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.

În ceea ce privește dreptul derivat, începând cu mijlocul anilor '90, Comunitatea Europeană a instituit o serie de instrumente menite să asigure protecția datelor cu caracter personal. Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date[1], adoptată pe baza articolului 100 A CE, constituie, în această privință, principalul act juridic al Uniunii în domeniu. Aceasta stabilește condiții generale privind legalitatea prelucrării acestor date și drepturile persoanelor vizate și prevede în special înființarea de autorități independente de supraveghere în statele membre.

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 L 281, 23.11.1995, p. 31, Ediție specială, 13/vol. 17, p. 10), versiune consolidată la 20.11.2003, abrogată începând cu data de 25 mai 2018 (a se vedea nota 5).

Directiva 2002/58/CE[2] a completat ulterior Directiva 95/46/CE 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].

De asemenea, în domeniul spațiului de libertate, securitate și justiție (ex-articolele 30 și 31 TUE), Decizia-cadru 2008/977/JAI[4] reglementează (până în luna mai a anului 2018) protecția datelor cu caracter personal în domeniul cooperării judiciare în materie penală și polițienească.

Uniunea Europeană a elaborat recent un nou cadru juridic global în acest domeniu. În acest scop, ea a adoptat în 2016 Regulamentul (UE) 2016/679[5] privind protecția datelor, care abrogă Directiva 95/46/CE și care va fi direct aplicabil începând cu 25 mai 2018, precum și Directiva (UE) 2016/680[6] 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 final, în cadrul prelucrării lor de către instituțiile și organele UE, protecția datelor cu caracter personal este asigurată de Regulamentul (CE) nr. 45/2001[7]. Acest regulament a permis în special crearea, în 2004, a Autorității Europene pentru Protecția Datelor. În luna ianuarie a anului 2017, Comisia a prezentat o propunere[8] pentru noul regulament de abrogare a Regulamentului nr. 45/2001 și a Deciziei nr. 1247/2002/CE care vizează modernizarea normelor din acest domeniu și alinierea acestora la noul regim instituit prin Regulamentul (UE) 2016/679.

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 L 201, 31.7.2002, p. 37, Ediție specială, 13/vol. 36, p. 63), versiune consolidată la 19.12.2009.

3 Directiva 2002/58/CE 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 L 105, 13.4.2006, 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 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 L 350, 30.12.2008, p. 60), abrogată începând cu 6 mai 2018 (a se vedea nota 6).

5 Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119 din 4.5.2016, p. 1), în vigoare începând din 25 mai 2018.

6 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 L 119, 4.5.2016, p. 89).

7 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 L 8, 12.1.2001, p. 1, Ediție specială, 13/vol. 30, p. 142).

8 Propunere de regulament al Parlamentului European și al Consiliului 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 [COM(2017) 8 final].

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)[9]

În această cauză, litigiile principale aveau ca părți producători agricoli și Land Hessen, în legătură cu publicarea pe pagina de 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 din Fondul european de garantare agricolă (FEGA) și ai Fondului european agricol pentru dezvoltare rurală (FEADR). Producătorii agricoli se opuneau acestei publicări susținând în special că aceasta nu era justificată de un interes public preponderent. Land Hessen considera că publicarea acestor date se baza pe Regulamentele (CE) nr. 1290/2005[10] și 259/2008[11], care privesc finanțarea politicii agricole comune și care impun publicarea unor informații referitoare la persoanele fizice care beneficiază de FEGA și de FEADR.

În acest context, Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden, Germania) a adresat o serie de întrebări Curții de Justiție privind validitatea anumitor dispoziții ale Regulamentului (CE) nr. 1290/2005 și a Regulamentului (CE) nr. 259/2008, care prevăd punerea unor astfel de informații la dispoziția publicului, în special prin intermediul unor pagini de 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 particular (punctele 56-64).

Pentru a fi justificată, o astfel de atingere trebuie să fie prevăzută de lege, să respecte substanța acestor drepturi și libertăți 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 totuşi obligate să realizeze un just echilibru între diferitele interese în cauză, ceea ce impunea, înainte de adoptarea dispozițiilor în litigiu, verificarea aspectului dacă publicarea 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).

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

10 Regulamentul (CE) nr. 1290/2005 al Consiliului din 21 iunie 2005 privind finanțarea politicii agricole comune (JO L 209, 11.8.2005, 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 L 347, 20.12.2013, p. 549).

11 Regulamentul (CE) nr. 259/2008 al Comisiei din 18 martie 2008 de stabilire a normelor de aplicare a Regulamentului (CE) nr. 1290/2005 al Consiliului în ceea ce privește publicarea informațiilor referitoare la beneficiarii fondurilor provenite din Fondul european de garantare agricolă (FEGA) și din Fondul european agricol pentru dezvoltare rurală (FEADR) (JO L 76, 19.3.2008, 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 L 255, 28.8.2014, p. 59).

Astfel, Curtea a declarat nevalide anumite dispoziții ale Regulamentului (CE) nr. 1290/2005, precum și Regulamentul (CE) 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, dispozitiv 1). Cu toate acestea, Curtea nu a pus în discuție efectele publicării listelor de beneficiari ai unui astfel de ajutor de către autoritățile naționale în perioada anterioară datei pronunțării hotărârii (punctul 94, 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[12] 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 de Justiție 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, deşi prelevarea și stocarea unor amprente digitale de către autoritățile naționale, reglementate de articolul 1 alineatul (2) din Regulamentul (CE) 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.

În primul rând, 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). Apoi, 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 final, 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

12 Regulamentul (CE) nr. 2252/2004 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 L 385, 29.12.2004, 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 L 142, 6.6.2009, p. 1).

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 P și C-594/12 P, EU:C:2014:238)[13]

Prezenta hotărâre își găsește originea în cererile privind aprecierea 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/CE în dreptul austriac.

Prin intermediul cererilor de decizie preliminară, instanțele irlandeze și austriece au adresat întrebări Curții de Justiție cu privire la validitatea Directivei 2006/24/CE în lumina articolelor 7, 8 și 11 din cartă. Mai precis, aceste instanțe au solicitat Curții să stabilească dacă obligația care revine, în temeiul acestei directive, furnizorilor de servicii de comunicații electronice accesibile publicului sau de rețele de comunicații publice de a păstra pentru o anumită perioadă date referitoare la viața privată a unei persoane și la comunicațiile sale și de a oferi acces autorităților naționale competente reprezenta o ingerință nejustificată în drepturile fundamentale respective. Tipurile de date în cauză includ în special datele necesare pentru trasarea și identificarea sursei unei comunicații și destinația acesteia, stabilirea datei, a orei, a duratei și a tipului unei comunicații, dispozitivele de comunicații ale utilizatorilor, precum și identificarea situării echipamentului de comunicație mobilă, date care includ printre altele numele și adresa abonatului sau ale utilizatorului înregistrat, numărul de telefon al apelantului și numărul apelat, precum și o adresă IP pentru serviciile de internet. Aceste date permit în special stabilirea persoanei cu care a comunicat un abonat sau un utilizator înregistrat și prin ce mijloace, precum și stabilirea duratei comunicației și a locului de unde a fost inițiată aceasta. În plus, cu ajutorul datelor în cauză se poate cunoaște frecvența comunicațiilor abonatului sau ale utilizatorului înregistrat cu anumite persoane într-o perioadă determinată.

În primul rând, Curtea a statuat că, prin impunerea unor astfel de obligații pentru furnizori, dispozițiile Directivei 2006/24/CE 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 statuat 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

13 Această hotărâre a fost prezentată în Raportul anual 2014, p. 60.

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/CE acoperea în mod generalizat orice persoană și orice mijloc de comunicare electronică, precum și ansamblul datelor de trafic, fără a face vreo 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 astfel de ingerință și nici condițiile materiale și procedurale ale unui astfel de acces sau 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 statuat că Directiva 2006/24/CE 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 impunea păstrarea datelor pe teritoriul Uniunii.

În consecință, această directivă nu garanta pe deplin verificarea respectării cerințelor de protecție și de securitate de 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)[14]

Ca urmare a Hotărârii Digital Rights Ireland și Seitlinger și alții, prin care Directiva 2006/24/CE a fost declarată nevalidă (a se vedea mai sus), Curtea de Justiție 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, a căror păstrare era 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 totuşi 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 de Justiție a fost invitată să se pronunțe cu privire la interpretarea articolului 15 alineatul (1) din Directiva 2002/58/CE, 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.

14 Această hotărâre a fost prezentată în Raportul anual 2016, p. 62.

În hotărârea sa, Curtea a statuat mai întâi că articolul 15 alineatul (1) din Directiva 2002/58/CE coroborat cu articolele 7, 8 și 11, precum și cu articolul 52 alineatul (1) din cartă se opune unei reglementări naționale, precum cea a Suediei, care prevede, în scopul combaterii criminalității, păstrarea generalizată și nediferențiată a tuturor datelor legate de trafic și de localizare ale tuturor abonaților și utilizatorilor înregistrați, în cazul tuturor mijloacelor de comunicații electronice. În opinia Curții, o asemenea reglementare depășește limitele strictului necesar și nu poate fi considerată justificată, într-o societate democratică, astfel cum impune articolul 15 alineatul (1) interpretat în lumina articolelor citate anterior din cartă (punctele 99-105, 107 și 112 și dispozitiv 1).

Aceeaşi 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 şi 125 şi dispozitiv 2).

În schimb, Curtea a considerat că articolul 15 alineatul (1) din Directiva 2002/58/CE 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 Directivei 95/46/CE

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

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 protecția datelor, Comisia a început negocieri cu autoritățile americane. În urma acestor negocieri, Comisia a adoptat, la 14 mai 2004, Decizia 2004/535/CE[15], 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[16] 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 de Justiție 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/CE. În acest context, Curtea a constatat că din decizia de adecvare reieşea 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, deşi 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 aceştia 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/CE nu poate să constituie temeiul competenței Comunității de a încheia acordul în cauză cu Statele Unite. Astfel, acest acord viza același transfer de date ca decizia de adecvare și, prin urmare, prelucrări ale datelor care sunt excluse din domeniul de aplicare al directivei. În consecință, Curtea a anulat decizia Consiliului de aprobare a încheierii acordului (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 prin camera de supraveghere a fost contestată de unul dintre suspecți în fața Oficiului pentru

15 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 L 235, 6.7.2004, p. 11).

16 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 L 183, 20.5.2004, p. 83, și rectificare în JO L 255, 30.9.2005, p. 168).

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) a întrebat Curtea de Justiție 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/CE, 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/CE, 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/CE 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 „date cu caracter personal"

Hotărârea din 19 octombrie 2016, Breyer (C-582/14, EU:C:2016:779)[17]

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.

17 Această hotărâre a fost prezentată în Raportul anual 2016, p. 61.

În acest context, Bundesgerichtshof (Curtea Federală de Justiție, Germania), sesizată cu un recurs, a solicitat Curții de Justiție să stabilească dacă o adresă IP care este înregistrată de un furnizor de servicii de comunicații electronice cu ocazia accesului la site-ul său de 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/CE, 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/CE (punctele 43 şi 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/CE, 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 şi dispozitiv 1).

Hotărârea din 20 decembrie 2017, Nowak (C-434/16, EU:C:2017:582)

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 personal care îl privesc, deținute de ordinul experților contabili. Aceasta din urmă 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 de Justiție să se pronunțe asupra întrebării dacă articolul 2 litera (a) din Directiva 95/46/CE 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/CE, 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. În plus, 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 a locului de muncă dorit. Constatarea că răspunsurile scrise furnizate de un candidat la un examen profesional constituie informații referitoare la acest candidat ca urmare a conținutului, a finalității și a efectului lor este valabilă, pe de altă parte, și atunci când este vorba, precum în speță, despre un examen cu cărțile deschise.

În al treilea rând, în ceea ce privește observațiile examinatorului cu privire la răspunsurile candidatului, Curtea a considerat că acestea constituie, împreună cu răspunsurile formulate de către candidat la momentul examenului, informații referitoare la respectivul candidat, întrucât 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.

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/CE, 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 comentarii, 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 în ceea ce privește prelucrarea datelor care îl privesc, iar aceasta independent de problema dacă respectivul candidat dispune sau nu dispune de un asemenea drept de acces și în temeiul reglementării naționale aplicabile procedurii de examen. 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/CE, nu se extind la întrebările din examen, care nu constituie, ca atare, date cu caracter personal ale candidatului.

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

3. Noțiunea „prelucrare a datelor cu caracter personal”

Hotărârea din 6 noiembrie 2003 (Adunarea Plenară), 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 de Justiție, 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/CE.

Curtea a constatat că operațiunea care constă în a se referi, pe o pagină de internet, la diverse persoane și de a le identifica fie prin nume, fie prin alte mijloace, de exemplu prin numărul de telefon sau prin informații privind condițiile de muncă şi modul de petrecere a timpului liber, constituie o „prelucrare a datelor cu caracter personal, automată integral sau parțial" în sensul acestei directive (punctul 27 şi 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 din 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 şi 43-48 şi 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 de Justiție.

Astfel, Curtea de Justiție a avut ocazia să clarifice noțiunea „prelucrarea datelor cu caracter personal" pe internet din perspectiva Directivei 95/46/CE.

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 şi 30).

4. Condiții de legalitate a unei prelucrări a datelor cu caracter personal având în vedere articolul 7 din Directiva 95/46/CE

Hotărârea din 16 decembrie 2008 (Marea Cameră), Huber (C-524/06, EU:C:2008:724)[18]

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

Domnul Huber, resortisant austriac, s-a stabilit în Germania în 1996 pentru a exercita în acest stat profesia de agent de asigurări independent. Întrucât se consideră discriminat prin faptul 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 adresat Curții o trimitere privind compatibilitatea cu dreptul Uniunii a prelucrării datelor cu caracter personal efectuate în registrul în cauză.

Curtea a amintit, în primul rând, 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 (devenit articolul 18 primul paragraf TFUE). Trebuie subliniat însă că 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 şi 59).

În ceea ce privește noțiunea de necesitate a prelucrării în sensul articolului 7 litera (e) din Directiva 95/46/CE, 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/CE, astfel cum este definit la articolul 1 alineatul (1). Apoi 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/CE stocarea și prelucrarea datelor cu caracter personal nominale în cadrul unui asemenea registru în scopuri statistice (punctele 52, 66 şi 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

18 Această hotărâre a fost prezentată în Raportul anual 2008, p. 45.

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/CE.

ASNEF și FECEMD considerau în special că dreptul spaniol, pentru a permite prelucrarea datelor cu caracter personal, în lipsa consimțământului persoanei în cauză, adaugă o condiție care nu este inclusă în Directiva 85/46/CE 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, acestea au susținut că legea menționată și Decretul regal 1720/2007 limitează domeniul de aplicare al articolului 7 litera (f) din Directiva 95/46/CE, 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/CE 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, 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 şi 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/CE 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/CE 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 şi 48).

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

În această hotărâre (a se vedea de asemenea secțiunea II.2., intitulată „Noțiunea «date cu caracter personal»"), Curtea de Justiție s-a pronunțat de asemenea cu privire la întrebarea dacă articolul 7 litera (f)

din Directiva 95/46/CE 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 şi 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/CE 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 prevaleze 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/CE, 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 şi 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, referitoare 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 a domiciliului, 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 de Justiție întrebarea dacă articolul 7 litera (f) din Directiva 95/46/CE 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/CE 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 şi 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 a sesizat Curtea de Justiție 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/CE 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/CE să fie îndeplinite (punctul 117 şi 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 şi dacă nu există alte mijloace mai puțin restrictive pentru atingerea acestor obiective (punctele 111, 112 şi 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 astfel de 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/CE, anumite drepturi prevăzute la articolele 6 şi 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).

III. Transfer de date cu caracter personal către țări terțe

Hotărârea din 6 noiembrie 2003 (Adunarea Plenară), Lindqvist (C-101/01, EU:C:2003:596)[19]

În această cauză (a se vedea de asemenea secțiunea II.3, intitulată „Noțiunea «prelucrarea 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/CE 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 stabilit în acelaşi 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 şi dispozitiv 4).

Astfel, având în vedere, pe de o parte, stadiul de dezvoltare a internetului la momentul elaborării Directivei 95/46/CE 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 a 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 „transfer către o țară terță de date" o astfel de 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)[20]

Domnul Schrems, cetățean austriac și utilizator al rețelei sociale Facebook, a depus o plângere la Data Protection Commissioner (comisarul pentru protecția datelor, Irlanda), ca urmare a faptului că Facebook Ireland transfera către Statele Unite datele cu caracter personal ale utilizatorilor săi și le stoca pe servere situate în această țară, unde erau prelucrate. În opinia domnului Schrems, dreptul și practicile Statelor Unite nu asigurau o protecție suficientă împotriva supravegherii exercitate de autoritățile publice a datelor transferate către această țară. Data Protection Commissioner a refuzat să investigheze această plângere pe motiv, printre altele, că, prin Decizia 2000/520/CE[21], Comisia a considerat că, în cadrul așa-numitului regim al „sferei de siguranță" (în engleză „safe harbour")[22], Statele Unite asigurau un nivel adecvat de protecție a datelor cu caracter personal transferate.

19 Această hotărâre a fost prezentată în Raportul anual 2003, p. 67.

20 Această hotărâre a fost prezentată în Raportul anual 2015, p. 53.

21 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 L 215, 25.8.2000, p. 7).

22 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.

În acest context, Curtea de Justiție 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 şi în esență cu o cerere având ca obiect stabilirea validității Deciziei 2000/520/CE, adoptată de Comisie în temeiul respectivului articol 25 alineatul (6) din Directiva 95/46/CE.

Curtea a declarat nevalidă decizia Comisiei în ansamblu, subliniind, în primul rând, că adoptarea sa necesita constatarea motivată în mod corespunzător de către Comisie că țara terță asigură 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/CE, nu a afirmat aceasta, articolul 1 din această decizie încalcă cerințele stabilite la articolul 25 alineatul (6) din Directiva 95/46/CE, 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/CE 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 şi 96-98 şi dispozitiv 2).

În plus, Curtea a declarat nevalid articolul 3 din Decizia 2000/520/CE în măsura în care privează autoritățile naționale de supraveghere de competențele întemeiate pe articolul 28 din Directiva 95/46/CE 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/CE 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 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 şi 95).

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

La 26 iulie 2017, Curtea de Justiție s-a pronunțat pentru prima dată cu privire la compatibilitatea unui proiect de acord internațional cu Carta drepturilor fundamentale a Uniunii Europene și, în particular, cu dispozițiile referitoare la respectarea vieții private și la protecția datelor cu caracter personal.

Canada și Uniunea Europeană au negociat un acord privind transferul și prelucrarea datelor din registrul cu numele pasagerilor (Acordul PNR), care a fost semnat în 2014. Întrucât Consiliul Uniunii Europene a solicitat Parlamentului European să îl aprobe, acesta a decis să sesizeze Curtea de Justiție 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 persoanei sau a 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 şi 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 şi 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, vreun raport, nici chiar 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 şi 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 şi 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 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 infracțiunilor 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).

IV. 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 «prelucrare a datelor cu caracter personal»”), Curtea de Justiție 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/CE.

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 prevăzute de articolul 12 litera (b) și de articolul 14 primul paragraf litera (a) din Directiva 95/46/CE și în măsura în care condițiile prevăzute de acestea sunt îndeplinite efectiv, operatorul unui motor de căutare este obligat 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 şi 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, în primul rând, că şi 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 şi dispozitiv 4).

În sfârşit, 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 şi 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)[23]

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 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.

23 Această hotărâre a fost prezentată în Raportul anual 2008, p. 46.

În aceste condiții, Juzgado de lo Mercantil no 5 de Madrid (Tribunalul Comercial nr. 5 din Madrid, Spania) a adresat Curții de Justiție 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 dreptul la respectarea vieții private, și, pe de altă parte, drepturile de proprietate și dreptul la o cale de atac efectivă.

În acest sens, 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")[24], Directiva 2001/29/CE privind armonizarea anumitor aspecte ale dreptului de autor și drepturilor conexe în societatea informațională[25], Directiva 2004/48/CE privind respectarea drepturilor de proprietate intelectuală[26] și Directiva 2002/58/CE 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)[27]

Societatea belgiană de autori, compozitori şi 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 „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 de Justiție, cu titlu preliminar, să stabilească dacă o astfel de somație este compatibilă cu dreptul Uniunii.

Curtea a considerat că Directivele 95/46/CE, 2000/31/CE, 2001/29/CE, 2002/58/CE și 2004/48/CE, coroborate și interpretate în raport cu cerințele care rezultă din protecția drepturilor fundamentale aplicabile, trebuie interpretate în sensul că se opun unei somații adresate către Scarlet de a institui un sistem de filtrare a tuturor comunicațiilor electronice care tranzitează prin intermediul serviciilor sale, în special prin utilizarea programelor informatice „peer-to-peer", care se aplică în mod nediscriminatoriu tuturor clienților săi, ca măsură preventivă, pe cheltuiala sa exclusivă și pe perioadă nelimitată, și care este apt să identifice în cadrul rețelei acestui furnizor circulația de fișiere electronice care conțin o operă

24 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 L 178, 17.7.2000, p. 1, Ediție specială, 13/vol. 29, p. 257).

25 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 L 167, 22.6.2001, p. 10, Ediție specială, 17/vol. 1, p. 230).

26 Directiva 2004/48/CE a Parlamentului European și a Consiliului din 29 aprilie 2004 privind respectarea drepturilor de proprietate intelectuală (JO L 157, 30.4.2004, p. 45, rectificare în JO L 195, 2.6.2004, p. 16, Ediție specială, 17/vol. 2, p. 56).

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

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/CE de a impune unui astfel de furnizor o obligație generală de supraveghere şi 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 şi 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, trebuie să se constate 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.

Hotărârea din 19 aprilie 2012, Bonnier Audio şi alţii (C-461/10, EU:C:2012:219)

Högsta domstolen (Curtea Supremă, Suedia) a sesizat Curtea de Justiție cu o cerere de decizie preliminară în vederea interpretării Directivelor 2002/58/CE și 2004/48/CE 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 de justiție să stabilească dacă dreptul Uniunii se opune aplicării unei dispoziții de drept național, instituită în temeiul articolului 8 din Directiva 2004/48/CE, 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 început prin a aminti că articolul 8 alineatul (3) din Directiva 2004/48/CE coroborat cu articolul 15 alineatul (1) din Directiva 2002/58/CE 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 şi 56).

În această privință, aceasta a constatat că legislația națională în discuție impunea, pentru a putea fi emisă o somație de a comunica datele în cauză, printre altele 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/CE și 2004/48/CE 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 şi dispozitivul).

V. Autorități naționale de supraveghere

1. Sfera de aplicare a cerinței privind independența

Hotărârea din 9 martie 2010 (Marea Cameră), Comisia/Germania (C-518/07, EU:C:2010:125)[28]

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/CE 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/CE impune o independență funcțională a autorităților de supraveghere, în sensul că aceste autorități trebuie să fie independente de celelalte sectoare decât cel public supus supravegherii acestora și că nu trebuie să fie expuse niciunei influențe externe. Or, în opinia acesteia, tutela statului exercitată în landurile germane nu constituie o asemenea influență exterioară, ci un mecanism de supraveghere internă a administrației, pus în aplicare de către autoritățile care aparțin aceluiași aparat

28 Această hotărâre a fost prezentată în Raportul anual 2010, p. 34.

administrativ ca autoritățile de supraveghere și care sunt obligate, la fel ca acestea din urmă, să îndeplinească obiectivele Directivei 95/46/CE.

Curtea a statuat că garanția de independență a autorităților naționale de supraveghere prevăzută de Directiva 95/46/CE 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 acestora, ci pentru a consolida protecția persoanelor și a organismelor care sunt avute în vedere prin deciziile acestora, autoritățile de supraveghere trebuind, așadar, 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 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, aşadar, compatibilă cu cerința de independență (punctele 30, 36 și 37 și dispozitivul).

Hotărârea din 16 octombrie 2012, Curții (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/CE.

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/CE, 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 DSK (punctul 66 și dispozitivul).

Curtea a constatat, mai întâi, că termenii „în condiții de independență deplină" de la articolul 28 alineatul (1) al doilea paragraf din Directiva 95/46/CE 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 şi 52).

Curtea a precizat că, pentru a putea îndeplini criteriul de independență prevăzut în dispoziția menționată anterior a Directivei 95/46/CE, 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 (CE) nr. 45/2001. Într-adevăr, statele membre nu sunt obligate să preia în legislația lor națională dispoziții analoage celor din capitolul V din Regulamentul (CE) 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/CE (punctul 58).

Hotărârea din 8 aprilie 2014 (Marea Cameră), Comisia/Ungaria (C-288/12, EU:C:2014:237)[29]

În această cauză, Comisia a solicitat Curții de Justiție 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/CE.

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 şi 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).

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 asemenea 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).

29 Această hotărâre a fost prezentată în Raportul anual 2014, p. 62.

2. Stabilirea dreptului aplicabil și a autorității de supraveghere competente

Hotărârea din 1 octombrie 2015, Weltimmo (C-230/14, EU:C:2015:639)[30]

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 acestor situri, în pofida cererii lor în acest sens, şi 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/CE.

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/CE. În consecință, aceasta a adresat o serie de întrebări preliminare Curții de Justiție.

În ceea ce privește dreptul național aplicabil, Curtea a statuat că articolul 4 alineatul (1) litera (a) din Directiva 95/46/CE 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, chiar minimă, în cadrul căreia este efectuată prelucrarea. Pentru a determina dacă aceste condiții sunt îndeplinite, instanța de trimitere poate îndeosebi să țină cont de faptul, pe de o parte, că activitatea operatorului de date, în cadrul căreia are loc prelucrarea, constă în exploatarea unor site-uri internet de anunțuri imobiliare privind bunuri imobile situate pe teritoriul statului membru menționat și redactate în limba acestuia și că ea este, în consecință, în principal sau chiar în întregime orientată către acest stat membru. De asemenea, instanța națională poate lua în considerare, pe de altă parte, faptul că persoana respectivă dispune de un reprezentant în statul membru menționat, care este însărcinat să recupereze creanțele care rezultă din această activitate, precum și să îl reprezinte în proceduri administrative și judiciare privind prelucrarea datelor în cauză. În schimb, Curtea a precizat că este lipsit de pertinență aspectul cetățeniei persoanelor vizate de această prelucrare de date (punctul 41 şi dispozitiv 1).

În ceea ce priveşte competența şi atribuțiile autorității de supraveghere sesizate cu o plângere, conform articolului 28 alineatul (4) din Directiva 95/46/CE, 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 şi 60 şi dispozitiv 2).

30 Această hotărâre a fost prezentată în Raportul anual 2015, p. 55.

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 III, intitulată „Transfer de date cu caracter personal către țări terțe"), Curtea de Justiție 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/CE, 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/CE 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/CE, 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 şi 47).

VI. 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 și secțiunea II.3., intitulată „Noțiunea «prelucrare a datelor cu caracter personal»", și secțiunea IV.1., intitulată „Dreptul de opoziție la prelucrarea datelor cu caracter personal («dreptul la uitare»)"], Curtea de Justiție s-a pronunțat și asupra domeniului de aplicare teritorial al Directivei 95/46/CE.

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/CE, în cazul în care operatorul unui motor de căutare, deşi 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 şi 60 şi dispozitiv 2).

Astfel, în asemenea împrejurări, activitățile operatorului motorului de căutare și cele ale sediului său situat în statul membru în cauză, deşi 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).

VII. 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, față de berea livrată la butoi, Comisia a informat Bavarian Lager cu privire la suspendarea procedurii de constatare a neîndeplinirii obligațiilor.

Întrucât 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, Comisia a respins ulterior cererea respectivă prin decizia din 18 martie 2004, invocând în special protecția vieții private a persoanelor fizice, astfel cum este garantată de Regulamentul privind protecția datelor personale.

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 de Justiție împotriva hotărârii Tribunalului.

Curtea a constatat mai întâi că, în cazul în care o cerere întemeiată pe Regulamentul (CE) nr. 1049/2001[31] privind accesul la documente vizează obținerea accesului la documente care conțin date cu caracter personal, dispozițiile Regulamentului (CE) 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 (CE) 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 proves-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 (CE) 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 (CE) nr. 45/2001 (punctul 78)[32].

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 pentru a elabora o orientare pentru a indica modul de punere în aplicare a articolului 8 alineatul (5) din Regulamentul (CE) nr. 1107/2009[33], în sensul că titularul unei cereri de autorizare a introducerii pe piață a unui produs fitosanitar anexează la dosar documentația științifică de specialitate, astfel cum a fost stabilită de către 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 (CE) nr. 1049/2001, precum și legislației Uniunii privind protecția datelor cu caracter personal, în special Regulamentul (CE) 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 (CE) nr. 45/2001, și că condițiile unui astfel de transfer prevăzute la acest articol nu erau îndeplinite în speță.

31 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 L 145, 31.5.2001, p. 43, Ediție specială, 01/vol. 3, p. 76).

32 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 L 309, p. 1).

33 Această hotărâre a fost prezentată în Raportul anual 2015, p. 55.

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[34] Tribunalului în fața Curții de Justiție.

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 (CE) nr. 45/2001. Dat fiind că noțiunile „date cu caracter personal", în sensul articolului 2 litera (a) din Regulamentul (CE) 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 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, 1.04.03.11, 2.04, 2.05.00, 4.11.01 și 4.11.07.

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