CURTEA DE JUSTIȚIE
A UNIUNII EUROPENE

DIRECȚIA CERCETARE
ȘI DOCUMENTARE

Fișă tematică

PROTECȚIA DATELOR CU CARACTER PERSONAL

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

Acest principiu este consacrat în Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta"), care prevede la articolul 8 că:

„(1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.

(2) Asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora.

(3) Respectarea acestor norme se supune controlului unei autorități independente."

În plus, acest drept fundamental este strâns legat de dreptul la respectarea vieții private și de familie, consacrat la articolul 7 din cartă.

Dreptul la protecția datelor cu caracter personal este de asemenea prevăzut la articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE), care este succesorul, în această privință, al articolului 286 CE.

Referitor la 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], adoptată pe baza articolului 100 A CE, constituia în

[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 5).

această privință principalul act juridic al Uniunii în domeniu. Aceasta stabilea condiții generale privind legalitatea prelucrării acestor date și drepturile persoanelor vizate și prevedea în special înființarea de autorități independente de supraveghere în statele membre.

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 legiuitorul Uniunii are în vedere revizuirea acestei directive. În această privință, Comisia a introdus, la 10 ianuarie 2017, o propunere de înlocuire a acestei directive printr-un regulament referitor la viața privată și la comunicațiile electronice[4].

De asemenea, în cadrul spațiului de libertate, securitate și justiție (ex-articolele 30 și 31 TUE), Decizia-cadru 2008/977/JAI[5] a reglementat, până în luna mai a anului 2018, protecția datelor cu caracter personal în domeniul cooperării judiciare în materie penală și polițienească.

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 (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, care abrogă Decizia-cadru 2008/977/JAI și a cărei dată de transpunere de către statele membre a fost stabilită pentru 6 mai 2018.

În sfârșit, în cadrul prelucrării lor de către instituțiile și organele Uniunii Europene, protecția datelor cu caracter personal era asigurată inițial de Regulamentul (CE) nr. 45/2001[8]. Acest regulament a permis în special crearea, în anul 2004, a Autorității Europene pentru Protecția Datelor. În anul 2018, Uniunea Europeană a instituit un nou cadru juridic în această materie, în special prin adoptarea Regulamentului (UE) 2018/1725[9], care abrogă Regulamentul nr. 45/2001

---

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 Propunere de Regulament al Parlamentului European și al Consiliului 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), COM/2017/010 final– 2017/03 (COD).

5 Decizia-cadru 2008/777/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (JO 2008, L 350, p. 60), abrogată începând de la 6 mai 2018 (a se vedea nota de subsol 6).

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).

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 (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO 2001, L 8, p. 1, Ediție specială, 13/vol. 30, p. 142).

9 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).

și Decizia nr. 1247/2002/CE[10] și care este aplicabil începând de la 11 decembrie 2018. În interesul unei abordări coerente a protecției datelor cu caracter personal în întreaga Uniune, acest nou regulament vizează alinierea cât mai mult posibil a normelor din domeniu cu regimul instituit prin RGPD.

[10] Decizia nr. 1247/2002/CE a Parlamentului European, a Consiliului și a Comisiei din 1 iulie 2002 privind statutul și condițiile generale de exercitare a atribuțiilor Autorității Europene pentru Protecția Datelor (JO 2002, L 183, p. 1, Ediție specială, 01/vol. 3, p. 194).

CUPRINS

I. DREPTUL LA PROTECȚIA DATELOR CU CARACTER PERSONAL RECUNOSCUT DE CARTA DREPTURILOR FUNDAMENTALE A UNIUNII EUROPENE 5

1. Conformitatea dreptului derivat al Uniunii cu dreptul la protecția datelor cu caracter personal **5**

2. Respectarea dreptului la protecția datelor cu caracter personal în cadrul punerii în aplicare a dreptului Uniunii .. **9**

II. PRELUCRAREA DATELOR CU CARACTER PERSONAL ÎN SENSUL REGLEMENTĂRII GENERALE ÎN MATERIE 10

1. Prelucrări ale datelor cu caracter personal excluse din domeniul de aplicare al Directivei 95/46 ..... **10**

2. Noțiunea de „date cu caracter personal” **12**

3. Noțiunea de „prelucrare a datelor cu caracter personal” **15**

4. Noțiunea de „sistem de evidență a datelor cu caracter personal” **20**

5. Noțiunea de „operator de date cu caracter personal” **20**

6. Condiții de legalitate a unei prelucrări de date cu caracter personal **23**

III. PRELUCRAREA DATELOR CU CARACTER PERSONAL ÎN SENSUL DIRECTIVEI 2002/58 ... 33

IV. TRANSFER DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE 39

V. PROTECȚIA DATELOR CU CARACTER PERSONAL PE INTERNET 46

1. Dreptul de opoziție la prelucrarea datelor cu caracter personal („dreptul la uitare”) **46**

2. Prelucrarea datelor cu caracter personal și drepturile de proprietate intelectuală **47**

3. Dezindexarea unor date cu caracter personal **52**

4. Consimțământul utilizatorului unui site internet privind stocarea informațiilor **56**

VI. AUTORITĂȚI NAȚIONALE DE SUPRAVEGHERE 57

1. Sfera de aplicare a cerinței privind independența **57**

2. Stabilirea dreptului aplicabil și a autorității de supraveghere competente **60**

3. Competențele autorităților naționale de supraveghere **61**

VII. APLICAREA TERITORIALĂ A LEGISLAȚIEI EUROPENE 65

VIII. DREPTUL DE ACCES PUBLIC LA DOCUMENTELE INSTITUȚIILOR UNIUNII EUROPENE ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL 66

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[11]

În această cauză, litigiile principale aveau ca părți producători agricoli și Land Hessen, în legătură cu publicarea pe site-ul internet a 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[12] și 259/2008[13], 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 (punctele 56-64).

---

11 Această hotărâre a fost prezentată în Raportul anual 2010, p. 11.

12 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).

13 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).

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 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 (punctul 65). 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 (punctele 77, 79, 85 și 86).

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 (punctul 92 și dispozitiv 1). 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 (punctul 94 și dispozitiv 2).

Hotărârea din 17 octombrie 2013, Schwarz (C-291/12, EU:C:2013:670)

Domnul Schwarz a solicitat autorităților orașului Bochum (Germania) eliberarea unui pașaport, refuzând totodată prelevarea cu această ocazie a amprentelor sale digitale. Întrucât cererea sa a fost respinsă, domnul Schwarz a introdus o acțiune la Verwaltungsgericht Gelsenkirchen (Tribunalul Administrativ din Gelsenkirchen, Germania) pentru obligarea municipalității să îi elibereze un pașaport fără prelevarea amprentelor sale digitale. În fața acestei instanțe, domnul Schwarz a contestat validitatea Regulamentului (CE) nr. 2252/2004[14] care a introdus obligația de prelevare a amprentelor digitale solicitanților de pașapoarte, susținând printre altele că regulamentul încălca dreptul la protecția datelor cu caracter personal și dreptul la respectarea vieții private.

În acest context, Verwaltungsgericht Gelsenkirchen a sesizat Curtea cu titlu preliminar cu privire la întrebarea dacă regulamentul menționat, în măsura în care obligă solicitantul unui pașaport să accepte prelevarea amprentelor sale digitale și stocarea lor în pașaport, este valid, în special având în vedere carta.

Curtea a răspuns afirmativ, hotărând că, deși prelevarea și stocarea unor amprente digitale de către autoritățile naționale, reglementate de articolul 1 alineatul (2) din Regulamentul nr. 2252/2004, constituie o atingere adusă drepturilor la respectarea vieții private și la protecția datelor cu caracter personal, această atingere este justificată de obiectivul de protecție a pașapoartelor împotriva oricărei utilizări frauduloase.

[14] Regulamentul (CE) nr. 2252/2004 al Consiliului din 13 decembrie 2004 privind standardele pentru elementele de securitate și elementele biometrice integrate în pașapoarte și în documente de călătorie emise de statele membre (JO 2004, L 385, p. 1, Ediție specială, 01/vol. 5, p. 155), astfel cum a fost modificat prin Regulamentul (CE) nr. 444/2009 al Parlamentului European și al Consiliului din 6 mai 2009 (JO 2009, L 142, p. 1)

Mai întâi, o astfel de limitare, prevăzută de lege, urmărește un obiectiv de interes general recunoscut de Uniune, în măsura în care vizează să împiedice în special intrarea ilegală a persoanelor pe teritoriul Uniunii (punctele 35-38). În continuare, prelevarea și stocarea amprentelor digitale sunt adecvate pentru atingerea acestui obiectiv. Astfel, pe de o parte, chiar dacă metoda de verificare a identității prin intermediul amprentelor digitale nu este pe deplin fiabilă, aceasta reduce în mod considerabil riscul de acceptare de persoane neautorizate. Pe de altă parte, neconcordanța amprentelor digitale ale deținătorului pașaportului cu datele integrate în acest document nu înseamnă că persoanei în cauză i se refuză în mod automat intrarea pe teritoriul Uniunii, având ca singură consecință demararea unui control aprofundat menit să îi stabilească în mod definitiv identitatea (punctele 42-45).

În sfârșit, în ceea ce privește caracterul necesar al unei astfel de prelucrări, nu s-a adus la cunoștința Curții existența unor măsuri suficient de eficiente, dar care să aducă mai puțin atingere drepturilor recunoscute la articolele 7 și 8 din cartă decât cele determinate de metoda întemeiată pe amprentele digitale (punctul 53). Articolul 1 alineatul (2) din Regulamentul nr. 2252/2004 nu implică prelucrări ale amprentelor digitale prelevate care depășesc ceea ce este necesar pentru realizarea obiectivului menționat. Astfel, acest regulament precizează în mod expres că amprentele digitale pot fi utilizate pentru unicul scop de a verifica autenticitatea pașaportului și identitatea titularului său. În plus, articolul 1 alineatul (2) din regulament oferă protecție împotriva riscului de citire a datelor care conțin amprente digitale de către persoane neautorizate și prevede stocarea amprentelor digitale numai în pașaport, care rămâne în posesia exclusivă a titularului său (punctele 54-57, 60 și 63).

Hotărârea din 8 aprilie 2014 (Marea Cameră), Digital Rights Ireland și Seitlinger și alții (cauzele conexate C-293/12 și C-594/12, EU:C:2014:238)[15]

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

[15] Această hotărâre a fost prezentată în Raportul anual 2014, p. 60.

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, desigur, că 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 (punctele 38-44).

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 (punctul 65). 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 (punctele 57-59). 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 (punctele 60-62). 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 (punctele 63 și 64).

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 (punctele 66-68).

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)[16]

Ca urmare a Hotărârii Digital Rights Ireland și Seitlinger și alții, 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 și alții, 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 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)], 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

[16] Această hotărâre a fost prezentată în Raportul anual 2016, p. 62.

alineatul (1) interpretat în lumina articolelor citate anterior din cartă (punctele 99-105, 107 și 112 și dispozitiv 1).

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 (punctele 118-122 și 125 și dispozitiv 2).

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 (punctele 108-111).

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

1. Prelucrări ale datelor cu caracter personal excluse din domeniul de aplicare al Directivei 95/46

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[17] 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[18] 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.

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 (punctele 56 și 57).

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 (punctele 58 și 59).

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

[17] Decizia 2004/355/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).

[18] 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).

directivei. În consecință, Curtea a anulat decizia Consiliului de aprobare a încheierii acordului (punctele 67-69).

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 hotărât 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 (punctul 35 și dispozitivul).

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 (punctele 27-29). 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 (punctele 30, 31 și 33).

2. Noțiunea de „date cu caracter personal”

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

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 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 (punctele 43 și 44).

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 acestei persoane (punctul 49 și dispozitiv 1).

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

Domnul Nowak, în calitate de expert contabil stagiar, nu a promovat examenul organizat de ordinul irlandez al experților contabili autorizați. Acesta a formulat, în temeiul articolului 4 din Legea privind protecția datelor, o cerere de acces care viza ansamblul datelor cu caracter

[19] Această hotărâre a fost prezentată în Raportul anual 2016, p. 61.

personal care îl privesc, deținute de ordinul experților contabili. Aceasta 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 răspuns la cererea sa 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 întrebării 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 un 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 (punctele 31 și 36-40).

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 acestea 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 tocmai ca finalitate să documenteze evaluarea de către examinator a performanțelor candidatului și sunt susceptibile să aibă efecte asupra acestuia din urmă (punctele 42 și 43).

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 această directivă, servește la realizarea obiectivului acesteia din urmă care constă în asigurarea protecției dreptului la viață privată al acestui candidat 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 (punctele 56 și 58).

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 (punctul 62 și dispozitivul).

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 comunicat, fără autorizație, către terțe țări 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 a datelor cu caracter personal, automată integral sau parțial”, 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 a datelor cu caracter personal, automată integral sau parțial”, în sensul acestei directive (punctul 27 și dispozitiv 1). 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 (punctele 38 și 43-48 și dispozitiv 2).

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 Spania 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.

Astfel, 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 (dispozitiv 1). 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 (punctele 29 și 30).

Hotărârea din 10 iulie 2018 (Marea Cameră), Jehovan todistajat (C-25/17, ECLI:EU:C:2018:551)[20]

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

[20] Această hotărâre a fost prezentată în Raportul anual 2018, p. 87 și 88.

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 (punctul 51 și dispozitiv 1).

Hotărârea din 14 februarie 2019, Buivids (C-345/17, EU:C:2019:122)

În această cauză, Curtea a analizat interpretarea, pe de o parte, a domeniului de aplicare al Directivei 95/46 și, pe de altă parte, a noțiunii de „prelucrare a datelor cu caracter personal efectuată numai în scopuri jurnalistice”, prevăzută la articolul 9 din această directivă.

Această hotărâre se înscrie în cadrul unei cereri de decizie preliminară formulate de Curtea Supremă din Letonia, sesizată cu un litigiu între domnul Buivids (denumit în continuare „reclamantul”) și Autoritatea națională pentru protecția datelor, în legătură cu o acțiune privind declararea nelegalității unei decizii a acestei autorități potrivit căreia domnul Buivids ar fi încălcat legislația națională în materie de protecție a datelor cu caracter personal întrucât a publicat pe un site internet o înregistrare video, efectuată chiar de acesta, a audierii sale de către agenți de poliție în incinta unei secții a poliției naționale în cadrul unei proceduri contravenționale. Astfel, în urma respingerii acțiunii sale de către două instanțe inferioare, reclamantul a declarat recurs la Curtea Supremă. El a invocat în fața acestei instanțe dreptul său la libertatea de exprimare, arătând că înregistrarea video în cauză ar privi funcționari ai poliției naționale, care au calitatea de persoane publice, într-un loc accesibil publicului, și că, pentru acest motiv, aceste persoane nu ar beneficia de aplicarea dispozițiilor Legii privind protecția datelor.

În ceea ce privește, în primul rând, domeniul de aplicare al Directivei 95/46, Curtea a reținut că, pe de o parte, imaginile cu agenții de poliție din înregistrarea video în cauză constituie date cu caracter personal și că, pe de altă parte, înregistrarea video a acestor persoane, stocată în memoria camerei utilizate de reclamant, constituie o prelucrare de date cu caracter personal. Astfel, Curtea a adăugat că faptul de a publica o înregistrare video în care figurează date cu caracter personal pe un site internet de materiale video pe care utilizatorii le pot viziona și distribui constituie o prelucrare automată, în totalitate sau parțial, a acestor date. De altfel, Curtea subliniază că înregistrarea menționată și publicarea sa nu intră sub incidența excepțiilor

de la domeniul de aplicare al Directivei 95/46, care privesc printre altele prelucrările de date cu caracter personal realizate în cadrul unor activități din afara domeniului de aplicare al acestei directive și prelucrările care se înscriu în cadrul exercitării unor activități exclusiv personale sau domestice. Prin urmare, Curtea a concluzionat că intră în domeniul de aplicare al acestei directive înregistrarea video a unor agenți de poliție în incinta unei secții de poliție, în timpul unei audieri, și publicarea materialului video astfel înregistrat pe un site internet de materiale video pe care utilizatorii le pot trimite, viziona și distribui (punctele 31, 32, 35, 39, 42 și 43 și dispozitiv 1).

În ceea ce privește, în al doilea rând, conținutul noțiunii de „prelucrare a datelor cu caracter personal efectuată numai în scopuri jurnalistice", Curtea a amintit mai întâi că, în temeiul unei interpretări largi a noțiunii de „jurnalism", excepțiile și derogările prevăzute la articolul 9 din Directiva 95/46 se aplică oricărei persoane care exercită activități jurnalistice. Astfel, Curtea a reținut că faptul că reclamantul nu este un jurnalist profesionist nu exclude ca efectuarea înregistrării video în cauză și transmiterea acesteia să poată fi calificată drept o „prelucrare a datelor cu caracter personal efectuată numai în scopuri jurnalistice". În plus, Curtea a subliniat că excepțiile și derogările prevăzute la articolul 9 din Directiva 95/46 trebuie aplicate numai în măsura în care se dovedesc necesare pentru a pune în acord două drepturi fundamentale, și anume dreptul la viață privată și cel la libertatea de exprimare. În această privință, Curtea a precizat că nu se poate exclude ca înregistrarea și publicarea materialului video în cauză, care au avut loc fără ca agenții de poliție care figurează în acest material video să fie informați cu privire la această înregistrare și la scopurile ei, să constituie o ingerință în dreptul fundamental la respectarea vieții private a acestor persoane. Prin urmare, ea a concluzionat că înregistrarea și publicarea materialului video în cauză pe un site internet de materiale video pot constitui o prelucrare de date cu caracter personal numai în scopuri jurnalistice atât timp cât reiese din acest material video că înregistrarea și publicarea menționate au ca unic scop aducerea la cunoștința publicului a unor informații, opinii sau idei, aspect a cărui verificare este de competența instanței de trimitere (punctele 51, 52, 55, 63 și 67 și dispozitiv 2).

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[21], 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

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

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”[22], pentru care RGPD prevede o protecție sporită din cauza caracterului deosebit de sensibil al datelor în cauză (punctele 10, 46, 74 și 94 și dispozitiv 1).

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 (punctele 60, 61 și 72).

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[23]. 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 (punctele 62 și 66-68).

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[24]. Curtea constată astfel că CSDD nu poate fi considerată, atunci când efectuează comunicarea menționată, o astfel de „autoritate competentă”[25] (punctele 69-71).

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”[26], care beneficiază de o protecție sporită, Curtea constată,

---

22 Articolul 10 din RGPD.

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

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

25 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).

26 Articolul 10 din RGPD.

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 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 (punctele 77, 80, 85, 87-90 și 93).

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

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

În această hotărâre (a se vedea de asemenea 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 (punctul 62 și dispozitiv 2).

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

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

În această cauză (a se vedea de asemenea 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 (punctele 74 și 75 și dispozitiv 3).

Hotărârea din 5 iunie 2018 (Marea Cameră), Wirtschaftsakademie Schleswig Holstein (C-210/16, ECLI:EU:C:2018:388)[27]

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 (punctul 39).

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.

[27] Această hotărâre a fost prezentată în Raportul anual 2018, p. 86 și 87.

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) (punctele 76 și 85 și dispozitiv 2).

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 (punctul 97 și dispozitiv 3).

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 (punctul 106 și dispozitiv 4).

Hotărârea din 9 iulie 2020, Land Hessen, C-272/19, EU:C:2020:535

Un cetățean care a adresat o petiție Comisiei pentru petiții din cadrul Parlamentului landului Hessen (Germania) i-a solicitat accesul la datele cu caracter personal care îl privesc, stocate de aceasta în cadrul prelucrării petiției sale. El își întemeiază respectiva cerere pe RGPD, care

prevede dreptul unei persoane vizate de a obține din partea operatorului accesul la datele cu caracter personal care o privesc.

Președintele Parlamentului landului Hessen a respins această cerere pentru motivul că procedura de petiționare constituie o misiune parlamentară și că parlamentul nu este supus RGPD.

Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden, Germania), sesizat de cetățean, consideră că legislația germană nu acordă niciun drept de acces la datele cu caracter personal în cadrul unei petiții precum cea în discuție. Apreciind totuși că un astfel de drept de acces ar putea rezulta din RGPD, Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden) a solicitat Curții de Justiție să se pronunțe cu privire la acest aspect. În plus, având îndoieli cu privire la propria independență și, prin urmare, la calitatea sa de instanță, autorizată să adreseze Curții întrebări preliminare, Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden) a solicitat Curții să se pronunțe și cu privire la acest aspect.

Prin hotărârea sa, Curtea răspunde că, în măsura în care o comisie pentru petiții a parlamentului unui stat federat al unui stat membru determină, singură sau împreună cu altele, scopurile și mijloacele de prelucrare a datelor cu caracter personal, această comisie trebuie calificată drept „operator" în sensul RGPD[28]. Prin urmare, prelucrarea datelor cu caracter personal efectuată de o asemenea comisie intră sub incidența acestui regulament, în special a dispoziției care conferă persoanelor vizate un drept de acces la datele cu caracter personal care le privesc[29].

Curtea constată printre altele că activitățile Comisiei pentru petiții din cadrul Parlamentului landului Hessen nu intră sub incidența unei excepții prevăzute de RGPD. Ea admite că astfel de activități sunt de natură publică și proprii acestui land, această comisie contribuind indirect la activitatea parlamentară, însă arată că respectivele activități sunt de asemenea atât de natură politică, cât și administrativă. În plus, nu reiese nicidecum din elementele de care dispune Curtea că aceste activități corespund, în speță, uneia dintre excepțiile prevăzute de RGPD (punctele 71-74 și dispozitivul).

6. 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)[30]

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.

[28] Articolul 4 punctul 7 din RGPD.
[29] Articolul 15 din RGPD.
[30] Această hotărâre a fost prezentată în Raportul anual 2008, p. 45.

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 Renania de Nord-Westfalia, 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). Însă, un astfel de registru nu poate conține alte informații decât cele care sunt necesare în acest scop în sensul Directivei privind protecția datelor cu caracter personal (punctele 54, 58 și 59).

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 (punctele 52, 66 și 68).

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 (punctele 78-80).

Hotărârea din 24 noiembrie 2011, ASNEF și FECEMD (C-468/10 și C-469/10, EU:C:2011:777)

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), pe de o parte, și Federación de Comercio Electrónico y Marketing Directo (FECEMD), pe de altă parte, au introdus la Tribunal Supremo (Spania) o acțiune în contencios administrativ împotriva mai multor articole din Decretul regal 1720/2007, care a pus în aplicare Legea organică 15/1999 de transpunere a Directivei 95/46.

ASNEF și FECEMD considerau în special că, pentru a permite prelucrarea datelor cu caracter personal în lipsa consimțământului persoanei în cauză, dreptul spaniol adaugă o condiție care nu este inclusă în Directiva 95/46 și care impune ca respectivele date să figureze în „surse accesibile publicului", astfel cum sunt enumerate la articolul 3 litera j) din Legea organică 15/1999. În acest sens, ele au susținut că legea menționată și Decretul regal 1720/2007 limitează domeniul de aplicare al articolului 7 litera (f) din Directiva 95/46, care supune prelucrarea datelor cu caracter personal în lipsa consimțământului persoanei vizate numai condiției referitoare la interesul legitim urmărit de operatorul prelucrării sau de terțul ori de terții cărora le sunt comunicate aceste date.

În această privință, Curtea a arătat mai întâi că articolul 7 din Directiva 95/46 prevede o listă exhaustivă și limitativă de cazuri în care o prelucrare de date cu caracter personal poate fi considerată ca fiind legală în lipsa consimțământului persoanei în cauză. Prin urmare, statele membre nu pot să introducă, în temeiul articolului 5 din directiva menționată, alte principii referitoare la legitimitatea prelucrărilor de date cu caracter personal decât cele prevăzute la articolul 7 și nici să modifice, prin cerințe suplimentare, domeniul de aplicare al principiilor prevăzute la articolul 7 menționat. Astfel, articolul 5 nu permite statelor membre decât să precizeze, în limitele capitolului II din directiva menționată și, prin urmare, ale articolului 7 din aceasta, condițiile în care prelucrările de date cu caracter personal sunt legale (punctele 30, 32 și 33).

În special, pentru a efectua ponderarea necesară a drepturilor și a intereselor opuse în cauză, prevăzută la articolul 7 litera (f) din directiva menționată, statele membre pot stabili principii directoare. Ele pot de asemenea să ia în considerare faptul că gravitatea atingerii aduse drepturilor fundamentale ale persoanei vizate de prelucrarea în cauză poate varia în funcție de împrejurarea dacă datele în cauză sunt sau nu sunt deja conținute în surse aflate la dispoziția publicului (punctele 44 și 46).

Cu toate acestea, Curtea a considerat că nu mai este vorba despre o precizare în sensul articolului 5 din Directiva 95/46 în cazul în care o reglementare națională exclude pentru anumite categorii de date cu caracter personal posibilitatea de a fi prelucrate, prin stabilirea pentru aceste categorii, în mod definitiv, a rezultatului ponderării drepturilor și intereselor opuse, fără a permite un rezultat diferit în funcție de împrejurările speciale ale unui caz concret. Prin urmare, Curtea a hotărât că articolul 7 litera (f) din Directiva 95/46 se opune ca un stat membru să excludă 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 (punctele 47 și 48).

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 întrebarea 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 (punctele 62-64 și dispozitiv 2).

Hotărârea din 4 mai 2017, Rīgas satiksme (C-13/16, EU:C:2017:336)

Această cauză se înscrie în contextul unui litigiu între poliția națională letonă și Rīgas satiksme, societate de troleibuze a orașului Riga, referitor la o cerere de comunicare a datelor de identificare a autorului unui accident. În speță, într-un accident rutier, un șofer de taxi a oprit vehiculul pe marginea carosabilului. La momentul la care un troleibuz al Rīgas satiksme trecea prin dreptul acestui taxi, pasagerul care se afla pe scaunul din spate al taxiului menționat a deschis portiera, care a lovit și a deteriorat troleibuzul. Pentru formularea unei acțiuni de drept civil, Rīgas satiksme a solicitat printre altele poliției naționale comunicarea datelor de identificare a autorului accidentului. Poliția a refuzat să comunice numărul actului de identitate și domiciliul pasagerului, precum și documentele referitoare la explicațiile persoanelor implicate în accident, pe motiv că documentele întocmite în cadrul unei proceduri administrative care a condus la aplicarea de sancțiuni pot fi transmise doar părților din procedura respectivă și, în ceea ce privește numărul actului de identitate și domiciliul, Legea privind protecția datelor persoanelor fizice interzice furnizarea informațiilor de acest tip referitoare la persoane fizice.

În aceste condiții, Augstākās tiesas Administratīvo lietu departaments (Curtea Supremă, Secția de contencios administrativ, Letonia) a decis să adreseze Curții întrebarea dacă articolul 7 litera (f) din Directiva 95/46 impune obligația comunicării datelor cu caracter personal unui terț în scopul de a-i permite să formuleze o acțiune în despăgubire în fața unei instanțe civile pentru un prejudiciu cauzat de persoana vizată de protecția acestor date și dacă faptul că persoana în cauză este un minor poate afecta interpretarea dispoziției respective.

Curtea a statuat că articolul 7 litera (f) din Directiva 95/46 trebuie interpretat în sensul că nu impune obligația comunicării datelor cu caracter personal unui terț în scopul de a-i permite să formuleze o acțiune în despăgubire în fața unei instanțe civile pentru un prejudiciu cauzat de persoana vizată de protecția acestor date. Totuși, dispoziția menționată nu se opune unei astfel de comunicări, în ipoteza în care aceasta ar fi efectuată în temeiul dreptului național, cu respectarea condițiilor prevăzute de această dispoziție (punctele 27 și 34 și dispozitivul).

În acest context, Curtea a arătat că, sub rezerva verificărilor care trebuie efectuate în această privință de instanța națională, nu este justificat, în condiții precum cele din litigiul principal, să se refuze unei părți vătămate comunicarea datelor cu caracter personal necesare pentru formularea unei acțiuni în despăgubire împotriva autorului prejudiciului sau, dacă este cazul, împotriva persoanelor care exercită autoritatea parentală, pentru motivul că acest autor ar fi minor (punctul 33).

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 (punctul 117 și dispozitiv 3).

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 pe 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 (punctele 111, 112 și 113).

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 (punctul 114).

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 (punctul 116).

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[31] prevede o listă a cazurilor în care o prelucrare de date cu caracter personal poate fi considerată legală. În special, consimțământul persoanei vizate trebuie să fie liber, specific, informat și lipsit de ambiguitate[32]. În această privință, absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu constituie un consimțământ dat în mod valabil (punctele 34, 36, 37 și 39).

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 (punctele 34, 36, 37, 39 și 41).

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 (punctele 42 și 46).

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 (punctele 49-51).

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 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

[31] Articolul 7 din Directiva 95/46 și articolul 6 din RGPD.
[32] Articolul 2 litera (h) din Directiva 95/46 și articolul 4 punctul 11 din RGPD.

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 (punctul 52 și dispozitivul).

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 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, iar aceasta 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 considera că, având în vedere această procedură anterioară, 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[33], 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[34].

În acest context, Tribunalul Administrativ din Wiesbaden a decis să întrebe Curtea cu privire la aplicarea principiului *ne bis in idem* și, 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

---

33 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").

34 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).

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 pe care se întemeiază respectiva notificare, cu condiția ca o astfel de prelucrare să îndeplinească cerințele prevăzute de directiva menționată (punctul 121 și dispozitiv 2).

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[35]. 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[36]. Această prelucrare efectuată de autoritățile statelor membre poate de altfel să se dovedească indispensabilă, tocmai pentru a se verifica dacă principiul menționat se aplică (punctele 111, 114, 116, 117 și 119).

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 această 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[37] (punctul 121 și dispozitiv 2).

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. În consecință, persoana vizată trebuie să poată solicita ștergerea datelor sale. Dacă totuși această înregistrare este 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* (punctul 120).

35 A se vedea articolul 2 alineatul (1) și articolul 3 punctul 2 din Directiva 2016/680.

36 A se vedea articolul 4 alineatul (1) litera (b) și articolul 8 alineatul (1) din Directiva 2016/680.

37 A se vedea articolul 1 alineatul (1) și articolul 8 alineatul (1) din Directiva 2016/680.

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 de asemenea 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 (punctele 113, 120-122 și dispozitiv 2).

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"[38]. 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 (punctele 109-113).

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 este registrul național al vehiculelor și al conducătorilor acestora, cât și asupra dreptului la libertatea de informare (punctele 120 și 121).

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 (punctul 126 și dispozitiv 3).

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 (punctul 137 și dispozitiv 4).

---

[38] 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 [...]".

III. Prelucrarea datelor cu caracter personal în sensul Directivei 2002/58

Hotărârea din 2 octombrie 2018 (Marea Cameră), Ministerio Fiscal (C-207/16, ECLI:EU:C:2018:788)[39]

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. Totuși, Curtea a subliniat 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 (punctele 38, 42 și 59-63 și dispozitivul).

În acest context, Curtea a precizat că, deși, în Hotărârea Tele2 Sverige și Watson și alții[40], 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

[39] Această hotărâre a fost prezentată în Raportul anual 2018, p. 88 și 89.
[40] Hotărârea Curții din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970).

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 (punctele 54-57).

În ceea ce privește speța, 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" (punctele 61 și 62).

Hotărârile din 6 octombrie 2020 (Marea Cameră), Privacy International (C-623/17, EU:C:2020:790) și La Quadrature du Net și alții (C-511/18, C-512/18 și C-520/18, EU:C:2020:791)[41]

Jurisprudența referitoare la stocarea datelor cu caracter personal și la accesul la acestea în domeniul comunicațiilor electronice – în special Hotărârea Tele2 Sverige și Watson și alții, 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 și alții, cauzele conexate C-511/18 și C-512/18), precum și Cour constitutionnelle (Curtea Constituțională, Belgia) (Ordre des barreaux francophones et germanophone și alții, 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 (punctul 49 și dispozitiv 1 din Hotărârea Privacy International și punctul 104 din Hotărârea La Quadrature du Net și alții).

În continuare, Curtea amintește că Directiva 2002/58[42] nu permite ca derogarea de la obligația de principiu de a garanta confidențialitatea comunicațiilor electronice și a datelor aferente

[41] Aceste hotărâri au fost prezentate în Raportul anual 2020, p. 29-32.

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[43], decât cu respectarea principiilor generale ale dreptului Uniunii, printre care figurează principiul proporționalității, și a drepturilor fundamentale garantate de cartă[44] (punctele 59 și 60 din Hotărârea Privacy International și punctele 111 și 113 din Hotărârea La Quadrature du Net și alții).

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 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 și alții, precum și în cauza Ordre des barreaux francophones et germanophone și alții, 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 (punctele 71 și 82 și dispozitiv 2 din Hotărârea Privacy International și punctele 146, 168, 174, 177 și 212 și dispozitiv 1 și 3 din Hotărârea La Quadrature du Net și alții).

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 (punctele 137-139 și 177-179 și dispozitiv 1 și 2 din Hotărârea La Quadrature du Net și alții).

42 Articolul 15 alineatele (1) și (3) din Directiva 2002/58.

43 Articolul 5 alineatul (1) din Directiva 2002/58.

44 În special, articolele 7, 8 și 11, precum și articolul 52 alineatul (1) din cartă.

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 (punctele 161, 163 și 168 și dispozitiv 3 din Hotărârea La Quadrature du Net și alții).

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 (punctul 192 și dispozitiv 2 din Hotărârea La Quadrature du Net și alții).

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 (punctele 222 și 228 și dispozitiv 4 din Hotărârea La Quadrature du Net și alții).

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[45] 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 și alții[46], 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 (punctele 45 și 59 și dispozitiv 1 și 2).

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

[45] 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.

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

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 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 (punctele 33 și 35).

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 (punctul 48).

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 (punctul 51).

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 diferitor 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 (punctele 52 și 53).

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 (punctele 54, 55 și 57).

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)[47]

În această cauză (a se vedea de asemenea 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 (punctul 71 și dispozitiv 4).

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 (punctele 63, 64 și 68).

Hotărârea din 6 octombrie 2015 (Marea Cameră), Schrems (C-362/14, EU:C:2015:650)[48]

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

[47] Această hotărâre a fost prezentată în Raportul anual 2003, p. 67.
[48] Această hotărâre a fost prezentată în Raportul anual 2015, p. 53.

altele, că, prin Decizia 2000/520/CE[49], Comisia a considerat că, în cadrul așa-numitului regim al „sferei de siguranță" (în engleză „safe harbour")[50], 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/CE, 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, în Decizia 2000/520, nu a afirmat aceasta, 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 la respectarea principiilor 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 eventualele ingerințe în aceste drepturi și fără a se afirma existența unei protecții juridice eficiente împotriva unor ingerințe de această natură (punctele 82, 87-89 și 96-98 și dispozitiv 2).

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 (punctele 102-104). Curtea a concluzionat că nevaliditatea articolelor 1 și 3 din Decizia 2000/520 are ca efect afectarea validității acestei decizii în ansamblu (punctele 105 și 106).

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

[49] 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).

[50] 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.

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 (punctul 91).

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 (punctul 92). Astfel, nu este limitată la strictul necesar o reglementare care autorizează în mod generalizat stocarea integralității datelor cu caracter personal ale tuturor persoanelor ale căror date au fost transferate din Uniune către Statele Unite, fără a se face vreo diferențiere, limitare sau excepție în funcție de obiectivul urmărit și fără a se prevedea un criteriu obiectiv care să permită delimitarea accesului autorităților publice la date și utilizarea lor ulterioară în scopuri precise, strict restrânse și susceptibile să justifice ingerința pe care o implică atât accesarea, cât și utilizarea acestor date (punctul 93). 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 a justițiabilului de a exercita căi legale pentru a avea acces la date cu caracter personal care îl privesc sau pentru a obține rectificarea sau ștergerea unor astfel de date nu respectă substanța dreptului fundamental la o protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din cartă (punctele 94 și 95).

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 drepturilor fundamentale a Uniunii Europene 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 (punctele 125 și 126).

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.) (punctul 128).

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 (punctele 165 și 232).

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 ședederea în această țară, chiar și pentru o perioadă de cinci ani (punctele 205-207 și 209).

În al treilea rând, Curtea a considerat că dreptul fundamental la respectarea vieții private, consacrat la articolul 7 din Carta drepturilor fundamentale a Uniunii Europene, 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, este important 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 (punctele 219, 220, 223 și 224).

Hotărârea din 16 iulie 2020 (Marea Cameră), Facebook Ireland și Schrems (C-311/18, ECLI:EU:C:2020:559)[51]

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[52]. 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[53]. 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[54].

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

---

51 Această hotărâre a fost prezentată în Raportul anual 2020, p. 26-29.
52 Articolul 45 din RGPD.
53 Articolul 46 alineatul (1) și alineatul (2) litera (c) din RGPD.
54 Articolul 49 din RGPD.

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 Decizia 2000/520[55], 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")[56] (punctele 52 și 53).

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[57]. 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[58] (punctele 54, 55 și 57).

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 (dispozitiv 4 și 5).

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 publică, de apărare și de securitate a

---

55 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 S. U.A (JO 2000, L 215, p. 7, Ediție specială, 16/vol. 01, p. 64).

56 Hotărârea Curții din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650 (a se vedea de asemenea CP nr. 117/15).

57 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).

58 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).

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 (punctele 86, 88 și 89 și dispozitiv 1).

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 (punctul 105 și dispozitiv 2).

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 (punctul 121 și dispozitiv 3).

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 (punctele 132, 136, 137, 142 și 148 și dispozitiv 4).

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 (punctele 164, 165, 180-182, 184 și 185).

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 (punctele 195-197 și 201 și dispozitiv 5).

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 secțiunea II.3, intitulată „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 (punctul 88 și dispozitiv 3).

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 (punctul 93). 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 (punctul 94). 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 (punctul 96 și dispozitiv 4).

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 (punctul 97 și dispozitiv 4).

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)[59]

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 cu privire la care cunoștea „adresa IP", precum și data și ora de conectare. 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

[59] Această hotărâre a fost prezentată în Raportul anual 2008, p. 46.

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 diferitor 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”)[60], Directiva 2001/29/CE privind armonizarea anumitor aspecte ale dreptului de autor și drepturilor conexe în societatea informațională[61], Directiva 2004/48/CE privind respectarea drepturilor de proprietate intelectuală[62] 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 (punctul 70 și dispozitivul).

Hotărârea din 24 noiembrie 2011, Scarlet Extended (C-70/10, EU:C:2011:771)[63]

Societatea belgiană de autori, compozitori și editori SCRL (SABAM) constatase că utilizatorii de internet care folosesc serviciile Scarlet Extended SA, furnizor de acces la internet (denumită în continuare „Scarlet”), descărcau pe internet, fără autorizație și fără plata unor drepturi, opere preluate din catalogul său prin intermediul rețelelor „peer-to-peer”. SABAM a formulat o acțiune în fața instanțelor naționale și a obținut în primă instanță o somație care obligă Scarlet să pună capăt acestor încălcări ale dreptului de autor făcând imposibilă, printr-un program informatic

60 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).

61 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).

62 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).

63 Această hotărâre a fost prezentată în Raportul anual 2011, p. 37.

„peer-to-peer", orice formă de transmitere sau de primire de către clienții săi a unor fișiere care conțin o operă muzicală din repertoriul SABAM.

Sesizată de Scarlet, cour d'appel de Bruxelles (Curtea de Apel din Bruxelles, Belgia) a hotărât să suspende judecarea cauzei pentru a solicita Curții, cu titlu preliminar, să stabilească dacă o astfel de somație este compatibilă cu dreptul Uniunii.

Curtea a statuat că Directivele 95/46, 2000/31, 2001/29, 2002/58 și 2004/48, coroborate și interpretate în raport cu cerințele care rezultă din protecția drepturilor fundamentale aplicabile, trebuie interpretate în sensul că se opun unei somații adresate Scarlet de a institui un sistem de filtrare a tuturor comunicațiilor electronice care circulă prin intermediul serviciilor sale, în special prin folosirea programelor informatice *„peer-to-peer"*, care se aplică, fără deosebire, întregii sale clientele, cu titlu preventiv, pe cheltuiala sa exclusivă și pentru o perioadă nelimitată, apt să identifice în cadrul rețelei acestui furnizor circulația de fișiere electronice care conțin o operă muzicală, cinematografică sau audiovizuală cu privire la care solicitantul pretinde că deține drepturi de proprietate intelectuală, în vederea blocării transferului de fișiere al căror schimb aduce atingere dreptului de autor (punctul 54 și dispozitivul).

Astfel, potrivit Curții, o asemenea somație nu respectă interdicția prevăzută la articolul 15 alineatul (1) din Directiva 2000/31 de a impune unui astfel de furnizor o obligație generală de supraveghere și nici cerința de a asigura un just echilibru între, pe de o parte, dreptul de proprietate intelectuală și, pe de altă parte, libertatea de a desfășura o activitate comercială și dreptul la protecția datelor cu caracter personal și libertatea de a primi sau de a comunica informații (punctele 40 și 49).

În acest context, Curtea a arătat că, pe de o parte, somația de a institui sistemul de filtrare în litigiu ar implica o analiză sistematică a tuturor conținuturilor, precum și colectarea și identificarea adreselor IP ale utilizatorilor care se află la originea transmiterii de conținuturi ilicite în cadrul rețelei, aceste adrese reprezentând date protejate cu caracter personal, deoarece permit identificarea precisă a utilizatorilor respectivi (punctul 51). Pe de altă parte, somația amintită ar risca să aducă atingere libertății de informare, din moment ce ar fi posibil ca acest sistem să nu facă în mod suficient distincția între un conținut ilicit și un conținut licit, astfel că utilizarea lui ar putea avea drept consecință blocarea comunicațiilor cu conținut licit. Astfel, nu se contestă faptul că răspunsul la problema caracterului licit al unei transmisii depinde de asemenea de aplicarea excepțiilor legale la dreptul de autor care variază de la un stat la altul. În plus, anumite opere pot face parte, în anumite state membre, din domeniul public sau pot face obiectul unei publicări gratuite pe internet din partea autorilor în cauză (punctul 52).

În consecință, Curtea a constatat că, prin adoptarea somației de obligare a Scarlet să instituie sistemul de filtrare în litigiu, instanța națională în cauză nu ar respecta cerința de a asigura un just echilibru între dreptul de proprietate intelectuală, pe de o parte, și libertatea de a desfășura o activitate comercială, dreptul la protecția datelor cu caracter personal și libertatea de a primi și de a transmite informații, pe de altă parte (punctul 53).

Hotărârea din 19 aprilie 2012, Bonnier Audio și alții (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 și alții") 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 și alții.

În speță, Bonnier Audio și alții 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.

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 (punctele 55 și 56).

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 (punctul 58).

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 (punctul 61 și dispozitivul).

Hotărârea din 17 iunie 2021, M. I. C. M. (C-597/19, EU:C:2021:492)

Întreprinderea Mircom International Content Management & Consulting (M. I. C. M.) Limited (denumită în continuare „Mircom") a formulat o cerere de informații îndreptată împotriva Telenet BVBA, un furnizor de acces la internet, la Ondernemingsrechtbank Antwerpen (Tribunalul pentru Întreprinderi din Antwerpen, Belgia, denumit în continuare „instanța de trimitere"). Această cerere are ca obiect obținerea unei decizii prin care Telenet să fie obligată să furnizeze datele de identificare ale clienților săi pe baza adreselor IP colectate, de o societate specializată, în numele Mircom. Conexiunile la internet ale clienților Telenet au fost utilizate pentru a partaja filme care fac parte din catalogul Mircom, pe o rețea de la utilizator la utilizator (*peer-to-peer*) cu ajutorul protocolului BitTorrent. Telenet se opune cererii formulate de Mircom.

În acest context, instanța de trimitere a întrebat mai întâi Curtea dacă partajarea în rețeaua respectivă de segmente ale unui fișier media care conține o operă protejată constituie o comunicare publică în temeiul dreptului Uniunii. În continuare, aceasta a urmărit să afle dacă titularul unor drepturi de proprietate intelectuală precum Mircom, care nu le utilizează, dar solicită daune interese de la contravenienți prezumați, poate beneficia de măsurile, procedurile și mijloacele de reparație prevăzute de dreptul Uniunii pentru a asigura respectarea acestor drepturi, de exemplu solicitând informații. În sfârșit, instanța de trimitere a solicitat Curții să clarifice problema legalității, pe de o parte, a modului în care adresele IP ale clienților au fost colectate de Mircom și, pe de altă parte, a comunicării datelor solicitate de Mircom de la Telenet.

Curtea statuează că dreptul Uniunii[64] nu se opune, în principiu, nici înregistrării sistematice de către titularul unor drepturi de proprietate intelectuală sau de către un terț în numele acestuia a adreselor IP ale utilizatorilor de rețele de la utilizator la utilizator (*peer-to-peer*) ale căror conexiuni la internet ar fi fost utilizate în activități de contrafacere (prelucrarea datelor în amonte), nici comunicării numelor și a adreselor poștale ale utilizatorilor către acest titular sau către un terț în scopul unei acțiuni în despăgubire (prelucrarea datelor în aval). Totuși, inițiativele și cererile în această privință trebuie să fie justificate, proporționale, neabuzive și prevăzute de o măsură legislativă națională care limitează întinderea drepturilor și obligațiilor care intră sub incidența dreptului Uniunii. Curtea precizează că acesta din urmă nu stabilește obligația unei societăți precum Telenet de a comunica unor persoane private datele cu caracter personal pentru a putea iniția, în fața instanțelor civile, proceduri judiciare împotriva încălcărilor dreptului de autor. Dreptul Uniunii permite totuși statelor membre să impună o astfel de obligație (punctele 97 și 125-127 și dispozitiv 3).

[64] Articolul 6 alineatul (1) litera (f) din RGPD și articolul 15 alineatul (1) din Directiva 2002/58.

3. Dezindexarea unor date cu caracter personal

Hotărârea din 24 septembrie 2019 (Marea Cameră), GC și alții (Dezindexarea unor date sensibile) (C-136/17, ECLI:EU:C:2019:773)[65]

În această hotărâre, Curtea, întrunită 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 respectiv, 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[66], 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[67] (punctele 39 și 40).

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 (punctele 42-44).

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 (punctele 46 și 47).

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

65 Această hotărâre a fost prezentată în Raportul anual 2019, p. 117 și 118.
66 Articolul 8 alineatul (1) din Directiva 95/46 și articolul 9 alineatul (1) din Regulamentul 2016/679.
67 Articolul 8 alineatul (5) din Directiva 95/46 și articolul 10 din Regulamentul 2016/679.

special să refuze admiterea unei astfel de cereri atunci când constată că linkurile duc spre date care sunt făcute publice de către persoana vizată[68], 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[69] (punctele 65 și 69).

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 (punctele 66 și 68).

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 (punctele 77 și 78).

Hotărârea din 24 septembrie 2019 (Marea Cameră), Google (Întinderea teritorială a dezindexării) (C-507/17, ECLI:EU:C:2019:772)[70]

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

68 Articolul 8 alineatul (2) litera (e) din Directiva 95/46 și articolul 9 alineatul (2) litera (e) din Regulamentul 2016/679.
69 Articolul 14 primul paragraf litera (a) din Directiva 95/46 și articolul 21 alineatul (1) din Regulamentul 2016/679.
70 Această hotărâre a fost prezentată în Raportul anual 2019, p. 118 și 119.

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[71].

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[72] că pentru realizarea unui astfel de obiectiv legiuitorul ar fi ales să confere dreptului la dezindexare o întindere care ar depăși teritoriul statelor membre. În special, 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 (punctele 62 și 73).

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 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 (punctul 70).

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

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

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 (punctele 65 și 72).

4. Consimțământul utilizatorului unui site internet privind stocarea informațiilor

Hotărârea din 1 octombrie 2019 (Marea Cameră), Planet49 (C-673/17, ECLI:EU:C:2019:801)[73]

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[74] coroborată cu Directiva 95/46/CE[75], precum și cu RGPD[76].

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 prezent prevăzut de RGPD[77] 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 (punctele 49, 52, 56 și 62).

---

73 Această hotărâre a fost prezentată în Raportul anual 2019, p. 120 și 121.

74 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).

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

76 Articolul 6 alineatul (1) litera (a) din Regulamentul 2016/679.

77 IDEM.

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 (punctul 63).

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 (punctele 69 și 71).

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 (punctele 73-75 și 81).

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, ECLI:EU:C:2010:125)[78]

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

[78] Această hotărâre a fost prezentată în Raportul anual 2010, p. 34.

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.

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 (punctul 25).

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 (punctele 30, 36 și 37 și dispozitivul).

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 al 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 cărui secretariat este integrat în serviciile guvernului național și al cărui cancelar federal dispune de un drept necondiționat la informare cu privire la toate aspectele legate de administrarea autorității menționate (punctul 66 și dispozitivul).

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 (punctele 41-43 și 52).

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 (punctul 58).

Hotărârea din 8 aprilie 2014 (Marea Cameră), Comisia/Ungaria (C-288/12, EU:C:2014:237)[79]

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 (punctul 62 și dispozitiv 1).

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 (punctul 51).

[79] Această hotărâre a fost prezentată în Raportul anual 2014, p. 62.

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 (punctele 52-55).

2. Stabilirea dreptului aplicabil și a autorității de supraveghere competente

Hotărârea din 1 octombrie 2015, Weltimmo (C-230/14, EU:C:2015:639)[80]

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

[80] Această hotărâre a fost prezentată în Raportul anual 2015, p. 55.

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 (punctul 41 și dispozitiv 1).

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 (punctul 54). 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 (punctele 57 și 60 și dispozitiv 2).

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 de asemenea 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 (punctul 43).

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 (punctul 44).

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 (punctele 45 și 47).

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

În această hotărâre (a se vedea de asemenea 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) (punctul 64 și dispozitiv 2).

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 (punctul 74 și dispozitiv 3).

Hotărârea din 15 iunie 2021 (Marea Cameră), Facebook Ireland și alții (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 diferitor tehnologii, cum ar fi cookies, extensii pentru social media[81] 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[82] 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 (punctele 36 și 37).

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[83], deși nu ea este autoritatea principală pentru această prelucrare (dispozitiv 1).

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

81 De exemplu butoanele „Îmi place" sau „Distribuie".

82 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".

83 În sensul articolului 4 punctul 23 din RGPD.

trebuie exercitată cu respectarea procedurilor de cooperare și de asigurare a coerenței prevăzute de acest regulament[84] (punctul 75 și dispozitiv 1).

Astfel, pentru prelucrările transfrontaliere, RGPD prevede mecanismul „ghișeului unic"[85], 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[86], în timp ce competența celorlalte autorități naționale de supraveghere de a adopta o asemenea decizie, fie și cu titlu provizoriu, constituie excepția[87]. 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 (punctele 50-53, 56-59 și 63-65).

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[88] 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 (punctul 67).

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[89] 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[90], ceea ce presupune că operatorul sau persoana împuternicită de operator pentru prelucrarea transfrontalieră dispune de un sediu pe teritoriul Uniunii (punctele 80, 83 și 84 și dispozitiv 2).

---

84 Prevăzute la articolul 56 și 60 din RGPD.

85 Articolul 56 alineatul (1) din RGPD.

86 Articolul 60 alineatul (7) din RGPD.

87 Articolul 56 alineatul (2) și articolul 66 din RGPD consacră excepțiile de la principiul competenței decizionale a autorității de supraveghere principale.

88 Prevăzute la articolele 55 și 56 coroborate cu articolul 60 din RGPD.

89 Potrivit articolului 58 alineatul (5) din RGPD.

90 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".

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 (punctele 94-96 și dispozitiv 3).

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 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 (punctul 105 și dispozitiv 4).

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 (punctul 113 și dispozitiv 5).

VII. Aplicarea teritorială a legislației europene

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

În această hotărâre [a se vedea de asemenea secțiunea II.3, intitulată „Noțiunea de «prelucrare a datelor cu caracter personal»", și secțiunea V.1, intitulată „Dreptul de opoziție la prelucrarea datelor cu caracter personal («dreptul la uitare»)"], Curtea s-a pronunțat și asupra domeniului 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 (punctele 55 și 60 și dispozitiv 2).

Prin urmare, 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 (punctul 56).

VIII. Dreptul de acces public la documentele instituțiilor Uniunii Europene și protecția datelor cu caracter personal

Hotărârea din 29 iunie 2010 (Marea Cameră), Comisia/Bavarian Lager (C-28/08 P, EU:C:2010:378)

Bavarian Lager, o societate creată cu scopul de a importa bere germană pentru magazinele specializate în vânzarea de băuturi alcoolice din Regatul Unit, nu a putut să își vândă produsul întrucât numeroase magazine specializate în vânzarea de băuturi alcoolice din Regatul Unit încheiaseră contracte de cumpărare exclusivă care le obligau să se aprovizioneze cu bere de la anumiți producători.

În conformitate cu reglementarea din Regatul Unit privind aprovizionarea cu bere (denumită în continuare „GBP"), producătorii de bere britanici sunt obligați să acorde administratorilor localurilor posibilitatea de a achiziționa bere provenită de la alt producător cu condiția ca berea să fie livrată la butoi. Or, majoritatea berilor produse în afara Regatului Unit nu pot fi considerate „livrate la butoi", în sensul GBP, și, prin urmare, nu intră în domeniul de aplicare al acestei dispoziții. Apreciind că reglementarea respectivă constituie o măsură cu efect echivalent unei restricții cantitative la import, Bavarian Lager a introdus o plângere la Comisie.

În cadrul procedurii de constatare a neîndeplinirii obligațiilor inițiate de Comisie împotriva Regatului Unit, reprezentanți ai autorităților comunitare și britanice, precum și reprezentanți ai Confederației Producătorilor de Bere din Piață Comună (CBMC) au participat la o reuniune care a avut loc la 11 octombrie 1996. În urma notificării din partea autorităților britanice a modificării legislației în discuție care viza să permită vânzarea berii la sticlă drept bere cu proveniență diferită, la fel ca berea livrată la butoi, Comisia a informat Bavarian Lager cu privire la suspendarea procedurii de constatare a neîndeplinirii obligațiilor.

Bavarian Lager a depus o cerere în vederea obținerii procesului-verbal complet al reuniunii din luna octombrie a anului 1996 care să cuprindă numele tuturor participanților, însă Comisia a respins cererea respectivă prin decizia din 18 martie 2004, invocând în special protecția vieții private a persoanelor fizice, astfel cum este garantată de Regulamentul 45/2001.

Bavarian Lager a introdus apoi o acțiune la Tribunal având ca obiect anularea deciziei Comisiei. Prin Hotărârea din 8 noiembrie 2007, Tribunalul a anulat decizia Comisiei, remarcând în special faptul că simpla menționare a numelui persoanelor interesate pe lista persoanelor care au participat la o reuniune în numele entităților reprezentate de acestea nu constituia o atingere și nici nu punea în pericol viața privată a acestor persoane. Comisia, susținută de Regatul Unit și de Consiliu, a formulat recurs în fața Curții împotriva hotărârii Tribunalului.

Curtea a constatat mai întâi că, în cazul în care o cerere întemeiată pe Regulamentul nr. 1049/2001[91] privind accesul la documente vizează obținerea accesului la documente care conțin date cu caracter personal, dispozițiile Regulamentului nr. 45/2001 devin pe deplin aplicabile, inclusiv dispoziția care impune destinatarului transferului de date cu caracter personal obligația de a demonstra necesitatea dezvăluirii acestora, precum și dispoziția care oferă persoanei vizate posibilitatea de a se opune în orice moment, din motive întemeiate și legitime legate de situația sa particulară, ca datele care o privesc sa facă obiectul prelucrării (punctul 63).

Ulterior, Curtea a constatat că lista participanților la reuniunea organizată în cadrul unei proceduri privind constatarea neîndeplinirii obligațiilor, cuprinsă în procesul-verbal al acestei reuniuni, conținea date cu caracter personal, în sensul articolului 2 litera (a) din Regulamentul nr. 45/2001, pentru că persoanele care au participat la această reuniune pot fi identificate (punctul 70).

În cele din urmă, Curtea a concluzionat că, solicitând ca pentru persoanele care nu și-au dat consimțământul în mod expres pentru divulgarea datelor personale care le privesc, cuprinse în acest proces-verbal, să se dovedească necesitatea transferului acestor date personale, Comisia s-a conformat dispozițiilor articolului 8 litera (b) din respectivul regulament (punctul 77).

Astfel, atunci când, în cadrul unei cereri de acces la procesul-verbal în temeiul Regulamentului nr. 1049/2001, nu se oferă nicio motivare expresă și legitimă și niciun argument convingător pentru a demonstra necesitatea transferului acestor date personale, Comisia nu poate să compare diferitele interese ale părților în cauză. Aceasta nu poate nici să verifice dacă nu exista niciun motiv să se presupună că acest transfer ar putea aduce atingere intereselor legitime ale persoanelor vizate, astfel cum prevede articolul 8 litera (b) din Regulamentul nr. 45/2001 (punctul 78)[92].

Hotărârea din 16 iulie 2015, ClientEarth și PAN Europe/EFSA (C-615/13 P, EU:C:2015:489)

Autoritatea Europeană pentru Siguranță Alimentară (EFSA) a constituit un grup de lucru în scopul de a elabora o orientare pentru a indica modul de punere în aplicare a articolului 8 alineatul (5) din Regulamentul (CE) nr. 1107/2009[93], în sensul că titularul unei cereri de autorizare a introducerii pe piață a unui produs fitosanitar anexează la dosar documentația

[91] Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO 2001, L 145, p. 43, Ediție specială, 01/vol. 3, p. 76).

[92] Această hotărâre a fost prezentată în Raportul anual 2010, p. 14.

[93] Regulamentul (CE) nr. 1107/2009 al Parlamentului European și al Consiliului din 21 octombrie 2009 privind introducerea pe piață a produselor fitosanitare și de abrogare a Directivelor 79/117/CEE și 91/414/CEE ale Consiliului (JO 2009, L 309, p. 1).

științifică de specialitate, astfel cum a fost stabilită de EFSA, validată de comunitatea științifică, privind efectele secundare asupra sănătății, a mediului înconjurător și a speciilor nețintă ale substanței active și ale metaboliților relevanți.

Întrucât proiectul de orientare a făcut obiectul unor consultări publice, ClientEarth și Pesticide Action Network Europe (PAN Europe) au prezentat observații privind acest proiect. În acest context, ele au formulat împreună la EFSA o cerere de acces la o serie de documente referitoare la pregătirea proiectului de orientare, inclusiv observațiile experților externi.

EFSA a autorizat accesul ClientEarth și al PAN Europe printre altele la observațiile individuale ale experților externi cu privire la proiectul de orientare. EFSA a arătat totuși că ocultase numele acestor experți, conform articolului 4 alineatul (1) litera (b) din Regulamentul nr. 1049/2001, precum și legislației Uniunii privind protecția datelor cu caracter personal, în special Regulamentul nr. 45/2001. Ea a arătat în această privință că divulgarea numelor acestor experți corespundea unui transfer de date cu caracter personal, în sensul articolului 8 din Regulamentul nr. 45/2001, și că condițiile unui astfel de transfer prevăzute la acest articol nu erau îndeplinite în speță.

Prin urmare, ClientEarth și PAN Europe au introdus o acțiune în fața Tribunalului având ca obiect anularea deciziei EFSA. Întrucât Tribunalul a respins acțiunea, ClientEarth și PAN Europe au formulat recurs împotriva hotărârii[94] Tribunalului în fața Curții.

În primul rând, Curtea a arătat că, prin faptul că informația solicitată ar permite să se identifice autorul unei anumite observații, ea privește persoane fizice identificate și, prin urmare, constituie un set de date cu caracter personal, în sensul articolului 2 litera (a) din Regulamentul nr. 45/2001. Dat fiind că noțiunile de „date cu caracter personal", în sensul articolului 2 litera (a) din Regulamentul nr. 45/2001, și „date privind viața privată" nu sunt echivalente, Curtea a mai considerat că este inoperantă afirmația ClientEarth și a PAN Europe potrivit căreia informația în litigiu nu privește viața privată a experților vizați (punctele 29 și 32).

Curtea a examinat, în al doilea rând, argumentul ClientEarth și al PAN Europe întemeiat pe existența unui climat de neîncredere cu privire la EFSA, acuzată frecvent de lipsă de imparțialitate din cauza folosirii de experți cu interesele personale dictate de legăturile lor cu industria de profil, precum și pe necesitatea de a asigura transparența procesului decizional al acestei autorități. Afirmația a fost fondată pe un studiu care prezintă legăturile întreținute de majoritatea experților membri ai unui grup de lucru din cadrul EFSA cu organizațiile de lobby ale industriei. În această privință, Curtea a hotărât că obținerea informației în litigiu se dovedea necesară pentru a permite verificarea concretă a imparțialității fiecărui expert în îndeplinirea misiunii sale științifice în serviciul EFSA. Prin urmare, Curtea a anulat hotărârea Tribunalului, constatând că Tribunalul a considerat în mod eronat că argumentul sus-menționat al ClientEarth și al PAN Europe nu era suficient pentru a demonstra necesitatea transferului informației în litigiu (punctele 57-59).

În al treilea rând, pentru a aprecia legalitatea deciziei în litigiu a EFSA, Curtea a examinat dacă exista sau nu exista un motiv de a considera că acest transfer ar fi putut aduce atingere

[94] Hotărârea Tribunalului din 13 septembrie 2013, ClientEarth și PAN Europe/EFSA (T-214/11, EU:T:2013:483).

intereselor legitime ale persoanelor vizate. În această privință, Curtea a constatat că afirmația EFSA potrivit căreia divulgarea informației în litigiu ar fi riscat să aducă atingere vieții private și integrității experților menționați reprezintă o considerație generală care nu este susținută de vreun element propriu speței. Curtea a statuat, dimpotrivă, că această divulgare ar fi permis, prin ea însăși, să se înlăture bănuielile de parțialitate în cauză sau ar fi oferit experților eventual vizați ocazia să conteste, dacă este cazul, prin căile de atac disponibile, temeinicia acestor afirmații de parțialitate. Având în vedere aceste elemente, Curtea a anulat și decizia EFSA (punctele 69 și 73).

* * *

Hotărârile cuprinse în această fișă sunt indexate în Repertoriul de jurisprudență la rubricile 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07, 4.11.11.01.