o declarație scrisă în prealabil la Datainspektion (organism public suedez de protecție a datelor transmise electronic), că le-a transferat fără autorizație către țări terțe și că a prelucrat date cu caracter personal sensibile.

În cadrul apelului formulat de doamna Lindqvist împotriva acestei decizii în fața Göta hovrätt (Curtea de Apel, Suedia), aceasta din urmă a sesizat cu titlu preliminar Curtea, în special pentru a stabili dacă doamna Lindqvist ar fi efectuat o „prelucrare automată, în totalitate sau parțial, a datelor cu caracter personal”, în sensul Directivei 95/46.

Curtea a constatat că operațiunea care constă în a se referi, pe o pagină de internet, la diverse persoane și în a le identifica fie prin nume, fie prin alte mijloace, de exemplu prin numărul de telefon sau prin informații privind condițiile de muncă și modul de petrecere a timpului liber, constituie o „prelucrare automată, în totalitate sau parțial, a datelor cu caracter personal", în sensul acestei directive. Astfel, o asemenea prelucrare a datelor cu caracter personal utilizată pentru exercitarea de activități voluntare sau religioase nu intră sub incidența niciuneia dintre excepțiile de la domeniul de aplicare al directivei, în măsura în care nu se încadrează nici în categoria de activități care au ca obiect siguranța publică, nici în categoria activităților exclusiv personale sau domestice, care nu intră în domeniul de aplicare al directivei.

Hotărârea din 13 mai 2014 (Marea Cameră), Google Spain și Google (C-131/12, EU:C:2014:317)

În această hotărâre (a se vedea și secțiunea II.1., intitulată „Domeniul de aplicare al reglementării generale"), Curtea a avut ocazia să clarifice noțiunea de „prelucrare a datelor cu caracter personal" pe internet din perspectiva Directivei 95/46.

Curtea a hotărât astfel că activitatea unui motor de căutare care constă în găsirea informațiilor publicate sau introduse pe internet de terți, în indexarea acestora în mod automat și în păstrarea lor temporară și, în cele din urmă, în punerea acestora la dispoziția utilizatorilor de internet într-o anumită ordine de preferință trebuie calificată drept prelucrare a datelor cu caracter personal atunci când informațiile respective conțin date cu caracter personal. De asemenea, Curtea a precizat că operațiunile vizate de directivă trebuie calificate ca fiind prelucrare și în ipoteza în care privesc exclusiv informații deja publicate ca atare în mass-media. O derogare generală de la aplicarea directivei într-o asemenea ipoteză ar lipsi directiva în mare parte de sens.

Hotărârea din 10 iulie 2018 (Marea Cameră), Jehovan todistajat (C-25/17, EU:C:2018:551)

Autoritatea finlandeză pentru protecția datelor a adoptat o decizie prin care a interzis Comunității Martorilor lui Iehova să colecteze sau să prelucreze date cu caracter personal în cadrul activității de predicare din casă în casă efectuate de membrii săi fără respectarea condițiilor prevăzute în legislația finlandeză privind prelucrarea unor asemenea date. Astfel, membrii acestei comunități, în cadrul activității lor de predicare din casă în casă, iau note privind vizitele efectuate la persoane pe care ei înșiși sau comunitatea menționată nu le cunosc. Datele respective sunt colectate pentru a servi drept aide-mémoire și pentru a putea fi recuperate în scopul unei eventuale vizite ulterioare, fără ca persoanele vizate să fi consimțit la aceasta sau să fi fost informate despre colectarea lor. În această privință, Comunitatea Martorilor lui Iehova a stabilit orientări referitoare la luarea unor astfel de note, care figurează cel puțin în una dintre revistele sale consacrate activității de predicare.

Curtea a considerat că colectarea de date cu caracter personal efectuată de membrii unei comunități religioase în cadrul unei activități de predicare din casă în casă și prelucrarea ulterioară a acestor date nu intră sub incidența excepțiilor de la domeniul de aplicare al Directivei 95/46, întrucât acestea nu constituie nici prelucrare de date cu caracter personal efectuată în scopul exercitării unor activități prevăzute la articolul 3 alineatul (2) prima liniuță din această directivă, nici prelucrare de date cu caracter personal efectuată de persoane fizice în scopul exercitării unei activități exclusiv personale sau domestice, în sensul articolului 3 alineatul (2) a doua liniuță din directiva menționată.

Hotărârea din 22 iunie 2021 (Marea Cameră), Latvijas Republikas Saeima (Puncte de penalizare) (C-439/19, EU:C:2021:504)

În urma uneia sau mai multor încălcări ale normelor de circulație rutieră, lui B, o persoană fizică, i-au fost aplicate puncte de penalizare. Aceste puncte de penalizare au fost înscrise de Ceļu satiksmes drošības direkcija (Direcția pentru Siguranța Rutieră, Letonia) (denumită în continuare „CSDD”) în registrul național al vehiculelor și al conducătorilor auto.

În temeiul reglementării letone privind circulația rutieră[34], informațiile referitoare la punctele de penalizare aplicate conducătorilor de vehicule înscrise în acest registru sunt accesibile publicului și sunt comunicate de CSDD oricărei persoane care solicită acest lucru, fără ca această persoană să fie ținută să justifice un interes specific în obținerea informațiilor respective, inclusiv operatorilor economici în vederea reutilizării. Ridicând problema legalității acestei reglementări, B a formulat o acțiune constituțională la Latvijas Republikas Satversmes tiesa (Curtea Constituțională, Letonia) pentru ca aceasta să examineze conformitatea reglementării menționate cu dreptul la respectarea vieții private.

Curtea Constituțională a considerat că, în cadrul aprecierii sale asupra acestui drept constituțional, trebuie să ia în considerare RGPD. Astfel, ea a solicitat Curții să clarifice înțelesul mai multor dispoziții din RGPD în scopul de a determina compatibilitatea reglementării letone privind circulația rutieră cu acest regulament.

Prin hotărârea sa, pronunțată în Marea Cameră, Curtea statuează că prelucrarea datelor cu caracter personal referitoare la punctele de penalizare constituie o „prelucrare de date cu caracter personal referitoare la condamnări penale și infracțiuni”[35], pentru care RGPD prevede o protecție sporită din cauza caracterului deosebit de sensibil al datelor în cauză.

---

[34] Articolul 14[1] alineatul (2) din Ceļu satiksmes likums (Legea privind circulația rutieră) din 1 octombrie 1997 (*Latvijas Vēstnesis*, 1997, nr. 274/276).

[35] Articolul 10 din RGPD.

În acest cadru, Curtea observă, cu titlu introductiv, că informațiile referitoare la punctele de penalizare sunt date cu caracter personal și că comunicarea lor de către CSDD unor terți constituie o prelucrare care intră în domeniul de aplicare material al RGPD. Astfel, acest domeniu de aplicare este foarte larg, iar această prelucrare nu intră sub incidența excepțiilor de la aplicabilitatea regulamentului menționat.

În acest sens, pe de o parte, această prelucrare nu intră sub incidența excepției referitoare la neaplicarea RGPD în cazul unei prelucrări efectuate în cadrul unei activități care nu intră sub incidența dreptului Uniunii[36]. Această excepție trebuie considerată ca având ca unic obiectiv excluderea din domeniul de aplicare al regulamentului menționat a prelucrărilor de date cu caracter personal efectuate de autoritățile de stat în cadrul unei activități de apărare a securității naționale sau al unei activități care poate fi încadrată în aceeași categorie. Aceste activități cuprind activitățile care urmăresc protejarea funcțiilor esențiale ale statului și a intereselor fundamentale ale societății. Or, activitățile referitoare la siguranța rutieră nu urmăresc acest obiectiv și nu pot fi încadrate, așadar, în categoria activităților care au ca scop apărarea securității naționale.

Pe de altă parte, comunicarea datelor personale referitoare la punctele de penalizare nu este o prelucrare acoperită de excepția care prevede neaplicarea RGPD în cazul prelucrării datelor cu caracter personal efectuate de autoritățile competente în materie penală[37]. Curtea constată astfel că CSDD nu poate fi considerată, atunci când efectuează comunicarea menționată, o astfel de „autoritate competentă”[38].

Pentru a stabili dacă accesul la datele cu caracter personal referitoare la încălcarea normelor de circulație, precum punctele de penalizare, constituie o prelucrare de date cu caracter personal referitoare la „infracțiuni”[39], care beneficiază de o protecție sporită, Curtea constată, întemeindu-se în special pe geneza RGPD, că această noțiune se referă exclusiv la infracțiunile penale. Faptul că în sistemul juridic leton încălcările normelor de circulație sunt calificate drept administrative nu este însă determinant pentru a aprecia dacă aceste încălcări intră sub incidența noțiunii de „infracțiune”, în măsura în care este vorba despre o noțiune autonomă de drept al Uniunii care necesită în întreaga Uniune o interpretare autonomă și uniformă. Astfel, după ce amintește cele trei criterii pertinente pentru aprecierea caracterului penal al unei fapte ilicite, și anume calificarea juridică a faptei ilicite în dreptul intern, natura faptei ilicite și gradul de severitate al sancțiunii aplicate, Curtea statuează că încălcările normelor de circulație în cauză intră sub incidența noțiunii de „infracțiune” în sensul RGPD. În ceea ce privește primele două criterii, Curtea constată că, deși faptele ilicite nu sunt calificate drept „penale” în dreptul

36 Articolul 2 alineatul (2) litera (a) din RGPD.

37 Articolul 2 alineatul (2) litera (d) din RGPD.

38 Articolul 3 alineatul (7) din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO 2016, L 119, p. 89).

39 Articolul 10 din RGPD.

național, un asemenea caracter poate decurge din natura faptei ilicite și în special din finalitatea represivă urmărită de sancțiunea pe care infracțiunea o poate antrena. Or, în speță, atribuirea unor puncte de penalizare pentru încălcarea normelor de circulație rutieră, precum și celelalte sancțiuni pe care aceste încălcări le pot antrena urmăresc printre altele o astfel de finalitate represivă. În ceea ce privește al treilea criteriu, Curtea observă că numai încălcările normelor de circulație rutieră de o anumită gravitate presupun atribuirea unor puncte de penalizare și că, prin urmare, acestea pot antrena sancțiuni de o anumită gravitate. Mai mult, aplicarea punctelor respective se adaugă în general sancțiunii impuse, iar cumularea punctelor menționate antrenează consecințe juridice care pot merge chiar până la interdicția de a conduce.

Hotărârea din 5 decembrie 2023 (Marea Cameră), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

În anul 2020, pentru a gestiona mai bine pandemia de COVID-19, autoritățile lituaniene au decis să organizeze achiziționarea unei aplicații informatice mobile. Această aplicație trebuia să contribuie la o monitorizare epidemiologică, permițând înregistrarea și monitorizarea datelor persoanelor expuse virusului COVID-19.

În acest scop, Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (Centrul Național de Sănătate Publică din cadrul Ministerului Sănătății, Lituania, denumit în continuare „CNSP”), însărcinat cu această achiziție, a contactat societatea UAB „IT sprendimai sėkmei” (denumită în continuare „societatea ITSS”), solicitându-i să procedeze la crearea unei astfel de aplicații mobile. Ulterior, e-mailuri privind în special aspectele care trebuiau să figureze în această aplicație au fost adresate acestei societăți de angajații CNSP.

În perioada aprilie-mai 2020, aplicația mobilă creată de societatea ITSS a fost pusă la dispoziția publicului. În consecință, 3 802 persoane au utilizat-o și au furnizat diferite date, solicitate de această aplicație, care le privesc. Cu toate acestea, din cauza unei lipse de finanțare, CNSP nu a atribuit societății ITSS niciun contract de achiziții publice pentru achiziționarea oficială a aplicației sale mobile și a pus capăt procedurii aferente.

Între timp, autoritatea națională de supraveghere a inițiat o investigație cu privire la prelucrarea datelor cu caracter personal care a rezultat din utilizarea acestei aplicații. Prin decizia respectivei autorități, adoptată la finalul investigației, au fost impuse amenzi administrative atât CNSP, cât și societății ITSS în calitate de operator asociat.

CNSP a contestat această decizie la Vilniaus apygardos administracinis teismas (Tribunalul Administrativ Regional din Vilnius, Lituania). Având îndoieli cu privire la interpretarea mai multor dispoziții ale RGPD, această instanță a sesizat Curtea cu titlu preliminar.

În hotărârea sa, Curtea, reunită în Marea Cameră, aduce precizări printre altele cu privire la noțiunea de „prelucrare”. Ea arată în această privință că utilizarea datelor cu

caracter personal în scopul testării informatice a unei aplicații mobile constituie o prelucrare în sensul RGPD. Cu toate acestea, situația este diferită dacă asemenea date ar fi fost anonimizate, așa încât persoana vizată de aceste date nu este sau nu mai este identificabilă ori este vorba despre date fictive care nu se referă la o persoană fizică existentă.

Astfel, pe de o parte, aspectul dacă datele cu caracter personal sunt utilizate pentru teste informatice sau în alt scop nu are incidență asupra calificării operațiunii în cauză drept „prelucrare". Pe de altă parte, numai o prelucrare care vizează date cu caracter personal poate fi calificată drept „prelucrare" în sensul RGPD. Or, datele fictive sau anonime nu constituie date cu caracter personal.

4. Noțiunea de „sistem de evidență a datelor cu caracter personal"

Hotărârea din 10 iulie 2018 (Marea Cameră), Jehovan todistajat (C-25/17, EU:C:2018:551)

În această hotărâre (a se vedea și secțiunea II.3, intitulată „Noțiunea de «prelucrare a datelor cu caracter personal»"), Curtea a precizat noțiunea de „sistem de evidență", prevăzută la articolul 2 litera (c) din Directiva 95/46.

Astfel, după ce a amintit că această directivă se aplică prelucrării manuale a datelor cu caracter personal numai atunci când datele prelucrate sunt cuprinse sau sunt destinate să facă parte dintr-un sistem de evidență, Curtea a arătat că noțiunea menționată acoperă o serie de date cu caracter personal colectate în cadrul unei activități de predicare din casă în casă, care include numele și adresele, precum și alte informații referitoare la persoanele abordate, din moment ce aceste date sunt structurate potrivit unor criterii determinate care permit în practică recuperarea lor cu ușurință în scopul unei utilizări ulterioare. Pentru ca o astfel de serie de date să intre în sfera acestei noțiuni, nu este necesar ca ea să cuprindă fișe, liste specifice sau alte sisteme de căutare.

5. Noțiunea de „operator de date cu caracter personal"

Hotărârea din 10 iulie 2018 (Marea Cameră), Jehovan todistajat (C-25/17, EU:C:2018:551)

În această cauză (a se vedea și secțiunile II.3 și II.4, intitulate „Noțiunea de «prelucrare a datelor cu caracter personal»" și „Noțiunea de «sistem de evidență a datelor cu caracter personal»"), Curtea s-a pronunțat cu privire la responsabilitatea unei comunități religioase în ceea ce privește prelucrarea datelor cu caracter personal efectuată în

cadrul unei activități de predicare din casă în casă organizate, coordonate și încurajate de această comunitate.

Astfel, Curtea a apreciat că obligația oricărei persoane de a respecta normele dreptului Uniunii referitoare la protecția datelor cu caracter personal nu poate fi considerată o ingerință în autonomia organizațională a comunităților religioase. În această privință, Curtea a concluzionat că articolul 2 litera (d) din Directiva 95/46, citit în lumina articolului 10 alineatul (1) din cartă, trebuie interpretat în sensul că permite ca o comunitate religioasă să fie considerată operator, împreună cu membrii săi predicatori, în ceea ce privește prelucrarea unor date cu caracter personal efectuată de aceștia din urmă în cadrul unei activități de predicare din casă în casă organizate, coordonate și încurajate de această comunitate, fără să fie necesar ca respectiva comunitate să aibă acces la date și fără să fie necesar să se fi stabilit că ea a dat membrilor săi orientări scrise sau instrucțiuni referitoare la o astfel de prelucrare.

Hotărârea din 5 iunie 2018 (Marea Cameră), Wirtschaftsakademie Schleswig Holstein (C-210/16, EU:C:2018:388)

Autoritatea germană de protecție a datelor, în calitatea sa de autoritate de supraveghere, în sensul articolului 28 din Directiva 95/46, a somat o societate germană specializată în domeniul educației și care oferă servicii de formare prin intermediul unei pagini pentru fani găzduite pe site-ul rețelei sociale Facebook să dezactiveze această pagină. Astfel, potrivit autorității menționate, nici această societate, nici Facebook nu au informat vizitatorii paginii pentru fani că aceasta din urmă colecta, cu ajutorul unor cookies, informații cu caracter personal care îi vizau și că societatea menționată și Facebook prelucrau apoi respectivele informații.

În acest context, Curtea a precizat noțiunea de „operator” de date cu caracter personal. În această privință, ea a considerat că administratorul unei pagini pentru fani găzduite de Facebook, precum societatea în discuție în litigiul principal, participă, prin acțiunea sa de stabilire a unor parametri (în funcție, printre altele, de audiența sa țintă, precum și de obiective de gestionare sau de promovare a activităților sale), la stabilirea scopurilor și a mijloacelor de prelucrare a datelor personale ale vizitatorilor paginii sale pentru fani. Pentru acest motiv, potrivit Curții, acest administrator trebuie să fie calificat drept operator, în cadrul Uniunii, împreună cu Facebook Ireland (filiala din Uniune a societății americane Facebook), în sensul articolului 2 litera (d) din Directiva 95/46.

Hotărârea din 29 iulie 2019, Fashion ID (C-40/17, EU:C:2019:629)

În această cauză, Curtea a avut ocazia să dezvolte noțiunea de „operator” în raport cu integrarea unui „plug in” într-o pagină web.

În speță, Fashion ID, o întreprindere germană care comercializează online articole de modă, a inserat pe site-ul său internet modulul social „îmi place” al rețelei sociale

Facebook. Această inserare pare să aibă drept consecință că, atunci când un vizitator consultă site-ul internet al Fashion ID, date cu caracter personal ale acestui vizitator sunt transmise societății Facebook Ireland. Rezultă că această transmitere se efectuează fără ca vizitatorul menționat să fie conștient de ea și indiferent dacă acesta este membru al rețelei Facebook sau a clicat pe butonul „îmi place” al Facebook.

Verbraucherzentrale NRW, asociație germană de utilitate publică pentru apărarea intereselor consumatorilor, reproșează societății Fashion ID că a transmis societății Facebook Ireland date cu caracter personal aparținând vizitatorilor site-ului său internet, pe de o parte, fără consimțământul acestora din urmă și, pe de altă parte, cu încălcarea obligațiilor de informare prevăzute de dispozițiile referitoare la protecția datelor personale. Sesizat cu litigiul, Oberlandesgericht Düsseldorf (Tribunalul Regional Superior din Düsseldorf, Germania) a solicitat Curții să interpreteze mai multe dispoziții ale Directivei 95/46.

Curtea a constatat mai întâi că administratorul unui site internet precum Fashion ID poate fi considerat operator, în sensul articolului 2 litera (d) din Directiva 95/46. Această calitate de operator este însă limitată la operațiunea sau la ansamblul operațiunilor de prelucrare de date cu caracter personal cărora el le stabilește efectiv scopurile și mijloacele, și anume colectarea și dezvăluirea prin transmitere a datelor în cauză. În schimb, potrivit Curții, pare, la prima vedere, exclus ca Fashion ID să stabilească scopurile și mijloacele operațiunilor de prelucrare de date cu caracter personal ulterioare, efectuate de Facebook Ireland după transmiterea lor către aceasta din urmă, astfel încât Fashion ID nu poate fi considerată operator în raport cu aceste operațiuni, în sensul acestui articol 2 litera (d).

În plus, Curtea a subliniat că este necesar ca administratorul unui site internet și furnizorul unui modul social precum Facebook Ireland să urmărească, fiecare, prin intermediul acestor operațiuni de prelucrare, un interes legitim, în sensul articolului 7 litera (f) din Directiva 95/46, pentru ca acestea să fie justificate în ceea ce îl privește.

În sfârșit, Curtea a precizat că consimțământul persoanei vizate, prevăzut la articolul 2 litera (h) și la articolul 7 litera (a) din Directiva 95/46, trebuie să fie obținut de administratorul unui site internet numai în ceea ce privește operațiunile de prelucrare a datelor cu caracter personal cărora administratorul menționat le stabilește scopurile și mijloacele. Într-o astfel de situație, obligația de informare prevăzută la articolul 10 din această directivă incumbă și administratorului menționat, informația pe care acesta din urmă are obligația să o furnizeze persoanei vizate netrebuind să privească însă decât operațiunea sau ansamblul de operațiuni de prelucrare a datelor cu caracter personal cărora el le stabilește scopurile și mijloacele.

Hotărârea din 5 decembrie 2023 (Marea Cameră), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

În această cauză (a se vedea și secțiunea II.3, intitulată „Noțiunea de «prelucrare a datelor cu caracter personal»”), Curtea arată că o entitate care a însărcinat o întreprindere să dezvolte o aplicație informatică mobilă și care, în acest context, a participat la stabilirea scopurilor și a mijloacelor prelucrării datelor cu caracter personal realizate prin intermediul acestei aplicații poate fi considerată operator[40]. Această considerație nu poate fi repusă în discuție de faptul că entitatea menționată nu a efectuat ea însăși operațiuni de prelucrare a unor astfel de date, nu și-a dat în mod explicit acordul pentru realizarea unor operațiuni concrete ale unei asemenea prelucrări sau pentru punerea la dispoziția publicului a aplicației mobile amintite și nu a achiziționat aceeași aplicație mobilă, cu excepția cazului în care, înainte de respectiva punere la dispoziția publicului, entitatea menționată s-a opus în mod expres acesteia și prelucrării datelor cu caracter personal care au rezultat din aceasta.

6. Noțiunea de „operator asociat”

Hotărârea din 5 decembrie 2023 (Marea Cameră), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

În această cauză (a se vedea și secțiunile II.3 și II.5, intitulate „Noțiunea de «prelucrare a datelor cu caracter personal»” și „Noțiunea de «operator de date cu caracter personal»”), Curtea observă că faptul de a califica două entități drept operatori asociați nu presupune nici existența unui acord între aceste entități cu privire la stabilirea scopurilor și a mijloacelor prelucrării datelor cu caracter personal în cauză, nici existența unui acord care stabilește condițiile referitoare la responsabilitatea comună privind prelucrarea. Desigur, în temeiul RGPD[41], operatorii asociați trebuie, prin intermediul unui acord între ei, să își stabilească în mod transparent obligațiile care le revin pentru a asigura respectarea cerințelor respectivului regulament. Cu toate acestea, existența unui asemenea acord nu constituie o condiție prealabilă pentru ca două sau mai multe entități să fie calificate drept operatori asociați, ci o obligație pe care RGPD o impune operatorilor asociați, odată calificați ca atare, pentru a asigura respectarea cerințelor care le revin în temeiul acestui regulament. Astfel, această calificare decurge din simplul fapt că mai multe entități au participat la stabilirea scopurilor și a mijloacelor prelucrării.

În ceea ce privește stabilirea în comun de către entitățile în cauză a scopurilor și a mijloacelor prelucrării, Curtea precizează că participarea lor la această stabilire se poate

[40] În sensul articolului 4 punctul 7 din RGPD.
[41] Articolul 26 alineatul (1) din RGPD, interpretat în lumina considerentului (79) al acestuia.

regăsi sub diferite forme și poate rezulta atât din decizia lor comună, cât și din deciziile convergente ale acestora. Or, în acest ultim caz, deciziile menționate trebuie să se completeze, astfel încât fiecare dintre ele să aibă un efect concret asupra stabilirii scopurilor și a mijloacelor prelucrării.

7. Condiții de legalitate a unei prelucrări de date cu caracter personal

Hotărârea din 16 decembrie 2008 (Marea Cameră), Huber (C-524/06, EU:C:2008:724)

Bundesamt für Migration und Flüchtlinge (Oficiul Federal pentru Migrație și Refugiați, Germania) asigura gestionarea unui registru național al străinilor care centraliza anumite date cu caracter personal referitoare la străinii care locuiesc pe teritoriul german pentru o perioadă mai lungă de trei luni. Registrul era utilizat în scopuri statistice și pentru exercitarea de către serviciile de securitate și de poliție, precum și de către autoritățile judiciare a competenței acestora în materie de cercetare și de urmărire penală a actelor infracționale sau a celor care pun în pericol siguranța publică.

Domnul Huber, resortisant austriac, s-a stabilit în Germania în anul 1996 pentru a exercita în acest stat profesia de agent de asigurări independent. Întrucât se consideră discriminat ca urmare a prelucrării datelor care îl privesc conținute în registrul menționat, o astfel de bază de date neexistând pentru resortisanții germani, domnul Huber a solicitat ștergerea acestor date.

În aceste condiții, Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Tribunalul Administrativ Superior al Landului Rinul de Nord-Westphalia, Germania), sesizat cu litigiul, a solicitat Curții să se pronunțe cu privire la compatibilitatea cu dreptul Uniunii a prelucrării datelor cu caracter personal efectuate în registrul în cauză.

Curtea a amintit, mai întâi, că dreptul de ședere pe teritoriul unui stat membru al unui cetățean al Uniunii care nu este resortisant al acestuia nu este unul necondiționat, ci poate fi supus limitărilor. Prin urmare, utilizarea unui astfel de registru în scopul de a sprijini autoritățile însărcinate cu aplicarea dispozițiilor privind dreptul de ședere este, în principiu, legitimă și, având în vedere natura sa, este compatibilă cu interzicerea discriminării exercitate pe motiv de cetățenie, conținută în articolul 12 primul paragraf CE (în prezent articolul 18 primul paragraf TFUE). Un astfel de registru nu poate conține însă alte informații decât cele care sunt necesare în acest scop în sensul Directivei privind protecția datelor cu caracter personal.

În ceea ce privește noțiunea de „necesitate” a prelucrării în sensul articolului 7 litera (e) din Directiva 95/46, Curtea a amintit mai întâi că este vorba despre o noțiune autonomă de drept al Uniunii, care trebuie să primească o interpretare de natură să reflecte pe deplin obiectul Directivei 95/46, astfel cum este definit la articolul 1 alineatul (1). În continuare, Curtea a constatat că un sistem de prelucrare a datelor cu caracter personal

nu respectă legislația Uniunii decât în cazul în care conține numai datele necesare pentru aplicarea de către autoritățile menționate a acestor dispoziții și în cazul în care caracterul său centralizat permite o aplicare mai eficientă a acestor dispoziții în ceea ce privește dreptul de ședere al cetățenilor Uniunii care nu sunt resortisanți ai acestui stat membru.

În orice caz, nu pot fi considerate necesare în sensul articolului 7 litera (e) din Directiva 95/46 stocarea și prelucrarea datelor cu caracter personal nominale în cadrul unui asemenea registru în scopuri statistice.

Pe de altă parte, în ceea ce privește utilizarea datelor cuprinse în registru în scopul combaterii criminalității, Curtea a remarcat în special că acest obiectiv vizează anchetarea infracțiunilor comise, indiferent de cetățenia autorilor acestora. Prin urmare, din punctul de vedere al unui stat membru, situația resortisanților săi nu poate fi diferită de cea a cetățenilor Uniunii care nu sunt resortisanți ai acestui stat membru și care locuiesc pe teritoriul său în ceea ce privește obiectivul combaterii criminalității. În consecință, diferența de tratament dintre acești resortisanți și acești cetățeni ai Uniunii, determinată de prelucrarea sistematică a datelor cu caracter personal referitoare numai la cetățenii Uniunii care nu sunt resortisanți ai statului membru în cauză și având ca obiectiv combaterea criminalității, constituie o discriminare interzisă de articolul 12 primul paragraf CE.

Hotărârea din 19 octombrie 2016, Breyer (C-582/14, EU:C:2016:779)

În această hotărâre (a se vedea și secțiunea II.2, intitulată „Noțiunea de «date cu caracter personal»”), Curtea s-a pronunțat de asemenea cu privire la chestiunea dacă articolul 7 litera (f) din Directiva 95/46 se opune unei dispoziții de drept național în temeiul căreia un furnizor de servicii de comunicații electronice poate colecta și utiliza datele cu caracter personal aferente unui utilizator în lipsa consimțământului acestuia numai în măsura în care această colectare și această utilizare sunt necesare pentru a permite și a factura utilizarea concretă a serviciilor respective de către acest utilizator și în temeiul căreia finalitatea care constă în asigurarea funcționalității generale a aceluiași servicii nu poate justifica utilizarea datelor după o sesiune de consultare a acestora.

Curtea a constatat că articolul 7 litera (f) din Directiva 95/46 se opune reglementării în cauză. Astfel, în temeiul acestei dispoziții, prelucrarea datelor cu caracter personal în sensul acestei dispoziții este legală în cazul în care este necesară în scopul realizării interesului legitim urmărit de operator sau de terțul ori de terții cărora le sunt comunicate datele, cu condiția să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate. Or, în speță, legislația germană a exclus în mod categoric și generalizat posibilitatea ca anumite categorii de date cu caracter personal să fie prelucrate, fără a permite o ponderare a drepturilor și a intereselor opuse în cauză într-un anumit caz. Astfel, aceasta a restrâns în mod ilicit domeniul de aplicare al acestui principiu prevăzut la articolul 7 litera (f) din Directiva 95/46, excluzând ca obiectivul de

asigurare a funcționalității generale a comunicațiilor electronice să poată face obiectul unei ponderări cu interesul sau cu drepturile și libertățile fundamentale ale utilizatorilor.

Hotărârea din 27 septembrie 2017, Puškár (C-73/16, EU:C:2017:725)

În litigiul principal, domnul Puškár a formulat o acțiune la Najvyšší súd Slovenskej republiky (Curtea Supremă a Republicii Slovace), solicitând obligarea Finančné riaditel'stvo (Direcția Finanțelor), a tuturor birourilor de impozite subordonate acesteia și a Kriminálny úrad finančnej správy (Biroul de Combatere a Criminalității Financiare) să nu înscrie numele său în lista persoanelor considerate de Direcția Finanțelor ca interpuși, întocmită de aceasta în cadrul perceperii impozitului și a cărei actualizare este asigurată de Direcția Finanțelor, precum și de Biroul de Combatere a Criminalității Financiare (denumită în continuare „lista în litigiu"). În plus, acesta a solicitat să se elimine orice mențiune care îl privește din aceste liste și din sistemul informatic al administrației financiare.

În aceste condiții, Najvyšší súd Slovenskej republiky (Curtea Supremă a Republicii Slovace) a sesizat Curtea printre altele cu problema dacă dreptul la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor, prevăzut la articolul 7, precum și dreptul la protecția datelor cu caracter personal, consacrat la articolul 8 din cartă, trebuie interpretate în sensul că nu permit unui stat membru să creeze, fără consimțământul persoanei în cauză, liste de date cu caracter personal în scopul perceperii impozitului, astfel încât obținerea de date cu caracter personal de către autoritățile publice în scopul combaterii fraudei fiscale să reprezinte un risc în sine.

Curtea a hotărât că articolul 7 litera (e) din Directiva 95/46 nu se opune unei prelucrări de date cu caracter personal de către autoritățile unui stat membru în scopul perceperii impozitului și al combaterii fraudei fiscale, precum cea care este efectuată în cauza principală prin întocmirea unei liste de persoane, fără consimțământul persoanelor în cauză, cu condiția, pe de o parte, ca aceste autorități să fi fost învestite prin legislația națională cu sarcini de interes public în sensul acestei dispoziții, ca întocmirea respectivei liste și înscrierea în aceasta a numelui persoanelor în cauză să fie efectiv apte și necesare în scopul realizării obiectivelor urmărite și să existe indicii suficiente pentru a prezuma că persoanele în cauză figurează în mod întemeiat în lista menționată și, pe de altă parte, ca toate condițiile de legalitate a acestei prelucrări de date cu caracter personal impuse prin Directiva 95/46 să fie îndeplinite.

În această privință, Curtea a statuat că revine instanței de trimitere obligația de a verifica dacă întocmirea listei în litigiu este necesară pentru executarea sarcinilor de interes public în discuție în litigiul principal, ținând seama printre altele de finalitatea exactă a întocmirii listei în litigiu, de efectele juridice la care sunt supuse persoanele care figurează în aceasta și de caracterul public sau nepublic al acestei liste. În plus, cu privire la principiul proporționalității, revine instanței de trimitere obligația de a verifica dacă întocmirea listei în litigiu și includerea în aceasta a numelor persoanelor în cauză sunt de

natură să realizeze obiectivele urmărite prin acestea și dacă nu există alte mijloace mai puțin restrictive pentru atingerea acestor obiective.

În plus, Curtea a constatat că includerea unei persoane în lista în litigiu este de natură să aducă atingere anumitor drepturi ale acesteia. Astfel, o înscriere în lista menționată ar putea dăuna reputației sale și ar putea afecta relațiile sale cu autoritățile fiscale. În mod similar, această înscriere ar putea afecta prezumția de nevinovăție a persoanei menționate, consacrată la articolul 48 alineatul (1) din cartă, precum și libertatea de a desfășura o activitate comercială, prevăzută la articolul 16 din cartă, a persoanelor juridice asociate persoanelor fizice înscrise în lista în litigiu. Rezultă că o asemenea atingere nu poate fi adecvată decât dacă există suficiente indicii pentru a suspecta persoana vizată că ocupă în mod fictiv funcții de conducere în cadrul persoanelor juridice care îi sunt asociate și că aduce astfel atingere perceperii impozitului și combaterii fraudei fiscale.

Pe de altă parte, Curtea a considerat că, dacă ar exista motive pentru a limita, în temeiul articolului 13 din Directiva 95/46, anumite drepturi prevăzute la articolele 6 și 10-12 din aceasta, precum dreptul de informare al persoanei în cauză, o astfel de limitare ar trebui să fie necesară pentru protejarea unui interes menționat la alineatul (1) al articolului 13 respectiv, precum, printre altele, un interes economic și financiar important în domeniul fiscal, și să se întemeieze pe măsuri legislative.

Hotărârea din 11 noiembrie 2020, Orange Romania (C-61/19, EU:C:2020:901)

Orange România SA furnizează servicii de telecomunicații mobile pe piața românească. La 28 martie 2018, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (România) i-a aplicat o amendă pentru colectarea și stocarea copiilor actelor de identitate ale clienților săi fără consimțământul expres al acestora.

Potrivit ANSPDCP, în perioada cuprinsă între 1 și 26 martie 2018, Orange România a încheiat contracte de furnizare a unor servicii de telecomunicații mobile care conțin o clauză potrivit căreia clienții au fost informați și și-au dat consimțământul pentru colectarea și stocarea unei copii a actului lor de identitate în scop de identificare. Căsuța referitoare la această clauză a fost bifată de operator înainte de semnarea contractului.

În acest context, Tribunalul București (România) a solicitat Curții să precizeze condițiile în care consimțământul clienților pentru prelucrarea datelor cu caracter personal poate fi considerat valabil.

Curtea amintește mai întâi că dreptul Uniunii[42] prevede o listă a cazurilor în care o prelucrare de date cu caracter personal poate fi considerată legală. În special,

[42] Articolul 7 din Directiva 95/46 și articolul 6 din RGPD.

consimțământul persoanei vizate trebuie să fie liber, specific, informat și lipsit de ambiguitate[43]. În această privință, absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu constituie un consimțământ dat în mod valabil.

În plus, în cazul în care consimțământul persoanei vizate este dat în cadrul unei declarații scrise care se referă și la alte aspecte, această declarație trebuie să fie prezentată într-o formă inteligibilă și ușor accesibilă și utilizând un limbaj clar și simplu. Pentru a asigura persoanei vizate o reală libertate de alegere, clauzele contractuale nu trebuie să o inducă în eroare cu privire la posibilitatea de a încheia același contract dacă refuză să își dea consimțământul pentru prelucrarea datelor sale.

Curtea precizează că, întrucât Orange România este operatorul datelor cu caracter personal, aceasta trebuie să fie în măsură să demonstreze legalitatea prelucrării acestor date și, prin urmare, în speță, existența unui consimțământ valabil al clienților săi. În această privință, dat fiind că clienții vizați nu par să fi bifat ei înșiși căsuța referitoare la colectarea și la stocarea copiilor actului lor de identitate, simplul fapt că această căsuță a fost bifată nu este de natură să stabilească o manifestare pozitivă a consimțământului lor. Sarcina de a efectua verificările necesare în acest scop revine instanței naționale.

Potrivit Curții, instanței naționale îi revine și sarcina de a aprecia dacă clauzele contractuale în discuție erau sau nu de natură să inducă clienții vizați în eroare cu privire la posibilitatea de a încheia contractul în pofida unui refuz de a-și da consimțământul pentru prelucrarea datelor lor, în lipsa unor precizări cu privire la această posibilitate. În plus, în cazul refuzului unui client de a-și da consimțământul pentru prelucrarea datelor sale, Curtea observă că Orange România impunea ca acesta să declare în scris că nu consimțea nici la colectarea, nici la stocarea copiei actului său de identitate. Potrivit Curții, o asemenea cerință suplimentară este de natură să afecteze în mod nejustificat libera alegere de a se opune acestei colectări și acestei stocări. În orice caz, întrucât societatea menționată avea obligația de a stabili că clienții săi și-au manifestat prin intermediul unui comportament activ consimțământul pentru prelucrarea datelor lor cu caracter personal, această societate nu poate pretinde ca ei să își manifeste în mod activ refuzul.

Prin urmare, Curtea concluzionează că un contract privind furnizarea de servicii de telecomunicații care conține o clauză potrivit căreia persoana vizată a fost informată și și-a dat consimțământul pentru colectarea și pentru stocarea unei copii a actului său de identitate, în scop de identificare, nu este de natură să demonstreze că această persoană și-a dat în mod valabil consimțământul pentru această colectare și pentru această stocare atunci când căsuța care se referă la această clauză a fost bifată de operatorul de date anterior semnării acestui contract, atunci când clauzele acestui contract sunt de natură să inducă persoana vizată în eroare cu privire la posibilitatea de a încheia contractul în discuție în pofida refuzului de a-și da consimțământul pentru

[43] Articolul 2 litera (h) din Directiva 95/46 și articolul 4 punctul 11 din RGPD.

prelucrarea datelor sale sau atunci când libera alegere de a se opune acestei colectări și acestei stocări este afectată în mod nejustificat de acest operator prin faptul că impune persoanei vizate să completeze, pentru a-și exprima refuzul de a-și da consimțământul pentru aceste prelucrări, un formular suplimentar în care să fie menționat un astfel de refuz.

Hotărârea din 22 iunie 2021 (Marea Cameră), Latvijas Republikas Saeima (Puncte de penalizare) (C-439/19, EU:C:2021:504)

În această hotărâre (a se vedea și secțiunea II.3, intitulată „Noțiunea de «prelucrare a datelor cu caracter personal»"), Curtea statuează că RGPD se opune reglementării care obligă Ceļu satiksmes drošības direkcija (Direcția pentru Siguranța Rutieră, Letonia) (denumită în continuare „CSDD") să facă accesibile publicului datele referitoare la punctele de penalizare aplicate conducătorilor de vehicule pentru încălcarea normelor de circulație fără ca persoana care solicită accesul să justifice un interes specific în obținerea acestora. Ea constată că nu este demonstrată necesitatea, în special în raport cu obiectivul de îmbunătățire a siguranței rutiere invocat de guvernul leton, a unei comunicări a datelor cu caracter personal referitoare la punctele de penalizare aplicate pentru încălcarea normelor de circulație. În plus, potrivit Curții, nici dreptul publicului de a avea acces la documentele oficiale, nici dreptul la libertatea de informare nu justifică o astfel de reglementare.

În acest context, Curtea subliniază că îmbunătățirea siguranței rutiere, pe care o urmărește reglementarea letonă, constituie un obiectiv de interes general recunoscut de Uniune și că, prin urmare, statele membre pot califica siguranța rutieră drept „sarcină care servește unui interes public"[44]. Cu toate acestea, nu este demonstrată necesitatea regimului leton de comunicare a datelor cu caracter personal referitoare la punctele de penalizare pentru garantarea obiectivului urmărit. Astfel, pe de o parte, legiuitorul leton dispune de o multitudine de modalități de acțiune care i-ar fi permis să atingă acest obiectiv prin alte mijloace, care aduc mai puțin atingere drepturilor fundamentale ale persoanelor vizate. Pe de altă parte, trebuie să se țină seama de caracterul sensibil al datelor referitoare la punctele de penalizare și de faptul că comunicarea acestora publicului poate constitui o ingerință gravă în drepturile la respectarea vieții private și la protecția datelor cu caracter personal, din moment ce poate provoca dezaprobarea socială și poate antrena stigmatizarea persoanei în cauză.

În plus, Curtea consideră că, ținând seama de caracterul sensibil al acestor date și de gravitatea acestei ingerințe în cele două drepturi fundamentale, aceste drepturi prevalează atât asupra interesului publicului de a avea acces la documente oficiale, cum

[44] În temeiul articolului 6 alineatul (1) litera (e) din RGPD, prelucrarea datelor cu caracter personal este legală atunci când este „necesară pentru îndeplinirea unei sarcini care servește unui interes public […]".

este registrul național al vehiculelor și al conducătorilor acestora, cât și asupra dreptului la libertatea de informare.

Pe de altă parte, pentru motive identice, Curtea statuează că RGPD se opune de asemenea reglementării letone în măsura în care aceasta autorizează CSDD să comunice datele referitoare la punctele de penalizare aplicate conducătorilor de vehicule pentru încălcarea normelor de circulație unor operatori economici pentru ca aceștia din urmă să le poată reutiliza și comunica publicului.

În sfârșit, Curtea precizează că principiul supremației dreptului Uniunii se opune ca instanța de trimitere, sesizată cu o acțiune împotriva reglementării letone, calificată de Curte ca incompatibilă cu dreptul Uniunii, să decidă menținerea efectelor juridice ale acestei reglementări până la data pronunțării hotărârii sale definitive.

III. Prelucrarea datelor cu caracter personal în sensul reglementării sectoriale

1. Prelucrarea datelor cu caracter personal în sectorul comunicațiilor electronice

Hotărârea din 2 octombrie 2018 (Marea Cameră), Ministerio Fiscal (C-207/16, EU:C:2018:788)

În această cauză era în discuție respingerea de către un judecător de instrucție spaniol a unei cereri formulate în cadrul unei anchete privind o tâlhărie având ca obiect un portofel și un telefon mobil. Mai exact, poliția judiciară a solicitat judecătorului menționat acordarea accesului, pentru o perioadă de douăsprezece zile de la data tâlhăriei, la datele de identificare ale utilizatorilor numerelor de telefon activate de pe telefonul furat. Această cerere a fost respinsă pentru motivul că faptele aflate la originea anchetei penale nu ar constitui o infracțiune „gravă” – adică, potrivit dreptului spaniol, o infracțiune sancționată cu o pedeapsă cu închisoarea de cel puțin cinci ani –, accesul la datele de identificare nefiind posibil decât pentru acest tip de infracțiuni.

După ce a amintit că accesul unor autorități publice, în cadrul unei proceduri de urmărire penală, la date cu caracter personal păstrate de furnizorii de servicii de comunicații electronice intră în domeniul de aplicare al Directivei 2002/58, Curtea a statuat că accesul autorităților publice la datele care vizează identificarea titularilor cartelelor SIM activate cu un telefon mobil furat, cum ar fi numele, prenumele și, dacă este cazul, adresa acestor titulari, constituie o ingerință în dreptul fundamental la respectarea vieții private, precum și în dreptul fundamental la protecția datelor cu caracter personal, consacrate de cartă, chiar și în absența unor împrejurări care permit

calificarea acestei ingerințe drept „gravă” și fără a fi relevant dacă informațiile vizate referitoare la viața privată prezintă sau nu prezintă un caracter sensibil sau dacă persoanele interesate au suferit sau nu au suferit eventuale inconveniente ca urmare a acestei ingerințe. Curtea a subliniat totuși că această ingerință nu prezintă o asemenea gravitate încât acest acces ar trebui să fie limitat, în materie de prevenire, de investigare, de detectare și de urmărire penală a infracțiunilor, la combaterea infracționalității grave. Astfel, deși Directiva 2002/58 enumeră în mod exhaustiv obiectivele susceptibile să justifice o reglementare națională care guvernează accesul autorităților publice la datele în cauză și care derogă, așadar, de la principiul confidențialității comunicațiilor electronice, întrucât acest acces trebuie să urmărească în mod efectiv și strict unul dintre aceste obiective, Curtea observă că, în ceea ce privește obiectivul prevenirii, investigării, detectării și urmăririi penale a infracțiunilor, textul Directivei 2002/58 nu limitează acest obiectiv numai la combaterea infracțiunilor grave, ci se referă la „infracțiuni” în general.

În acest context, Curtea a precizat că, deși în Hotărârea Tele2 Sverige și Watson ș.a.[45] a statuat că numai combaterea infracționalității grave este susceptibilă să justifice un acces al autorităților publice la date cu caracter personal păstrate de furnizorii de servicii de comunicații care, considerate în ansamblu, permit deducerea unor concluzii precise privind viața privată a persoanelor ale căror date sunt vizate, o asemenea interpretare a fost motivată prin faptul că obiectivul urmărit de o reglementare care guvernează acest acces trebuie să se raporteze la gravitatea ingerinței în drepturile fundamentale în cauză pe care o determină această operațiune. Astfel, în conformitate cu principiul proporționalității, o ingerință gravă nu poate fi justificată în acest domeniu decât prin obiectivul privind combaterea infracționalității, care trebuie de asemenea să fie calificată drept „gravă”. În schimb, dacă ingerința nu este gravă, respectivul acces este susceptibil să fie justificat de un obiectiv privind prevenirea, investigarea, detectarea și urmărirea penală a unor „infracțiuni” în general.

În ceea ce privește spața, Curtea a apreciat că accesul doar la datele care fac obiectul cererii în discuție nu poate fi calificat drept ingerință „gravă” în drepturile fundamentale ale persoanelor ale căror date sunt vizate, din moment ce aceste date nu permit să se tragă concluzii precise cu privire la viața lor privată. Prin urmare, Curtea a concluzionat că ingerința pe care ar implica-o un acces la astfel de date este susceptibilă să fie justificată de obiectivul privind prevenirea, detectarea, investigarea și urmărirea penală a unor „infracțiuni” în general, fără a fi necesar ca aceste infracțiuni să fie calificate drept „grave”.

[45] Hotărârea Curții din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970).

Hotărârile din 6 octombrie 2020 (Marea Cameră), Privacy International (C-623/17, EU:C:2020:790) și La Quadrature du Net ș.a. (C-511/18, C-512/18 și C-520/18, EU:C:2020:791)

Jurisprudența referitoare la stocarea datelor cu caracter personal și la accesul la acestea în domeniul comunicațiilor electronice – în special Hotărârea Tele2 Sverige și Watson ș.a., în care Curtea a considerat printre altele că statele membre nu pot impune furnizorilor de servicii de comunicații electronice o obligație de stocare generalizată și nediferențiată a datelor de transfer și de localizare – a creat motive de îngrijorare pentru unele state, care se tem că au fost private de un instrument pe care îl consideră necesar pentru protejarea securității naționale și pentru combaterea infracționalității.

În acest context, Investigatory Powers Tribunal (Tribunalul pentru Litigii referitoare la Competențele de Investigare, Regatul Unit) (Privacy International, C-623/17), Conseil d'État (Consiliul de Stat, Franța) (La Quadrature du Net ș.a., cauzele conexate C-511/18 și C-512/18), precum și Cour constitutionnelle (Curtea Constituțională, Belgia) (Ordre des barreaux francophones et germanophone ș.a., C-520/18) au fost sesizate cu litigii privind legalitatea reglementărilor adoptate de anumite state membre în aceste domenii, care prevăd în special o obligație a furnizorilor de servicii de comunicații electronice de a transmite unei autorități publice sau de a stoca în mod generalizat și nediferențiat datele de transfer și de localizare ale utilizatorilor.

Prin două hotărâri pronunțate în Marea Cameră la 6 octombrie 2020, Curtea consideră, mai întâi, că reglementările naționale care impun furnizorilor de servicii de comunicații electronice să stocheze date de transfer și de localizare sau chiar să transmită aceste date autorităților naționale de securitate și de informații în acest scop intră în domeniul de aplicare al Directivei 2002/58.

În continuare, Curtea amintește că Directiva 2002/58[46] nu permite ca derogarea de la obligația de principiu de a garanta confidențialitatea comunicațiilor electronice și a datelor aferente acestora și de la interdicția de a stoca datele respective să devină regula. Acest lucru implică faptul că directiva menționată nu permite statelor membre să adopte, printre altele în scopuri legate de securitatea națională, măsuri legislative prin care se urmărește să se limiteze întinderea drepturilor și a obligațiilor prevăzute de această directivă, în special a obligației de a garanta confidențialitatea comunicațiilor și a datelor de transfer[47], decât cu respectarea principiilor generale ale dreptului Uniunii, printre care figurează principiul proporționalității, și a drepturilor fundamentale garantate de cartă[48].

În acest context, Curtea consideră, pe de o parte, în cauza Privacy International, că Directiva 2002/58, interpretată în lumina cartei, se opune unei reglementări naționale care impune furnizorilor de servicii de comunicații electronice, în vederea protejării

[46] Articolul 15 alineatele (1) și (3) din Directiva 2002/58.
[47] Articolul 5 alineatul (1) din Directiva 2002/58.
[48] În special articolele 7, 8 și 11, precum și articolul 52 alineatul (1) din cartă.

securității naționale, transmiterea generalizată și nediferențiată către serviciile de securitate și de informații a datelor de transfer și de localizare. Pe de altă parte, în cauzele conexate La Quadrature du Net ș.a., precum și în cauza Ordre des barreaux francophones et germanophone ș.a., Curtea apreciază că aceeași directivă se opune unor măsuri legislative care impun furnizorilor de servicii de comunicații electronice, cu titlu preventiv, o stocare generalizată și nediferențiată a datelor de transfer și de localizare.

Astfel, aceste obligații de transmitere și de stocare generalizată și nediferențiată a unor asemenea date constituie ingerințe deosebit de grave în drepturile fundamentale garantate de cartă, fără ca comportamentul persoanelor ale căror date sunt vizate să prezinte vreo legătură cu obiectivul urmărit de reglementarea în cauză. În mod similar, Curtea interpretează articolul 23 alineatul (1) din RGPD, citit în lumina cartei, în sensul că se opune unei reglementări naționale care impune furnizorilor de acces la servicii de comunicații publice online și furnizorilor de servicii de stocare-hosting stocarea generalizată și nediferențiată printre altele a datelor cu caracter personal aferente acestor servicii.

În schimb, Curtea apreciază că, în situațiile în care statul membru în cauză se confruntă cu o amenințare gravă la adresa securității naționale, care se dovedește reală și actuală sau previzibilă, Directiva 2002/58, interpretată în lumina cartei, nu se opune obligării furnizorilor de servicii de comunicații electronice să stocheze în mod generalizat și nediferențiat date de transfer și de localizare. În acest context, Curtea precizează că decizia care prevede obligația respectivă, pentru o perioadă limitată la strictul necesar, trebuie să facă obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie are efect obligatoriu, pentru a se verifica existența uneia dintre aceste situații, precum și respectarea condițiilor și a garanțiilor prevăzute. În aceleași condiții, directiva menționată nu se opune nici analizei automatizate a datelor, în special a celor de transfer și de localizare, ale ansamblului utilizatorilor de mijloace de comunicații electronice.

Curtea adaugă că Directiva 2002/58, interpretată în lumina cartei, nu se opune unor măsuri legislative care permit recurgerea la o stocare direcționată, limitată în timp la strictul necesar, a datelor de transfer și de localizare, care să fie delimitată, pe baza unor elemente obiective și nediscriminatorii, în funcție de categoriile de persoane vizate sau prin intermediul unui criteriu geografic. De asemenea, această directivă nu se opune unor astfel de măsuri care prevăd o stocare generalizată și nediferențiată a adreselor IP atribuite sursei unei comunicații, cu condiția ca durata de stocare să fie limitată la strictul necesar, și nici celor care prevăd o asemenea stocare a datelor referitoare la identitatea civilă a utilizatorilor mijloacelor de comunicații electronice, statele membre nefiind obligate, în acest din urmă caz, să limiteze în timp stocarea. Mai mult, directiva menționată nu se opune unei măsuri legislative care permite recurgerea la o stocare rapidă a datelor de care dispun furnizorii de servicii în cazul în care există situații în care survine necesitatea stocării datelor respective dincolo de termenele legale de stocare a

datelor în scopul elucidării unor infracțiuni grave sau a unor atingeri aduse securității naționale, atunci când aceste infracțiuni sau atingeri au fost deja constatate sau când existența lor poate fi suspectată în mod rezonabil.

În plus, Curtea consideră că Directiva 2002/58, interpretată în lumina cartei, nu se opune unei reglementări naționale care impune furnizorilor de servicii de comunicații electronice să recurgă la colectarea în timp real printre altele a datelor de transfer și de localizare atunci când această colectare este limitată la persoanele în privința cărora există un motiv valabil pentru a suspecta că sunt implicate într-un mod sau altul în activități de terorism și este supusă unui control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă, a cărei decizie are efect obligatoriu, asigurându-se că o astfel de colectare în timp real nu este autorizată decât în limita a ceea ce este strict necesar. În caz de urgență, controlul trebuie să aibă loc în termen scurt.

În sfârșit, Curtea abordează problema menținerii efectelor în timp ale unei reglementări naționale declarate incompatibilă cu dreptul Uniunii. În această privință, ea consideră că o instanță națională nu poate aplica o dispoziție a dreptului său național care îi permite să limiteze în timp efectele unei declarații de nelegalitate pe care trebuie să o facă în privința unei reglementări naționale care impune furnizorilor de servicii de comunicații electronice o stocare generalizată și nediferențiată a datelor de transfer și de localizare, considerată incompatibilă cu Directiva 2002/58 interpretată în lumina cartei.

În acest condiții, pentru a da un răspuns util instanței naționale, Curtea amintește că admisibilitatea și aprecierea elementelor de probă care au fost obținute printr-o stocare a datelor contrară dreptului Uniunii, în cadrul unei proceduri penale inițiate împotriva unor persoane suspectate de infracțiuni grave, intră, în stadiul actual al dreptului Uniunii, numai sub incidența dreptului național. Cu toate acestea, Curtea precizează că Directiva 2002/58, interpretată în lumina principiului efectivității, impune ca instanța penală națională să înlăture elementele de probă care au fost obținute printr-o stocare generalizată și nediferențiată a datelor de transfer și de localizare, incompatibilă cu dreptul Uniunii, în cadrul unei asemenea proceduri penale în cazul în care persoanele suspectate de săvârșirea unor infracțiuni nu sunt în măsură să își exprime în mod eficient poziția cu privire la aceste elemente de probă.

Hotărârea din 2 martie 2021 (Marea Cameră), Prokuratuur (Condițiile de acces la datele privind comunicațiile electronice) (C-746/18, EU:C:2021:152)

În Estonia s-a inițiat o procedură penală împotriva lui H. K. pentru infracțiunile de furt, de utilizare a cardului bancar al unui terț și de violență față de persoane care participă la o procedură judiciară. H. K. a fost condamnată pentru aceste infracțiuni de un tribunal de primă instanță la o pedeapsă cu închisoarea de doi ani. Ulterior, această decizie a fost confirmată în apel. Procesele-verbale pe care este întemeiată constatarea acestor infracțiuni au fost întocmite în special pe baza unor date cu caracter personal generate

în cadrul furnizării unor servicii de comunicații electronice. Riigikohus (Curtea Supremă, Estonia), în fața căreia H. K a declarat recurs, a exprimat îndoieli cu privire la compatibilitatea cu dreptul Uniunii[49] a condițiilor în care serviciile de investigare au avut acces la aceste date.

Aceste îndoieli privesc, în primul rând, aspectul dacă întinderea perioadei pentru care serviciile de investigare au avut acces la date constituie un criteriu care permite să se evalueze gravitatea ingerinței constituite de acest acces în drepturile fundamentale ale persoanelor vizate. Astfel, în cazul în care această perioadă este foarte scurtă sau volumul datelor colectate este foarte limitat, instanța de trimitere a ridicat problema stabilirii faptului dacă obiectivul privind combaterea criminalității în general, iar nu numai a criminalității grave, poate justifica o asemenea ingerință. În al doilea rând, instanța de trimitere a avut îndoieli cu privire la posibilitatea de a considera că Ministerul Public estonian, ținând seama de diferitele misiuni care îi sunt încredințate de reglementarea națională, este o autoritate administrativă „independentă”, în sensul Hotărârii Tele2 Sverige și Watson ș.a.[50], susceptibilă să autorizeze accesul autorității de investigare la datele vizate.

Prin hotărârea sa, pronunțată în Marea Cameră, Curtea statuează că Directiva 2002/58, citită în lumina cartei, se opune unei reglementări naționale care, în scopul prevenirii, investigării, detectării și urmăririi penale a infracțiunilor, permite accesul autorităților publice la un ansamblu de date de transfer sau de date de localizare care pot să furnizeze informații cu privire la comunicațiile efectuate de un utilizator al unui mijloc de comunicare electronică sau cu privire la localizarea echipamentelor terminale pe care le utilizează acesta și pot să permită să se deducă concluzii precise cu privire la viața sa privată, fără ca acest acces să fie limitat la proceduri care vizează combaterea infracționalității grave sau prevenirea amenințărilor grave la adresa siguranței publice. Potrivit Curții, întinderea perioadei pentru care se solicită accesul la aceste date și volumul sau natura datelor disponibile pentru o astfel de perioadă nu sunt relevante în această privință. În plus, Curtea consideră că aceeași directivă, citită în lumina cartei, se opune unei reglementări naționale care conferă Ministerului Public competența de a autoriza accesul unei autorități publice la datele de transfer și la datele de localizare în scopul desfășurării unei urmăriri penale.

În ceea ce privește obiectivul de prevenire, investigare, detectare și urmărire penală a infracțiunilor urmărit prin reglementarea în discuție, în conformitate cu principiul proporționalității, Curtea consideră că numai obiectivele de combatere a infracționalității grave sau de prevenire a amenințărilor grave pentru siguranța publică sunt de natură să justifice accesul autorităților publice la un ansamblu de date de transfer sau de date de localizare care permit deducerea unor concluzii precise privind viața privată a

---

[49] Mai precis cu articolul 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă.

[50] Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970, punctul 120).

persoanelor vizate, fără ca alți factori referitori la proporționalitatea unei cereri de acces, precum perioada pentru care se solicită accesul la astfel de date, să poată avea ca efect ca obiectivul de prevenire, investigare, detectare și urmărire penală a infracțiunilor în general să fie susceptibil să justifice un astfel de acces.

În ceea ce privește competența conferită Ministerului Public de a autoriza accesul unei autorități publice la datele de transfer și la datele de localizare pentru a desfășura o urmărire penală, Curtea amintește că revine dreptului național sarcina de a stabili condițiile în care furnizorii de servicii de comunicații electronice trebuie să acorde autorităților naționale competente accesul la datele de care dispun. Pentru a îndeplini cerința proporționalității, o astfel de reglementare trebuie să prevadă însă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime astfel încât persoanele ale căror date cu caracter personal sunt vizate să dispună de garanții suficiente care să permită protejarea în mod eficient a acestor date împotriva riscurilor de abuz. Această reglementare trebuie să aibă forță juridică obligatorie în dreptul intern și în special să indice în ce împrejurări și în ce condiții materiale și procedurale poate fi luată o măsură care prevede prelucrarea unor asemenea date, garantând în acest mod că o ingerință este limitată la strictul necesar.

Potrivit Curții, în scopul de a garanta în practică deplina respectare a acestor condiții, este esențial ca accesul autorităților naționale competente la datele stocate să fie condiționat de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă și ca decizia acestei instanțe sau a acestei entități să intervină în urma unei cereri motivate formulate de autoritățile respective, printre altele în cadrul unor proceduri de prevenire, de detectare sau de urmărire penală. În caz de urgență justificată corespunzător, controlul trebuie să aibă loc în termene scurte.

În această privință, Curtea precizează că un control prealabil impune printre altele ca instanța sau entitatea însărcinată cu efectuarea controlului prealabil menționat să dispună de toate atribuțiile și să prezinte toate garanțiile necesare în vederea asigurării unei concilieri a diferitelor interese și drepturi în cauză. În ceea ce privește mai concret o investigație penală, un asemenea control impune ca această instanță sau această entitate să fie în măsură să asigure un just echilibru între, pe de o parte, interesele legate de nevoile investigației în cadrul combaterii infracționalității și, pe de altă parte, drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal ale persoanelor ale căror date sunt vizate prin acces. Atunci când acest control nu este efectuat de o instanță, ci de o entitate administrativă independentă, aceasta trebuie să beneficieze de un statut care să îi permită să acționeze în cadrul exercitării misiunilor sale în mod obiectiv și imparțial și trebuie să fie în acest scop protejată de orice influență externă.

În opinia Curții, din acestea rezultă că cerința privind independența pe care trebuie să o îndeplinească autoritatea însărcinată cu exercitarea controlului prealabil impune ca această autoritate să aibă calitatea de terț în raport cu cea care solicită accesul la date, astfel încât prima să fie în măsură să exercite respectivul control în mod obiectiv și

imparțial la adăpost de orice influență exterioară. În special în domeniul penal, cerința privind independența presupune ca autoritatea însărcinată cu acest control prealabil, pe de o parte, să nu fie implicată în desfășurarea investigației penale în cauză și, pe de altă parte, să aibă o poziție de neutralitate față de părțile din procedura penală. Or, această situație nu se regăsește în cazul unui minister public, precum Ministerul Public estonian, care conduce procedura de investigare și exercită, dacă este cazul, acțiunea publică. Rezultă că Ministerul Public nu este în măsură să efectueze controlul prealabil sus-menționat.

Hotărârea din 5 aprilie 2022 (Marea Cameră), Commissioner of An Garda Síochána ș.a. (C-140/20, EU:C:2022:258)

În prezenta cauză, cererea de decizie preliminară a fost formulată de Supreme Court (Curtea Supremă, Irlanda) în cadrul unei proceduri civile inițiate de o persoană condamnată la pedeapsa închisorii pe viață pentru un omor săvârșit în Irlanda. Aceasta din urmă a contestat compatibilitatea cu dreptul Uniunii a anumitor dispoziții din legea națională referitoare la păstrarea datelor generate în cadrul comunicațiilor electronice. În temeiul acestei legi, date de transfer și date de localizare aferente unor apeluri telefonice ale inculpatului fuseseră păstrate de furnizorii de servicii de comunicații electronice și fuseseră puse la dispoziția autorităților polițienești. Îndoielile exprimate de instanța de trimitere priveau în special compatibilitatea cu Directiva 2002/58, interpretată în lumina cartei, a unui regim de păstrare generalizată și nediferențiată a acestor date, în legătură cu combaterea criminalității grave.

Prin hotărârea sa, pronunțată în Marea Cameră, Curtea confirmă, precizând în același timp domeniul său de aplicare, jurisprudența rezultată din Hotărârea La Quadrature du Net ș.a.[51], amintind că păstrarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare aferente comunicațiilor electronice nu este autorizată în scopul combaterii criminalității grave și al prevenirii amenințărilor grave împotriva siguranței publice. Aceasta confirmă de asemenea jurisprudența rezultată din Hotărârea Prokuratuur (Condițiile de acces la datele privind comunicațiile electronice)[52], în special în ceea ce privește obligația de a condiționa accesul autorităților naționale competente la respectivele date păstrate de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă, în privința unui funcționar al poliției.

Curtea statuează în primul rând că Directiva 2002/58, interpretată în lumina cartei, se opune unor măsuri legislative care prevăd, cu titlu preventiv, în scopul combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare. Astfel, ținând seama, pe de o parte, de efectele disuasive asupra exercitării drepturilor

[51] Hotărârea din 6 octombrie 2020, La Quadrature du Net și alții (C-511/18, C-512/18 și C-520/18, EU:C:2020:791).
[52] Hotărârea din 2 martie 2021, Prokuratuur (Condițiile de acces la datele privind comunicațiile electronice) (C-746/18, EU:C:2021:152).

fundamentale[53] pe care le poate cauza această păstrare și, pe de altă parte, de gravitatea ingerinței pe care o implică, o asemenea păstrare trebuie să constituie excepția, iar nu regula în sistemul instituit prin directiva menționată, așa încât datele respective să nu poată face obiectul unei păstrări sistematice și continue. Criminalitatea, chiar deosebit de gravă, nu poate fi asimilată unei amenințări la adresa securității naționale, în măsura în care o asemenea asimilare ar putea introduce o categorie intermediară între securitatea națională și siguranța publică în scopul de a aplica celei de a doua cerințele inerente celei dintâi.

În schimb, Directiva 2002/58, interpretată în lumina cartei, nu se opune unor măsuri legislative care prevăd, în scopul combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o păstrare direcționată a datelor de transfer și a datelor de localizare care să fie delimitată, pe baza unor elemente obiective și nediscriminatorii, în funcție de categoriile de persoane vizate sau prin intermediul unui criteriu geografic, pentru o perioadă limitată la strictul necesar, dar care poate fi reînnoită. Aceasta adaugă că o asemenea măsură de păstrare care vizează locuri sau infrastructuri frecventate în mod regulat de un număr foarte mare de persoane sau de locuri strategice, precum aeroporturi, gări, porturi maritime sau zone de taxare, poate permite autorităților competente să obțină informații cu privire la prezența în aceste locuri sau zone geografice a persoanelor care utilizează acolo un mijloc de comunicare electronică și să tragă concluzii cu privire la prezența și la activitatea lor în locurile sau în zonele geografice respective în scopul combaterii criminalității grave. În orice caz, eventuala existență a unor dificultăți în definirea precisă a ipotezelor și a condițiilor în care poate fi efectuată o păstrare direcționată nu poate justifica faptul că unele state membre prevăd o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare.

Această directivă, interpretată în lumina cartei, nu se opune nici unor măsuri legislative care prevăd, în același scop, o păstrare generalizată și nediferențiată a adreselor IP atribuite sursei unei conexiuni, pentru o perioadă limitată la strictul necesar, precum și a datelor referitoare la identitatea civilă a utilizatorilor de comunicații electronice. În ceea ce privește acest din urmă aspect, Curtea precizează în special că nici Directiva 2002/58, nici vreun alt act din dreptul Uniunii nu se opune unei legislații naționale care are ca obiect combaterea criminalității grave, în temeiul căreia achiziționarea unui mijloc de comunicare electronică precum o cartelă SIM preplătită este condiționată de verificarea documentelor oficiale care stabilesc identitatea cumpărătorului și de înregistrarea de către vânzător a informațiilor care rezultă din aceasta, vânzătorul fiind obligat, dacă este cazul, să permită accesul la aceste informații autorităților naționale competente.

Situația este diferită în ceea ce privește măsurile legislative care prevăd, tot în scopul combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței

[53] Consacrate la articolele 7-11 din cartă.

publice, impunerea unei obligații furnizorilor de servicii de comunicații electronice, prin intermediul unei decizii a autorității competente supuse unui control jurisdicțional efectiv, de a efectua, pentru o perioadă determinată, păstrarea rapidă („quick freeze”) a datelor de transfer și a datelor de localizare de care dispun. Astfel, numai combaterea criminalității grave și, *a fortiori*, apărarea securității naționale sunt de natură să justifice o asemenea păstrare, cu condiția ca această măsură, precum și accesul la datele păstrate să respecte limitele strictului necesar. Curtea amintește că o asemenea măsură de păstrare rapidă poate fi extinsă la datele de transfer și la datele de localizare aferente altor persoane decât cele care sunt suspectate de planificarea sau de săvârșirea unei infracțiuni grave sau a unei atingeri aduse securității naționale cu condiția ca aceste date să poată contribui, pe baza unor elemente obiective și nediscriminatorii, la elucidarea unei asemenea infracțiuni sau a unei asemenea atingeri aduse securității naționale, precum datele victimei acesteia și ale anturajului său social sau profesional.

Cu toate acestea, Curtea arată în continuare că toate măsurile legislative menționate mai sus trebuie să garanteze, prin norme clare și precise, că păstrarea datelor în cauză este subordonată respectării condițiilor materiale și procedurale aferente și că persoanele vizate dispun de garanții efective împotriva riscurilor de abuz. Diferitele măsuri de păstrare a datelor de transfer și a datelor de localizare pot fi aplicate împreună, potrivit alegerii legiuitorului național și cu respectarea în același timp a limitelor strictului necesar.

În plus, Curtea precizează că a autoriza, în scopul combaterii criminalității grave, un acces la asemenea date păstrate în mod generalizat și nediferențiat pentru a face față unei amenințări grave la adresa securității naționale ar fi contrar ierarhiei obiectivelor de interes general care pot justifica o măsură luată în temeiul Directivei 2002/58. Așadar, aceasta ar echivala cu a permite ca accesul să poată fi justificat printr-un obiectiv cu o importanță mai redusă decât cel care a justificat păstrarea, și anume apărarea securității naționale, riscând astfel să priveze de orice efect util interdicția de a efectua o păstrare generalizată și nediferențiată în scopul combaterii criminalității grave.

În al doilea rând, Curtea decide că Directiva 2002/58, interpretată în lumina cartei, se opune unei reglementări naționale în temeiul căreia prelucrarea centralizată a cererilor de acces la date păstrate de furnizorii de servicii de comunicații electronice, care provin de la poliție în cadrul investigării și al urmăririi penale a infracțiunilor grave, revine unui funcționar al poliției, chiar și atunci când el este asistat de o unitate instituită în cadrul poliției, care beneficiază de un anumit grad de autonomie în exercitarea misiunii sale și ale cărui decizii pot face ulterior obiectul unui control jurisdicțional. Astfel, pe de o parte, un asemenea funcționar nu îndeplinește cerințele privind independența și imparțialitatea care se impun unei autorități administrative care exercită controlul prealabil al cererilor de acces la datele care provin de la autoritățile naționale competente, în măsura în care nu are calitatea de terț în raport cu aceste autorități. Pe de altă parte, deși decizia unui asemenea funcționar poate face obiectul unui control jurisdicțional exercitat *a posteriori*, acest control nu se poate substitui unui control

independent și, cu excepția cazurilor de urgență justificate în mod corespunzător, prealabil.

În sfârșit, în al treilea rând, Curtea confirmă jurisprudența sa potrivit căreia dreptul Uniunii se opune ca o instanță națională să limiteze în timp efectele unei declarații de nevaliditate pe care are obligația să o efectueze în temeiul dreptului național în ceea ce privește o legislație națională care impune furnizorilor de servicii de comunicații electronice o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare din cauza incompatibilității acestei legislații cu Directiva 2002/58. Curtea amintește însă că admisibilitatea elementelor de probă obținute prin intermediul unei asemenea păstrări intră în sfera de aplicare a dreptului național, în conformitate cu principiul autonomiei procedurale a statelor membre, sub rezerva respectării printre altele a principiilor echivalenței și efectivității.

Hotărârea din 20 septembrie 2022 (Marea Cameră), VD și SR (C-339/20 și C-397/20, EU:C:2022:703)

În urma unei investigații efectuate de Autorité des marchés financiers [Autoritatea Piețelor Financiare (AMF), Franța], au fost inițiate proceduri penale împotriva lui VD și a lui SR, două persoane fizice acuzate de săvârșirea unor utilizări abuzive a informațiilor privilegiate, de tăinuire a unor utilizări abuzive ale informațiilor privilegiate, de complicitate, de corupție și de spălare de bani. În cadrul acestei investigații, AMF a utilizat date cu caracter personal provenite din apeluri telefonice efectuate de VD și de SR, generate în temeiul Code des postes et des communications électroniques (Codul serviciilor poștale și al comunicațiilor electronice) francez, în cadrul furnizării de servicii de comunicații electronice.

În măsura în care trimiterea lor în judecată era întemeiată pe datele de transfer furnizate de AMF, VD și SR au sesizat fiecare cu o acțiune cour d'appel de Paris (Curtea de Apel din Paris, Franța), invocând printre altele un motiv bazat pe încălcarea articolului 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă. Mai precis, întemeindu-se pe jurisprudența rezultată din Hotărârea Tele2 Sverige și Watson ș.a.[54], VD și SR au contestat faptul că AMF a utilizat ca temei juridic pentru a colecta datele menționate dispozițiile naționale în cauză, în condițiile în care, în opinia lor, aceste dispoziții, pe de o parte, nu erau conforme cu dreptul Uniunii, în măsura în care prevedeau o păstrare generalizată și nediferențiată a datelor de conectare, și, pe de altă parte, nu stabileau nicio limită în privința competenței investigatorilor AMF de a obține comunicarea datelor păstrate.

Prin două hotărâri, din 20 decembrie 2018 și din 7 martie 2019, cour d'appel de Paris (Curtea de Apel din Paris) a respins acțiunile formulate de VD și de SR. Pentru a înlătura

[54] Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970).

motivul sus-menționat, instanța de fond s-a întemeiat în special pe faptul că Regulamentul privind abuzul de piață[55] autorizează autoritățile competente să solicite, în măsura în care dreptul intern permite acest lucru, înregistrările existente ale datelor de transfer deținute de operatorii de servicii de comunicații electronice dacă există bănuieli rezonabile privind o încălcare a interdicției vizând utilizarea abuzivă a informațiilor privilegiate și dacă aceste înregistrări ar putea fi concludente pentru investigarea încălcării respective.

VD și SR au formulat recurs la Cour de cassation (Curtea de Casație, Franța), instanța de trimitere în prezentele cauze.

În acest context, instanța menționată ridică problema concilierii articolului 15 alineatul (1) din Directiva 2002/58, citit în lumina cartei, cu cerințele care reies din articolul 12 alineatul (2) literele (a) și (d) din Directiva privind abuzul de piață[56] și din articolul 23 alineatul (2) literele (g) și (h) din Regulamentul privind abuzul de piață. Această întrebare își are originea în măsurile legislative în discuție în litigiile principale, care prevăd, cu titlu preventiv, în sarcina operatorilor de servicii de comunicații electronice o păstrare generalizată și nediferențiată a datelor de transfer un an de la data înregistrării, în vederea combaterii infracțiunilor de abuz de piață, dintre care fac parte utilizările abuzive ale informațiilor confidențiale. În ipoteza în care Curtea ar trebui să considere că legislația privind păstrarea datelor de conectare în discuție în litigiile principale nu este conformă cu dreptul Uniunii, instanța de trimitere ridică problema menținerii provizorii a efectelor acestei legislații în vederea evitării unei insecurități juridice și pentru a permite ca datele colectate și păstrate anterior să fie utilizate în scopul detectării și al urmăririi penale a utilizărilor abuzive ale informațiilor confidențiale.

Prin hotărârea sa, Curtea, reunită în Marea Cameră, consideră că păstrarea generalizată și nediferențiată a datelor de transfer un an de la data înregistrării de către operatorii de servicii de comunicații electronice nu este autorizată cu titlu preventiv în vederea combaterii infracțiunilor de abuz de piață. Pe de altă parte, ea își confirmă jurisprudența potrivit căreia dreptul Uniunii se opune ca o instanță națională să limiteze în timp efectele unei declarații de nevaliditate care îi revine în privința unor dispoziții legislative naționale incompatibile cu dreptul Uniunii.

Curtea amintește mai întâi că, pentru a interpreta o dispoziție de drept al Uniunii, trebuie să se facă referire nu numai la termenii acesteia, ci și să se țină seama de contextul său și de obiectivele urmărite de reglementarea din care face parte această dispoziție.

---

[55] Regulamentul (UE) nr. 596/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 privind abuzul de piață (regulamentul privind abuzul de piață) și de abrogare a Directivei 2003/6 și a Directivelor 2003/124/CE, 2003/125/CE și 2004/72/CE ale Comisiei (JO 2014, L 173, p. 1).

[56] Directiva 2003/6/CE a Parlamentului European și a Consiliului din 28 ianuarie 2003 privind utilizările abuzive ale informațiilor confidențiale și manipulările pieței (abuzul de piață) (JO 2003, L 96, p. 16, Ediție specială, 06/vol. 5, p. 210).

În ceea ce privește modul de redactare a dispozițiilor vizate de întrebările preliminare, Curtea constată că, în timp ce articolul 12 alineatul (2) litera (d) din Directiva privind abuzul de piață se referă la prerogativa AMF „de a cere înregistrările telefonice și schimburile de date existente”, articolul 23 alineatul (2) literele (g) și (h) din Regulamentul privind abuzul de piață face trimitere la competența acestei autorități de a solicita, pe de o parte, „înregistrări […] ale datelor de transfer deținute de societățile de investiții, instituțiile de creditare sau instituțiile financiare” și, pe de altă parte, „în măsura în care dreptul intern permite acest lucru, înregistrări existente ale datelor de transfer deținute de operatorii de telecomunicații”. Potrivit Curții, reiese fără ambiguitate din modul de redactare a acestor dispoziții că ele se limitează să încadreze competența AMF de „a cere” sau de „a solicita” datele de care dispun acești operatori, ceea ce corespunde unui acces la aceste date. În plus, referirea la înregistrările „existente”, astfel cum sunt „deținute” de operatorii menționați, lasă să se înțeleagă că legiuitorul Uniunii nu a intenționat să reglementeze posibilitatea legiuitorului național de a institui o obligație de păstrare a unor asemenea înregistrări. Potrivit Curții, această interpretare ar fi de altfel confirmată atât de contextul în care se înscriu dispozițiile menționate, cât și de obiectivele urmărite de reglementarea din care fac parte aceleași dispoziții.

În ceea ce privește contextul în care se înscriu dispozițiile vizate de întrebările preliminare, Curtea observă că, deși, potrivit dispozițiilor relevante ale Directivei privind abuzul de piață și ale Regulamentului privind abuzul de piață[57], legiuitorul Uniunii a intenționat să impună statelor membre obligația de a lua măsurile necesare pentru ca autoritățile competente în materie financiară să dispună de un ansamblu de instrumente, de competențe și de resurse adecvate, precum și de competențele de supraveghere și de anchetă necesare pentru a asigura eficacitatea sarcinilor lor, aceste dispoziții nu se pronunță nici cu privire la eventuala posibilitate a statelor membre de a institui în acest scop în sarcina operatorilor de servicii de comunicații electronice o obligație de păstrare generalizată și nediferențiată a datelor de transfer, nici cu privire la condițiile în care aceste date trebuie să fie păstrate de operatorii menționați în vederea transmiterii lor, dacă este cazul, către autoritățile competente.

În ceea ce privește obiectivele urmărite de reglementarea în cauză, Curtea arată că reiese atât din Directiva privind abuzul de piață, cât și din Regulamentul privind abuzul de piață[58] că aceste instrumente au ca finalitate asigurarea integrității piețelor financiare ale Uniunii și consolidarea încrederii investitorilor în aceste piețe, încredere care se întemeiază printre altele pe faptul că aceștia vor fi plasați pe picior de egalitate și vor fi protejați împotriva utilizării ilicite a informațiilor privilegiate. Interdicția utilizărilor abuzive ale informațiilor privilegiate enunțată de respectivele instrumente[59] urmărește

[57] Articolul 12 alineatul (1) din Directiva privind abuzul de piață și, respectiv, articolul 23 alineatul (3) din Regulamentul privind abuzul de piață, interpretat în lumina considerentului (62) al acestuia.

[58] Considerentele (2) și (12) ale Directivei privind abuzul de piață și, respectiv, articolul 1 din Regulamentul privind abuzul de piață, interpretat în lumina considerentelor (2) și (24) ale acestuia.

[59] Articolul 2 alineatul (1) din Directiva privind abuzul de piață și articolul 8 alineatul (1) din Regulamentul privind abuzul de piață.

astfel să asigure egalitatea dintre cocontractanți în cadrul unei tranzacții bursiere, evitând ca unul dintre aceștia, care deține o informație privilegiată și se plasează, datorită acestui fapt, într-o poziție avantajoasă în raport cu ceilalți investitori să profite de această informație în detrimentul celor care nu o cunosc. Deși, potrivit Regulamentului privind abuzul de piață[60], înregistrările datelor de conectare reprezintă probe cruciale, uneori chiar singurele probe, care ajută la detectarea și dovedirea existenței unei utilizări abuzive a informațiilor privilegiate sau a unei manipulări a pieței, nu este mai puțin adevărat că acest regulament se referă numai la înregistrările „deținute" de operatorii de servicii de comunicații electronice, precum și la prerogativa autorității competente în materie financiară de a „cere" de la acești operatori comunicarea datelor „existente". Astfel, din acest regulament nu reiese nicidecum că legiuitorul Uniunii a intenționat prin intermediul său să recunoască statelor membre competența de a impune operatorilor de servicii de comunicații electronice o obligație generală de păstrare a datelor. Rezultă că nici Directiva privind abuzul de piață, nici Regulamentul privind abuzul de piață nu pot constitui temeiul juridic al unei obligații generale de păstrare a înregistrărilor de date de transfer deținute de operatorii de servicii de comunicații electronice în scopul exercitării competențelor conferite autorității competente în materie financiară în temeiul acestor acte.

În continuare, Curtea amintește că Directiva 2002/58 constituie actul de referință în materie de păstrare și, în mod mai general, de prelucrare a datelor cu caracter personal în sectorul comunicațiilor electronice, așa încât interpretarea dată de Curte în raport cu această directivă guvernează și înregistrările datelor de transfer deținute de operatorii de servicii de comunicații electronice, pe care autoritățile competente în materie financiară, în sensul Directivei privind abuzul de piață și al Regulamentului privind abuzul de piață[61], le pot solicita de la aceștia. Aprecierea legalității prelucrării înregistrărilor deținute de operatorii de servicii de comunicații electronice[62] trebuie, prin urmare, să se efectueze în lumina condițiilor prevăzute de Directiva 2002/58, precum și a interpretării acestei directive de către Curte în jurisprudența sa.

Astfel, Curtea statuează că Directiva privind abuzul de piață și Regulamentul privind abuzul de piață, interpretate în coroborare cu Directiva 2002/58 și în lumina cartei, se opun unor măsuri legislative care prevăd, cu titlu preventiv, în vederea combaterii infracțiunilor de abuz de piață, dintre care fac parte utilizările abuzive ale informațiilor privilegiate, o păstrare temporară, dar generalizată și nediferențiată de către operatorii de comunicații electronice a datelor de transfer un an de la data înregistrării.

În sfârșit, Curtea confirmă jurisprudența sa potrivit căreia dreptul Uniunii se opune ca o instanță națională să limiteze în timp efectele unei declarații de nevaliditate pe care are

60 Considerentul (62) al Regulamentului privind abuzul de piață.
61 Articolul 11 din Directiva privind abuzul de piață și, respectiv articolul 22 din Regulamentul privind abuzul de piață.
62 În sensul articolului 12 alineatul (2) litera (d) din Directiva privind abuzul de piață și al articolului 23 alineatul (2) literele (g) și (h) din Regulamentul privind abuzul de piață.

obligația să o efectueze în temeiul dreptului național în privința dispozițiilor naționale care, pe de o parte, impun operatorilor de servicii de comunicații electronice o păstrare generalizată și nediferențiată a datelor de transfer și, pe de altă parte, permit comunicarea unor asemenea date autorității competente în materie financiară fără autorizarea prealabilă a unei instanțe sau a unei autorități administrative independente, ca urmare a incompatibilității acestor dispoziții cu Directiva 2002/58, interpretată în lumina Cartei. Curtea amintește însă că admisibilitatea elementelor de probă obținute prin intermediul unei asemenea păstrări intră în sfera de aplicare a dreptului național, în conformitate cu principiul autonomiei procedurale a statelor membre, sub rezerva respectării printre altele a principiilor echivalenței și efectivității. Acest din urmă principiu impune instanței penale naționale să înlăture informațiile și elementele de probă care au fost obținute prin intermediul unei păstrări generalizate și nediferențiate, incompatibilă cu dreptul Uniunii, în cazul în care persoanele respective nu sunt în măsură să prezinte în mod eficient observații cu privire la aceste informații și elemente de probă, care provin dintr-un domeniu care nu este cunoscut de judecători și care pot influența în mod preponderent aprecierea faptelor.

Hotărârea din 30 aprilie 2024 (Plenul), La Quadrature du Net ș.a. (Date personale și combaterea contrafacerii) (C-470/21, EU:C:2024:370)

Sesizat cu titlu preliminar de Conseil d'État (Consiliul de Stat, Franța), Plenul Curții dezvoltă jurisprudența sa privind Directiva 2002/58 aducând precizări, pe de o parte, cu privire la condițiile în care o păstrare generalizată a adreselor IP de către furnizorii de servicii de comunicații electronice poate să nu fie considerată ca determinând o ingerință gravă în drepturile la respectarea vieții private, la protecția datelor cu caracter personal și la libertatea de exprimare garantate de cartă[63] și, pe de altă parte, cu privire la posibilitatea unei autorități publice de a avea acces la anumite date cu caracter personal, păstrate cu respectarea unor astfel de condiții, în cadrul combaterii încălcărilor drepturilor de proprietate intelectuală săvârșite online.

În speță, patru asociații au adresat Premier ministre (prim-ministrul, Franța) o cerere de abrogare a decretului privind prelucrarea prin mijloace automatizate a datelor cu caracter personal[64]. Întrucât nu s-a dat curs acestei cereri, aceste asociații au sesizat Conseil d'État (Consiliul de Stat) cu o acțiune având ca obiect anularea acestei decizii

[63] Articolele 7, 8 și 11 din cartă.

[64] Décret nº 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé «Système de gestion des mesures pour la protection des œuvres sur internet» (Decretul nr. 2010-236 din 5 martie 2010 privind prelucrarea prin mijloace automatizate a datelor cu caracter personal autorizată prin articolul L. 331-29 din Codul proprietății intelectuale, intitulat „Sistemul de gestionare a măsurilor pentru protecția operelor pe internet") (JORF nr. 56 din 7 martie 2010, textul nr. 19), astfel cum a fost modificat prin décret nº 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (Decretul nr. 2017-924 din 6 mai 2017 privind gestionarea drepturilor de autor și a drepturilor conexe de către un organism de gestiune a drepturilor și de modificare a Codului proprietății intelectuale) (JORF nr. 109 din 10 mai 2017, textul nr. 176).

implicite de respingere. În opinia lor, acest decret, ca și dispozițiile în temeiul cărora a fost adoptat,[65] încalcă dreptul Uniunii.

Potrivit legislației franceze, Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Înalta Autoritate pentru Difuzarea Operelor și Protecția Drepturilor pe Internet, Hadopi), pentru a putea identifica persoanele răspunzătoare de încălcările drepturilor de autor sau ale drepturilor conexe săvârșite online, este autorizată să aibă acces la anumite date pe care furnizorii de servicii de comunicații electronice sunt obligați să le păstreze. Aceste date privesc identitatea civilă a unei persoane vizate care sunt corelative unei adrese IP colectate în prealabil de organismele titularilor de drepturi. Din momentul în care titularul adresei IP utilizate pentru desfășurarea de activități prin care se săvârșesc astfel de încălcări este identificat, Hadopi urmează procedura denumită de „răspuns gradual”. În mod concret, ea este abilitată să îi trimită acestei persoane două recomandări care sunt similare cu avertismentele și, dacă activitățile continuă, o scrisoare prin care îi notifică faptul că activitățile sale pot face obiectul urmăririi penale. În sfârșit, ea poate să sesizeze Ministerul Public în vederea urmăririi penale a persoanei respective[66].

În acest context, Conseil d'État (Consiliul de Stat) a adresat Curții întrebări cu privire la interpretarea Directivei 2002/58 în lumina dispozițiilor cartei[67].

În primul rând, în ceea ce privește păstrarea datelor referitoare la identitatea civilă și a adreselor IP corelative, Curtea subliniază că nu orice păstrare generalizată și nediferențiată a adreselor IP constituie neapărat o ingerință gravă în drepturile la respectarea vieții private, la protecția datelor cu caracter personal și la libertatea de exprimare, garantate de cartă.

Obligația de a asigura o astfel de păstrare poate fi justificată prin obiectivul combaterii infracțiunilor în general, atunci când este efectiv exclus ca această păstrare să determine ingerințe grave în viața privată a persoanei vizate din cauza posibilității de a trage concluzii precise cu privire la aceasta prin intermediul printre altele al corelării acestor adrese cu un set de date de transfer sau de localizare.

Prin urmare, un stat membru care intenționează să impună furnizorilor de servicii de comunicații electronice o atare obligație trebuie să se asigure că modalitățile de păstrare a acestor date exclud posibilitatea de a se trage concluzii precise cu privire la viața privată a persoanelor vizate.

Curtea precizează că modalitățile de păstrare trebuie, în acest scop, să privească chiar structura păstrării, care, în esență, trebuie organizată în așa fel încât să garanteze o

65 În special articolul L. 331-21 al treilea-al cincilea paragraf din Codul proprietății intelectuale.

66 Începând de la data de 1 ianuarie 2022, Hadopi a fuzionat cu Conseil supérieur de l'audiovisuel (Consiliul Superior al Audiovizualului) (CSA), o altă autoritate publică independentă, în vederea constituirii Autorité de régulation de la communication audiovisuelle et numérique (Autoritatea de Reglementare a Comunicațiilor Audiovizuale și Digitale) (ARCOM). Procedura de răspuns gradual a rămas însă în esență neschimbată.

67 Articolul 15 alineatul (1) din Directiva 2002/58.

separare efectiv etanșă a diferitelor categorii de date păstrate. Astfel, normele naționale referitoare la aceste modalități trebuie să garanteze că fiecare categorie de date, inclusiv datele referitoare la identitatea civilă și adresele IP, este păstrată pe deplin separat de alte categorii de date păstrate și că această separare este efectiv etanșă cu ajutorul unui dispozitiv informatic securizat și fiabil. Mai mult, în măsura în care aceste norme prevăd posibilitatea unei corelări a adreselor IP păstrate cu identitatea civilă a persoanei vizate în vederea combaterii infracționalității, ele nu trebuie să permită o astfel de corelare decât prin utilizarea unui procedeu tehnic performant care să nu pună sub semnul întrebării eficacitatea separării etanșe a acestor categorii de date. Fiabilitatea acestei separări trebuie să facă obiectul unui control regulat de către o autoritate publică terță. În măsura în care legislația națională aplicabilă prevede astfel de cerințe stricte, ingerința rezultată din această păstrare a adreselor IP nu poate fi calificată drept „gravă”.

În consecință, Curtea concluzionează că, în cazul în care există o măsură legislativă care garantează că nicio combinare de date nu va permite să se tragă concluzii precise cu privire la viața privată a persoanelor ale căror date sunt păstrate, Directiva 2002/58, interpretată în lumina cartei, nu se opune ca un stat membru să impună o obligație de păstrare generalizată și nediferențiată a adreselor IP, pentru o durată care să nu depășească strictul necesar, în vederea atingerii obiectivului combaterii infracțiunilor în general.

În al doilea rând, în ceea ce privește accesul la datele referitoare la identitatea civilă care sunt corelative unei adrese IP, Curtea statuează că Directiva 2002/58, interpretată în lumina cartei, nu se opune în principiu unei reglementări naționale care permite accesul unei autorități publice la aceste date, păstrate de furnizorii de servicii de comunicații electronice în mod separat și efectiv etanș, doar cu scopul ca această autoritate să poată identifica titularii acestor adrese suspectați a fi răspunzători pentru aceste încălcări ale drepturilor de autor și ale drepturilor conexe săvârșite pe internet și să poată lua măsuri în privința lor. Într-un astfel de caz, reglementarea națională trebuie să interzică agenților care dispun de un asemenea acces, *primo*, să divulge sub orice formă informații cu privire la conținutul fișierelor consultate de acești titulari, mai puțin în cazul în care se are exclusiv în vedere sesizarea Ministerului Public, *secundo*, să efectueze orice reconstituire a parcursului de navigare al acestor titulari și, *tertio*, să utilizeze aceste adrese IP în alte scopuri decât cel al adoptării acestor măsuri.

În acest context, Curtea amintește în special că, deși libertatea de exprimare și confidențialitatea datelor cu caracter personal constituie preocupări primordiale, aceste drepturi fundamentale nu sunt totuși absolute. Astfel, în cadrul unei evaluări comparative a drepturilor și intereselor în cauză, acestea trebuie uneori să fie eliminate în prezența altor drepturi fundamentale și a imperativelor de interes general precum apărarea ordinii publice și prevenirea infracțiunilor sau protecția drepturilor și libertăților celorlalți. Aceasta este situația în special atunci când importanța majoră acordată acestor preocupări primordiale este de natură să împiedice eficacitatea unei anchete penale, printre altele atunci când face ca identificarea efectivă a autorului unei

infracțiuni și impunerea unei sancțiuni în privința acestuia să devină imposibile sau excesiv de dificile.

În același context, Curtea face de asemenea trimitere la jurisprudența sa potrivit căreia, în privința combaterii infracțiunilor care aduc atingere drepturilor de autor sau drepturilor conexe săvârșite online, împrejurarea că accesul la adresele IP poate constitui singurul mijloc de investigare ce permite identificarea persoanei vizate tinde să demonstreze că păstrarea acestor adrese și accesul la ele sunt strict necesare pentru realizarea obiectivului urmărit și îndeplinesc, așadar, cerința privind proporționalitatea. A nu permite un astfel de acces ar implica de altfel un risc real de impunitate sistemică a infracțiunilor săvârșite online sau a căror săvârșire ori pregătire este facilitată de caracteristicile proprii internetului. Or, existența unui asemenea risc constituie o împrejurare relevantă pentru a aprecia, în cadrul unei evaluări comparative a diferitelor drepturi și interese în cauză, dacă o ingerință în drepturile la respectarea vieții private, la protecția datelor personale și la libertatea de exprimare constituie o măsură proporțională în raport cu obiectivul combaterii infracțiunilor.

În al treilea rând, pronunțându-se asupra aspectului dacă accesul autorității publice la date referitoare la identitatea civilă care sunt corelative unei adrese IP trebuie condiționat de un control prealabil efectuat de o instanță sau de o entitate administrativă independentă, Curtea consideră că cerința unui astfel de control se impune atunci când, în contextul unei reglementări naționale, acest acces implică riscul unei ingerințe grave în drepturile fundamentale ale persoanei vizate, în sensul că ar putea permite acestei autorități publice să tragă concluzii precise cu privire la viața privată a acestei persoane și, dacă este cazul, să îi realizeze un profil detaliat. În sens invers, această cerință privind efectuarea unui control prealabil nu are vocația de a se aplica atunci când ingerința în drepturile fundamentale nu poate fi calificată drept gravă.

În această privință, Curtea precizează că, în cazul în care se instituie o măsură de păstrare care garantează o separare efectiv etanșă a diferitelor categorii de date păstrate, accesul autorității publice la datele referitoare la identitatea civilă care sunt corelative adreselor IP nu este în principiu condiționat de cerința efectuării unui control prealabil. Astfel, un asemenea acces doar cu scopul de a identifica titularul unei adrese IP nu constituie, ca regulă generală, o ingerință gravă în drepturile sus-menționate.

Cu toate acestea, Curtea nu exclude că, în situații atipice, există un risc ca, în cadrul unei proceduri precum procedura de răspuns gradual în discuție în litigiul principal, autoritatea publică să poată tragă concluzii precise cu privire la viața privată a persoanei vizate, în special atunci când această persoană desfășoară activități care aduc atingere drepturilor de autor sau drepturilor conexe pe rețele peer-to-peer în mod repetat sau chiar la scară largă, în legătură cu opere protejate de natură specială, care dezvăluie informații, eventual sensibile, cu privire la viața privată a acestei persoane.

În speță, titularul unei adrese IP poate fi deosebit de expus unui asemenea risc atunci când autoritatea publică este chemată să decidă dacă sesizează sau nu Ministerul Public

în vederea efectuării urmăririi penale. Astfel, intensitatea atingerii aduse dreptului la respectarea vieții private este susceptibilă să crească pe măsură ce procedura de răspuns gradual, care operează potrivit unui proces secvențial, parcurge diferitele etape care o compun. Accesul autorității competente la setul de date referitoare la persoana vizată și cumulate în cursul diferitelor etape ale acestei proceduri poate permite să se tragă concluzii precise cu privire la viața sa privată. În consecință, reglementarea națională trebuie să prevadă un control prealabil care să intervină înainte ca autoritatea publică să poată corela datele de identitate civilă cu un astfel de set de date și înainte de eventuala transmitere a scrisorii de notificare privind constatarea faptului că această persoană a săvârșit fapte care pot face obiectul urmăririi penale. Acest control trebuie, prin urmare, să conserve eficacitatea procedurii de răspuns gradual permițând în special să se identifice cazurile de noi repetări posibile ale comportamentului infracțional în discuție. În acest scop, procedura trebuie să fie organizată și structurată astfel încât datele de identitate civilă ale unei persoane care corespund unor adrese IP colectate în prealabil pe internet să nu poată fi corelate în mod automat de persoanele însărcinate cu examinarea faptelor din cadrul autorității publice competente cu elemente de care aceasta din urmă dispune deja și care ar putea permite să se tragă concluzii precise cu privire la viața privată a acestei persoane.

În plus, în ceea ce privește obiectul unui control prealabil, Curtea arată că, în cazurile în care persoana vizată este bănuită că ar fi săvârșit o încălcare care constituie în general o infracțiune, instanța sau entitatea administrativă independentă însărcinată cu acest control trebuie să refuze accesul atunci când accesul ar permite autorității publice să tragă concluzii precise cu privire la viața privată a persoanei respective. În schimb, chiar un acces care permite să se tragă concluzii precise ar trebui autorizat în cazurile în care persoana vizată este bănuită că ar fi săvârșit infracțiuni pe care statul membru în cauză le consideră ca aducând atingere unui interes fundamental al societății și ca intrând astfel sub incidența unor forme grave de infracționalitate.

Curtea precizează de asemenea că un control prealabil nu poate fi în niciun caz realizat în totalitate prin mijloace automatizate, întrucât un atare control impune, în ceea ce privește o anchetă penală, evaluarea comparativă între, pe de o parte, interesele legitime legate de combaterea infracționalității și, pe de altă parte, respectarea vieții private și protecția datelor cu caracter personal. Respectiva evaluare comparativă necesită intervenția unei persoane fizice, aceasta fiind cu atât mai necesară cu cât automatizarea și prelucrarea la scară largă a datelor în cauză implică riscuri pentru viața privată.

Astfel, Curtea concluzionează că posibilitatea persoanelor însărcinate cu examinarea faptelor din cadrul autorității publice de a corela datele referitoare la identitatea civilă a unei persoane care corespund unei adrese IP cu fișierele care conțin elemente ce permit aflarea titlului unor opere protejate a căror punere la dispoziție pe internet a justificat colectarea adreselor IP de către organismele titularilor de drepturi trebuie să fie supusă unui control exercitat de o instanță sau de o entitate administrativă independentă în

cazul în care survine o nouă repetare a unei activități care aduce atingere drepturilor de autor sau drepturilor conexe săvârșite de către aceeași persoană. Acest control nu poate fi efectuat în totalitate prin mijloace automatizate și trebuie să aibă loc înainte de a se face o astfel de corelare, întrucât această corelare poate permite, în astfel de ipoteze, să se tragă concluzii precise cu privire la viața privată a persoanei menționate a cărei adresă IP a fost utilizată pentru activități care pot aduce atingere drepturilor de autor sau drepturilor conexe.

În al patrulea și ultimul rând, Curtea arată că sistemul de prelucrare a datelor utilizat de autoritatea publică trebuie, la intervale regulate, să facă obiectul unui control efectuat de către un organism independent și care are calitatea de terț în raport cu această autoritate publică. Acest control are ca scop să se verifice integritatea sistemului, inclusiv garanțiile efective împotriva riscurilor de acces și de utilizare, abuzive sau ilegale, a acestor date, precum și eficacitatea și fiabilitatea sa în depistarea eventualelor încălcări ale obligațiilor.

În acest cadru, Curtea observă că în speță prelucrarea prin mijloace automatizate a datelor cu caracter personal efectuată de autoritatea publică pe baza informațiilor referitoare la contrafacerile constatate de organismele titularilor de drepturi poate conține un anumit număr de cazuri fals pozitive și mai ales poate implica riscul ca un număr de date potențial foarte ridicat să fie deturnate de terți în scopuri abuzive sau ilicite, fapt ce explică necesitatea unui atare control. În plus, Curtea adaugă că această prelucrare trebuie să respecte normele specifice de protecție a datelor cu caracter personal prevăzute de Directiva 2016/680. Astfel, în speță, chiar dacă autoritatea publică nu dispune de puteri decizionale proprii în cadrul procedurii denumite de răspuns gradual, ea trebuie calificată drept „autoritate publică” implicată în prevenirea și depistarea infracțiunilor și intră, așadar, în domeniul de aplicare al acestei directive. Drept urmare, persoanele implicate într-o asemenea procedură trebuie să beneficieze de un ansamblu de garanții materiale și procedurale prevăzute de Directiva 2016/680, instanței de trimitere revenindu-i sarcina de a verifica dacă ele sunt prevăzute de legislația națională.

2. Prelucrarea datelor cu caracter personal în materie penală

Hotărârea din 12 mai 2021 (Marea Cameră), Bundesrepublik Deutschland (Notificare roșie a Interpol) (C-505/19, EU:C:2021:376)

În anul 2012, Organizația Internațională de Poliție Criminală (denumită în continuare „Interpol”) a publicat, la cererea Statelor Unite și pe baza unui mandat de arestare emis de autoritățile acestei țări, o notificare roșie referitoare la WS, un resortisant german, în vederea unei eventuale extrădări a acestuia. Atunci când o persoană care face obiectul unei asemenea notificări este localizată într-un stat membru al Interpol, acesta trebuie

în principiu să procedeze la arestarea sa provizorie sau să îi supravegheze ori să îi restrângă deplasările.

Cu toate acestea, chiar înainte de publicarea acestei notificări roșii, o procedură de anchetă privind, potrivit instanței de trimitere, aceleași fapte ca și cele aflate la originea acestei notificări fusese inițiată împotriva lui WS în Germania. Această procedură s-a încheiat definitiv în anul 2010, după plata unei sume de bani de către WS, în conformitate cu o procedură specifică de tranzacție prevăzută în dreptul penal german. Ulterior, Bundeskriminalamt (Oficiul Federal al Poliției Judiciare, Germania) a informat Interpol că, având în vedere această procedură anterioară, considera că în speță era aplicabil principiul *ne bis in idem*. Acest principiu, consacrat atât la articolul 54 din Convenția de punere în aplicare a Acordului Schengen[68], cât și la articolul 50 din cartă, interzice printre altele ca o persoană împotriva căreia a fost pronunțată o hotărâre definitivă să facă din nou obiectul urmăririi penale pentru aceeași infracțiune.

În anul 2017, WS a introdus o acțiune împotriva Republicii Federale Germania la Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden, Germania) prin care a solicitat obligarea acestui stat membru să ia măsurile necesare pentru retragerea acestei notificări roșii. În această privință, WS invocă, pe lângă încălcarea principiului *ne bis in idem*, o încălcare a dreptului său la liberă circulație, garantat de articolul 21 TFUE, întrucât nu se poate deplasa într-un stat parte la Acordul Schengen sau într-un stat membru fără a risca să fie arestat. El apreciază de asemenea că, din cauza acestor încălcări, prelucrarea datelor sale cu caracter personal, care figurează în notificarea roșie, este contrară Directivei 2016/680 privind protecția datelor cu caracter personal în materie penală[69].

În acest context, Tribunalul Administrativ din Wiesbaden a decis să întrebe Curtea cu privire la aplicarea principiului *ne bis in idem*, mai precis cu privire la posibilitatea de a proceda la arestarea provizorie a unei persoane care face obiectul unei notificări roșii într-o situație precum cea în discuție. În plus, în cazul aplicabilității acestui principiu, instanța menționată urmărește să afle care sunt consecințele asupra prelucrării de către statele membre a datelor cu caracter personal conținute într-o astfel de notificare.

În hotărârea sa de Mare Cameră, Curtea statuează *inter alia* că dispozițiile Directivei 2016/680, citite în lumina articolului 54 din CAAS și a articolului 50 din cartă, trebuie interpretate în sensul că nu se opun prelucrării datelor cu caracter personal cuprinse într-o notificare roșie emisă de Interpol atât timp cât nu s-a stabilit, prin intermediul unei asemenea decizii judecătorești, că principiul *ne bis in idem* se aplică în legătură cu faptele

---

[68] Convenția de punere în aplicare a Acordului Schengen din 14 iunie 1985 între guvernele statelor din Uniunea Economică Benelux, Republicii Federale Germania și Republicii Franceze privind eliminarea treptată a controalelor la frontierele comune (JO 2000, L 239, p. 19, Ediție specială, 19/vol. 1, p. 183) (denumită în continuare „CAAS”).

[69] Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO 2016, L 119, p. 89).

pe care se întemeiază respectiva notificare, cu condiția ca o astfel de prelucrare să îndeplinească cerințele prevăzute de directiva menționată.

În ceea ce privește întrebarea referitoare la datele cu caracter personal care figurează într-o notificare roșie a Interpol, Curtea arată că orice operațiune efectuată asupra acestor date, precum înregistrarea în bazele de date ale unui stat membru, constituie o „prelucrare” care intră sub incidența Directivei 2016/680[70]. În plus, ea consideră, pe de o parte, că această prelucrare urmărește o finalitate legitimă și, pe de altă parte, că ea nu poate fi considerată nelegală pentru singurul motiv că principiul *ne bis in idem* s-ar putea aplica faptelor pe care se întemeiază notificarea roșie[71]. Această prelucrare efectuată de autoritățile statelor membre poate de altfel să se dovedească indispensabilă tocmai pentru a se verifica dacă principiul menționat se aplică.

În aceste condiții, Curtea statuează de asemenea că Directiva 2016/680, interpretată în lumina articolului 54 din CAAS și a articolului 50 din cartă, nu se opune prelucrării datelor cu caracter personal cuprinse într-o notificare roșie atât timp cât nu s-a stabilit, prin intermediul unei decizii judecătorești definitive, că principiul *ne bis in idem* se aplică în speță. Cu toate acestea, o astfel de prelucrare trebuie să respecte condițiile prevăzute de respectiva directivă. Din această perspectivă, trebuie în special ca ea să fie necesară pentru îndeplinirea unei misiuni efectuate de o autoritate națională competentă în scopul prevenirii, al depistării, al investigării sau al urmăririi penale a infracțiunilor sau al executării pedepselor[72].

În schimb, atunci când se aplică principiul *ne bis in idem*, înregistrarea în bazele de date ale statelor membre a datelor cu caracter personal care figurează într-o notificare roșie a Interpol nu mai este necesară, dat fiind că persoana în cauză nu mai poate face obiectul unei urmăriri penale pentru faptele acoperite de notificarea menționată și, în consecință, nu mai poate fi arestată pentru aceleași fapte. Rezultă că persoana vizată trebuie să poată solicita ștergerea datelor sale. Dacă această înregistrare este totuși menținută, ea trebuie să fie însoțită de indicarea faptului că persoana în cauză nu mai poate fi urmărită într-un stat membru sau într-un stat contractant pentru aceleași fapte datorită principiului *ne bis in idem*.

Hotărârea din 21 iunie 2022 (Marea Cameră), Ligue des droits humains (C-817/19, EU:C:2022:491)

În această cauză (a se vedea și secțiunea I.1., intitulată „Conformitatea dreptului derivat al Uniunii cu dreptul la protecția datelor cu caracter personal”), după ce a constatat

[70] A se vedea articolul 2 alineatul (1) și articolul 3 punctul 2 din Directiva 2016/680.
[71] A se vedea articolul 4 alineatul (1) litera (b) și articolul 8 alineatul (1) din Directiva 2016/680.
[72] A se vedea articolul 1 alineatul (1) și articolul 8 alineatul (1) din Directiva 2016/680.

validitatea Directivei PNR, Curtea aduce precizări cu privire la interpretarea unora dintre dispozițiile sale[73].

În primul rând, Curtea arată că directiva enumeră în mod exhaustiv obiectivele urmărite de prelucrarea datelor din PNR. Prin urmare, această directivă se opune unei legislații naționale care autorizează prelucrarea datelor din PNR în alte scopuri decât combaterea infracțiunilor de terorism și a infracțiunilor grave. Astfel, o legislație națională care admite în plus, ca scop al prelucrării datelor din PNR, supravegherea activităților vizate de serviciile de informații și de securitate poate să încalce caracterul exhaustiv al acestei enumerări. Sistemul instituit de Directiva PNR nu poate fi prevăzut nici în scopul îmbunătățirii controalelor la frontiere și al combaterii imigrației clandestine. Rezultă de asemenea că datele din PNR nu pot fi păstrate într-o bază de date unică ce poate fi consultată în scopul urmăririi atât a scopurilor Directivei PNR, cât și a altor scopuri.

În al doilea rând, Curtea explicitează noțiunea de autoritate națională independentă competentă să verifice dacă condițiile pentru dezvăluirea datelor din PNR în scopul evaluării ulterioare sunt îndeplinite și să aprobe o astfel de dezvăluire. Mai precis, autoritatea instituită în calitate de UIP nu poate fi calificată ca atare întrucât nu are calitatea de terț în raport cu autoritatea care solicită accesul la date. Astfel, întrucât membrii personalului său pot fi agenți detașați de autoritățile abilitate să solicite un asemenea acces, UIP pare în mod necesar legată de aceste autorități. Prin urmare, Directiva PNR se opune unei legislații naționale potrivit căreia autoritatea înființată ca UIP are totodată calitatea de autoritate națională competentă abilitată să aprobe comunicarea datelor din PNR la expirarea celor șase luni ulterioare transferului acestor date către UIP.

În al treilea rând, în ceea ce privește termenul de păstrare a datelor din PNR, Curtea statuează că articolul 12 din Directiva PNR, interpretat în lumina articolelor 7 și 8, precum și a articolului 52 alineatul (1) din cartă, se opune unei legislații naționale care prevede o durată generală de păstrare a acestor date de cinci ani, aplicabilă fără distincție tuturor pasagerilor aerieni.

Astfel, în opinia Curții, după expirarea perioadei de păstrare inițiale de șase luni, păstrarea datelor din PNR nu apare ca fiind limitată la strictul necesar în ceea ce îi privește pe pasagerii aerieni pentru care nici evaluarea prealabilă, nici eventualele verificări efectuate în perioada de păstrare inițială de șase luni și nicio altă împrejurare nu au dezvăluit existența unor elemente obiective – cum ar fi faptul că datele din PNR ale pasagerilor vizați au dat naștere unui rezultat pozitiv verificat în cadrul evaluării prealabile – de natură a demonstra existența unui risc în materie de infracțiuni de terorism sau de infracțiuni grave care au o legătură obiectivă, cel puțin indirectă, cu călătoria aeriană efectuată de acești pasageri. În schimb, Curtea apreciază că, în

[73] În special articolul 2 („Aplicarea [directivei] în cazul zborurilor intra-UE”), articolul 6 („Prelucrarea datelor din PNR”) și articolul 12 („Perioada de păstrare a datelor și depersonalizarea”) din Directiva PNR.

perioada inițială de șase luni, păstrarea datelor din PNR ale tuturor pasagerilor aerieni supuși sistemului instituit prin această directivă nu pare, în principiu, să depășească limitele strictului necesar.

În al patrulea rând, Curtea furnizează indicații privind o eventuală aplicare a Directivei PNR, în scopul combaterii infracțiunilor de terorism și a infracțiunilor grave, altor moduri de transport pentru deplasarea pasagerilor în Uniune. Or, directiva, interpretată în lumina articolului 3 alineatul (2) TUE, a articolului 67 alineatul (2) TFUE și a articolului 45 din cartă, se opune unui sistem de transfer și de prelucrare a datelor din PNR ale ansamblului de transporturi efectuate cu alte mijloace în interiorul Uniunii în lipsa unei amenințări teroriste reale și actuale sau previzibile cu care se confruntă statul membru în cauză. Într-o asemenea situație, la fel ca în cazul zborurilor intra-UE, aplicarea sistemului instituit prin Directiva PNR trebuie să fie limitată la datele din PNR ale transporturilor referitoare în special la anumite legături sau scheme de călătorie ori chiar la anumite aeroporturi, gări sau porturi maritime pentru care există indicii de natură să justifice această aplicare. Revine statului membru în cauză sarcina de a selecționa transporturile pentru care există asemenea indicii și de a reexamina periodic această aplicare în funcție de evoluția condițiilor care au justificat selectarea lor.

IV. Transfer de date cu caracter personal către țări terțe

Hotărârea din 6 noiembrie 2003 (Marea Cameră), Lindqvist (C-101/01, EU:C:2003:596)

În această cauză (a se vedea și secțiunea II.3, intitulată „Noțiunea de «prelucrare a datelor cu caracter personal»”), instanța de trimitere a solicitat să se stabilească în special dacă doamna Lindqvist a efectuat un transfer de date către o țară terță în sensul directivei respective.

Curtea a statuat că nu există „transfer către o țară terță de date”, în sensul articolului 25 din Directiva 95/46, atunci când o persoană care se află într-un stat membru introduce pe o pagină de internet, stocată la o persoană fizică sau juridică care găzduiește site-ul internet pe care poate fi consultată pagina și care este stabilită în același stat sau într-un alt stat membru, date cu caracter personal, făcându-le astfel accesibile oricărei persoane care se conectează la internet, inclusiv persoane din țări terțe.

Astfel, având în vedere, pe de o parte, stadiul de dezvoltare a internetului la momentul elaborării Directivei 95/46 și, pe de altă parte, lipsa unor criterii aplicabile utilizării internetului în capitolul IV, care include articolul 25 menționat, care să vizeze asigurarea unui control de către statele membre al transferurilor de date cu caracter personal către țări terțe și interzicerea acestor transferuri atunci când nu oferă un nivel adecvat de protecție, nu se poate prezuma că legiuitorul comunitar intenționa să includă cu

anticipare în noțiunea de „transfer către o țară terță de date” o asemenea înregistrare de date pe o pagină de internet, chiar dacă acestea sunt astfel puse la dispoziția persoanelor din țări terțe care dispun de mijloacele tehnice pentru a le accesa.

Hotărârea din 6 octombrie 2015 (Marea Cameră), Schrems (C-362/14, EU:C:2015:650)

Domnul Schrems, cetățean austriac și utilizator al rețelei sociale Facebook, a depus o plângere la Data Protection Commissioner (Comisarul pentru protecția datelor, Irlanda) ca urmare a faptului că Facebook Ireland transfera către Statele Unite datele cu caracter personal ale utilizatorilor săi și le stoca pe servere situate în această țară, unde erau prelucrate. În opinia domnului Schrems, dreptul și practicile Statelor Unite nu asigurau o protecție suficientă împotriva supravegherii exercitate de autoritățile publice a datelor transferate către această țară. Data Protection Commissioner a refuzat să investigheze această plângere pe motiv, printre altele, că, prin Decizia 2000/520/CE[74], Comisia a considerat că, în cadrul așa-numitului regim al „sferei de siguranță” (în engleză, „safe harbour”)[75], Statele Unite asigurau un nivel adecvat de protecție a datelor cu caracter personal transferate.

În acest context, Curtea a fost sesizată de High Court (Înalta Curte, Irlanda) cu o cerere de interpretare a articolului 25 alineatul (6) din Directiva 95/46, în temeiul căruia Comisia poate constata că o țară terță asigură un nivel adecvat de protecție a datelor transferate, precum și, în esență, cu o cerere având ca obiect stabilirea validității Deciziei 2000/520, adoptată de Comisie în temeiul respectivului articol 25 alineatul (6) din Directiva 95/46.

Curtea a declarat nevalidă decizia Comisiei în ansamblu, subliniind, mai întâi, că adoptarea sa necesita constatarea motivată în mod corespunzător de către Comisie că țara terță respectivă asigură efectiv un nivel de protecție a drepturilor fundamentale în esență echivalent cu cel garantat în ordinea juridică a Uniunii. Or, întrucât Comisia nu a afirmat aceasta în Decizia 2000/520, articolul 1 din această decizie încalcă cerințele stabilite la articolul 25 alineatul (6) din Directiva 95/46, interpretat în lumina cartei, și din acest motiv este nevalidă. Astfel, principiile „sferei de siguranță” sunt aplicabile numai organizațiilor americane autocertificate care primesc date cu caracter personal din Uniune, fără a se impune ca autoritățile publice americane să fie obligate să respecte principiile menționate. În plus, Decizia 2000/520 face posibile unele ingerințe în drepturile fundamentale ale persoanelor ale căror date cu caracter personal sunt sau ar putea fi transferate din Uniune către Statele Unite, fără a cuprinde vreo constatare în privința existenței în Statele Unite a unor norme cu caracter statal destinate să limiteze

[74] Decizia 2000/520/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță” privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al Statelor Unite ale Americii (JO 2000, L 215, p. 7, Ediție specială, 16/vol. 1, p. 64).

[75] Regimul sferei de siguranță include o serie de principii referitoare la protecția datelor cu caracter personal pe care companiile americane le pot aplica în mod voluntar.

eventualele ingerințe în aceste drepturi și fără a se afirma existența unei protecții juridice eficiente împotriva unor ingerințe de această natură.

În plus, Curtea a declarat nevalid articolul 3 din Decizia 2000/520 în măsura în care privează autoritățile naționale de supraveghere de competențele întemeiate pe articolul 28 din Directiva 95/46 în cazul în care o persoană invocă elemente susceptibile să repună în discuție compatibilitatea cu protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor a unei decizii a Comisiei care a constatat că o țară terță asigură un nivel de protecție adecvat. Curtea a concluzionat că nevaliditatea articolelor 1 și 3 din Decizia 2000/520 are ca efect afectarea validității acestei decizii în ansamblu.

În ceea ce privește imposibilitatea de a justifica o astfel de ingerință, Curtea a arătat, mai întâi, că o reglementare a Uniunii care implică o ingerință în drepturile fundamentale garantate de articolele 7 și 8 din cartă trebuie să prevadă norme clare și precise care să reglementeze domeniul de aplicare și aplicarea unei măsuri și să impună cerințe minime, astfel încât persoanele ale căror date cu caracter personal sunt vizate să aibă garanții suficiente pentru a-și proteja în mod eficient datele împotriva riscurilor de abuz, precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date. Necesitatea de a dispune de asemenea garanții este cu atât mai importantă în cazul în care datele cu caracter personal sunt supuse unei prelucrări automate și există un risc important de acces ilicit la aceste date.

În plus și mai ales, protecția dreptului fundamental la respectarea vieții private la nivelul Uniunii impune ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele strictului necesar. Astfel, nu este limitată la strictul necesar o reglementare care autorizează în mod generalizat stocarea integralității datelor cu caracter personal ale tuturor persoanelor ale căror date au fost transferate din Uniune către Statele Unite, fără a se face nicio diferențiere, limitare sau excepție în funcție de obiectivul urmărit și fără a se prevedea un criteriu obiectiv care să permită delimitarea accesului autorităților publice la date și utilizarea lor ulterioară în scopuri precise, strict restrânse și susceptibile să justifice ingerința pe care o implică atât accesarea, cât și utilizarea acestor date. În special, o reglementare care permite autorităților publice să acceadă în mod generalizat la conținutul comunicărilor electronice aduce atingere substanței dreptului fundamental la respectarea vieții private. De asemenea, o reglementare care nu prevede nicio posibilitate pentru justițiabil de a exercita căi legale pentru a avea acces la date cu caracter personal care îl privesc sau pentru a obține rectificarea sau ștergerea unor astfel de date nu respectă substanța dreptului fundamental la o protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din cartă.

Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017 (Marea Cameră) (EU:C:2017:592)

La 26 iulie 2017, Curtea s-a pronunțat pentru prima dată cu privire la compatibilitatea unui proiect de acord internațional cu carta și în special cu dispozițiile referitoare la respectarea vieții private și la protecția datelor cu caracter personal.

Uniunea Europeană și Canada au negociat un acord privind transferul și prelucrarea datelor din registrul cu numele pasagerilor (Acordul PNR), care a fost semnat în anul 2014. Întrucât Consiliul Uniunii Europene a solicitat Parlamentului European să îl aprobe, acesta a decis să sesizeze Curtea pentru a afla dacă acordul preconizat este compatibil cu dreptul Uniunii.

Acordul preconizat permite transferul sistematic și continuu de date PNR ale tuturor pasagerilor aerieni către o autoritate canadiană în vederea utilizării și a stocării acestora, precum și a eventualului lor transfer ulterior către alte autorități și către alte țări terțe, în scopul combaterii terorismului și a altor infracțiuni transnaționale grave. În acest scop, acordul preconizat prevede printre altele o perioadă de cinci ani de păstrare a datelor și stabilește cerințele specifice referitoare la siguranța și integritatea PNR, precum măsuri imediate de mascare a datelor sensibile, și prevede totodată drepturi de acces, de rectificare și de ștergere a datelor, precum și posibilitatea de a formula căi de atac administrative sau judiciare.

Datele PNR care intră sub incidența prevederilor acordului preconizat includ în special, pe lângă numele și datele de contact ale pasagerului sau ale pasagerilor aerieni, informațiile necesare pentru rezervare, cum ar fi datele de călătorie și itinerariul călătoriei, informații cu privire la bilet, grupurile de persoane înscrise în aceeași rezervare, informații referitoare la mijloacele de plată sau la facturare, informații referitoare la bagaje, precum și remarci generale cu privire la pasageri.

În avizul său, Curtea a statuat că acordul PNR nu poate fi încheiat în forma sa actuală ca urmare a incompatibilității anumitor dispoziții ale acestuia cu drepturile fundamentale recunoscute de Uniune.

Curtea a constatat, în primul rând, că atât transferul datelor PNR din Uniune către autoritatea canadiană competentă, cât și cadrul negociat de Uniune cu Canada referitor la condițiile privind păstrarea acestor date, utilizarea lor și eventualul transfer ulterior către alte autorități canadiene, Europol, Eurojust, autoritățile de poliție sau judiciare ale statelor membre sau alte autorități din țări terțe constituie ingerințe în dreptul garantat de articolul 7 din cartă. Aceste operațiuni constituie de asemenea o ingerință în dreptul fundamental la protecția datelor cu caracter personal garantat de articolul 8 din cartă întrucât constituie prelucrări ale datelor cu caracter personal.

Mai mult, Curtea a subliniat că, chiar dacă anumite date PNR, privite izolat, nu par să poată revela informații importante privind viața privată a persoanelor vizate, totuși, considerate în ansamblu, respectivele date pot revela printre altele un itinerar de călătorie complet, obiceiuri de călătorie, relațiile existente între două sau mai multe

persoane, precum și informații privind situația financiară a pasagerilor aerieni, obiceiurile lor alimentare sau starea lor de sănătate și ar putea furniza chiar informații sensibile despre acești pasageri, precum cele definite la articolul 2 litera (e) din acordul preconizat (informații care dezvăluie originea rasială sau etnică, opiniile politice, credințele religioase etc.).

În această privință, Curtea a statuat că, deși ingerințele în cauză ar putea fi justificate de urmărirea unui obiectiv de interes public (garantarea siguranței publice în cadrul combaterii infracțiunilor de terorism și a altor infracțiuni transnaționale grave), mai multe dispoziții din acord nu se limitează la ceea ce este strict necesar și nu prevăd norme clare și precise.

În particular, Curtea a constatat că, având în vedere riscul unei prelucrări a datelor contrare principiului nediscriminării, un transfer al datelor sensibile către Canada ar necesita o justificare precisă și deosebit de solidă, întemeiată pe alte motive decât protecția securității publice împotriva terorismului și a altor infracțiuni transnaționale grave. Or, în speță, o asemenea justificare lipsește. Curtea a concluzionat că dispozițiile acordului privind transferul de date sensibile către Canada și prelucrarea și păstrarea acestor date sunt incompatibile cu drepturile fundamentale.

În al doilea rând, Curtea a statuat că, după plecarea pasagerilor aerieni din Canada, stocarea continuă a datelor PNR provenite de la toți pasagerii aerieni, permisă de acordul preconizat, nu este limitată la strictul necesar. Astfel, în ceea ce privește pasagerii aerieni pentru care riscul de terorism sau de alte infracțiuni transnaționale grave nu a fost identificat la sosirea în Canada și până la plecarea din țara respectivă, nu pare să existe, odată cu plecarea acestora, niciun raport, nici măcar indirect, între datele lor PNR și obiectivul urmărit de acordul preconizat care ar justifica păstrarea unor astfel de date. În schimb, păstrarea datelor PNR ale pasagerilor aerieni pentru care sunt identificate elemente obiective care permit să se considere că ar putea să prezinte, chiar și după plecarea lor din Canada, un risc în termeni de combatere a terorismului și a altor infracțiuni transnaționale grave apare ca admisibilă și după ședereа în această țară, chiar și pentru o perioadă de cinci ani.

În al treilea rând, Curtea a considerat că dreptul fundamental la respectarea vieții private, consacrat la articolul 7 din cartă, presupune ca persoana vizată să poată să se asigure că datele sale cu caracter personal sunt prelucrate în mod exact și legal. Pentru a efectua verificările necesare, această persoană trebuie să dispună de un drept de acces la datele cu caracter personal care o privesc și care fac obiectul prelucrării.

În această privință, Curtea arată că în acordul preconizat trebuie ca pasagerii aerieni să fie informați în privința transferului datelor lor din dosarele pasagerilor către țara terță în cauză și a utilizării acestor date din momentul în care această comunicare nu poate compromite anchetele desfășurate de autoritățile publice menționate în acordul preconizat. Astfel, o asemenea informare se dovedește de fapt necesară pentru a le permite pasagerilor aerieni să își exercite dreptul de a solicita accesul la datele care îi

privesc și, dacă este cazul, rectificarea acestora, precum și de a introduce o cale de atac efectivă în fața unei instanțe, conform articolului 47 primul paragraf din cartă.

Astfel, în cazurile în care se prezintă elemente obiective care justifică utilizarea datelor dosarelor pasagerilor în vederea combaterii terorismului și a altor infracțiuni transnaționale grave și care necesită o autorizație prealabilă din partea unei autorități judiciare sau a unei entități administrative independente, este necesară o informare individuală a pasagerilor aerieni. Același lucru este valabil și în cazul în care datele dosarelor pasagerilor aerieni sunt comunicate altor autorități publice sau unor particulari. Cu toate acestea, o astfel de informare nu trebuie să fie efectuată decât din momentul în care ea nu poate compromite anchetele desfășurate de autoritățile publice vizate de acordul preconizat.

Hotărârea din 16 iulie 2020 (Marea Cameră), Facebook Ireland și Schrems (C-311/18, EU:C:2020:559)

RGPD prevede că transferul unor astfel de date către o țară terță se poate realiza, în principiu, numai dacă țara terță în cauză asigură un nivel de protecție adecvat în privința acestor date. Potrivit acestui regulament, Comisia poate să decidă că o țară terță asigură, ca urmare a legislației sale interne sau a angajamentelor sale internaționale, un nivel de protecție adecvat[76]. În absența unei asemenea decizii privind caracterul adecvat al nivelului de protecție, un astfel de transfer se poate realiza numai dacă exportatorul datelor cu caracter personal, stabilit în Uniune, oferă garanții adecvate, care pot să rezulte în special din clauze standard de protecție a datelor adoptate de Comisie, și cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate[77]. Pe de altă parte, RGPD stabilește în mod precis condițiile în care se poate realiza un astfel de transfer în absența unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate[78].

Domnul Maximilian Schrems, resortisant austriac cu reședința în Austria, este un utilizator al Facebook din anul 2008. La fel ca în cazul celorlalți utilizatori cu reședința în Uniune, datele cu caracter personal ale domnului Schrems sunt, în tot sau în parte, transferate de Facebook Ireland către servere care aparțin Facebook Inc., situate pe teritoriul Statelor Unite, unde fac obiectul unei prelucrări. Domnul Schrems a depus o plângere la autoritatea de supraveghere irlandeză, având ca obiect în esență interzicerea acestor transferuri. El a susținut că dreptul și practicile Statelor Unite nu oferă o protecție suficientă împotriva accesului autorităților publice la datele transferate către această țară. Plângerea menționată a fost respinsă în special pentru motivul că, în

[76] Articolul 45 din RGPD.
[77] Articolul 46 alineatul (1) și alineatul (2) litera (c) din RGPD.
[78] Articolul 49 din RGPD.

Decizia 2000/520[79], Comisia constatase că Statele Unite asigurau un nivel de protecție adecvat. Prin Hotărârea din 6 octombrie 2015, Curtea, sesizată cu o întrebare preliminară adresată de High Court (Înalta Curte, Irlanda), a declarat nevalidă această decizie (denumită în continuare „Hotărârea Schrems I”)[80].

În urma Hotărârii Schrems I și a anulării consecutive de către instanța irlandeză a deciziei prin care s-a respins plângerea domnului Schrems, autoritatea de supraveghere irlandeză l-a invitat să își reformuleze plângerea ținând seama de declararea nevalidității de către Curte a Deciziei 2000/520. În plângerea sa reformulată, domnul Schrems susține că Statele Unite nu oferă o protecție suficientă a datelor transferate către această țară. El solicită să se suspende sau să se interzică pentru viitor transferurile datelor sale cu caracter personal din Uniune către Statele Unite, pe care Facebook Ireland le realizează în prezent în temeiul clauzelor standard de protecție care figurează în anexa la Decizia 2010/87/UE[81]. Întrucât a considerat că soluționarea plângerii domnului Schrems depinde în special de validitatea Deciziei 2010/87, autoritatea de supraveghere irlandeză a inițiat o procedură în fața High Court pentru ca aceasta să sesizeze Curtea cu o cerere de decizie preliminară. După deschiderea acestei proceduri, Comisia a adoptat Decizia (UE) 2016/1250 privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA[82]).

Prin intermediul cererii de decizie preliminară, instanța de trimitere solicită Curții să se pronunțe cu privire la aplicabilitatea RGPD în cazul unor transferuri de date cu caracter personal întemeiate pe clauze standard de protecție care figurează în Decizia 2010/87, cu privire la nivelul de protecție impus de acest regulament în cadrul unui astfel de transfer și cu privire la obligațiile care revin autorităților de supraveghere în acest context. În plus, High Court ridică problema validității atât a Deciziei 2010/87, cât și a Deciziei 2016/1250.

Curtea constată că analiza Deciziei 2010/87 în raport cu carta nu evidențiază niciun element de natură să afecteze validitatea sa. În schimb, aceasta declară nevalidă Decizia 2016/1250.

Curtea consideră, mai întâi, că dreptul Uniunii și în special RGPD se aplică în cazul unui transfer de date cu caracter personal efectuat în scopuri comerciale de un operator economic stabilit într-un stat membru către un alt operator economic stabilit într-o țară terță, chiar dacă în cursul sau în urma acestui transfer datele menționate sunt susceptibile de a fi prelucrate de autoritățile țării terțe în cauză în scopuri de siguranță

[79] Decizia Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță” privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al SUA (JO 2000, L 215, p. 7, Ediție specială, 16/vol. 1, p. 64).

[80] Hotărârea Curții din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650.

[81] Decizia Comisiei din 5 februarie 2010 privind clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele stabilite în țări terțe în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului (JO 2010, L 39, p 5), astfel cum a fost modificată prin Decizia de punere în aplicare (UE) 2016/2297 a Comisiei din 16 decembrie 2016 (JO 2016, L 344, p. 100).

[82] Decizia de punere în aplicare a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA (JO 2016, L 207, p. 1).

publică, de apărare și de securitate a statului. Ea precizează că acest tip de prelucrare a datelor de către autoritățile unei țări terțe nu poate exclude un asemenea transfer din domeniul de aplicare al RGPD.

În ceea ce privește nivelul de protecție impus în cadrul unui astfel de transfer, Curtea statuează că cerințele prevăzute în acest scop de dispozițiile RGPD, care se referă la garanții adecvate, drepturi opozabile și căi de atac eficiente, trebuie interpretate în sensul că persoanele ale căror date cu caracter personal sunt transferate către o țară terță în temeiul unor clauze standard de protecție a datelor trebuie să beneficieze de un nivel de protecție în esență echivalent cu cel garantat în cadrul Uniunii de regulamentul menționat, interpretat în lumina cartei. În acest context, ea precizează că evaluarea acestui nivel de protecție trebuie să ia în considerare atât stipulațiile contractuale convenite între exportatorul datelor stabilit în Uniune și destinatarul transferului stabilit în țara terță în cauză, cât și, în ceea ce privește un eventual acces al autorităților publice ale acestei țări terțe la datele cu caracter personal astfel transferate, elementele relevante ale sistemului său juridic.

În ceea ce privește obligațiile care revin autorităților de supraveghere în contextul unui astfel de transfer, Curtea declară că, cu excepția cazului în care există o decizie privind caracterul adecvat al nivelului de protecție adoptată în mod valabil de Comisie, aceste autorități sunt în special obligate să suspende sau să interzică un transfer de date cu caracter personal către o țară terță atunci când consideră, în lumina împrejurărilor proprii transferului menționat, că clauzele standard de protecție a datelor nu sunt sau nu pot fi respectate în această țară și că protecția datelor transferate, impusă de dreptul Uniunii, nu poate fi asigurată prin alte mijloace, în cazul în care însuși exportatorul stabilit în Uniune nu a suspendat ori nu a încetat un astfel de transfer.

Curtea examinează apoi validitatea Deciziei 2010/87. Potrivit Curții, validitatea acestei decizii nu este repusă în discuție prin simplul fapt că clauzele standard de protecție a datelor care figurează în aceasta nu sunt obligatorii, ca urmare a caracterului lor contractual, pentru autoritățile țării terțe către care ar putea fi efectuat un transfer. În schimb, precizează Curtea, această validitate depinde de aspectul dacă decizia menționată cuprinde mecanisme eficiente care permit în practică să se asigure respectarea nivelului de protecție impus de dreptul Uniunii și suspendarea sau interzicerea transferurilor de date cu caracter personal, întemeiate pe astfel de clauze, în cazul încălcării acestor clauze sau al imposibilității de a le onora. Curtea constată că Decizia 2010/87 prevede asemenea mecanisme. În această privință, ea subliniază în special că decizia menționată instituie o obligație a exportatorului datelor și a destinatarului transferului de a verifica în prealabil respectarea acestui nivel de protecție în țara terță în cauză și că obligă acest destinatar să informeze exportatorul datelor cu privire la eventuala sa imposibilitate de a asigura conformitatea cu clauzele menționate, ultimul având în acest caz sarcina de a suspenda transferul de date și/sau de a rezilia contractul încheiat cu primul.

În sfârșit, Curtea examinează validitatea Deciziei 2016/1250 în raport cu cerințele care decurg din RGPD, interpretat în lumina dispozițiilor cartei care garantează respectarea vieții private și de familie, protecția datelor cu caracter personal și dreptul la protecție jurisdicțională efectivă. În această privință, Curtea arată că decizia menționată consacră, asemenea Deciziei 2000/520, supremația cerințelor privind securitatea națională, interesul public și respectarea legislației americane, făcând astfel posibile unele ingerințe în drepturile fundamentale ale persoanelor ale căror date sunt transferate către această țară terță. Potrivit Curții, limitările protecției datelor cu caracter personal care decurg din reglementarea internă a Statelor Unite privind accesul și utilizarea de către autoritățile publice americane a unor astfel de date transferate din Uniune către această țară terță, pe care Comisia le-a evaluat în Decizia 2016/1250, nu sunt circumscrise astfel încât să îndeplinească cerințe în esență echivalente cu cele prevăzute în dreptul Uniunii de principiul proporționalității, în sensul că programele de supraveghere întemeiate pe această reglementare nu sunt limitate la strictul necesar. Întemeindu-se pe constatările care figurează în această decizie, Curtea arată că, pentru anumite programe de supraveghere, respectiva reglementare nu evidențiază în niciun mod existența unor limitări ale abilitării pe care o presupune pentru punerea în aplicare a acestor programe și nici existența unor garanții pentru persoane care nu sunt cetățeni americani potențial vizate. Curtea adaugă că, deși aceeași reglementare prevede cerințe pe care autoritățile americane trebuie să le respecte cu ocazia punerii în aplicare a programelor de supraveghere în cauză, ea nu conferă persoanelor vizate drepturi opozabile autorităților americane în fața instanțelor judecătorești.

În ceea ce privește cerința protecției jurisdicționale, Curtea statuează că, în mod contrar celor considerate de Comisie în Decizia 2016/1250, mecanismul de tip Ombudsman prevăzut de decizia menționată nu furnizează acestor persoane o cale de atac în fața unui organ care oferă garanții în esență echivalente cu cele impuse de dreptul Uniunii, de natură să asigure atât independența Ombudsmanului prevăzut de acest mecanism, cât și existența unor norme care abilitează Ombudsmanul menționat să adopte decizii obligatorii în privința serviciilor americane de informații. Pentru toate aceste motive, Curtea declară nevalidă Decizia 2016/1250.

V. Protecția datelor cu caracter personal pe internet

1. Dreptul de opoziție la prelucrarea datelor cu caracter personal („dreptul la uitare”)

Hotărârea din 13 mai 2014 (Marea Cameră), Google Spain și Google (C-131/12, EU:C:2014:317)

În această hotărâre (a se vedea și secțiunile II.1. și II.3, intitulate „Domeniul de aplicare al reglementării generale” și „Noțiunea de «prelucrare a datelor cu caracter personal»”), Curtea a clarificat domeniul de aplicare al drepturilor de acces și de opoziție la prelucrarea datelor cu caracter personal pe internet, prevăzute de Directiva 95/46.

Astfel, atunci când s-a pronunțat cu privire la întinderea răspunderii operatorului unui motor de căutare pe internet, Curtea a statuat în esență că, pentru respectarea drepturilor de acces și de opoziție prevăzute de articolul 12 litera (b) și de articolul 14 primul paragraf litera (a) din Directiva 95/46 și în măsura în care condițiile prevăzute de acestea sunt îndeplinite efectiv, operatorul unui motor de căutare este obligat, în anumite condiții, să elimine din lista de rezultate afișată în urma unei căutări efectuate plecând de la numele unei persoane linkurile către paginile de internet publicate de terți care conțin informații referitoare la această persoană. Curtea a precizat că o astfel de obligație poate exista și în ipoteza în care acest nume sau aceste informații nu sunt șterse în prealabil sau simultan de pe paginile de internet respective, iar aceasta, dacă este cazul, chiar dacă publicarea lor în sine pe paginile menționate este licită.

Pe de altă parte, sesizată cu întrebarea dacă directiva permite persoanei vizate să solicite ștergerea linkurilor către pagini de internet dintr-o astfel de listă de rezultate pentru motivul că ar dori ca informațiile conținute în aceasta care se referă la persoana sa să fie „uitate” după o anumită perioadă, Curtea observă, mai întâi, că și o prelucrare inițial licită a unor date exacte poate deveni cu timpul incompatibilă cu această directivă în cazul în care datele respective nu mai sunt necesare în raport cu scopurile pentru care au fost colectate sau prelucrate, în special dacă aceste date sunt inadecvate, atunci când nu sunt sau nu mai sunt pertinente ori sunt excesive în raport cu scopurile amintite și cu timpul care s-a scurs. Prin urmare, în ipoteza în care se constată, ca urmare a unei cereri formulate de persoana vizată, că includerea în lista de rezultate a acestor linkuri este, în stadiul actual, incompatibilă cu directiva, informațiile și linkurile care apar în această listă trebuie eliminate. În acest context, constatarea unui drept al persoanei vizate ca informația referitoare la persoana sa să nu mai fie asociată cu numele său printr-o listă de rezultate nu necesită ca includerea informației respective în lista de rezultate să cauzeze un prejudiciu persoanei vizate.

În sfârșit, Curtea a precizat că, întrucât persoana vizată poate, având în vedere drepturile sale fundamentale prevăzute la articolele 7 și 8 din cartă, să solicite ca informația în cauză să nu mai fie pusă la dispoziția marelui public prin includerea sa într-o asemenea listă de rezultate, aceste drepturi prevalează în principiu nu numai asupra interesului

economic al operatorului motorului de căutare, ci și asupra interesului acestui public de a găsi informația respectivă cu ocazia unei căutări referitoare la numele acelei persoane. Nu aceasta ar fi însă situația dacă ar reieși că, din motive speciale, precum rolul jucat de persoana respectivă în viața publică, ingerința în drepturile sale fundamentale este justificată de interesul preponderent al publicului menționat de a avea acces, prin intermediul acestei includeri, la informația în cauză.

2. Prelucrarea datelor cu caracter personal și drepturile de proprietate intelectuală

Hotărârea din 29 ianuarie 2008 (Marea Cameră), Promusicae (C-275/06, EU:C:2008:54)

Promusicae, o asociație spaniolă fără scop lucrativ care cuprinde producători și editori de înregistrări muzicale și audiovizuale, a sesizat instanțele spaniole pentru a obliga Telefónica de España SAU (societate comercială care are ca activitate printre altele furnizarea de servicii de acces la internet) să dezvăluie identitatea și adresa fizică a anumitor persoane cărora aceasta din urmă le furniza un serviciu de acces la internet și ale căror adresă IP, precum și data și ora de conectare erau cunoscute. Potrivit Promusicae, aceste persoane utilizau programul de schimb de arhive denumit „peer-to-peer” sau „P2P” (modalitate transparentă de schimb de date, independentă, descentralizată și dotată cu funcții de căutare și de transfer avansate) și permiteau accesul, în directorul partajat din calculatorul personal (*shared folder*), la fonograme cu privire la care drepturile patrimoniale de exploatare aparțineau asociaților Promusicae. Acesta a solicitat comunicarea acestor informații pentru a putea iniția proceduri civile împotriva persoanelor implicate.

În aceste condiții, Juzgado de lo Mercantil nº 5 de Madrid (Tribunalul Comercial nr. 5 din Madrid, Spania) a adresat Curții întrebarea dacă legislația europeană obligă statele membre să prevadă, pentru a asigura protecția eficientă a drepturilor de autor, obligația de divulgare a datelor cu caracter personal în cadrul unei proceduri civile.

Potrivit Curții, respectiva cerere de decizie preliminară a ridicat problema concilierii necesare a cerințelor legate de protecția diferitelor drepturi fundamentale, și anume, pe de o parte, dreptul la respectarea vieții private, și, pe de altă parte, drepturile de proprietate și dreptul la o cale de atac efectivă.

În această privință, Curtea a concluzionat că Directiva 2000/31/CE privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului

electronic, pe piața internă („Directiva privind comerțul electronic”)[83], Directiva 2001/29/CE privind armonizarea anumitor aspecte ale dreptului de autor și drepturilor conexe în societatea informațională[84], Directiva 2004/48/CE privind respectarea drepturilor de proprietate intelectuală[85] și Directiva 2002/58 nu impun statelor membre să prevadă, într-o situație precum cea din acțiunea principală, obligația de divulgare a datelor cu caracter personal în vederea asigurării unei protecții efective a dreptului de autor în cadrul unei proceduri civile. Totuși, dreptul Uniunii impune acestor state ca, la transpunerea directivelor menționate, să se asigure că se întemeiază pe o interpretare a acestora care să permită asigurarea unui just echilibru între diferitele drepturi fundamentale protejate de ordinea juridică comunitară. Apoi, la punerea în aplicare a măsurilor de transpunere a acestor directive, incumbă autorităților și instanțelor din statele membre nu numai să interpreteze dreptul lor național într-un mod conform directivelor menționate, ci și să nu se întemeieze pe o interpretare a acestora care ar intra în conflict cu drepturile fundamentale respective sau cu celelalte principii generale ale dreptului comunitar, precum principiul proporționalității.

Hotărârea din 19 aprilie 2012, Bonnier Audio ș.a. (C-461/10, EU:C:2012:219)

Högsta domstolen (Curtea Supremă, Suedia) a sesizat Curtea cu o cerere de decizie preliminară în vederea interpretării Directivelor 2002/58 și 2004/48 în cadrul unui litigiu între Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB și Storyside AB (denumite în continuare „Bonnier Audio ș.a.”) și Perfect Communication Sweden AB (denumită în continuare „ePhone”) în ceea ce privește opoziția acesteia din urmă față de cererea de emitere a unei somații de comunicare de date formulată de Bonnier Audio ș.a.

În speță, Bonnier Audio ș.a. sunt societăți de editare, titulare printre altele ale unor drepturi exclusive de reproducere, de editare și de punere la dispoziția publicului a 27 de lucrări prezentate sub formă de cărți audio. Acestea apreciază că prin difuzarea publică a celor 27 de opere, fără acordul lor, cu ajutorul unui server FTP („file transfer protocol”), care permite partajarea de fișiere și transferul de date între calculatoare conectate la internet, s-ar fi adus atingere drepturilor lor exclusive. Prin urmare, acestea au sesizat instanțele suedeze cu o cerere de emitere a unei somații de comunicare a numelui și a adresei persoanei care a utilizat adresa IP de la care se prezumă că au fost transmise fișierele respective.

---

83 Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (Directiva privind comerțul electronic) (JO 2000, L 178, p. 1, Ediție specială, 13/vol. 29, p. 257).

84 Directiva 2001/29/CE a Parlamentului European și a Consiliului din 22 mai 2001 privind armonizarea anumitor aspecte ale dreptului de autor și drepturilor conexe în societatea informațională (JO 2001, L 167, p. 10, Ediție specială, 17/vol. 1, p. 230).

85 Directiva 2004/48/CE a Parlamentului European și a Consiliului din 29 aprilie 2004 privind respectarea drepturilor de proprietate intelectuală (JO 2004, L 157, p. 45, Ediție specială, 17/vol. 2, p. 56, rectificare în JO 2004, L 195, p. 16).

În acest context, Högsta domstolen, sesizată cu recurs, a solicitat Curții să stabilească dacă dreptul Uniunii se opune aplicării unei dispoziții de drept național, instituită în temeiul articolului 8 din Directiva 2004/48, care, în scopul de a identifica un abonat, permite somarea unui furnizor de acces la internet să comunice titularului unui drept de autor sau succesorului său în drepturi, în cadrul unei proceduri civile, identitatea abonatului căruia i-a fost atribuită o adresă IP care ar fi fost utilizată pentru a se aduce atingere respectivului drept. S-a presupus, pe de o parte, că solicitantul somației a reunit indicii reale ale unei atingeri aduse dreptului de proprietate intelectuală și, pe de altă parte, că măsura solicitată este proporțională.

Curtea a amintit mai întâi că articolul 8 alineatul (3) din Directiva 2004/48 coroborat cu articolul 15 alineatul (1) din Directiva 2002/58 nu se opune stabilirii de către statele membre a unei obligații de transmitere către persoane private a unor date cu caracter personal pentru a se permite inițierea unor proceduri judiciare civile împotriva atingerilor aduse dreptului de autor, dar nici nu impune ca aceste state să prevadă o asemenea obligație. Cu toate acestea, revine autorităților și instanțelor din statele membre nu numai sarcina de a interpreta dreptul lor național într-un mod conform acelorași directive, ci și cea de a nu se întemeia pe o interpretare a acestora care ar intra în conflict cu drepturile fundamentale respective sau cu alte principii generale ale dreptului Uniunii, precum principiul proporționalității.

În această privință, ea a constatat că legislația națională în discuție impunea, pentru a putea fi emisă o somație de a comunica datele în cauză, printre altele să existe indicii reale cu privire la o atingere adusă unui drept de proprietate intelectuală asupra unei opere, ca informațiile solicitate să poată facilita ancheta cu privire la încălcarea dreptului de autor sau la atingerea adusă unui asemenea drept și ca motivele care stau la baza acestei somații să fie de un interes superior inconvenientelor sau altor prejudicii pe care le poate provoca destinatarului ei sau oricăror interese care se opun acesteia.

În consecință, Curtea a concluzionat că Directivele 2002/58 și 2004/48 nu se opun unei legislații naționale precum cea în cauză în litigiul principal, în măsura în care această legislație permite instanței naționale sesizate cu o cerere de emitere a unei somații de comunicare a datelor cu caracter personal, formulată de o persoană care are calitate procesuală activă, să pondereze, în funcție de împrejurările fiecărei cauze și ținând seama în mod corespunzător de cerințele care rezultă din principiul proporționalității, interesele opuse existente.

3. Dezindexarea unor date cu caracter personal

Hotărârea din 24 septembrie 2019 (Marea Cameră), GC ș.a. (Dezindexarea unor date sensibile) (C-136/17, EU:C:2019:773)

În această hotărâre, Curtea, reunită în Marea Cameră, a precizat obligațiile operatorului unui motor de căutare în cadrul unei cereri de dezindexare cu privire la date sensibile.

Google a refuzat să admită cererile a patru persoane de a dezindexa, în lista de rezultate afișată de motorul de căutare ca răspuns la o căutare efectuată plecând de la numele respective, diverse linkuri care duc spre pagini web publicate de terți, în special articole de presă. În urma plângerilor acestor patru persoane, Commission nationale de l'informatique et des libertés (CNIL) (Comisia Națională pentru Informatică și Libertăți, Franța) a refuzat să pună în întârziere Google să procedeze la dezindexările solicitate. Conseil d'État (Consiliul de Stat, Franța), sesizat cu litigiul, a solicitat Curții să precizeze obligațiile care revin operatorului unui motor de căutare cu ocazia soluționării unei cereri de dezindexare în temeiul Directivei 95/46.

În primul rând, Curtea a amintit că prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice, apartenența sindicală, precum și prelucrarea datelor privind sănătatea și viața sexuală este interzisă[86], sub rezerva anumitor excepții și derogări. În ceea ce privește prelucrarea datelor referitoare la infracțiuni, condamnări penale sau măsuri de siguranță, aceasta nu se poate efectua, în principiu, decât sub controlul autorității publice sau dacă în dreptul intern sunt prevăzute garanții corespunzătoare și specifice[87].

Curtea a statuat că interdicția și restricțiile referitoare la prelucrarea acestor categorii speciale de date se aplică operatorului unui motor de căutare, la fel ca oricărui alt operator de date cu caracter personal. Astfel, finalitatea acestor interdicții și restricții constă în a asigura o protecție sporită împotriva unor asemenea prelucrări, care, din cauza caracterului deosebit de sensibil al acestor date, sunt susceptibile să constituie o ingerință deosebit de gravă în drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal.

Cu toate acestea, operatorul unui motor de căutare nu răspunde pentru faptul că datele cu caracter personal figurează pe o pagină web publicată de un terț, ci pentru indexarea acestei pagini. În aceste condiții, interdicția și restricțiile referitoare la prelucrarea datelor sensibile nu se aplică acestui operator decât în temeiul acestei indexări și, așadar, prin intermediul unei verificări care trebuie efectuată, sub controlul autorităților naționale competente, pe baza unei cereri formulate de persoana vizată.

---

86 Articolul 8 alineatul (1) din Directiva 95/46 și articolul 9 alineatul (1) din Regulamentul 2016/679.
87 Articolul 8 alineatul (5) din Directiva 95/46 și articolul 10 din Regulamentul 2016/679.

În al doilea rând, Curtea a considerat că, atunci când operatorul este sesizat cu o cerere de dezindexare cu privire la date sensibile, acesta este în principiu obligat, sub rezerva anumitor excepții, să admită cererea menționată. În ceea ce privește aceste excepții, operatorul poate în special să refuze admiterea unei astfel de cereri atunci când constată că linkurile duc spre date care sunt făcute publice de către persoana vizată[88], în mod manifest, cu condiția ca indexarea unor asemenea linkuri să îndeplinească celelalte condiții de legalitate a unei prelucrări de date cu caracter personal și cu excepția cazului în care această persoană are dreptul de a se opune indexării respective din motive legate de situația sa particulară[89].

În orice caz, atunci când este sesizat cu o cerere de dezindexare, operatorul unui motor de căutare trebuie să verifice dacă includerea în lista de rezultate a linkului către o pagină web pe care sunt publicate date sensibile, care este afișată în urma unei căutări efectuate plecând de la numele acestei persoane, este strict necesară pentru a proteja libertatea de informare a utilizatorilor de internet potențial interesați de a avea acces la această pagină web prin intermediul unei asemenea căutări. În această privință, Curtea a subliniat că, deși drepturile la respectarea vieții private și la protecția datelor cu caracter personal prevalează, ca regulă generală, asupra libertății de informare a utilizatorilor de internet, acest echilibru poate să depindă însă, în cazuri particulare, de natura informației în cauză și de caracterul sensibil al acesteia în ceea ce privește viața privată a persoanei vizate, precum și de interesul publicului de a dispune de informația respectivă, care poate varia în special în funcție de rolul jucat de această persoană în viața publică.

În al treilea rând, Curtea a statuat că, în cadrul unei cereri de dezindexare cu privire la date referitoare la o procedură judiciară în materie penală desfășurată împotriva persoanei vizate, care se referă la o etapă anterioară a acestei proceduri și nu mai corespund situației actuale, revine operatorului unui motor de căutare sarcina de a aprecia dacă, având în vedere ansamblul împrejurărilor speței, persoana respectivă are dreptul ca informațiile în discuție să nu mai fie, în stadiul actual, legate de numele său prin intermediul unei liste de rezultate afișate în urma unei căutări efectuate plecând de la acest nume. Cu toate acestea, chiar dacă nu aceasta este situația, pentru motivul că includerea linkului în cauză se dovedește strict necesară pentru a concilia drepturile la respectarea vieții private și protecția datelor persoanei vizate cu libertatea de informare a utilizatorilor de internet potențial interesați, operatorul este obligat, cel târziu cu ocazia cererii de dezindexare, să organizeze lista de rezultate astfel încât imaginea globală care rezultă pentru utilizatorul de internet să reflecte situația judiciară actuală, ceea ce necesită în special ca linkurile către pagini web care includ informații cu privire la acest subiect să apară în primul rând pe această listă.

---

88 Articolul 8 alineatul (2) litera (e) din Directiva 95/46 și articolul 9 alineatul (2) litera (e) din Regulamentul 2016/679.

89 Articolul 14 primul paragraf litera (a) din Directiva 95/46 și articolul 21 alineatul (1) din Regulamentul 2016/679.

Hotărârea din 24 septembrie 2019 (Marea Cameră), Google (Întinderea teritorială a dezindexării) (C-507/17, EU:C:2019:772)

Commission nationale de l'informatique et des libertés (CNIL) (Comisia Națională pentru Informatică și Libertăți, Franța) a pus în întârziere Google ca, atunci când această societate admite o cerere de dezindexare, să procedeze la eliminarea din lista de rezultate afișată în urma unei căutări efectuate plecând de la numele persoanei în cauză a unor linkuri care duc spre pagini web pe care figurează date cu caracter personal ale acesteia din urmă, în privința tuturor extensiilor numelui de domeniu al motorului său de căutare. Ca urmare a refuzului Google de a se conforma acestei puneri în întârziere, CNIL a aplicat acestei societăți o sancțiune de 100 000 de euro. Conseil d'État (Consiliul de Stat), sesizat de Google, a solicitat Curții să precizeze întinderea teritorială a obligației operatorului motorului de căutare de a pune în aplicare dreptul la dezindexare în temeiul Directivei 95/46.

Mai întâi, Curtea a amintit posibilitatea persoanelor fizice de a-și valorifica în temeiul dreptului Uniunii dreptul lor la dezindexare împotriva operatorului unui motor de căutare care dispune de unu sau mai multe sedii pe teritoriul Uniunii, independent de aspectul dacă prelucrarea datelor cu caracter personal (în speță, indexarea unor linkuri către pagini web pe care figurează date cu caracter personal care o privesc pe persoana care se prevalează de acest drept) are loc sau nu în Uniune[90].

În ceea ce privește întinderea dreptului la dezindexare, Curtea a considerat că operatorul unui motor de căutare nu este obligat să efectueze dezindexarea în ansamblul versiunilor motorului său, ci în versiunile acestuia care corespund ansamblului statelor membre. Ea a reținut în această privință că, deși o dezindexare universală ar fi, ținând seama de caracteristicile internetului și ale motoarelor de căutare, de natură să satisfacă pe deplin obiectivul legiuitorului Uniunii care constă în a garanta un nivel ridicat de protecție a datelor cu caracter personal în întreaga Uniune, nu reiese totuși nicidecum din dreptul Uniunii[91] că pentru realizarea unui astfel de obiectiv legiuitorul ar fi ales să confere dreptului la dezindexare o întindere care ar depăși teritoriul statelor membre. Mai precis, în timp ce dreptul Uniunii instituie mecanisme de cooperare între autoritățile de supraveghere din statele membre pentru a ajunge la o decizie comună întemeiată pe o evaluare comparativă între dreptul la respectarea vieții private și la protecția datelor cu caracter personal, pe de o parte, și interesul publicului din diferite state membre de a avea acces la o informație, pe de altă parte, asemenea mecanisme nu sunt prevăzute în prezent în ceea ce privește întinderea unei dezindexări în afara Uniunii.

În stadiul actual al dreptului Uniunii, operatorul unui motor de căutare are obligația de a efectua dezindexarea solicitată nu numai în versiunea motorului ce corespunde statului

[90] Articolul 4 alineatul (1) litera (a) din Directiva 95/46 și articolul 3 alineatul (1) din Regulamentul 2016/679.
[91] Articolul 12 litera (b) și articolul 14 primul paragraf litera (a) din Directiva 95/46 și articolul 17 alineatul (1) din Regulamentul 2016/679.

membru de reședință al beneficiarului acestei dezindexări, ci și în versiunile motorului care corespund statelor membre, și aceasta printre altele pentru a se asigura un nivel consecvent și ridicat de protecție în întreaga Uniune. De altfel, îi revine unui astfel de operator sarcina de a lua, dacă este necesar, măsuri suficient de eficiente pentru a-i împiedica sau cel puțin pentru a-i descuraja în mod serios pe utilizatorii de internet din Uniune de la a avea acces, eventual plecând de la o versiune a motorului ce corespunde unui stat terț, la linkurile care fac obiectul dezindexării, iar instanței de trimitere îi revine sarcina de a verifica dacă măsurile adoptate de operator îndeplinesc această cerință.

În sfârșit, Curtea a subliniat că, deși dreptul Uniunii nu impune operatorului unui motor de căutare să opereze o dezindexare în ansamblul versiunilor motorului său, el nici nu interzice acest lucru. Prin urmare, o autoritate de supraveghere sau o autoritate judiciară dintr-un stat membru rămâne competentă să efectueze, în raport cu standardele naționale de protecție a drepturilor fundamentale, o evaluare comparativă între dreptul persoanei vizate la respectarea vieții sale private și la protecția datelor sale cu caracter personal, pe de o parte, și dreptul la libertatea de informare, pe de altă parte, și, în urma acestei evaluări comparative, să impună, dacă este cazul, operatorului acestui motor de căutare să procedeze la o dezindexare privind ansamblul versiunilor motorului menționat.

Hotărârea din 8 decembrie 2022 (Marea Cameră), Google (Dezindexarea unui conținut pretins inexact) (C-460/20, EU:C:2022:962***)***

Reclamanții din litigiul principal, TU, care ocupă posturi cu răspundere și deține participații în diferite societăți, și RE, care era partenera sa și care, până în luna mai 2015, era mandatara uneia dintre aceste societăți, au făcut obiectul a trei articole publicate pe un site internet în anul 2015 de G LLC, operatorul acestui site internet. Aceste articole, dintre care unul era ilustrat cu patru fotografii care îi reprezentau pe reclamanți și care sugerau că aceștia duceau o viață de lux, prezentau în mod critic modelul de investiții al mai multora dintre societățile lor. Accesul la aceste articole era posibil prin introducerea în motorul de căutare operat de Google LLC (denumit în continuare „Google”) a numelor și prenumelor reclamanților, atât separat, cât și în combinație cu anumite nume de societăți. Lista de rezultate trimitea la aceste articole, prin intermediul unui link, și la fotografiile afișate sub formă de imagini de previzualizare („thumbnails”).

Reclamanții din litigiul principal au solicitat Google, în calitate de operator al prelucrării datelor cu caracter personal efectuate de motorul său de căutare, pe de o parte, să elimine din lista rezultatelor căutării linkurile către articolele în discuție în litigiul principal, pentru motivul că acestea ar conține afirmații inexacte și opinii defăimătoare, și, pe de altă parte, să retragă imaginile de previzualizare din lista rezultatelor căutării. Google a refuzat să dea curs acestei cereri.

Întrucât această cerere a fost respinsă atât în primă instanță, cât și în apel, reclamanții din litigiul principal au formulat recurs la Bundesgerichtshof (Curtea Federală de Justiție, Germania), în cadrul căruia Bundesgerichtshof a sesizat Curtea cu o cerere preliminară privind interpretarea RGPD și a Directivei 95/46[92].

Prin hotărârea sa, pronunțată în Marea Cameră, Curtea își dezvoltă jurisprudența privind condițiile aplicabile cererilor de dezindexare adresate operatorului unui motor de căutare în temeiul normelor privind protecția datelor cu caracter personal. În special, ea examinează, pe de o parte, întinderea obligațiilor și a responsabilităților care incumbă operatorului unui motor de căutare în prelucrarea unei cereri de dezindexare întemeiate pe pretinsa inexactitate a informațiilor care figurează în conținutul indexat și, pe de altă parte, sarcina probei impuse persoanei vizate în ceea ce privește această inexactitate. De asemenea, ea se pronunță cu privire la necesitatea, în vederea examinării unei cereri de eliminare a fotografiilor afișate sub formă de imagini de previzualizare din lista rezultatelor unei căutări de imagini, de a ține seama de contextul inițial al publicării acestor fotografii pe internet.

În primul rând, Curtea declară că, în cadrul evaluării comparative dintre, pe de o parte, dreptul la respectarea vieții private și la protecția datelor cu caracter personal și, pe de altă parte, dreptul la libertatea de exprimare și de informare[93], în vederea examinării unei cereri de dezindexare adresate operatorului unui motor de căutare și având ca obiect eliminarea din lista de rezultate ale unei căutări a linkului care conduce la un conținut ce cuprinde informații pretins inexacte, această dezindexare nu este supusă condiției ca problema exactității conținutului indexat să fi fost soluționată, cel puțin cu titlu provizoriu, în cadrul unei acțiuni intentate de persoana respectivă împotriva furnizorului de conținut.

Cu titlu introductiv, pentru a examina în ce condiții este obligat operatorul unui motor de căutare să admită o cerere de dezindexare și, așadar, să șteargă din lista de rezultate afișată în urma unei căutări efectuate după numele persoanei vizate linkul către o pagină de internet pe care figurează afirmații pe care persoana menționată le consideră inexacte, Curtea a amintit printre altele cele ce urmează:

• în măsura în care activitatea unui motor de căutare este susceptibilă să afecteze semnificativ și în mod adițional în raport cu cea a editorilor de site-uri internet drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal, operatorul acestui motor, în calitate de persoană care stabilește scopurile și mijloacele acestei activități, trebuie să asigure, în cadrul responsabilităților, al competențelor și al posibilităților sale, că garanțiile prevăzute de Directiva 95/46 și RGDP își pot produce efectul deplin și că o protecție eficientă și completă a persoanelor în cauză poate să fie realizată efectiv;

---

92 Articolul 17 alineatul (3) litera (a) din RGPD și, respectiv, articolul 12 litera (b) și articolul 14 primula paragraf litera (a) din Directiva 95/46.
93 Drepturi fundamentale garantate la articolele 7, 8 și, respectiv, 11 din cartă.

• când este sesizat cu o cerere de dezindexare, operatorul unui motor de căutare trebuie să verifice dacă includerea linkului către pagina de internet în discuție în lista rezultatelor este necesară pentru exercitarea dreptului la libertatea de informare al utilizatorilor de internet potențial interesați de a avea acces la această pagină de internet prin intermediul unei asemenea căutări, protejată de dreptul la libertatea de exprimare și de informare;

• RGPD consacră explicit cerința unei evaluări comparative între, pe de o parte, drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal și, pe de altă parte, dreptul fundamental la libertatea de informare.

Mai întâi, Curtea arată că, deși drepturile la respectarea vieții private și la protecția datelor cu caracter personal ale persoanei vizate prevalează, ca regulă generală, asupra interesului legitim al utilizatorilor de internet de a avea acces la informația respectivă, acest echilibru poate să depindă totuși de circumstanțele pertinente din fiecare caz în parte, în special de natura acestei informații și de caracterul sensibil al acesteia în ceea ce privește viața privată a persoanei vizate, precum și de interesul publicului de a dispune de informația respectivă, care poate varia în special în funcție de rolul jucat de persoana menționată în viața publică.

Problema caracterului exact sau inexact al conținutului indexat constituie de asemenea un element pertinent în cadrul acestei aprecieri. Astfel, în anumite împrejurări, dreptul la informare al utilizatorilor de internet și libertatea de exprimare a furnizorului de conținut pot prevala asupra drepturilor la protecția vieții private și la protecția datelor cu caracter personal, în special atunci când persoana vizată joacă un rol în viața publică. Totuși, acest raport se inversează atunci când cel puțin o parte dintre informațiile vizate de cererea de dezindexare, care nu prezintă un caracter minor în raport cu ansamblul conținutului, se dovedesc inexacte. Într-o asemenea ipoteză, dreptul de informare și dreptul de a fi informat nu pot fi luate în considerare întrucât nu pot include dreptul de a difuza asemenea informații și de a avea acces la acestea.

În continuare, în ceea ce privește, pe de o parte, obligațiile privind stabilirea caracterului exact sau inexact al informațiilor care figurează în conținutul indexat, Curtea precizează că persoana care solicită dezindexarea ca urmare a inexactității unor asemenea informații este obligată să stabilească inexactitatea vădită a acestor informații sau cel puțin a unei părți dintre aceste informații care nu prezintă un caracter minor în raport cu ansamblul acestui conținut. Cu toate acestea, pentru a evita ca respectivei persoane să i se impună o sarcină excesivă susceptibilă să dăuneze efectului util al dreptului la dezindexare, acesteia îi revine numai obligația de a furniza elementele de probă cu privire la care, ținând seama de împrejurările speței, se poate pretinde în mod rezonabil de la aceasta să le identifice. În principiu, această persoană nu poate fi obligată să prezinte încă din etapa precontencioasă, în susținerea cererii sale de dezindexare, o hotărâre judecătorească obținută împotriva editorului site-ului internet în cauză, nici măcar sub forma unei decizii de măsuri provizorii.

Pe de altă parte, în ceea ce privește obligațiile și responsabilitățile impuse operatorului motorului de căutare, Curtea subliniază că acesta din urmă trebuie, pentru a verifica dacă un conținut poate continua să fie inclus în lista de rezultate ale căutărilor efectuate prin intermediul motorului său de căutare în urma unei cereri de dezindexare, să se întemeieze pe ansamblul drepturilor și intereselor prezente în cauză, precum și pe ansamblul împrejurărilor speței. Cu toate acestea, acest operator nu poate fi obligat să investigheze faptele și, în acest sens, să organizeze o dezbatere în contradictoriu cu furnizorul de conținut prin care să urmărească obținerea unor elemente lipsă cu privire la exactitatea conținutului indexat. O obligație de a contribui la stabilirea caracterului exact sau inexact al conținutului indexat ar impune acestui operator o sarcină care depășește ceea ce se poate aștepta în mod rezonabil de la el în raport cu responsabilitățile, cu competențele și cu posibilitățile sale. Această soluție ar implica un risc serios ca niște conținuturi care răspund unei nevoi de informare legitime și preponderente a publicului să fie dezindexate și să devină în acest mod dificil de găsit pe internet. Astfel, ar exista un risc real de efect disuasiv asupra exercitării libertății de exprimare și de informare dacă un asemenea operator ar efectua o dezindexare într-un mod aproape sistematic pentru a evita să trebuiască să suporte sarcina de a investiga faptele pertinente pentru a stabili caracterul exact sau inexact al conținutului indexat.

În consecință, în cazul în care persoana care a introdus o cerere de dezindexare prezintă elemente de probă care stabilesc caracterul vădit inexact al informațiilor care figurează în conținutul indexat sau cel puțin al unei părți dintre aceste informații care nu prezintă un caracter minor în raport cu ansamblul conținutului, operatorul motorului de căutare este obligat să o admită. Situația este aceeași atunci când persoana în cauză prezintă o hotărâre judecătorească pronunțată împotriva editorului site-ului internet, care se întemeiază pe constatarea că informațiile ce figurează în conținutul indexat, care nu prezintă un caracter minor în raport cu ansamblul acestuia, sunt, cel puțin la prima vedere, inexacte. În schimb, în cazul în care caracterul inexact al unor asemenea informații nu rezultă în mod vădit având în vedere elementele de probă furnizate de persoana vizată, operatorul motorului de căutare nu este obligat, în lipsa unei asemenea hotărâri judecătorești, să admită o astfel de cerere de dezindexare. Atunci când informațiile în cauză pot contribui la o dezbatere de interes general, este necesar, având în vedere toate celelalte împrejurări ale speței, să se acorde o importanță deosebită dreptului la libertatea de exprimare și de informare.

În sfârșit, Curtea adaugă că, atunci când operatorul unui motor de căutare nu dă curs cererii de dezindexare, persoana vizată trebuie să poată sesiza autoritatea de supraveghere sau autoritatea judiciară pentru ca acestea să efectueze verificările necesare și să dispună ca operatorul respectiv să adopte măsurile care se impun. În această privință, revine în special autorităților judiciare sarcina de a asigura ponderarea intereselor concurente, ele fiind cel mai bine plasate să efectueze o evaluare comparativă complexă și aprofundată, care să țină seama de toate criteriile și de toate elementele stabilite de jurisprudența relevantă.

În al doilea rând, Curtea declară că, în cadrul evaluării comparative a drepturilor fundamentale menționate mai sus, în vederea examinării unei cereri de dezindexare având ca obiect eliminarea din rezultatele unei căutări de imagini efectuate după numele unei persoane fizice a fotografiilor afișate sub formă de imagini de previzualizare care o reprezintă pe această persoană, trebuie să se țină seama de valoarea informativă a acestor fotografii independent de contextul inițial al publicării lor pe pagina de internet de unde sunt extrase. Totuși, trebuie luat în considerare orice element textual care însoțește direct afișarea acestor fotografii în rezultatele căutării și care poate să aducă o clarificare cu privire la valoarea informativă a acestora.

Curtea subliniază că, pentru a ajunge la această concluzie, căutările de imagini efectuate prin intermediul unui motor de căutare pe internet după numele unei persoane sunt supuse acelorași principii ca acelea aplicabile căutărilor de pagini de internet și informațiilor cuprinse în acestea. Ea arată că afișarea, în urma unei căutări după nume, sub formă de imagini de previzualizare, a unor fotografii cu persoana vizată este de natură să constituie o ingerință deosebit de importantă în drepturile la protecția vieții private și a datelor cu caracter personal ale acestei persoane.

Prin urmare, atunci când operatorul unui motor de căutare este sesizat cu o cerere de dezindexare având ca obiect eliminarea din rezultatele unei căutări de imagini efectuate după numele unei persoane a fotografiilor afișate sub forma unor imagini de previzualizare care o reprezintă pe această persoană, el trebuie să verifice dacă afișarea fotografiilor în discuție este necesară pentru exercitarea dreptului la libertatea de informare al utilizatorilor de internet potențial interesați să aibă acces la aceste fotografii prin intermediul unei asemenea căutări.

Or, în măsura în care motorul de căutare afișează fotografii cu persoana vizată în afara contextului în care acestea sunt publicate pe pagina de internet indexată, cel mai adesea pentru a ilustra elementele textuale pe care le conține această pagină, este necesar să se stabilească dacă acest context trebuie totuși luat în considerare cu ocazia evaluării comparative a drepturilor și intereselor concurente care trebuie să fie efectuată. În acest cadru, problema dacă aprecierea menționată trebuie să includă și conținutul paginii de internet în care figurează fotografia în privința căreia se solicită eliminarea afișării sub forma unei imagini de previzualizare depinde de obiectul și de natura prelucrării în cauză.

În ceea ce privește, *primo*, obiectul prelucrării în cauză, Curtea arată că publicarea de fotografii ca mijloc de comunicare nonverbal poate avea un impact mai puternic asupra utilizatorilor de internet decât publicațiile textuale. Fotografiile sunt astfel, ca atare, un mijloc important de atragere a atenției utilizatorilor de internet și pot suscita interesul accesării articolelor pe care le ilustrează. Or, ținând seama mai ales de împrejurarea că fotografiile se pretează adesea la mai multe interpretări, afișarea lor în lista rezultatelor căutării ca imagini de previzualizare poate determina o ingerință deosebit de gravă în dreptul persoanei vizate la protecția imaginii sale, ceea ce trebuie luat în considerare în cadrul evaluării comparative a drepturilor și intereselor concurente. O evaluare

comparativă distinctă se impune după cum sunt în discuție, pe de o parte, articole care conțin fotografii publicate de editorul paginii de internet și care, inserate în contextul lor de origine, ilustrează informațiile furnizate în aceste articole și opiniile exprimate în acestea și, pe de altă parte, fotografii afișate sub formă de imagini de previzualizare în lista de rezultate de către operatorul unui motor de căutare în afara contextului în care acestea au fost publicate pe pagina de internet de origine.

În această privință Curtea amintește că nu numai că motivul care justifică publicarea unei date cu caracter personal pe un site internet nu coincide în mod necesar cu cel care se aplică activității motoarelor de căutare, dar și că, chiar dacă situația ar fi aceasta, rezultatul evaluării comparative a drepturilor și a intereselor în cauză care trebuie efectuată poate fi diferit după cum este vorba despre prelucrarea efectuată de operatorul unui motor de căutare sau despre cea efectuată de editorul acestei pagini de internet. Pe de o parte, interesele legitime care justifică respectivele prelucrări pot fi diferite și, pe de altă parte, consecințele pe care le au prelucrările menționate pentru persoana vizată, în special pentru viața sa privată, nu sunt în mod necesar aceleași.

În ceea ce privește, *secundo*, natura prelucrării efectuate de operatorul motorului de căutare, Curtea constată că, prin reperarea fotografiilor unor persoane fizice publicate pe internet și prin afișarea acestora separat, în rezultatele căutării unor imagini, sub formă de imagini de previzualizare, operatorul unui motor de căutare oferă un serviciu care implică o prelucrare a datelor cu caracter personal autonomă și distinctă de prelucrarea efectuată de editorul paginii de internet de pe care sunt extrase fotografiile, precum și de prelucrarea, de care acest operator este de asemenea responsabil, privind indexarea acestei pagini.

În consecință, se impune o apreciere autonomă a activității operatorului motorului de căutare, constând în afișarea rezultatelor căutării unor imagini sub formă de imagini de previzualizare, dat fiind că atingerea suplimentară adusă drepturilor fundamentale care rezultă dintr-o astfel de activitate poate fi deosebit de intensă ca urmare a agregării, cu ocazia unei căutări după nume, a tuturor informațiilor referitoare la persoana în cauză care se află pe internet. În cadrul acestei aprecieri autonome, trebuie să se țină seama de faptul că această afișare constituie în sine rezultatul urmărit de utilizatorul de internet, independent de decizia sa ulterioară de a avea sau nu acces la pagina de internet de origine.

Curtea adaugă însă că o atare evaluare comparativă specifică, ce ia în considerare natura autonomă a prelucrării efectuate de operatorul motorului de căutare, nu aduce atingere eventualei relevanțe a elementelor textuale care pot însoți în mod direct afișarea unei fotografii în lista rezultatelor unei căutări, asemenea elemente fiind susceptibile să aducă o clarificare cu privire la valoarea informativă a fotografiei respective pentru public și, prin urmare, să influențeze evaluarea comparativă a drepturilor și intereselor prezente în cauză.

4. Consimțământul utilizatorului unui site internet privind stocarea informațiilor

Hotărârea din 1 octombrie 2019 (Marea Cameră), Planet49 (C-673/17, EU:C:2019:801)

Prin această hotărâre Curtea a statuat că consimțământul privind stocarea informațiilor sau dobândirea accesului la informații prin intermediul cookie-urilor instalate pe echipamentul terminal al utilizatorului unui site internet nu este dat în mod valabil atunci când autorizarea rezultă dintr-o căsuță bifată în prealabil, iar aceasta indiferent de faptul că informațiile în cauză constituie sau nu date cu caracter personal. În plus, Curtea a precizat că furnizorul de servicii trebuie să îi indice utilizatorului unui site internet durata de funcționare a cookie-urilor, precum și posibilitatea sau imposibilitatea ca terții să aibă acces la aceste cookie-uri.

Litigiul principal privea organizarea unui joc promoțional de către Planet49 pe site-ul internet www.dein-macbook.de. Pentru a participa, utilizatorii de internet trebuiau să comunice numele și adresa lor pe o pagină web pe care se găseau căsuțe care trebuiau bifate. Căsuța care autoriza instalarea cookie-urilor era bifată în prealabil. Sesizată cu un recurs de către Federația Germană a Asociațiilor de Consumatori, Bundesgerichtshof (Curtea Federală de Justiție, Germania) avea îndoieli cu privire la validitatea obținerii consimțământului utilizatorilor prin intermediul căsuței bifate în prealabil, precum și cu privire la întinderea obligației de informare care revine furnizorului de servicii.

Cererea de decizie preliminară privea în esență interpretarea noțiunii de „consimțământ” vizate de Directiva 2002/58[94] coroborată cu Directiva 95/46/CE[95], precum și cu RGPD[96].

În primul rând, Curtea a observat că articolul 2 litera (h) din Directiva 95/46/CE, la care face trimitere articolul 2 litera (f) din Directiva 2002/58, definește consimțământul drept „orice manifestare de voință, liberă, specifică și informată prin care persoana vizată acceptă să fie prelucrate datele cu caracter personal care o privesc”. Aceasta a arătat că cerința unei „manifestări” de voință a persoanei vizate indică în mod clar un comportament activ, iar nu unul pasiv. Or, un consimțământ dat prin intermediul unei căsuțe bifate în prealabil nu presupune un comportament activ din partea utilizatorului unui site internet. În plus, geneza articolului 5 alineatul (3) din Directiva 2002/58, care prevede, de la modificarea sa prin Directiva 2009/136, că utilizatorul trebuie să își fi „dat acordul” pentru plasarea cookie-urilor, urmărește să arate că consimțământul utilizatorului nu mai poate fi în prezent prezumat și trebuie să rezulte dintr-un comportament activ al acestuia din urmă. În sfârșit, un consimțământ activ este în

[94] Articolul 2 litera (f) și articolul 5 alineatul (3) din Directiva 2002/58, astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 (JO 2009, L 337, p. 11).

[95] Articolul 2 litera (h) din Directiva 95/46.

[96] Articolul 6 alineatul (1) litera (a) din Regulamentul 2016/679.

prezent prevăzut de RGPD[97], al cărui articol 4 punctul 11 impune o manifestare de voință care ia printre altele forma unei „acțiuni fără echivoc” și al cărui considerent (32) exclude în mod expres ca „absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni” să constituie un consimțământ.

Prin urmare, Curtea a statuat că consimțământul nu este dat în mod valabil atunci când stocarea de informații sau dobândirea accesului la informațiile deja stocate în echipamentul terminal al utilizatorului unui site internet este autorizată prin intermediul unei căsuțe bifate în prealabil, pe care acest utilizator trebuie să o debifeze în cazul în care refuză să își dea consimțământul. Ea a adăugat că faptul că un astfel de utilizator activează butonul de participare la jocul promoțional în cauză nu poate să fie suficient pentru a considera că acesta și-a dat în mod valabil consimțământul pentru plasarea cookie-urilor.

În al doilea rând, Curtea a constatat că articolul 5 alineatul (3) din Directiva 2002/58 urmărește să protejeze utilizatorul de orice ingerință în viața sa privată, indiferent dacă această ingerință privește sau nu date cu caracter personal. Din aceasta rezultă că noțiunea de „consimțământ” nu trebuie să fie interpretată diferit în funcție de aspectul dacă informațiile stocate sau consultate în echipamentul terminal al utilizatorului unui site internet constituie sau nu date cu caracter personal.

În al treilea rând, Curtea a arătat că articolul 5 alineatul (3) din Directiva 2002/58 impune ca utilizatorul să își fi dat acordul, după ce a primit informații clare și complete în special cu privire la scopurile prelucrării. Or, o informare clară și completă presupune faptul că un utilizator este în măsură să stabilească cu ușurință consecințele consimțământului pe care l-ar putea da și garantează că acest consimțământ este dat în deplină cunoștință de cauză. În această privință, Curtea a considerat că durata de funcționare a cookie-urilor, precum și posibilitatea sau imposibilitatea ca terții să aibă acces la aceste cookie-uri fac parte din informarea clară și completă care trebuie să fie oferită utilizatorului unui site internet de către furnizorul de servicii.

5. Prelucrarea datelor cu caracter personal pe rețelele sociale online

Hotărârea din 4 iulie 2023 (Marea Cameră), Meta Platforms ș.a. (Condiții generale de utilizare a unei rețele sociale) (C-252/21, EU:C:2023:537)

Societatea Meta Platforms este proprietara rețelei sociale online „Facebook”, care este gratuită pentru utilizatorii privați. Modelul de afaceri al acestei rețele sociale se bazează pe finanțarea prin publicitate online, care se face personalizat pentru utilizatorii

[97] *Idem.*

individuali ai acesteia. O astfel de publicitate este posibilă din punct de vedere tehnic prin alcătuirea automată a unor profiluri foarte detaliate ale utilizatorilor rețelei și ai serviciilor online oferite la nivelul grupului Meta. Astfel, pentru a putea utiliza rețeaua socială menționată, utilizatorii trebuie, la momentul înscrierii lor, să accepte condițiile generale stabilite de Meta Platforms, care fac trimitere la politicile de utilizare a datelor și a modulelor „cookie” stabilite de această societate. În temeiul acestora din urmă, pe lângă datele pe care acești utilizatori le furnizează în mod direct cu ocazia înregistrării lor, Meta Platforms colectează de asemenea date referitoare la activitățile utilizatorilor respectivi în cadrul și în afara rețelei sociale și le asociază conturilor Facebook ale utilizatorilor respectivi. În ceea ce privește aceste din urmă date, desemnate de asemenea ca „date *off* Facebook”, este vorba, pe de o parte, despre date privind consultarea unor pagini de internet și a unor aplicații terțe și, pe de altă parte, despre date referitoare la utilizarea altor servicii online care aparțin grupului Meta (printre care Instagram și WhatsApp). Datele astfel colectate, în ansamblu, permit să se desprindă concluzii detaliate cu privire la preferințele și interesele acelorași utilizatori.

Prin decizia din 6 februarie 2019, Bundeskartellamt (Oficiul Federal al Concurenței, Germania) a interzis Meta Platforms, pe de o parte, să subordoneze, în condițiile generale în vigoare la acel moment, utilizarea rețelei sociale Facebook de către utilizatori privați care au reședința în Germania de prelucrarea datelor lor *off* Facebook și, pe de altă parte, să prelucreze fără consimțământul lor aceste date. În plus, Oficiul Federal al Concurenței i-a impus să adapteze aceste condiții generale astfel încât să reiasă cu claritate că datele menționate nu vor fi nici colectate, nici asociate cu conturile de utilizatori Facebook, nici utilizate fără consimțământul utilizatorilor în cauză. În sfârșit, această autoritate a subliniat că un asemenea consimțământ nu este valid atunci când reprezintă o condiție pentru utilizarea rețelei sociale. Acesta și-a motivat decizia prin faptul că prelucrarea datelor în cauză, care nu ar fi conformă cu RGPD, ar constitui o exploatare abuzivă a poziției dominante a Meta Platforms pe piața rețelelor sociale online.

Meta Platforms a introdus o acțiune împotriva acestei decizii la Oberlandesgericht Düsseldorf (Tribunalul Regional Superior din Düsseldorf, Germania). Având îndoieli cu privire, printre altele, la interpretarea și aplicarea anumitor dispoziții din RGPD, Tribunalul Regional Superior din Düsseldorf a sesizat Curtea cu titlu preliminar.

Prin hotărârea sa, Curtea, reunită în Marea Cameră, aduce precizări cu privire la posibilitatea prelucrării de către un operator al unei rețele sociale a unor date cu caracter personal „sensibile” ale utilizatorilor săi, cu privire la condițiile de legalitate a prelucrării datelor efectuate de un astfel de operator, precum și cu privire la validitatea consimțământului dat în scopul unei astfel de prelucrări de către acești utilizatori unei întreprinderi care are o poziție dominantă pe piața națională a rețelelor sociale online.

În ceea ce privește prelucrarea unor categorii speciale de date cu caracter personal[98], Curtea apreciază că, în cazul în care un utilizator al unei rețele sociale online consultă site-uri internet sau aplicații în raport cu una sau mai multe dintre aceste categorii și, dacă este cazul, introduce acolo date înscriindu-se sau efectuând comenzi online, prelucrarea datelor cu caracter personal de către operatorul acestei rețele sociale online[99] trebuie să fie considerată o „prelucrare de categorii speciale de date cu caracter personal", în sensul articolului 9 alineatul (1) din RGPD, atunci când această prelucrare de date permite să se divulge informații care se încadrează în una dintre aceste categorii speciale, indiferent dacă aceste informații privesc un utilizator al acestei rețele sau orice altă persoană fizică. O astfel de prelucrare a datelor este în principiu interzisă, sub rezerva anumitor derogări[100].

În această din urmă privință, Curtea precizează că, atunci când consultă site-uri internet sau aplicații în raport cu una sau mai multe dintre categoriile speciale de date, un utilizator al unei rețele sociale online nu face publice în mod manifest[101] datele referitoare la consultarea menționată, colectate de operatorul acestei rețele sociale online prin intermediul modulelor „cookie" sau al tehnologiilor de stocare similare. Pe de altă parte, atunci când introduce date pe astfel de site-uri internet sau în astfel de aplicații sau atunci când acționează butoane de selecție integrate în aceste site-uri și aplicații, cum ar fi butoanele „Îmi place" sau „Distribuie" sau butoanele care permit utilizatorului să se identifice pe aceste site-uri sau aplicații cu ajutorul datelor de acces legate de contul său de utilizator al rețelei sociale, al numărului său de telefon sau al adresei de e-mail, un atare utilizator face publice în mod manifest datele astfel introduse sau care rezultă din acționarea acestor butoane numai în cazul în care și-a exprimat în mod explicit opțiunea în prealabil, dacă este cazul pe baza unei configurări individuale efectuate în deplină cunoștință de cauză, de a face datele care îl privesc accesibile unui număr nelimitat de persoane.

În ceea ce privește, mai general, condițiile de legalitate a unei prelucrări de date cu caracter personal, Curtea amintește că, în temeiul RGPD, o prelucrare este legală dacă și în măsura în care persoana vizată și-a dat consimțământul pentru prelucrarea datelor

---

98 Prevăzute la articolul 9 alineatul (1) din RGPD. Această dispoziție prevede că „[s]e interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice".

99 Această prelucrare constă în colectarea, prin intermediul unor interfețe integrate, al unor module „cookie" sau al unor tehnologii de stocare similare, a datelor provenite din consultarea acestor site-uri și a acestor aplicații, precum și a datelor inserate de utilizator, în asocierea tuturor acestor date cu contul rețelei sociale al acestuia și în utilizarea datelor menționate de către operatorul respectiv.

100 Prevăzute la articolul 9 alineatul (2) din RGPD. Această dispoziție prevede: „[a]lineatul (1) nu se aplică în următoarele situații:

(a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicția prevăzută la alineatul (1) să nu poată fi ridicată prin consimțământul persoanei vizate; […]

(e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;

(f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;

[…]"

101 În sensul articolului 9 alineatul 2 litera (e) din RGPD.

sale cu caracter personal pentru unu sau mai multe scopuri specifice[102]. În lipsa unui astfel de consimțământ sau atunci când acest consimțământ nu a fost dat în mod liber, specific, informat și lipsit de ambiguitate, o astfel de prelucrare este totuși justificată atunci când îndeplinește una dintre cerințele de necesitate[103], care sunt de strictă interpretare. Or, prelucrarea datelor cu caracter personal ale utilizatorilor săi efectuată de un operator al unei rețele sociale online poate fi considerată necesară pentru executarea unui contract la care acești utilizatori sunt părți numai cu condiția ca prelucrarea respectivă să fie în mod obiectiv indispensabilă pentru realizarea unui scop care face parte integrantă din prestația contractuală destinată utilizatorilor menționați, astfel încât obiectul principal al contractului nu ar putea fi atins în lipsa acestei prelucrări.

În plus, potrivit Curții, prelucrarea datelor în cauză poate fi considerată necesară în scopul intereselor legitime urmărite de operator sau de un terț numai dacă operatorul menționat a indicat utilizatorilor de la care au fost colectate datele un interes legitim urmărit prin prelucrarea lor, dacă această prelucrare este efectuată în limitele strictului necesar pentru realizarea acestui interes legitim și dacă reiese dintr-o evaluare comparativă a intereselor opuse, în raport cu ansamblul circumstanțelor relevante, că interesele sau libertățile și drepturile fundamentale ale acestor utilizatori nu prevalează asupra interesului legitim menționat al operatorului sau al unui terț. Or, Curtea consideră printre altele că, în lipsa unui consimțământ din partea lor, interesele și drepturile fundamentale ale utilizatorilor menționați prevalează asupra interesului operatorului unei rețele sociale online pentru personalizarea publicității prin care își finanțează activitatea.

În sfârșit, Curtea precizează că prelucrarea datelor în cauză este justificată dacă este într-adevăr necesară în vederea respectării unei obligații legale care îi revine operatorului, în temeiul unei dispoziții de drept al Uniunii sau al dreptului statului membru în cauză, dacă acest temei juridic urmărește un obiectiv de interes public și este proporțional cu obiectivul legitim urmărit, iar prelucrarea respectivă este efectuată în limitele strictului necesar.

În ceea ce privește validitatea consimțământului utilizatorilor în cauză pentru prelucrarea datelor lor în temeiul RGPD, Curtea consideră că împrejurarea că operatorul unei rețele sociale online ocupă o poziție dominantă pe piața rețelelor sociale online nu se opune ca atare posibilității ca utilizatorii unei astfel de rețele să își dea în mod valabil consimțământul pentru prelucrarea datelor lor cu caracter personal efectuată de acest operator. Cu toate acestea, având în vedere că o asemenea poziție poate afecta

[102] Potrivit articolului 6 alineatul (1) primul paragraf litera (a) din Directiva RGPD.

[103] Menționate la articolul 6 alineatul (1) primul paragraf literele (b)-(f) din RGPD. În temeiul acestor dispoziții, prelucrarea este legală numai dacă și în măsura în care aceasta este printre altele necesară pentru executarea unui contract la care persoana vizată este parte [articolul 6 alineatul (1) primul paragraf litera (b) din RGPD], în vederea îndeplinirii unei obligații legale care îi revine operatorului [articolul 6 alineatul (1) primul paragraf litera (c) din RGPD] sau în scopul intereselor legitime urmărite de operator sau de o parte terță [articolul 6 alineatul (1) primul paragraf litera (f) din RGPD].

libertatea de alegere a acestor utilizatori și poate crea un dezechilibru vădit între aceștia și operatorul menționat, ea constituie un element important pentru a stabili dacă, într-adevăr, consimțământul a fost dat în mod valabil și în special în mod liber, aspect care trebuie dovedit de același operator[104].

Mai ales, utilizatorii rețelei sociale în discuție trebuie să dispună de libertatea de a refuza în mod individual, în cadrul procesului contractual, să își dea consimțământul pentru anumite operațiuni de prelucrare de date care nu sunt necesare pentru executarea contractului, fără a fi însă obligați să renunțe integral la utilizarea acestei rețele sociale online, ceea ce implică faptul ca respectivilor utilizatori să li se ofere, dacă este cazul în schimbul unei remunerații adecvate, o alternativă echivalentă care nu este însoțită de asemenea operațiuni de prelucrare a datelor. În plus, este necesar ca un consimțământ distinct să poată fi dat pentru prelucrarea datelor *off* Facebook.

VI. Autorități naționale de supraveghere

1. Sfera de aplicare a cerinței privind independența

Hotărârea din 9 martie 2010 (Marea Cameră), Comisia/Germania (C-518/07, EU:C:2010:125)

Prin cererea introductivă, Comisia a solicitat Curții să constate că Republica Federală Germania nu și-a îndeplinit obligațiile care îi revin în temeiul articolului 28 alineatul (1) al doilea paragraf din Directiva 95/46 prin supunerea la tutela statului a autorităților de supraveghere competente pentru supravegherea prelucrării datelor cu caracter personal în celelalte sectoare decât cel public din diferitele landuri și astfel prin transpunerea în mod eronat a cerinței de „independență deplină” a autorităților responsabile de garantarea protecției acestor date.

Republica Federală Germania consideră, la rândul său, că articolul 28 alineatul (1) al doilea paragraf din Directiva 95/46 impune o independență funcțională a autorităților de supraveghere, în sensul că aceste autorități trebuie să fie independente de celelalte sectoare decât cel public supus supravegherii acestora și că nu trebuie să fie expuse niciunei influențe externe. Or, în opinia acesteia, tutela statului exercitată în landurile germane nu constituie o asemenea influență exterioară, ci un mecanism de supraveghere internă a administrației, pus în aplicare de către autoritățile care aparțin aceluiași aparat administrativ ca autoritățile de supraveghere și care sunt obligate, la fel ca acestea din urmă, să îndeplinească obiectivele Directivei 95/46.

[104] În temeiul articolului 7 alineatul (1) din RGPD.

Curtea a statuat că garanția de independență a autorităților naționale de supraveghere prevăzută de Directiva 95/46 are în vedere să asigure eficiența și fiabilitatea supravegherii respectării dispozițiilor în domeniul protecției persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și trebuie să fie interpretată în lumina acestui obiectiv. Aceasta nu a fost instituită în scopul de a conferi un statut special acestor autorități în sine, precum și reprezentanților lor, ci pentru a consolida protecția persoanelor și a organismelor care sunt avute în vedere prin deciziile acestora, autoritățile de supraveghere trebuind, așadar, în exercitarea atribuțiilor lor, să acționeze într-un mod obiectiv și imparțial.

Curtea a considerat că aceste autorități de supraveghere competente pentru supravegherea prelucrării datelor cu caracter personal în celelalte sectoare decât cel public trebuie să beneficieze de o independență care să le permită să își exercite atribuțiile fără nicio influență exterioară. Această independență exclude nu numai orice influență exercitată de către organismele supravegheate, ci și orice ingerință și orice altă influență exterioară, indiferent dacă aceasta este directă sau indirectă, care ar putea să pună în discuție îndeplinirea de către autoritățile menționate a sarcinii acestora care constă în stabilirea unui echilibru just între protecția dreptului la viață privată și libera circulație a datelor cu caracter personal. Simplul risc ca autoritățile de tutelă să poată exercita o influență politică asupra deciziilor autorităților de supraveghere competente este suficient pentru a împiedica exercitarea în mod independent a atribuțiilor acestora. Pe de o parte, ar putea exista situația unei „supuneri anticipate” a acestor autorități în ceea ce privește practica decizională a autorității de tutelă. Pe de altă parte, rolul de gardian al dreptului la viață privată pe care și-l asumă autoritățile menționate impune ca deciziile acestora și, așadar, ele însele să fie mai presus de orice suspiciune de părtinire. Conform Curții, tutela statului exercitată asupra autorităților naționale de supraveghere nu este, așadar, compatibilă cu cerința de independență.

Hotărârea din 16 octombrie 2012 (Marea Cameră), Comisia/Austria (C-614/10, EU:C:2012:631***)***

Prin cererea introductivă, Comisia a solicitat Curții să constate că, întrucât nu a adoptat toate dispozițiile necesare pentru ca legislația în vigoare în Austria să respecte criteriul de independență a Datenschutzkommission (Comisia de Protecție a Datelor), instituită ca autoritate de supraveghere pentru protecția datelor cu caracter personal, Austria nu și-a îndeplinit obligațiile care îi revin în temeiul articolului 28 alineatul (1) al doilea paragraf din Directiva 95/46.

Curtea a constatat o încălcare a obligațiilor din partea Austriei, considerând în esență că nu satisface criteriul de independență a autorității de supraveghere prevăzut de Directiva 95/46 statul membru care stabilește un cadru de reglementare pe baza căruia membrul administrator al respectivei autorități este un funcționar al statului supus unui control ierarhic, al cărei secretariat este integrat în serviciile guvernului național, iar cancelarul federal dispune de un drept necondiționat la informare cu privire la toate aspectele legate de administrarea autorității menționate.

Curtea a amintit, mai întâi, că termenii „în condiții de independență deplină” de la articolul 28 alineatul (1) al doilea paragraf din Directiva 95/46 presupun că autoritățile de supraveghere a protecției datelor cu caracter personal trebuie să beneficieze de o independență care să le permită să își exercite atribuțiile fără nicio influență exterioară. În această privință, împrejurarea că o asemenea autoritate dispune de o independență funcțională, în sensul că membrii săi sunt independenți și, în exercitarea atribuțiilor lor, nu sunt ținuți de niciun fel de instrucțiuni, nu este, ca atare, suficientă pentru a feri autoritatea de supraveghere menționată de orice influență exterioară. Or, independența impusă în acest cadru vizează să excludă nu numai influența directă, sub forma unor instrucțiuni, ci și orice formă de influență indirectă susceptibilă să orienteze deciziile autorității de supraveghere. Pe de altă parte, având în vedere rolul de gardieni ai dreptului la viață privată pe care și-l asumă autoritățile de supraveghere, deciziile lor și, prin urmare, ele însele trebuie să se situeze mai presus de orice suspiciune de părtinire.

Curtea a precizat că, pentru a putea îndeplini criteriul de independență prevăzut în dispoziția menționată anterior a Directivei 95/46, o autoritate națională de supraveghere nu trebuie să dispună de o poziție bugetară autonomă, ca în cazul prevăzut la articolul 43 alineatul (3) din Regulamentul nr. 45/2001. Într-adevăr, statele membre nu sunt obligate să preia în legislația lor națională dispoziții analoage celor din capitolul V din Regulamentul nr. 45/2001 pentru a garanta o totală independență autorităților lor de supraveghere și pot astfel să prevadă că, din punctul de vedere al dreptului bugetar, autoritatea de supraveghere depinde de un departament ministerial determinat. Cu toate acestea, atribuirea mijloacelor umane și materiale necesare unei asemenea autorități nu trebuie să o împiedice să își exercite atribuțiile „în condiții de independență deplină”, în sensul articolului 28 alineatul (1) al doilea paragraf din Directiva 95/46.

Hotărârea din 8 aprilie 2014 (Marea Cameră), Comisia/Ungaria (C-288/12, EU:C:2014:237)

În această cauză, Comisia a solicitat Curții să constate că, prin faptul că a pus capăt în mod anticipat mandatului autorității de supraveghere a protecției datelor cu caracter personal, Ungaria nu și-a îndeplinit obligațiile care îi revin în temeiul Directivei 95/46.

Curtea a constatat că nu își îndeplinește obligațiile care îi revin în temeiul Directivei 95/46/CE un stat membru care pune capăt în mod anticipat mandatului autorității de supraveghere a protecției datelor cu caracter personal.

Astfel, în opinia Curții, independența de care trebuie să beneficieze autoritățile de supraveghere competente pentru supravegherea prelucrării datelor menționate exclude printre altele orice ingerință și orice altă influență exterioară, sub orice formă, fie directă, fie indirectă, care ar fi susceptibile să le orienteze deciziile și care astfel ar putea să pună în discuție îndeplinirea de către autoritățile menționate a sarcinii lor care constă în stabilirea unui echilibru just între protecția dreptului la viață privată și libera circulație a datelor cu caracter personal.

Curtea a reamintit de asemenea că independența funcțională nu este, ca atare, suficientă pentru a feri autoritățile de supraveghere de orice influență exterioară, simplul risc ca autoritățile de tutelă ale unui stat să poată exercita o influență politică asupra deciziilor autorităților de supraveghere fiind suficient pentru a împiedica exercitarea în mod independent a atribuțiilor acestora. Or, dacă fiecare stat membru ar avea dreptul să pună capăt mandatului unei autorități de supraveghere înainte de termenul inițial prevăzut al acestuia, fără a respecta normele și garanțiile prestabilite în acest scop prin legislația aplicabilă, pericolul unei astfel de încetări anticipate care ar plana asupra autorității respective pe tot parcursul exercitării mandatului său ar putea conduce la o formă de supunere a acesteia față de puterea politică, incompatibilă cu cerința de independență menționată. În plus, într-o asemenea situație, nu s-ar putea considera că autoritatea de supraveghere poate opera în orice împrejurări mai presus de orice suspiciune de părtinire.

2. Stabilirea dreptului aplicabil și a autorității de supraveghere competente

Hotărârea din 1 octombrie 2015, Weltimmo (C-230/14, EU:C:2015:639)

Nemzeti Adatvédelmi és Információszabadság Hatóság (Autoritatea Națională pentru Protecția Datelor și Libertatea Informației, Ungaria) a aplicat o amendă societății Weltimmo, înregistrată în Slovacia și care administrează pagini de internet de anunțuri imobiliare privind bunuri situate în Ungaria, pentru motivul că aceasta nu a procedat la eliminarea datelor cu caracter personal ale autorilor anunțurilor de pe aceste site-uri, în pofida cererii lor în acest sens, și a comunicat aceste date către agenții de recuperare a creanțelor pentru a obține achitarea unor facturi neplătite. Potrivit autorității de supraveghere maghiare, societatea Weltimmo a încălcat astfel legislația maghiară de transpunere a Directivei 95/46.

Sesizată cu un recurs, Kúria (Curtea Supremă, Ungaria) a exprimat îndoieli cu privire la determinarea dreptului aplicabil și cu privire la competențele autorității maghiare de supraveghere, având în vedere articolul 4 alineatul (1) și articolul 28 din Directiva 95/46. În consecință, aceasta a adresat Curții o serie de întrebări preliminare.

În ceea ce privește dreptul național aplicabil, Curtea a statuat că articolul 4 alineatul (1) litera (a) din Directiva 95/46 permite aplicarea legislației privind protecția datelor cu caracter personal a unui alt stat membru decât statul în care operatorul responsabil cu prelucrarea acestor date este înregistrat, în măsura în care acesta exercită, într-o formă de instalare stabilă pe teritoriul acestui stat membru, o activitate efectivă și reală, fie și minimă, în cadrul căreia este efectuată prelucrarea. Pentru a determina dacă aceste condiții sunt îndeplinite, instanța de trimitere poate îndeosebi să țină cont de faptul, pe de o parte, că activitatea operatorului de date, în cadrul căreia are loc prelucrarea, constă în exploatarea unor site-uri internet de anunțuri imobiliare privind bunuri

imobile situate pe teritoriul statului membru menționat și redactate în limba acestuia și că ea este, în consecință, în principal sau chiar în întregime orientată către acest stat membru. De asemenea, instanța națională poate lua în considerare, pe de altă parte, faptul că persoana respectivă dispune de un reprezentant în statul membru menționat, care este însărcinat să recupereze creanțele care rezultă din această activitate, precum și să îl reprezinte în proceduri administrative și judiciare privind prelucrarea datelor în cauză. În schimb, Curtea a precizat că este lipsit de pertinență aspectul cetățeniei persoanelor vizate de această prelucrare de date.

În ceea ce privește competența și atribuțiile autorității de supraveghere sesizate cu o plângere, conform articolului 28 alineatul (4) din Directiva 95/46, Curtea a considerat că această autoritate poate examina aceste plângeri indiferent de dreptul aplicabil și chiar înainte de a ști care este dreptul național care este aplicabil prelucrării în cauză. Cu toate acestea, dacă ajunge la concluzia că este aplicabil dreptul unui alt stat membru, ea nu poate impune sancțiuni în afara teritoriului statului membru din care provine. Într-o asemenea situație, îi revine, în executarea obligației de cooperare pe care o prevede articolul 28 alineatul (6) din această directivă, să solicite autorității de supraveghere din acest alt stat membru să constate o eventuală încălcare a acestui drept și să impună sancțiuni, dacă acesta din urmă le permite, sprijinindu-se eventual pe informațiile pe care ea i le va fi transmis.

3. Competențele autorităților naționale de supraveghere

Hotărârea din 6 octombrie 2015 (Marea Cameră), Schrems (C-362/14, EU:C:2015:650)

În această cauză (a se vedea și secțiunea IV, intitulată „Transfer de date cu caracter personal către țări terțe”), Curtea a statuat în special că autoritățile naționale de supraveghere sunt competente să controleze transferul datelor cu caracter personal către țări terțe.

În această privință, Curtea a constatat mai întâi că autoritățile naționale de supraveghere dispun de o gamă largă de competențe, iar acestea, enumerate în mod neexhaustiv la articolul 28 alineatul (3) din Directiva 95/46, constituie tot atâtea mijloace necesare pentru a-și îndeplini sarcinile. Astfel, autoritățile menționate beneficiază printre altele de competențe de investigare, cum ar fi aceea de a colecta toate informațiile necesare pentru îndeplinirea îndatoririlor de supraveghere, de competențe efective de intervenție, cum ar fi aceea de a impune interdicția temporară sau definitivă de prelucrare a datelor, sau de competența de a acționa în justiție.

În ceea ce privește competența de supraveghere a transferurilor de date cu caracter personal către țările terțe, Curtea a hotărât că din cuprinsul articolului 28 alineatele (1) și (6) din Directiva 95/46 reiese că competențele autorităților naționale de supraveghere

privesc prelucrările de date cu caracter personal efectuate pe teritoriul statului membru din care aceste autorități provin, astfel încât ele nu dispun de competențe, în temeiul acestui articol 28, în ceea ce privește prelucrările unor astfel de date efectuate pe teritoriul unei țări terțe.

Cu toate acestea, operațiunea care constă în transferarea de date cu caracter personal dintr-un stat membru către o țară terță constituie în sine o prelucrare a datelor cu caracter personal efectuată pe teritoriul unui stat membru. În consecință, autoritățile naționale de supraveghere fiind, conform articolului 8 alineatul (3) din cartă și articolului 28 din Directiva 95/46, responsabile de supravegherea respectării normelor Uniunii referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, fiecare dintre acestea este învestită cu competența de a verifica dacă un transfer de date cu caracter personal din statul membru din care provine către o țară terță respectă cerințele stabilite de această directivă.

Hotărârea din 5 iunie 2018 (Marea Cameră), Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388)

În această hotărâre (a se vedea și secțiunea II.5, intitulată „Noțiunea de «operator de date cu caracter personal»”), care privește printre altele interpretarea articolelor 4 și 28 din Directiva 95/46, Curtea s-a pronunțat cu privire la întinderea competențelor de intervenție de care dispun autoritățile de supraveghere în privința unei prelucrări de date cu caracter personal care implică participarea mai multor actori.

Astfel, Curtea a statuat că, atunci când o întreprindere stabilită în afara Uniunii Europene (precum societatea americană Facebook) dispune de mai multe sedii în diferite state membre, autoritatea de supraveghere a unui stat membru este abilitată să exercite competențele pe care i le conferă articolul 28 alineatul (3) din această directivă în privința unui sediu al acestei întreprinderi situat pe teritoriul acestui stat membru (în speță Facebook Germany), deși, potrivit repartizării misiunilor în cadrul grupului, pe de o parte, acest sediu răspunde doar de vânzarea de spații publicitare și de alte activități de marketing pe teritoriul statului membru menționat și, pe de altă parte, răspunderea exclusivă a colectării și a prelucrării datelor cu caracter personal incumbă, pentru întregul teritoriu al Uniunii Europene, unui sediu situat într-un alt stat membru (în speță Facebook Ireland).

În plus, Curtea a precizat că, atunci când autoritatea de supraveghere a unui stat membru intenționează să exercite în privința unui organism stabilit pe teritoriul acestui stat membru competențele de intervenție prevăzute la articolul 28 alineatul (3) din Directiva 95/46 ca urmare a unor atingeri aduse normelor referitoare la protecția datelor cu caracter personal săvârșite de un terț operator al acestor date care are sediul în alt stat membru (în speță Facebook Ireland), această autoritate de supraveghere este competentă să aprecieze, în mod autonom în raport cu autoritatea de supraveghere a acestui din urmă stat membru (Irlanda), legalitatea unei astfel de prelucrări de date și își

poate exercita competențele de intervenție în privința organismului stabilit pe teritoriul său fără a solicita în prealabil autorității de supraveghere a celuilalt stat membru să intervină.

Hotărârea din 15 iunie 2021 (Marea Cameră), Facebook Ireland ș.a. (C-645/19, EU:C:2021:483)

La 11 septembrie 2015, președintele Comisiei belgiene pentru protecția vieții private (denumită în continuare „CPVP") a sesizat Nederlandstalige rechtbank van eerste aanleg Brussel (Tribunalul de Primă Instanță neerlandofon din Bruxelles, Belgia) cu o acțiune în încetare împotriva Facebook Ireland, a Facebook Inc. și a Facebook Belgium, având ca obiect încetarea unor încălcări, pretins săvârșite de Facebook, ale legislației referitoare la protecția datelor. Aceste încălcări constau în special în colectarea și în utilizarea de informații privind comportamentul de navigare al utilizatorilor de internet belgieni, deținători sau nedeținători ai unui cont de Facebook, prin intermediul diferitelor tehnologii, cum ar fi cookies, extensiile pentru social media[105] sau pixelii.

La 16 februarie 2018, instanța menționată s-a declarat competentă să se pronunțe cu privire la această acțiune și, pe fond, a statuat că rețeaua socială Facebook nu informase suficient utilizatorii de internet belgieni cu privire la colectarea și la utilizarea informațiilor în cauză. Pe de altă parte, consimțământul dat de utilizatorii de internet pentru colectarea și prelucrarea informațiilor menționate a fost considerat nevalabil.

La 2 martie 2018, Facebook Ireland, Facebook Inc. și Facebook Belgium au declarat apel împotriva acestei hotărâri la Hof van beroep te Brussel (Curtea de Apel din Bruxelles, Belgia), instanța de trimitere din prezenta cauză. În fața acestei instanțe, Autoritatea de Protecție a Datelor belgiană (denumită în continuare „APD") a acționat în calitate de succesor legal al președintelui CPVP. Instanța de trimitere s-a declarat competentă să se pronunțe doar cu privire la apelul formulat de Facebook Belgium.

Instanța de trimitere a exprimat îndoieli cu privire la incidența aplicării mecanismului „ghișeului unic" prevăzut de RGPD[106] asupra competențelor APD și a ridicat mai precis problema dacă, pentru faptele ulterioare intrării în vigoare a RGPD, și anume 25 mai 2018, APD poate acționa împotriva Facebook Belgium, din moment ce Facebook Ireland a fost identificat drept operator al datelor în cauză. Astfel, de la această dată și în special în temeiul principiului „ghișeului unic" prevăzut de RGPD, numai Comisarul pentru protecția datelor irlandez ar fi competent să introducă o acțiune în încetare, sub controlul instanțelor irlandeze.

[105] De exemplu butoanele „Îmi place" sau „Distribuie".

[106] Potrivit articolului 56 alineatul (1) din RGPD: „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 hotărârea sa, pronunțată în Marea Cameră, Curtea precizează competențele autorităților naționale de supraveghere în cadrul RGPD. Astfel, aceasta statuează printre altele că regulamentul menționat autorizează, în anumite condiții, o autoritate de supraveghere a unui stat membru să își exercite competența de a aduce orice pretins caz de încălcare a RGPD în fața unei instanțe a acestui stat și să inițieze proceduri judiciare în ceea ce privește o prelucrare de date transfrontalieră[107], deși nu ea este autoritatea principală pentru această prelucrare.

În primul rând, Curtea precizează condițiile în care o autoritate națională de supraveghere care nu are calitatea de autoritate principală în ceea ce privește o prelucrare transfrontalieră trebuie să își exercite competența de a aduce orice pretins caz de încălcare a RGPD în fața unei instanțe a unui stat membru și, după caz, de a iniția proceduri judiciare pentru a asigura aplicarea acestui regulament. În acest sens, pe de o parte, RGPD trebuie să confere acestei autorități de supraveghere competența de a adopta o decizie prin care se constată că prelucrarea menționată încalcă normele prevăzute de acesta și, pe de altă parte, această competență trebuie exercitată cu respectarea procedurilor de cooperare și de asigurare a coerenței prevăzute de acest regulament[108].

Astfel, pentru prelucrările transfrontaliere, RGPD prevede mecanismul „ghișeului unic”[109], care se întemeiază pe o repartizare a competențelor între o „autoritate de supraveghere principală” și celelalte autorități naționale de supraveghere în cauză. Acest mecanism impune o cooperare strânsă, loială și eficientă între aceste autorități pentru a asigura o protecție coerentă și omogenă a normelor privind protecția datelor cu caracter personal și pentru a menține astfel efectul său util. RGPD consacră în această privință competența de principiu a autorității de supraveghere principale de a adopta o decizie prin care se constată că o prelucrare transfrontalieră încalcă normele prevăzute de acest regulament[110], în timp ce competența celorlalte autorități naționale de supraveghere de a adopta o asemenea decizie, fie și cu titlu provizoriu, constituie excepția[111]. Cu toate acestea, în exercitarea competențelor sale, autoritatea de supraveghere principală nu poate renunța la un dialog indispensabil, precum și la o cooperare loială și eficientă cu celelalte autorități de supraveghere vizate. Prin urmare, în cadrul acestei cooperări, 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.

[107] În sensul articolului 4 punctul 23 din RGPD.
[108] Prevăzute la articolul 56 și 60 din RGPD.
[109] Articolul 56 alineatul (1) din RGPD.
[110] Articolul 60 alineatul (7) din RGPD.
[111] Articolul 56 alineatul (2) și articolul 66 din RGPD consacră excepțiile de la principiul competenței decizionale a autorității de supraveghere principale.

Pe de altă parte, Curtea precizează că împrejurarea că o autoritate de supraveghere a unui stat membru care nu este autoritatea de supraveghere principală în ceea ce privește o prelucrare transfrontalieră de date nu își poate exercita competența de a aduce orice pretins caz de încălcare a RGPD în fața unei instanțe a acestui stat și de a iniția proceduri judiciare decât cu respectarea normelor de repartizare a competențelor decizionale între autoritatea de supraveghere principală și celelalte autorități de supraveghere[112] este conformă cu articolele 7, 8 și 47 din cartă, care garantează persoanei vizate dreptul la protecția datelor sale cu caracter personal și dreptul la o cale de atac efectivă.

În al doilea rând, Curtea statuează că, în cazul prelucrării transfrontaliere de date, exercitarea competenței de către o autoritate de supraveghere a unui stat membru, alta decât autoritatea de supraveghere principală, de a iniția o procedură judiciară[113] nu impune ca operatorul sau persoana împuternicită de operator în ceea ce privește prelucrarea transfrontalieră de date cu caracter personal vizată de această procedură să dispună de un sediu principal sau de un alt sediu pe teritoriul acestui stat membru. Cu toate acestea, exercitarea acestei competențe trebuie să intre în domeniul de aplicare teritorial al RGPD[114], ceea ce presupune că operatorul sau persoana împuternicită de operator pentru prelucrarea transfrontalieră dispune de un sediu pe teritoriul Uniunii.

În al treilea rând, Curtea declară că, în cazul prelucrării de date transfrontaliere, 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 RGPD și, după caz, de a iniția proceduri judiciare 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.

Curtea precizează însă că exercitarea acestei competențe presupune ca RGPD să fie aplicabil. În speță, întrucât activitățile sediului grupului Facebook situat în Belgia sunt indisociabil legate de prelucrarea datelor cu caracter personal în discuție în litigiul principal, iar Facebook Ireland este operatorul acestuia în ceea ce privește teritoriul Uniunii, această prelucrare este efectuată „în cadrul activităților unui sediu al operatorului” și, prin urmare, intră în domeniul de aplicare al RGPD.

În al patrulea rând, Curtea statuează că, atunci când o autoritate de supraveghere a unui stat membru care nu este „autoritatea de supraveghere principală” a introdus, înainte

[112] Prevăzute la articolele 55 și 56 coroborate cu articolul 60 din RGPD.
[113] Potrivit articolului 58 alineatul (5) din RGPD.
[114] Articolul 3 alineatul (1) din RGPD prevede că acest 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”.

de data intrării în vigoare a RGPD, o acțiune în justiție având ca obiect o prelucrare transfrontalieră de date cu caracter personal, această acțiune poate fi menținută, potrivit dreptului Uniunii, 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 data intrării în vigoare a RGPD, cu condiția ca aceasta să intre sub incidența uneia dintre situațiile în care, cu titlu de excepție, acest regulament conferă aceleiași autorități o competență de a adopta o decizie prin care să se constate că prelucrarea datelor în cauză încalcă normele prevăzute de acest regulament și cu respectarea procedurilor de cooperare și de asigurare a coerenței pe care acesta din urmă le prevede.

În al cincilea și ultimul rând, Curtea recunoaște efectul direct al dispoziției din RGPD în temeiul căreia fiecare stat membru prevede prin lege că autoritatea sa de supraveghere are competența de a aduce orice caz de încălcare a acestui regulament în fața autorităților judiciare și, după caz, să inițieze proceduri judiciare. În consecință, o astfel de autoritate poate invoca această dispoziție 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.

Hotărârea din 16 ianuarie 2024 (Marea Cameră), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

În această cauză (a se vedea și secțiunea II.1., intitulată „Domeniul de aplicare al reglementării generale”), Curtea arată că dispozițiile RGPD referitoare la competența autorităților naționale de supraveghere și la dreptul de plângere[115] nu necesită adoptarea unor măsuri naționale de aplicare și sunt suficient de clare, de precise și de necondiționate pentru a produce un efect direct. Rezultă că, deși RGPD lasă o marjă de apreciere statelor membre în ceea ce privește numărul de autorități de supraveghere care urmează să fie instituite[116], acesta stabilește în schimb întinderea competenței lor pentru a monitoriza aplicarea regulamentului menționat. Astfel, în cazul în care un stat membru decide să instituie o singură autoritate națională de supraveghere, aceasta este în mod necesar dotată cu totalitatea competențelor prevăzute de acest regulament. Orice altă interpretare ar repune în discuție efectul util al acestor dispoziții și ar risca să slăbească efectul util al tuturor celorlalte dispoziții din RGDP care pot fi vizate de o plângere.

În ceea ce privește împrejurarea că dispozițiile naționale de ordin constituțional exclud posibilitatea unei autorități de supraveghere care depinde de puterea executivă de a monitoriza aplicarea RGPD de către un organ care face parte din puterea legislativă,

[115] Articolul 55 alineatul (1) și, respectiv, articolul 77 alineatul (1) din RGDP.
[116] Potrivit articolului 51 alineatul (1) din RGPD.

Curtea subliniază că tocmai cu respectarea structurii constituționale a statelor membre RGPD se limitează să impună acestora din urmă să stabilească cel puțin o autoritate de supraveghere, oferindu-le în același timp posibilitatea de a institui mai multe autorități. Regulamentul menționat recunoaște astfel fiecărui stat membru o marjă de apreciere care să îi permită să instituie atâtea autorități de supraveghere câte impun, printre altele, cerințele legate de structura sa constituțională.

În plus, invocarea unor dispoziții de drept național de către un stat membru nu poate să aducă atingere unității și eficacității dreptului Uniunii. Astfel, efectele asociate principiului supremației dreptului Uniunii se impun tuturor organelor unui stat membru, fără, în special, ca dispozițiile interne, inclusiv de ordin constituțional, să poată împiedica acest lucru.

Prin urmare, din moment ce un stat membru a ales să instituie o singură autoritate de supraveghere, acesta nu poate invoca dispoziții de drept național, nici chiar de ordin constituțional, pentru a sustrage prelucrările de date cu caracter personal care intră în domeniul de aplicare al RGPD de la supravegherea din partea acestei autorități.

4. Condiții de impunere a unor amenzi administrative

Hotărârea din 5 decembrie 2023 (Marea Cameră), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

În această cauză (a se vedea și secțiunile II.3., II.5. și II.6., intitulate „Noțiunea de «prelucrare a datelor cu caracter personal»”, „Noțiunea de «operator de date cu caracter personal»” și „Noțiunea de «operator asociat»”), Curtea constată că, în temeiul articolului 83 din RGPD, o amendă administrativă poate fi impusă unui operator numai dacă se stabilește că acesta a săvârșit, intenționat sau din neglijență, o încălcare a normelor conținute în acest regulament[117].

În această privință, Curtea precizează că legiuitorul Uniunii nu a lăsat statelor membre o marjă de apreciere în ceea ce privește condițiile de fond care trebuie respectate de o autoritate de supraveghere atunci când aceasta decide să impună o amendă administrativă unui operator în temeiul acestei dispoziții. Faptul că RGPD oferă statelor membre posibilitatea de a prevedea excepții în raport cu autoritățile publice și cu organismele publice stabilite pe teritoriul lor[118], precum și cerințe privind procedura care trebuie urmată de autoritățile de supraveghere pentru impunerea unei amenzi

[117] Încălcare menționată la articolul 83 alineatele (4)-(6).

[118] În temeiul articolului 83 alineatul (7) din RGPD, conform căruia „[...] fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi impuse amenzi administrative autorităților publice și organismelor publice stabilite în statul membru respectiv”.

administrative[119] nu înseamnă nicidecum că acestea ar fi de asemenea abilitate să prevadă astfel de condiții de fond.

În ceea ce privește aceste condiții, Curtea observă că printre elementele enumerate în RGPD în temeiul cărora autoritatea de supraveghere impune operatorului o amendă administrativă figurează cel referitor la faptul „dacă încălcarea a fost comisă intenționat sau din neglijență”[120]. În schimb, niciunul dintre aceste elemente nu menționează vreo posibilitate de a trage la răspundere operatorul în lipsa unui comportament culpabil din partea sa. Așadar, numai încălcările dispozițiilor RGPD comise de operator în mod intenționat sau din neglijență pot conduce la impunerea unei amenzi administrative acestuia din urmă în temeiul articolului 83 din acest regulament.

Curtea adaugă că această interpretare este confirmată de economia generală și de scopul RGPD. În acest context, ea precizează că existența unui sistem de sancțiuni în temeiul RGPD care permite să se impună, atunci când împrejurările specifice fiecărei spețe justifică acest lucru, o amendă administrativă creează, pentru operatori și pentru persoanele împuternicite de operatori, un stimulent pentru a se conforma acestui regulament și că, prin efectul lor disuasiv, amenzile administrative contribuie la consolidarea protecției persoanelor vizate. Cu toate acestea, legiuitorul Uniunii nu a considerat necesar să prevadă impunerea unor amenzi administrative în lipsa vinovăției. Ținând seama de faptul că RGPD vizează un nivel de protecție în același timp echivalent și omogen și că trebuie, în acest scop, să fie aplicat în mod coerent în întreaga Uniune, ar fi contrar acestui scop să se permită statelor membre să prevadă un atare regim pentru impunerea unei amenzi.

În plus, Curtea concluzionează că o asemenea amendă poate fi impusă unui operator în ceea ce privește operațiunile de prelucrare a datelor cu caracter personal efectuate de o persoană împuternicită de operator în numele acesteia, cu excepția cazului în care, în cadrul acestor operațiuni, persoana împuternicită respectivă a efectuat prelucrări în scopuri proprii sau a prelucrat aceste date într-un fel incompatibil cu cadrul ori cu modalitățile de prelucrare așa cum au fost stabilite de operator sau într-un fel cu privire la care nu se poate considera în mod rezonabil că operatorul respectiv și-ar fi dat consimțământul. În această ipoteză, persoana împuternicită de operator trebuie să fie considerată operator al unei astfel de prelucrări.

Hotărârea din 5 decembrie 2023 (Marea Cameră), Deutsche Wohnen (C-807/21, EU:C:2023:950)

Deutsche Wohnen SE (denumită în continuare „DW”) este o societate imobiliară care deține indirect, prin intermediul unor participații la diferite societăți, numeroase unități

[119] În temeiul articolului 83 alineatul (8) din RGPD, interpretat în lumina considerentului (129) al acestuia.
[120] Articolul 83 alineatul (2) litera (b) din RGPD.

comerciale și rezidențiale. Ea prelucrează, în cadrul activităților sale comerciale, date cu caracter personal ale locatarilor acestor unități.

În urma a două controale efectuate în anii 2017 și 2019, Berliner Beauftragte für den Datenschutz (Autoritatea de supraveghere din Berlin, Germania) a constatat o serie de încălcări ale RGPD săvârșite de DW. Prin decizia din 30 octombrie 2019, această autoritate de supraveghere i-a aplicat, pentru acest motiv, amenzi administrative.

DW a formulat o acțiune împotriva acestei decizii la Landgericht Berlin (Tribunalul Regional din Berlin, Germania), care a clasat procedura. Această instanță a arătat că, în temeiul legii germane[121], o încălcare administrativă nu ar putea fi constatată decât împotriva unei persoane fizice, iar nu împotriva unei persoane juridice. În plus, în cazul angajării răspunderii unei persoane juridice, ar putea să îi fie imputate numai actele membrilor organelor sale sau ale reprezentanților săi. Staatsanwaltschaft Berlin (Parchetul din Berlin, Germania) a introdus o cale de atac împotriva acestei decizii la Kammergericht Berlin (Tribunalul Regional Superior din Berlin, Germania). În acest context, instanța menționată a sesizat Curtea cu titlu preliminar cu privire la interpretarea RGPD.

În hotărârea sa, Curtea, reunită în Marea Cameră, se pronunță cu privire la condițiile referitoare la impunerea unor amenzi administrative în temeiul RGPD. În primul rând, aceasta examinează aspectul dacă statele membre pot supune impunerea unei amenzi administrative unei persoane juridice condiției ca încălcarea acestui regulament să fie imputată în prealabil unei persoane fizice identificate. În al doilea rând, ea analizează de asemenea, la fel ca în Hotărârea Nacionalinis visuomenės sveikatos centras (a se vedea mai sus) aspectul dacă încălcarea sancționată a dispozițiilor RGPD trebuie să fie comisă cu intenție sau din neglijență.

În ceea ce privește impunerea unei amenzi administrative în temeiul RGPD unei persoane juridice, Curtea arată mai întâi că principiile, interdicțiile și obligațiile prevăzute de RGPD se adresează în special „operatorilor”, a căror responsabilitate se extinde la orice prelucrare a datelor cu caracter personal efectuată de aceștia sau în numele lor. Această responsabilitate este cea care constituie, în cazul încălcării dispozițiilor RGPD, temeiul pentru impunerea unei amenzi administrative operatorului conform articolului 83 din respectivul regulament. Cu toate acestea, legiuitorul Uniunii nu a efectuat, în vederea stabilirii unei asemenea responsabilități, o distincție între persoanele fizice și persoanele juridice, respectiva responsabilitate fiind supusă numai condiției ca acestea, singure sau împreună cu altele, să stabilească scopurile și mijloacele prelucrării datelor cu caracter personal[122]. Prin urmare, în principiu, orice persoană care îndeplinește această condiție răspunde printre altele pentru orice încălcare a RGPD săvârșită de ea

[121] Gesetz über Ordnungswidrigkeiten (Legea privind încălcările administrative) din 24 mai 1968 (BGBl. 1968 I, p. 481), în versiunea comunicată la 19 februarie 1987 (BGBl. 1987 I, p. 602), astfel cum a fost adaptată prin Legea din 19 iunie 2020 (BGBl. 2020 I, p. 1350).

[122] Potrivit articolului 4 punctul 7 din RGPD.

însăși sau în numele său. Aceasta implică, pe de o parte, că persoanele juridice răspund nu numai pentru încălcările săvârșite de reprezentanții, directorii sau administratorii lor, ci și de orice altă persoană care acționează în cadrul activității comerciale a acestor persoane juridice și în numele lor. Pe de altă parte, amenzile administrative prevăzute de RGPD în cazul unor asemenea încălcări trebuie să poată fi aplicate direct unor persoane juridice atunci când acestea pot fi calificate drept operatori.

În continuare, Curtea observă că nicio dispoziție din RGPD nu permite să se considere că aplicarea unei amenzi administrative unei persoane juridice în calitate de operator ar fi supusă constatării prealabile că această încălcare a fost comisă de o persoană fizică identificată. În plus, legiuitorul Uniunii nu a lăsat statelor membre o marjă de apreciere în această privință. Faptul că RGPD le oferă acestora posibilitatea de a prevedea cerințe privind procedura care trebuie urmată de autoritățile de supraveghere pentru a impune o amendă administrativă[123] nu înseamnă nicidecum că acestea ar fi de asemenea abilitate să prevadă condiții de fond suplimentare față de cele stabilite de RGPD.

În acest context, Curtea precizează că a permite statelor membre să impună în mod unilateral și ca o condiție necesară pentru aplicarea unei amenzi administrative în temeiul articolului 83 din RGPD unui operator care este o persoană juridică ca încălcarea în cauză să fie imputată sau imputabilă în prealabil unei persoane fizice identificate ar fi contrar scopului RGPD. În plus, o asemenea cerință suplimentară ar risca, în definitiv, să diminueze efectivitatea și efectul disuasiv al amenzilor administrative impuse unor persoane juridice în calitate de operatori.

În sfârșit, Curtea subliniază că noțiunea de „întreprindere”, în sensul articolelor 101 și 102 TFUE[124], nu are incidență asupra aspectului dacă și în ce condiții o amendă administrativă poate fi impusă în temeiul RGPD unui operator care este o persoană juridică și este relevantă numai pentru stabilirea cuantumului unei asemenea amenzi.

Prin urmare, Curtea concluzionează că RGPD[125] se opune unei reglementări naționale în temeiul căreia o amendă administrativă poate fi aplicată unei persoane juridice în calitatea sa de operator pentru o încălcare a acestui regulament[126] numai în măsura în care această încălcare a fost imputată în prealabil unei persoane fizice identificate.

În ceea ce privește aspectul dacă statele membre pot prevedea impunerea unei amenzi administrative chiar și atunci când încălcarea sancționată nu a fost comisă în mod intenționat sau din neglijență, Curtea amintește mai întâi că condițiile de fond care trebuie respectate de o autoritate de supraveghere atunci când aplică o astfel de amendă unui operator intră exclusiv sub incidența dreptului Uniunii, iar statele membre nu dispun de nicio marjă de manevră în această privință. Urmând un raționament

[123] Astfel cum reiese din articolul 58 alineatul (4) și din articolul 83 alineatul (8) din RGPD, interpretate în lumina considerentului (129) al acestuia.
[124] La care se face trimitere în considerentul (150) al RGPD.
[125] Articolul 58 alineatul (2) litera (i) și articolul 83 alineatele (1)-(6) din RGPD.
[126] Menționată la articolul 83 alineatele (4)-(6) din RGPD.

identic cu cel adoptat în Hotărârea Nacionalinis visuomenės sveikatos centras citată anterior, Curtea constată că, în temeiul articolului 83 din RGPD, o amendă administrativă poate fi impusă numai dacă se stabilește că operatorul, care este în același timp o persoană juridică și o întreprindere, a comis în mod intenționat sau din neglijență o încălcare a normelor cuprinse în acest regulament.

5. Corelarea competențelor autorităților naționale de supraveghere cu competențele celorlalte autorități naționale

Hotărârea din 4 iulie 2023 (Marea Cameră), Meta Platforms ș.a. (Condiții generale de utilizare a unei rețele sociale) (C-252/21, EU:C:2023:537)

În această cauză (a se vedea și secțiunea V.5., intitulată „Prelucrarea datelor cu caracter personal pe rețelele sociale online”), pronunțându-se cu privire la competența unei autorități de concurență de a constata neconformitatea cu RGPD a unei prelucrări de date cu caracter personal, Curtea arată că, sub rezerva respectării obligației sale de cooperare loială[127] cu autoritățile de supraveghere a protecției datelor cu caracter personal, o astfel de autoritate poate constata, în cadrul examinării unui abuz de poziție dominantă al unei întreprinderi[128], că nu sunt conforme cu acest regulament condițiile generale de utilizare stabilite de această întreprindere referitoare la prelucrarea datelor cu caracter personal și punerea lor în aplicare, atunci când constatarea respectivă este necesară pentru a stabili existența unui asemenea abuz. Cu toate acestea, atunci când o autoritate de concurență constată o încălcare a RGPD în cadrul constatării unui abuz de poziție dominantă, aceasta nu se substituie autorităților de supraveghere.

Astfel, ținând seama de acest principiu, atunci când autoritățile naționale de concurență sunt chemate, în exercitarea competențelor lor, să examineze conformitatea unui comportament al unei întreprinderi cu dispozițiile RGPD, ele trebuie să se pună de acord și să coopereze în mod loial cu autoritățile de supraveghere naționale vizate sau cu autoritatea de supraveghere principală. Toate aceste autorități sunt, așadar, obligate să respecte atribuțiile și competențele lor, așa încât obligațiile care decurg din RGPD, precum și obiectivele acestui regulament să fie respectate, iar efectul lor util să fie menținut. Rezultă că, atunci când, în cadrul examinării prin care se urmărește constatarea unui abuz de poziție dominantă săvârșit de o întreprindere, o autoritate de concurență consideră că este necesar să examineze conformitatea unui comportament al acestei întreprinderi în lumina dispozițiilor RGPD, autoritatea menționată trebuie să verifice dacă acest comportament sau un comportament similar a făcut deja obiectul

[127] Consacrată la articolul 4 alineatul (3) TUE.
[128] În sensul articolului 102 TFUE.

unei decizii din partea autorității de supraveghere naționale competente sau a autorității de supraveghere principale sau chiar a Curții. Dacă aceasta este situația, autoritatea de concurență nu se poate abate de la aceasta, rămânând totodată liberă să rețină propriile concluzii din perspectiva aplicării dreptului concurenței.

Atunci când are îndoieli cu privire la întinderea aprecierii efectuate de autoritatea națională de supraveghere competentă sau de autoritatea de supraveghere principală, atunci când comportamentul în cauză sau un comportament similar face în același timp obiectul unei examinări din partea acestor autorități sau atunci când, în lipsa unei investigații a autorităților menționate, consideră că un comportament al unei întreprinderi nu este conform cu dispozițiile RGPD, autoritatea de concurență trebuie să consulte aceste autorități și să le solicite cooperarea pentru a-și înlătura îndoielile sau pentru a stabili dacă este necesar să aștepte adoptarea unei decizii de către autoritatea de supraveghere în cauză înainte de a începe propria apreciere. În absența unei obiecții din partea acestora sau a unui răspuns într-un termen rezonabil, autoritatea de concurență își poate continua propria investigație.

CURTEA DE JUSTIȚIE
A UNIUNII EUROPENE

Direcția cercetare și documentare

Iulie 2024