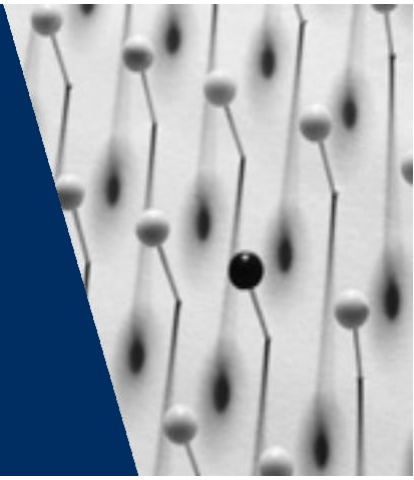
1

Contextul şi cadrul legislaţiei europene privind protecţia datelor



UE	Aspecte vizate	CoE
Dreptul la protecţia datelor		
Tratat privind funcţionarea Uniunii Europene, Articolul16 Carta Drepturilor Fundamentale ale Uniunii Europene (Carta), Articlolul 8 (dreptul la protecţia datelor personale) Directiva 95/46/CE asupra protecţiei persoanelor cu privire la prelucrarea datelor personale şi asupra liberei circulaţii a acestor date (Directiva privind protecţia datelor), MO 1995 L281 (în vigoare până în mai 2018) Decizia-cadru 2008/977/JAI privind protecţia datelor cu caracter personal prelucrate în cadrul poliţiei şi cercetării penale, MO 2008 L 350 (în vigoare până în mai 2018) Regulamentul (UE) 2016/679 asupra protecţiei persoanelor fizice cu privire la prelucrarea datelor personale şi libera circulaţie a acestor date, abrogând Directiva 95/46/CE (Regulamentul general privind protecţia datelor), MO 2016 L119 Directiva (UE) 2016/680 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, cercetării, detectării sau urmăririi penale a infracțiunilor sau al executării de sancțiuni penale, libera circulație a acestor date și abrogarea		CEDO, Articolul 8 (dreptul la respectarea vieţii private, familiale, domiciliului şi corespondenţei) Convenţia modernizată pentru protecţia persoanelor cu privire la prelucrarea automatizată a datelor cu caracter personal (Convenţia modernizată 108)

UE	Aspecte vizate	CoE
Decizia-cadru 2008/977/JAI (Protecţia datelor pentru Autorităţile de poliţie şi justiţie), MO 2016 L119 Directiva 2002/58/CE privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice (Directiva privind confidenţialitatea şi comunicaţiile electronice), MO 2002 L201 Regulamentul (CE) nr. 45/2001 asupra protecţiei persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituţiile şi organele comunitare şi libera circulaţie a acestora (Regulamentul Protecţiei datelor instituţiilor UE), MO 2001 L8		
Limitări privind dreptul la protecţia datelor cu caracter personal		
Carta, Articolul 52 alin. (1) Regulamentul general privind protecţia datelor, Articolul 23 Hotărârea CJUE din 2010, în cauzele conexate C-92/09 şi C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/ Land Hessen*		CEDO, Articolul 8 alin. (2) Convenţia modernizată 108, Articolul 11 Hotărârea CtEDO nr. 30562/04 şi 30566/04 din 2008, în cauza *S. și Marper/ RegatulUnit*
Echilibrarea drepturilor		
Hotărârea CJUE din 2010, în cauzele conexate C-92/09 şi C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/ Land Hessen*	**În general**	
Hotărârea CJUE din 2008, în cauza C-73/07, *Tietosuojavaltuutettu/ Satakunnan Markkinapörssi Oy şi Satamedia Oy* Hotărârea CJUE din 2014, în cauza C-131/12, *GoogleSpain SL, Google Inc./ Agencia Española de Protección de Datos (AEPD), Mario Costeja González*	**Libertatea de exprimare**	CtEDO, Axel Springer AG/ Germania, nr. 39954/08, 20 Hotărârea CtEDO nr. 48009/08 din 2011, în cauza *Mosley/ Regatul Unit* Hotărârea CtEDO Nr. 53495/09 din 2015, în cauza *Bohlen/ Germania*
Hotărârea CJUE din 2010, în cauza C-28/08P, *Comisia Europeană/The Bavarian Lager Co. Ltd* Hotărârea CJUE din 2015, în cauza C-615/13P, *Client Earth, PAN Europe/ EFSA*	**Accesul la documente**	Hotărârea CtEDO nr. 18030/11 din 2016, în cauza *Magyar Helsinki Bizottság/ Ungaria*
Regulamentul general privind protecţia datelor, Articolul 90	**Secretul profesional**	Hotărârea CtEDO nr. 30181/05 din 2015, în cauza *Pruteanu/ România*
Regulamentul general privind protecţia datelor, Articolul 91	**Libertatea la religie şi credinţă**	

UE	Aspecte vizate	CoE
	Libertatea artelor şi ştiinţelor	Hotărârea CtEDO nr. 68345/01 din 2007, în cauza *Vereinigung bildender Künstler/ Austria*
Hotărârea CJUE din 2008, în cauza C-275/06, *Productores de Música de España (Promusicae)/ Telefónica de España SAU*	**Protecţia proprietăţii**	
Hotărârea CJUE din 2014, în cauza C-131/12, *Google Spain SL, Google Inc./ Agencia Española de Protección de Datos (AEPD), Mario Costeja González* Hotărârea CJUE din 2017, în cauza C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/ SalvatoreManni*	**Drepturi economice**	

1.1. Dreptul la protecţia datelor

Puncte-cheie

- În conformitate cu articolul 8 din CEDO, dreptul persoanei la protecție în ceea ce privește prelucrarea datelor cu caracter personal face parte din dreptul la respectarea vieții private și de familie, a domiciliului și a corespondenței.
- Convenția 108 a CoE este primul și, până în prezent, singurul instrument internațional obligatoriu din punct de vedere juridic care se ocupă de protecția datelor. Convenția a suferit un proces de modernizare, finalizat prin adoptarea Protocolului de modificare CETS nr. 223.
- În conformitate cu legislația UE, protecția datelor a fost recunoscută drept un drept fundamental distinct. Acest lucru este afirmat în articolul 16 din Tratatul privind funcționarea UE, precum și în articolul 8 din Carta Drepturilor Fundamentale a UE.
- În conformitate cu legislaţia UE, protecţia datelor a fost reglememntată pentru prima dată de Directiva protecţiei datelor în 1995.
- Având în vedere evoluțiile tehnologice rapide, UE a adoptat o nouă legislație în 2016 pentru a adapta normele privind protecția datelor la epoca digitală. Regulamentul general privind protecția datelor a devenit aplicabil în mai 2018, abrogând Directiva privind protecția datelor.
- Împreună cu Regulamentul general privind protecția datelor, UE a adoptat legislația privind prelucrarea datelor cu caracter personal de către autoritățile statului în scopul aplicării legii. Directiva (UE) 2017/680 stabilește normele și principiile privind protecția datelor care guvernează prelucrarea datelor cu caracter personal în scopul prevenirii, investigării, detectării și urmăririi penale a infracțiunilor sau executării de sancțiuni penale.

1.1.1. Dreptul la respectarea vieţii private şi dreptul al protecţia datelor cu caracter personal: scurtă introducere

Dreptul la respectarea vieții private și dreptul la protecția datelor cu caracter personal, deși strâns legate, sunt drepturi distincte. Dreptul la viața privată - menționat în legislaţia europeană ca drept la respectarea vieții private - a apărut în cadrul legislaţiei internaționale privind drepturile omului în Declarația Universală a Drepturilor Omului (DUDO), adoptată în 1948, ca fiind unul dintre drepturile fundamentale protejate ale omului. La scurt timp după adoptarea DUDO, Europa a confirmat acest drept - în Convenția Europeană a Drepturilor Omului (CEDO), un tratat care este obligatoriu din punct de vedere juridic pentru părțile contractante și care a fost redactat în 1950. CEDO prevede că fiecare persoană are dreptul la respectarea vieții sale private și familiale, a domiciliului și a corespondenței. Interferența cu acest drept de către o autoritate publică este interzisă, cu excepția cazurilor în care interferența este conformă legii, urmărește interese publice importante și legitime și este necesară într-o societate democratică.

DUDO și CEDO au fost adoptate cu mult înainte de dezvoltarea computerelor și a internetului și de creșterea societății informaționale. Aceste evoluții au adus avantaje considerabile persoanelor și societății, îmbunătățind calitatea vieții, eficiența și productivitatea. În același timp, acestea prezintă noi riscuri pentru dreptul la respectarea vieții private. Ca răspuns la necesitatea unor reguli specifice care reglementează colectarea și utilizarea informațiilor personale, a apărut un nou concept de confidențialitate, cunoscut în unele jurisdicții drept "confidențialitate informațională", iar în altele "dreptul la autodeterminare informațională".[1] Acest concept a dus la elaborarea unor reglementări legale speciale care să asigure protecția datelor cu caracter personal.

Protecția datelor în Europa a început în anii 1970, odată cu adoptarea legislației - de către unele state - de a controla prelucrarea informațiilor personale de către autoritățile publice și întreprinderile mari.[2] Instrumentele de protecție a datelor au

1 Curtea Constituţională Germană a afirmat un drept de autodeterminare informaţională prin hotărârea în cauza din anul 1983, *Volkszählungsurteil*, BverfGE Bd.65, S.1ff. Curtea a considerat că autodeterminarea informaţională rezultă din dreptul fundamental la respectarea personalităţii, protejat de Constituţia Germaniei. CEDO a recuoscut printr-o hotărâre din 2017 că articolul 8 din CEDO „prevede dreptul la o formă de autodeterminare informaţională”. A se vedea hotărârea CtEDO nr. 931/13 din 27 iunie 2017, în cauza *Satakunnan Markkinapörssi Oy și Satamedia Oy/ Finlanda*, punctul 137.

2 Statul german Hessa a adoptat prima lege privind protecţia datelor în 1970, aplicabilă doar în acest stat. În1973, Suediaa adoptat prima lege naţională privind protecţia datelor. Până la sfârşitul anilor 80, mai multe state europene (Franţa, Germania, Olanda şi Regatul Unit) au adoptat de asemenea, legislaţia privind protecţia datelor.

fost apoi instituite la nivel european[3] și, peste ani, protecția datelor a devenit o valoare distinctă care nu este subsumată de dreptul la respectarea vieții private. În ordinea juridică comunitară, protecția datelor este recunoscută ca fiind un drept fundamental, separat de dreptul fundamental la respectarea vieții private. Această separare ridică problema relației și a diferențelor dintre aceste două drepturi.

Dreptul la respectarea vieții private și dreptul la protecția datelor cu caracter personal sunt strâns legate. Ambele protejezează valori similare, adică autonomia și demnitatea umană a persoanelor, acordându-le o sferă personală în care își pot dezvolta liber personalitățile, își gândesc și își modelează opiniile. Acestea sunt, așadar, condițiile esențiale pentru exercitarea altor libertăți fundamentale, precum libertatea de exprimare, libertatea de întrunire și asociere pașnică și libertatea religioasă.

Cele două drepturi diferă în ceea ce privește formularea și domeniul de aplicare. Dreptul la respectarea vieții private constă într-o interdicție generală de interferență, sub rezerva unor criterii de interes public care pot justifica interferența în anumite cazuri. Protecția datelor cu caracter personal este privită ca un drept modern și activ,[4] punând în aplicare un sistem de verificări și echilibrări pentru a proteja indivizii ori de câte ori datele lor personale sunt prelucrate. Prelucrarea trebuie să respecte componentele esențiale ale protecției datelor cu caracter personal, și anume supravegherea independentă și respectarea drepturilor persoanelor vizate.[5]

Articolul 8 din Cartă Drepturilor Fundamentale a Uniunii Europene (Carta) nu numai că afirmă dreptul la protecția datelor cu caracter personal, ci și clarifică valorile fundamentale asociate acestui drept. Aceasta prevede că prelucrarea datelor cu caracter personal trebuie să fie corectă, în scopuri specificate și pe baza consimțământului persoanei în cauză sau a unei baze legitime prevăzute de lege. Persoanele fizice trebuie să aibă dreptul de a accesa datele lor personale și de a le rectifica, iar respectarea acestui drept trebuie să facă obiectul controlului de către o autoritate independentă.

---

3 Convenția Consiliului Europeipentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (Convenția 108) a fost adoptată în 1981. UE a adoptat primul său instrument cuprinzător de protecție a datelor în 1995: Directiva 95/46 / CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date.

4 Avocatul Sharpston a descris cazul ca implicând două drepturi distincte: dreptul „clasic" la protecţia vieţi private şi dreptul mai „modern", dreptul la protecţia datelor. A se vedea hotărârea CJUE din 17 iunie 2010 privind cauzele conexate C-92/09 ş iC-93/02, *Volkerund Markus Schecke GbR* LandHessen, Concluziile avocatului Sharpston*, punctul 71.

5 Hustinx, P., EDPS Speeches&Articles, *Legislaţia UE privind protecţia datelor: revizuiread irectivei9 5/46/CE şi propunerea regulamentului general privind protecţia datelor*, iulie 2013.

Dreptul la protecția datelor cu caracter intervine ori de câte ori sunt prelucrate date cu caracter personal; astfel, el este mai amplu decât dreptul la respectarea vieții private. Orice prelucrare a datelor cu caracter personal este supusă unei protecții adecvate. Protecția datelor se referă la toate tipurile de date cu caracter personal și la prelucrarea datelor, indiferent de relația și impactul asupra vieții private. Prelucrarea datelor cu caracter personal poate, de asemenea, să încalce dreptul la viața privată, după cum se arată în exemplele de mai jos. Cu toate acestea, nu este necesar să se demonstreze o încălcare a vieții private pentru ca regulile de protecție a datelor să fie declanșate.

Dreptul la confidențialitate se referă la situațiile în care un interes privat sau "viața privată" a unui individ a fost compromis. După cum s-a demonstrat în acest manual, conceptul de "viață privată" a fost interpretat în mare măsură în jurisprudență, în sensul că include situații intime, informații sensibile sau confidențiale, informații care ar putea prejudicia percepția publicului asupra unui individ și chiar aspecte ale vieții profesionale și a comportamentului în public. Cu toate acestea, aprecierea dacă există sau a existat o interferență cu "viața privată" depinde de contextul și faptele fiecărui caz.

Prin contrast, orice operațiune care implică prelucrarea datelor cu caracter personal ar putea intra sub incidența normelor de protecție a datelor și ar putea declanșa dreptul la protecția datelor cu caracter personal. De exemplu, în cazul în care un angajator înregistrează informații referitoare la numele și remunerația plătită salariaților, simpla înregistrare a acestor informații nu poate fi considerată drept o ingerință în viața privată. O astfel de ingerință ar putea fi totuși susținută dacă, de exemplu, angajatorul a transferat informațiile personale ale angajaților către terți. Angajatorii trebuie, în orice caz, să respecte regulile de protecție a datelor, deoarece înregistrarea informațiilor angajaților reprezintă prelucrarea datelor.

Exemplu: În cauza *Drepturi digitale Irlanda*[6], CJUE a fost chemată să decidă validitatea Directivei 2006/24/CE în lumina drepturilor fundamentale ale protecției datelor cu caracter personal și respectării vieții private, afirmată în Carta Drepturilor Fundamentale a UE. Directiva impunea furnizorilor de servicii de comunicații electronice destinate publicului sau rețelelor de comunicații publice să păstreze datele de telecomunicații ale cetățenilor pe o perioadă de până la doi ani, pentru a se asigura că datele erau disponibile pentru prevenirea, cercetarea și urmărirea penală a infracțiunilor grave. Măsura viza numai metadatele, datele despre locație și datele necesare identificării abonatului sau a utilizatorului. Aceasta nu s-a aplicat în cazul conținutului comunicațiilor electronice.

6 Hotărârea CJUE din 8 aprilie 2014 ,cauzele asociale C-293/12 şi C-594/12, *Drepturi digitale Irlanda Ltd/ Ministerul Comunicaţiilor, Marinei şi a Resurselor Naturale şi alţii şi Kärntner Landesregierung şi alţii*.

CJUE a considerat că directiva constituie o interferență cu dreptul fundamental la protecția datelor cu caracter personal "deoarece prevede prelucrarea datelor cu caracter personal".[7] În plus, aceasta a constatat că directiva interferează cu dreptul la respectarea vieții private.[8] Luate în ansamblu, datele cu caracter personal în conformitate cu directiva, care ar putea fi accesate de autoritățile competente, ar putea permite "tragerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, cum ar fi obiceiurile vieții cotidiene, locurile de ședere permanente sau temporare, mișcările cotidiene sau de altă natură, activitățile desfășurate, relațiile sociale ale acelor persoane și mediile sociale frecventate de aceștia".[9] Interferența cu cele două drepturi a fost amplă și deosebit de gravă.

CJUE a declarat invalidă Directiva 2006/24/CE, constatând că, deși a urmărit un obiectiv legitim, interferența cu drepturile la protecția datelor cu caracter personal și la viața privată era gravă și nu se limita la ceea ce era strict necesar.

1.1.2. Cadrul juridic internaţional: Statele Unite ale Americii

Cadrul legal al Națiunilor Unite nu recunoaște protecția datelor cu caracter personal drept un drept fundamental, deși dreptul la viața privată este un drept fundamental stabilit în cadrul juridic internațional. Articolul 12 din DUDO privind respectarea vieții private și de familie[10] a remarcat pentru prima dată că un instrument internațional a stabilit dreptul unui individ la protecția sferei private împotriva intruziunilor din alte state, mai ales din partea statului. Deși este o declarație fără caracter obligatoriu, DUDO are statutul considerabil de instrument fundamental al legislației internaționale în domeniul drepturilor omului și a influențat dezvoltarea altor instrumente ale drepturilor omului în Europa. Pactul internațional privind drepturile civile și politice a intrat în vigoare în 1976. Acesta proclamă că nimeni nu poate fi supus unei interferențe arbitrare sau ilegale la viața privată, la domiciliu sau corespondență și nici la atacuri ilegale asupra onoarei și reputației lor. Pactul este un tratat internațional care angajează pe cele 169 de părți să respecte și să asigure exercitarea drepturilor civile ale persoanelor, inclusiv viața privată.

7 *Ibidem*, punctul 36.

8 *Ibidem*, punctele 32-35.

9 *Ibidem*, punctul 27.

10 Naţiunile Unite (NU), *Declaraţia Universală a Drepturilor Omului (DUDO)*, 10 decembrie 1948.

Începând cu anul 2013, Organizația Națiunilor Unite a adoptat două rezoluții privind problemele de confidențialitate sub denumirea "dreptul la viața privată în era digitală"[11] ca răspuns la dezvoltarea de noi tehnologii și la dezvăluirile privind supravegherea în masă desfășurate în unele state (dezvăluirile Snowden). Ei condamnă cu fermitate supravegherea în masă și subliniază impactul pe care o astfel de supraveghere îl poate avea asupra drepturilor fundamentale la viața privată și a libertății de exprimare și asupra funcționării unei societăți vibrante și democratice. Deși nu sunt obligatorii din punct de vedere juridic, acestea au declanșat o importantă dezbatere politică la nivel înalt, privind confidențialitatea, noile tehnologii și supravegherea. De asemenea, acestea au condus la înființarea unui raportor special privind dreptul la viața privată, cu un mandat de promovare și protecție a acestui drept. Sarcinile specifice ale raportorului includ colectarea de informații privind practicile și experiențele naționale în ceea ce privește confidențialitatea și provocările generate de noile tehnologii, schimbul și promovarea celor mai bune practici și identificarea eventualelor obstacole.

Deși rezoluțiile anterioare s-au axat pe efectele negative ale supravegherii în masă și asupra responsabilității statelor de a restrânge puterile autorităților de informații, rezoluțiile mai recente reflectă o evoluție esențială în dezbaterea privind viața privată a Națiunilor Unite.[12] Rezoluțiile adoptate în 2016 și 2017 reafirmă necesitatea de a limita competențele agențiilor de informații și de a condamna supravegherea în masă. Cu toate acestea, ele afirmă în mod explicit că "capacitățile crescânde ale mediului de afaceri de a colecta, procesa și utiliza date cu caracter personal pot constitui un risc pentru exercitarea dreptului confidenţialităţii în era digitală". Astfel, pe lângă responsabilitatea autorităților de stat, rezoluțiile indică responsabilitatea sectorului privat de respectare a drepturilor omului și solicită companiilor să informeze utilizatorii cu privire la colectarea, utilizarea, partajarea și păstrarea datelor cu caracter personal și să stabilească politici de prelucrare transparente.

1.1.3. Convenţia Europenă a Drepturilor Omului

Consiliul Europei a fost format în perioada celui de-al doilea război mondial pentru a reuni statele Europei şi a promova statul de drept, democrația, drepturile omului și dezvoltarea socială. În acest scop, a adoptat CEDO în 1950, care a intrat în vigoare în 1953.

11 Ase vedea Adunarea generală a Naţiunilor Unite din 18 decembrie 2013, *Rezoluţia privind dreptul la viaţa privată în era digitală,* A/RES/68/167, New York; şi Adunarea generală a Naţiunilor Unite din 19 noiembrie 2014, *Rezoluţia revizuită privind dreptul la viaţa privată în era digitală*, A/C.3/69/L.26/Rev.1, New York.

12 Adunarea generală a Naţiunilor Unite din 16 noiembrie 2016, *Rezoluţia revizuită privind dreptul la viaţa privată în era digitală*, A/C.3/71/L.39/Rev.1, New York; Consiliul Naţiunilor Unite privind drepturile omului, Dreptul la viaţa privată în era digitală, A/HRC/34/L.7/Rev.1, 22 martie 2017.

Părțile contractante au o obligație internațională de a se conforma CEDO. Toate statele membre ale Consiliului Europei au încorporat sau au aplicat CEDO în legislaţia lor naţională, ceea ce le cere să acționeze în conformitate cu prevederile convenției. Părțile contractante trebuie să respecte drepturile prevăzute de convenție în exercitarea oricărei activități. Acestea includ activitățile întreprinse pentru securitatea națională. Rezoluțiile hotărâtoare ale Curții Europene a Drepturilor Omului (CEDO) au implicat activități de stat în domeniile sensibile ale legislației și practicii securității naționale.[13] Curtea nu a ezitat să afirme că activitățile de supraveghere constituie o interferență cu respectarea vieții private.[14]

Pentru a se asigura că părțile contractante își respectă obligațiile care le revin în temeiul CEDO, Curtea Europeană a Drepturilor Omului a fost înființată la Strasbourg, Franța, în 1959. CEDO se asigură că statele își respectă obligațiile care le revin în temeiul convenției, examinând plângerile persoanelor, grupurilor de persoane, ONG-urilor sau a persoanelor juridice. De asemenea, CEDO poate examina cauzele interstatale aduse de unul sau mai multe state membre ale Consiliului Europei împotriva unui alt stat membru.

Începând cu 2018, Consiliul Europei cuprinde 47 de părți contractante, dintre care 28 sunt state membre ale UE. Un reclamant în fața CtEDO nu e nevoie să fie cetățean al uneia dintre părțile contractante, deși presupusele încălcări trebuie să aibă loc în jurisdicția uneia dintre părțile contractante.

Dreptul la protecția datelor cu caracter personal face parte din drepturile protejate în temeiul articolului 8 din CEDO, care garantează dreptul la respectarea vieții private și de familie, a domiciliului și corespondenței și stabilește condițiile în care sunt permise restricții ale acestui drept.[15]

CtEDO a examinat multe situații care implică probleme legate de protecția datelor. Acestea includ interceptarea comunicațiilor,[16] diverse forme de supraveghere atât din sectorul privat, cât și din cel public,[17] și protecția

13 A se vedea, de exemplu, hotărârea CtEDO nr. 5029/71 din 6 septembrie 1978 în cauza *Klass şi alţii/ Germania*; hotărârea CtEDO nr. 28341/95 din 4 mai 2000 în cauza *Rotaru/România* şi hotărârea CtEDO nr. 37138/14 din 12 ianuarie 2016 în cauza *Szabóand Vissy/ Ungaria*.

14 *Ibidem*.

15 Consiliul Europei, Convenţia Europeană a Drepturilor Omului, CETS Nr. 005, 1950.

16 A se vedea, de exemplu, hotărârea CtEDO nr. 8691/79, din 2august 1984, în cauza *Malone/ Regatul Unit*; hotărârea CtEDO nr. 62617/00 din 3 aprilie 2007, în cauza *Copland/ Regatul Unit*, sau hotărârea CtEDO nr. 27473/06 din 18 iulie 2017, în cauza *Mustafa SezginTanrıkulu/ Turcia*.

17 A se vedea, de exemplu, hotărârea CtEDO nr. 5029/71 din 6 septembrie 1978, în cauza Klass şi alţii/ Germania; hotărârea CtEDO nr. 35623/05 din 2 septembrie 2010, în cauza Uzun/ Germania.

împotriva stocării datelor cu caracter personal de către autorităţile publice.[18] Respectul vieții private nu este un drept absolut, deoarece exercitarea dreptului la viață privată ar putea compromite alte drepturi, cum ar fi libertatea de exprimare și accesul la informații și invers. Prin urmare, Curtea încearcă să găsească un echilibru între diferitele drepturi în cauză. Ea a clarificat că articolul 8 al CEDO nu numai că obligă statele să se abțină de la orice acțiune care ar putea încălca acest drept al convenției, dar că, în anumite circumstanțe, acestea sunt obligate să asigure în mod activ respectul efectiv pentru viața privată și de familie.[19] Capitolele respective descriu în detaliu multe dintre aceste cazuri.

1.1.4. Convenţia 108 a Consiliului Europei

Odată cu apariția tehnologiei informației în anii 1960, a existat o nevoie crescândă de norme mai detaliate pentru protejarea persoanelor prin protejarea datelor cu caracter personal. La mijlocul anilor 1970, Comitetul de Miniștri al Consiliului Europei a adoptat diverse rezoluții privind protecția datelor cu caracter personal, făcând referire la articolul 8 al CEDO.[20] În 1981, o Convenție pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (Convenția 108)[21] a fost deschisă spre semnare. Convenția 108 a fost și rămâne singurul instrument internațional obligatoriu din punct de vedere juridic în domeniul protecției datelor.

Convenția 108 se aplică tuturor prelucrărilor de date efectuate de sectorul privat și cel public, inclusiv de prelucrarea datelor de către sistemul judiciar și autoritățile de aplicare a legii. Convenția protejează persoanele împotriva abuzurilor care pot însoți prelucrarea datelor cu caracter personal și urmărește, în același timp, reglementarea fluxurilor transfrontaliere de date cu caracter personal. În ceea ce privește prelucrarea datelor cu caracter personal, principiile stabilite în convenție privesc, în special, colectarea corectă și legală și prelucrarea automată a datelor, în scopuri legitime specificate. Aceasta înseamnă că datele nu ar trebui utilizate pentru scopuri incompatibile cu aceste scopuri și nu ar trebui să fie păstrate mai mult decât este necesar. Acestea se

18 A se vedea, de exemplu, hotărârea CtEDO nr. 47143/06 din 4 decembrie 2015, în cauza *RomanZakharov/ Rusia*; hotărârea CtEDO nr. 37138/14 din 12 ianuarie 2016 în cauza *Szabó şi Vissy/ Ungaria*.

19 A se vedea, de exemplu, hotărârea CtEDO nr. 20511/03, din 17 iulie 2008, în cauza*l/ Finlanda*; hotărârea CtEDO nr. 2872/02 din 2 decembrie 2008 în cauza *K.U./ Finlanda*.

20 Consiliul Europei, Comitetul de Miniştri (1973), Rezoluţia(73)22 privind protecţia intimităţii persoanelor legat de bazele de date electronice din sectorul privat, 26 septembrie1973; Consiliul Europei, Comitetul de Miniştri (1974), Rezoluţia (74) 29 privind protecţia intimităţi ipersoanelor legat de bazele de date electronice din sectorul privat, 20 septembrie 1974.

21 Consiliul Europei, Convenţia pentru protecţia persoanelor cu privire la prelucrarea automatizată a datelor cu caracter personal, CETS nr. 108, 1981.

referă, în particular la faptul că acestea trebuie să fie adecvate, relevante şi neexcesive (proporţionalitatea), precum şi corecte.

În plus față de furnizarea de garanții privind prelucrarea datelor cu caracter personal și a obligațiilor privind securitatea datelor, ea interzice, în lipsa unor garanții juridice corespunzătoare, prelucrarea datelor "sensibile" - cum ar fi etnia, politica, sănătatea, religia, viața sexuală sau cazierul judiciar.

Convenția consacră, de asemenea, dreptul individului de a fi informat asupra datelor stocate despre el/ea și, dacă este necesar, să le corecteze. Restricțiile privind drepturile prevăzute în convenție sunt posibile numai atunci când sunt în joc interese de importanță majoră, cum ar fi securitatea statului sau apărarea. În plus, convenția prevede circulația liberă a datelor cu caracter personal între părțile contractante și impune anumite restricții asupra fluxurilor către state în care reglementarea juridică nu oferă o protecție echivalentă.

Trebuie remarcat faptul că Convenția 108 este obligatorie pentru statele care l-au ratificat. Ea nu este supusă supravegherii judiciare a CEDO, ci a fost luată în considerare în jurisprudența CEDO în contextul articolului 8 al CEDO. De-a lungul anilor, Curtea a hotărât că protecția datelor cu caracter personal este o parte importantă a dreptului la respectarea vieții private (articolul 8) și a fost ghidată de principiile Convenției 108 pentru a determina dacă a intervenit sau nu o interferență cu acest drept fundamental.[22]

Pentru a dezvolta în continuare principiile și regulile generale prevăzute în Convenția 108, Comitetul de Miniștri al CoE a adoptat câteva recomandări obligatorii din punct de vedere juridic. Aceste recomandări au influențat dezvoltarea legislației privind protecția datelor în Europa. De exemplu, de ani de zile, singurul instrument din Europa care oferă îndrumări cu privire la utilizarea datelor cu caracter personal în sectorul poliției a fost Recomandarea Poliției.[23] Principiile cuprinse în recomandare, cum ar fi mijloacele de păstrare a fișierelor de date și necesitatea punerii în aplicare a unor norme clare privind persoanele cărora li s-a permis accesul la aceste dosare, au fost dezvoltate în continuare și sunt reflectate în legislația UE ulterioară.[24] Mai multe recomandări recente urmăresc să răspundă

22 A se vedea, de exemplu, hotărârea CtEDO nr. 22009/93 din 25 februarie 199 7 în cauza *Z/Finlanda*.

23 Consiliul Europei, Comitetul de Miniştri(1987), Recomandarea Rec(87)15 către statele membre care reglementează utilizarea datelor cu caracter personal în sectorul poliţiei, Strasburg, 17 septembrie 1987.

24 Directiva 95/46/CE a Parlamentului Europeanşi a Consiliuluil din 24 octombrie 1995 asupra protecţiei persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, MO 281, 23 noiembrie 1995.

provocărilor din era digitală – de exemplu, prelucrarea datelor cu caracter personal în contextul ocupării forţei de muncă. (vezi Capitolul 9).

Toate statele membre ale UE au ratificat Convenția 108. În 1999, au fost propuse amendamente la Convenția 108 pentru a permite UE să devină parte, dar nu a intrat niciodată în vigoare.[25] În 2001, a fost adoptat un protocol adițional la Convenția 108. Acesta a introdus dispoziții privind fluxurile transfrontaliere de date către țări care nu sunt părți, așa-numitele țări terțe, și privind instituirea obligatorie a autorităților naționale de supraveghere a protecției datelor.[26]

Convenția 108 este deschisă pentru aderarea părților necontractante ale CoE. Potențialul Convenției ca standard universal, împreună cu caracterul său deschis, servesc drept bază pentru promovarea protecției datelor la nivel mondial. Până în prezent, 51 de state sunt părți la Convenția 108. Acestea includ toate statele membre ale Consiliului Europei (47 de țări); Uruguay, prima țară non-europeană care a aderat în luna august 2013; și Mauriţius, Senegal și Tunisia, care au aderat în 2016 și 2017.

Convenția a suferit recent un proces de modernizare. O consultare publică efectuată în 2011 a confirmat cele două obiective principale ale acestei activități: consolidarea protecției vieții private în domeniul digital și întărirea mecanismului de urmărire a convenției. Procesul de modernizare s-a axat pe aceste obiective și s-a încheiat cu adoptarea unui protocol de modificare a Convenției 108 (Protocolul CETS nr. 223). Lucrările au fost desfășurate în paralel cu alte reforme ale instrumentelor de protecție a datelor internaționale alături de reforma normelor UE privind protecția datelor, lansată în 2012. Autoritățile de reglementare de la nivelul Consiliului Europei și UE au luat toate măsurile pentru a asigura coerența și compatibilitatea dintre cele două cadre juridice. Modernizarea păstrează caracterul general și flexibil al convenției și își consolidează potențialul ca instrument universal pentru protecția datelor. Acesta reafirmă și stabilește principii importante și oferă noi drepturi persoanelor, în același timp crescând responsabilitățile entităților care procesează datele cu caracter personal, asigurând o mai mare responsabilitate. De exemplu, persoanele fizice ale căror date cu caracter personal sunt prelucrate au dreptul să cunoască procesul de prelucrare a acestor date și dreptul de a se opune prelucrării respective.

25 Consiliul Europei, Modificări la Convenţia pentru protecţia persoanelor cu privire la prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108) adoptată de Comitetul de Miniştri la Strasbourg, pe data de 15 iunie 1999.

26 Consiliul Europei, Protocol adiţional la Convenţia pentru protecţia persoanelor cu privire la prelucrarea automatizată a datelor cu caracter personal, privind autorităţile de supraveghere şi fluxurile de date transfrontaliere. O dată cu modernizarea Convenţiei 108, prezentul protocol nu mai este aplicabil, întrucât prevederile sale au fost actualizate şi intregrate în convenţie.

Pentru a contracara utilizarea sporită a profilării în lumea online, convenția stabilește, de asemenea, dreptul persoanei de a nu se supune deciziilor bazate exclusiv pe prelucrarea automată fără a lua în considerare opiniile proprii. Aplicarea eficientă a normelor de protecție a datelor de către autoritățile independente de supraveghere din părțile contractante este considerată esențială pentru implementarea practică a convenției. În acest scop, convenția modernizată subliniază necesitatea ca autoritățile de supraveghere să aibă atribuții și funcții eficiente și să se bucure de o adevărată independență în îndeplinirea misiunii lor.

1.1.5. Legislaţia Uniunii Europene privind protecţia datelor

Legislația UE este compusă din legislația primară și secundară a UE. Tratatele, și anume Tratatul privind Uniunea Europeană (TUE) și Tratatul privind Funcționarea Uniunii Europene (TFUE), au fost ratificate de toate statele membre ale UE; ele constituie "legea primară a UE". Reglementările, directivele și deciziile UE au fost adoptate de instituțiile UE cărora le-a fost acordată această autoritate în temeiul tratatelor; acestea constituie "legea secundară a UE".

Protecţia datelor în legislaţia primară a UE

Tratatele originale ale Comunităților Europene nu conțin nici o referire la drepturile omului sau la protecția acestora, dat fiind că Comunitatea Economică Europeană a fost inițial prevăzută ca o organizație regională axată pe integrarea economică și pe stabilirea unei piețe comune. Un principiu fundamental care stă la baza creării și dezvoltării Comunităților Europene - și unul valabil și astăzi - este principiul conferirii. În conformitate cu acest principiu, UE acționează numai în limitele competențelor care îi sunt conferite de statele membre, astfel cum se reflectă în tratatele UE. Spre deosebire de Consiliul Europei, tratatele UE nu includ competențe explicite în materie de drepturi fundamentale.

Cu toate acestea, CJUE a oferit o interpretare importantă a tratatelor, în ciuda cazurilor în care CJUE a invocat încălcări ale drepturilor omului în domeniile care intră sub incidența legislației UE. Pentru a acorda protecția persoanelor, CJUE a adus drepturi fundamentale în așa-numitele principii generale ale dreptului european. Potrivit CJUE, aceste principii generale reflectă conținutul protecției drepturilor omului constatat în constituțiile naționale și tratatele privind drepturile omului, în special CEDO. CJUE a declarat că va asigura conformitatea legislației UE cu aceste principii.

Recunoscând că politicile sale ar putea avea un impact asupra drepturilor omului și că într-un efort de a face cetățenii să se simtă "mai aproape de UE", UE a

proclamat în 2009 Carta Fundamentală a Drepturilor Fundamentale a UE (Carta). Aceasta încorporează întreaga gamă de drepturi civile, politice, economice și sociale ale cetățenilor europeni, prin sintetizarea tradițiilor constituționale și a obligațiilor internaționale comune statelor membre. Drepturile descrise în Cartă sunt împărțite în șase secțiuni: demnitatea, libertățile, egalitatea, solidaritatea, drepturile cetățenilor și justiția.

Inițial, fiind doar un document politic, Carta a devenit obligatorie din punct de vedere juridic[27], drept lege primară a UE (a se vedea articolul 6 alineatul (1) din TUE), atunci când Tratatul de la Lisabona a intrat în vigoare pe 1 decembrie 2009.[28] Dispozițiile Cartei sunt adresate instituțiilor și organismelor UE, obligându-le să respecte drepturile enumerate în aceasta în timpul îndeplinirii atribuțiilor lor. De asemenea, dispozițiile Cartei unesc statele membre atunci când pun în aplicare legislația UE.

Carta nu numai că garantează respectarea vieții private și familiale (articolul 7), dar stabilește și dreptul la protecția datelor cu caracter personal (articolul 8). Carta ridică în mod explicit nivelul acestei protecții la cel al unui drept fundamental în legislația UE. Instituțiile și organismele UE trebuie să garanteze și să respecte acest drept, la fel ca și statele membre atunci când pun în aplicare dreptul Uniunii (articolul 51 din Cartă). Formalizat la mai mulți ani după Directiva privind protecția datelor, articolul 8 din Cartă trebuie interpretat ca incluzând o legislație UE existentă în materie de protecție a datelor. Prin urmare, Carta nu doar menționează în mod explicit dreptul de protecție a datelor în articolul 8 alineatul (1), ci se referă, de asemenea, la principiile esențiale de protecție a datelor prevăzute la articolul 8 alineatul (2). În concluzie, articolul 8 alineatul (3) din Cartă solicită unei autorități independente să controleze punerea în aplicare a acestor principii.

Adoptarea Tratatului de la Lisabona este un punct de reper în elaborarea legislației privind protecția datelor, nu numai pentru ridicarea Cartei la statutul unui document juridic obligatoriu la nivelul dreptului primar, ci și pentru asigurarea dreptului la protecția datelor cu caracter personal. Acest drept este prevăzut în mod specific în articolul 16 din TFUE, în cadrul părții tratatului dedicat principiilor generale ale UE. Articolul 16 creează, de asemenea, un nou temei juridic, care conferă UE competența de a legifera în materie de protecție a datelor. Aceasta este o evoluție importantă deoarece normele UE privind protecția datelor - în special Directiva privind protecția datelor - au fost inițial bazate pe temeiul juridic al pieței interne și pe necesitatea de a armoniza legislațiile naționale astfel încât să nu se împiedice libera circulație a datelor în

27 UE (2012), Carta Drepturilor Fundamentale aUniunii Europene, MO 2012 C326.

28 A se vedea versiunile consolidate ale Comunităţilor Europene (2012), Tratat privind Uniunea Europeană, MO 2012 C326; şi aComunităţilor Europene(2012), TFUE, MO 2012 C326.

cadrul UE. Articolul 16 din TFUE oferă acum un temei juridic independent pentru o abordare modernă și cuprinzătoare a protecției datelor, care acoperă toate aspectele de competența UE, inclusiv cooperarea polițienească și judiciară în materie de cercetare penală. Articolul 16 din TFUE afirmă, de asemenea, că respectarea normelor de protecție a datelor adoptate în temeiul acestuia trebuie să facă obiectul controlului autorităților independente de supraveghere. Articolul 16 a servit ca temei juridic pentru adoptarea reformei cuprinzătoare a normelor privind protecția datelor în 2016, și anume Regulamentul general privind protecția datelor și Directiva privind protecția datelor pentru autoritățile de poliție și cercetare penală (a se vedea mai jos).

Regulamentul general privind protecţia datelor cu caracter personal

Din 1995 până în mai 2018, principalul instrument juridic al UE privind protecția datelor a fost 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 lor circulație a acestora (Directiva privind protecția datelor).[29] A fost adoptată în 1995, într-un moment în care mai multe state membre au adoptat deja legi naționale privind protecția datelor[30] și a reieșit din necesitatea armonizării acestor legi pentru a asigura un nivel ridicat de protecție și liberă circulație a datelor cu caracter personal în rândul diferitelor state membre. Libera circulație a mărfurilor, a capitalului, a serviciilor și a persoanelor în cadrul pieței interne a impus fluxul liber de date, care nu putea fi realizat decât dacă statele membre s-ar putea baza pe un nivel ridicat uniform de protecție a datelor.

Directiva privind protecția datelor a reflectat principiile de protecție a datelor deja conținute în legislațiile naționale și în Convenția 108, extinzându-le adesea. Aceasta a făcut apel la posibilitatea, prevăzută la articolul 11 din Convenția 108, de a adăuga instrumente de protecție. În special, introducerea în directivă a supravegherii independente ca instrument de îmbunătățire a respectării normelor privind protecția datelor s-a dovedit a fi o contribuție importantă la funcționarea eficientă a legislației europene privind protecția datelor. În consecință, această caracteristică a fost încorporată în legea CoE în 2001 prin Protocolul adițional la Convenția 108. Aceasta ilustrează interacțiunea strânsă și influența pozitivă a celor două instrumente asupra celorlalte instrumente de-a lungul anilor.

29 Directiva 95/46/CE a Parlamentului European şi a Consiliului din 24 octombrie 1995 asupra protecţiei persoanelor cu privire la prelucrarea datelor cu caracter personal şi a liberei circulaţii a acestor date, MO 1995 L281.

30 Statul german Hessa a adoptat prima lege din lume privind protecţia datelor în1970, aplicabilă numai în acest stat. Suedia a adoptat *Datalagen* în 1973; Germania a adoptat *Bundesdatenschutzgestez* în 1976; şi Franţa a adoptat *Loi relatif à l'informatique,aux fichiers et aux libertés* în1977. În Regatul Unit, Data Protection Act a fost adoptat în 1984. În cele din urmă, Olanda a adoptat *Wet Persoonregistraties* în 1989.

Directiva privind protecția datelor a stabilit un sistem detaliat și cuprinzător de protecție a datelor în UE. Cu toate acestea, în conformitate cu sistemul juridic al UE, directivele nu se aplică direct și trebuie transpuse în legislațiile naționale ale statelor membre. În mod inevitabil, statele membre dispun de o marjă de apreciere în ceea ce privește transpunerea dispozițiilor directivei. Chiar dacă directiva era menită să asigure o armonizare completă[31] (și un nivel de protecție complet), în practică aceasta a fost transpusă în mod diferit în statele membre. Aceasta a dus la stabilirea unor norme diverse privind protecția datelor în UE, cu definiții și reguli interpretate diferit în legislațiile naționale. Nivelurile de aplicare și severitatea sancțiunilor s-au modificat, de asemenea, în toate statele membre. În cele din urmă, au avut loc schimbări semnificative în domeniul tehnologiei informației de la redactarea directivei la mijlocul anilor 1990. Luate împreună, aceste motive au determinat reforma legislației UE privind protecția datelor.

Reforma a dus la adoptarea Regulamentului general privind protecția datelor în aprilie 2016, după ani de discuții intense. Dezbaterile privind necesitatea modernizării normelor UE privind protecția datelor au început în 2009, când Comisia a lansat o consultare publică cu privire la viitorul cadru juridic al dreptului fundamental la protecția datelor cu caracter personal. Propunerea de regulament a fost publicată de Comisie în ianuarie 2012, începând un lung proces legislativ de negocieri între Parlamentul European și Consiliul UE. După adoptare, Regulamentul general privind protecția datelor a prevăzut o perioadă de tranziție de doi ani. Acesta a devenit aplicabil la 25 mai 2018, când a fost abrogată directiva privind protecția datelor.

Adoptarea regulamentului general privind protecția datelor în 2016 a modernizat legislația UE privind protecția datelor, făcând-o adecvată pentru protejarea drepturilor fundamentale în contextul provocărilor economice și sociale ale epocii digitale. RGPD păstrează și dezvoltă principiile și drepturile fundamentale ale persoanei prevăzute în directiva privind protecția datelor. În plus, aceasta a introdus noi obligații pentru ca organizațiile să pună în aplicare protecția datelor prin design și în mod implicit; să numească un responsabil cu protecția datelor în anumite circumstanțe; să respecte un nou drept la portabilitatea datelor; și să respecte principiul responsabilității. În conformitate cu legislația UE, reglementările sunt direct aplicabile; nu este necesară implementarea la nivel național. Regulamentul general privind protecția datelor prevede astfel un set unic de norme privind protecția datelor în întreaga UE. Aceasta creează reguli coerente de protecție a datelor în întreaga UE, creând un mediu de securitate juridică de care pot beneficia operatorii economici și persoanele fizice ca "persoane vizate".

31 Hotărârea CJUE din 24 noiembrie 2011 în cauzele conexate C-468/10 şi C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) şi Federación de Comercio Electrónico y Marketing Directo (FECEMD)/ Administración del Estado*, punctul 29.

Cu toate acestea, deşi RGPD este direct aplicabil, statele membre trebuie să-şi actualizeze legile naţionale existente privind protecţia datelor pentru a se alinia complet cu regulamentul, reflectând, de asemenea, o marjă de apreciere pentru dispozițiile specifice ale acestuia[10]. Principalele reguli și principii stabilite în regulament, precum și drepturile puternice pe care le oferă persoanelor fizice, constituie o mare parte a manualului și sunt prezentate în capitolele ce urmează. Regulamentul conține norme cuprinzătoare privind domeniul de aplicare teritorial. Se aplică întreprinderilor stabilite în UE, controlorilor și prelucrătorilor care nu sunt stabiliți în UE şi care oferă bunuri sau servicii persoanelor vizate în UE sau le monitorizează comportamentul. Dat fiind faptul că mai multe întreprinderi tehnologice de peste mări au o cotă-cheie pe piața europeană și milioane de clienți din UE, supunerea acestor organizații la normele UE privind protecția datelor este importantă pentru a asigura protecția persoanelor și pentru a asigura condiții de concurență echitabile.

Protecţia datelor în aplicarea legii – Directiva 2016/680

Directiva abrogată privind protecția datelor a oferit un regim cuprinzător de protecție a datelor. Acest regim a fost îmbunătățit în continuare prin adoptarea Regulamentului general privind protecția datelor. Deși cuprinzător, domeniul de aplicare a directivei privind abrogarea Directivei privind protecția datelor a fost limitat la activitățile care se încadrează în piața internă și la activitățile autorităților publice, altele decât cele de aplicare a legii. Prin urmare, a fost necesară adoptarea unor instrumente speciale pentru a obține claritatea și echilibrul necesar între protecția datelor și alte interese legitime și pentru a răspunde provocărilor care sunt deosebit de pertinente în anumite sectoare. Acesta este cazul normelor care reglementează prelucrarea datelor cu caracter personal de către autoritățile de aplicare a legii.

Primul instrument juridic al UE pentru reglementarea acestei chestiuni a fost Decizia-cadru 2008/977/JAI a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală. Normele sale au fost aplicate numai datelor polițienești și judiciare atunci când au fost schimbate între statele membre. Transformarea internă a datelor cu caracter personal de către organele de drept a fost exclusă din domeniul său de aplicare.

Directiva 2016/680 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul

32 Directiva (UE) 2016/680 din 27 aprilie 2016 a Parlamentului şi Consiliului European asupra protecţiei persoanelor fizicecu privire la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenţiei, investigaţiei, detecţieisau a urmăririi penale a infracţiunilorşi asupra liberei circulaţii a acestor date, MO L119, 4 mai 2016

prevenirii, investigării, detectării sau urmăririi penale a infracțiunilor sau al executării de sancțiuni penale și privind libera circulație a acestor date[32], denumită Directiva privind protecția datelor pentru autoritățile de poliție și cercetare penală, a remediat această situație. Adoptat în paralel cu Regulamentul general privind protecția datelor, directiva a abrogat Decizia-cadru 2008/977/JAI și a stabilit un sistem cuprinzător de protecție a datelor cu caracter personal în contextul aplicării legii, recunoscând în același timp particularitățile prelucrării datelor referitoare la securitatea publică. În timp ce regulamentul general privind protecția datelor stabilește norme generale pentru protejarea persoanelor în ceea ce privește prelucrarea datelor cu caracter personal și pentru asigurarea liberei circulații a acestor date în UE, directiva stabilește norme specifice privind protecția datelor în domeniile justiției, cooperării în materie penală și cooperării polițienești. În cazul în care o autoritate competentă prelucrează date cu caracter personal în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor, se aplică Directiva 2016/680. Atunci când autoritățile competente procesează date cu caracter personal pentru alte scopuri decât cele menționate anterior, se aplică regimul general în temeiul Regulamentului general privind protecția datelor. Spre deosebire de predecesorul său (Decizia-cadru 2008/977/JAI a Consiliului), domeniul de aplicare al Directivei 2016/680 se extinde la prelucrarea internă a datelor cu caracter personal de către autoritățile de aplicare a legii și nu este limitat la schimburile de astfel de date între statele membre. În plus, directiva încearcă să realizeze un echilibru între drepturile persoanelor fizice și obiectivele legitime ale procesării legate de securitate.

În acest scop, directiva afirmă dreptul la protecția datelor cu caracter personal și principiile fundamentale care ar trebui să acopere prelucrarea datelor, respectând cu strictețe regulile și principiile consacrate în Regulamentul general privind protecția datelor. Drepturile persoanelor și obligațiile impuse controlorilor - de exemplu, în ceea ce privește securitatea datelor, protecția datelor prin design sau implicit și notificările privind încălcările datelor - se aseamănă cu drepturile și obligațiile din regulamentul general privind protecția datelor. De asemenea, directiva ia în considerare și încearcă să abordeze provocări tehnologice grave emergente care pot avea un impact deosebit de oneros asupra persoanelor, cum ar fi utilizarea tehnicilor de profilare de către autoritățile de aplicare a legii. În principiu, deciziile bazate exclusiv pe prelucrarea automată, inclusiv profilarea, trebuie să fie interzise.[33] În plus, acestea nu trebuie să se bazeze pe date sensibile. Aceste principii fac obiectul anumitor excepții prevăzute de directivă. În plus, o astfel de prelucrare nu trebuie să ducă la discriminare împotriva oricărei persoane.[34]

Directiva conține, de asemenea, reguli care să asigure responsabilitatea controlorilor. Aceștia trebuie să desemneze un responsabil pentru protecția

33 Directiva privind protecţia datelor pentru autorităţile de poliţie şi justiţie penală, articolul 11 alin. (1).

34 *Ibidem*, articolul 11 alin. (2) şi (3).

datelor care să monitorizeze respectarea normelor privind protecția datelor, să informeze și să consilieze autoritatea și angajații în efectuarea obligațiilor lor și să coopereze cu autoritatea de supraveghere. Prelucrarea datelor cu caracter personal în sectorul polițienesc și al justiției penale este supusă în prezent supravegherii autorităților independente de supraveghere. Atât regimul juridic general privind protecția datelor, cât și regimul special de protecție a datelor în materie de aplicare a legii și de cercetare penală trebuie să respecte în egală măsură cerințele Cartei UE.

Regimul special pentru prelucrarea datelor în contextul cooperării polițienești și judiciare instituit prin Directiva privind protecția datelor pentru autoritățile de poliție și justiție penală este descris în detaliu în Capitolul 8.

Directiva privind confidenţialitatea şi comunicaţiile electronice

Stabilirea unor norme speciale privind protecția datelor a fost, de asemenea, considerată necesară în sectorul comunicațiilor electronice. Odată cu dezvoltarea internetului, a telefoniei fixe și mobile, a fost important să se asigure respectarea drepturilor utilizatorilor la intimitate și confidențialitate. Directiva 2002/58/CE35 privind prelucrarea datelor cu caracter personal și protecția vieții private în domeniul comunicațiilor electronice (Directiva privind confidențialitatea și comunicațiile electronice sau Directiva privind confidențialitatea și e-confidențialitatea) stabilește norme privind securitatea datelor cu caracter personal în aceste rețele, notificarea încălcărilor de date cu caracter personal și a confidențialității comunicaţiilor.

În ceea ce privește securitatea, operatorii de servicii de comunicații electronice trebuie, printre altele, să se asigure că accesul la datele cu caracter personal este limitat doar la persoanele autorizate și să ia măsuri pentru a împiedica distrugerea, pierderea sau deteriorarea accidentală a datelor cu caracter personal. Dacă există un risc deosebit de încălcare a securității rețelei publice de comunicații, operatorii trebuie să informeze abonații.[37] Dacă, în pofida măsurilor de securitate puse în aplicare, se produce o încălcare a securității, operatorii trebuie să notifice autoritatea națională competentă însărcinată cu implementarea şi aplicarea directivei de încălcarea datelor cu caracter personal. Operatorii sunt uneori obligați să notifice, de asemenea, încălcările de date cu caracter personal, și anume atunci când încălcarea este susceptibilă să afecteze în mod negativ datele lor personale sau confidențialitatea.[38]

35 Directiva 2002/58/CE a Parlamentului şi Consiliului European din 12 iulie 2002 cu privire la prelucrarea datelor şi protecţia confidenţialităţii în comunicaţiile electronice, MO L201 (Directiva privind confidenţialitatea şi comunicaţiile electronice sau Directiva e-confidenţialităţi).

36 Directiva privind confidenţialitatea şi coumnicaţiile electronice, articolul 4 alin. (1).

37 *Ibidem*, articolul 4 alin. (2).

38 *Ibidem*, articolul 4 alin. (3).

Confidențialitatea comunicațiilor necesită ascultarea, capturarea, stocarea sau orice alt tip de supraveghere sau interceptare a comunicațiilor iar metadatele sunt, în principiu, interzise. De asemenea, directiva interzice comunicările nesolicitate (adesea denumite "spam"), cu excepția cazului în care utilizatorii și-au dat acordul și conțin reguli privind stocarea "cookie-urilor" pe computere și dispozitive. Aceste obligații fundamentale negative indică în mod clar că confidențialitatea comunicărilor este în mod semnificativ legată de protecția dreptului la respectarea vieții private consacrate în articolul 7 din Cartă și de dreptul la protecția datelor cu caracter personal consacrat la articolul 8 din Cartă.

În ianuarie 2017, Comisia a publicat o propunere de regulament privind respectarea vieții private și protecția datelor cu caracter personal în domeniul comunicațiilor electronice, menită să înlocuiască Directiva privind confidențialitatea și e-confidențialitatea. Reforma urmărește să alinieze normele care reglementează comunicațiile electronice la noul regim de protecție a datelor instituit prin Regulamentul general privind protecția datelor. Noul regulament va fi direct aplicabil în întreaga UE; toți indivizii se vor bucura de același nivel de protecție a comunicațiilor lor electronice, în timp ce operatorii și întreprinderile de telecomunicații vor beneficia de claritate, siguranță juridică și existența unui set unic de norme în întreaga UE. Normele propuse privind confidențialitatea comunicațiilor electronice se vor aplica, de asemenea, noilor furnizori de servicii de comunicații electronice care nu sunt reglementați de Directiva privind confidențialitatea și e-confidențialitatea. Acestea din urmă acopereau doar furnizorii tradiționali de servicii de telecomunicații. Având o masivă implicare în utilizarea serviciilor cum ar fi Skype, WhatsApp, Facebook Messenger și Viber pentru a trimite mesaje sau apelare, aceste servicii (OTT) vor fi în prezent în domeniul de aplicare al regulamentului și vor trebui să respecte cerințele sale privind protecția datelor, confidențialitatea și securitatea datelor. La momentul publicării acestui manual, un proces legislativ privind regulile privind confidențialitatea în e-mail era în curs de desfășurare.

Regulamentul nr. 45/2001

Deoarece Directiva privind protecția datelor ar putea fi aplicată numai statelor membre ale UE, a fost nevoie de un instrument juridic suplimentar pentru a stabili protecția datelor pentru prelucrarea datelor personale de către instituțiile și organismele UE. Regulamentul (CE) nr. 45/2001 privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele Comunității și privind libera circulație a acestor date (Regulamentul privind protecția datelor instituțiilor UE) îndeplinește această sarcină.[39]

39 Regulamentul(CE) nr. 45/2001 al Parlamentului European şi al Consiliuluidin 18 decembrie 2000 privind protecţia persoanelor fizice în prelucrarea datelor cu caracter personal de către instituţiile şi organele Comunităţii şi privind libera circulaţie a acestor date, MO 2001 L8.

Regulamentul nr. 45/2001 respectă principiile regimului general al UE de protecție a datelor și aplică aceste principii la prelucrarea datelor realizate de instituțiile și organismele UE în exercitarea funcțiilor lor. În plus, instituie o autoritate independentă de supraveghere pentru a monitoriza aplicarea dispozițiilor sale, Autoritatea Europeană pentru Protecția Datelor (AEPD), care deține competențe de supraveghere și obligația de a monitoriza prelucrarea datelor cu caracter personal în instituțiile și organismele UE, de a audia și investiga plângerile pentru presupusele încălcări ale normelor privind protecția datelor. De asemenea, oferă consiliere instituțiilor și organelor UE cu privire la toate aspectele legate de protecția datelor cu caracter personal, de la propuneri pentru o nouă legislație până la elaborarea unor norme interne privind prelucrarea datelor.

În ianuarie 2017, Comisia Europeană a prezentat o propunere de un nou regulament privind prelucrarea datelor de către instituțiile UE, care va abroga actualul regulament. Ca și în cazul reformei directivei privind confidențialitatea și e-confidențialitatea, reforma Regulamentului nr. 45/2001 va moderniza și alinia normele sale la noul regim de protecție a datelor instituit prin Regulamentul general privind protecția datelor.

Rolul CJUE

CJUE are competența de a stabili dacă un stat membru și-a îndeplinit obligațiile care îi revin în temeiul legislației UE privind protecția datelor și de a interpreta legislația UE pentru a asigura aplicarea eficientă și uniformă a acesteia în statele membre. De la adoptarea directivei privind protecția datelor în 1995, s-a acumulat un ansamblu considerabil de jurisprudență, clarificând domeniul de aplicare și sensul principiilor protecției datelor și dreptul fundamental la protecția datelor cu caracter personal, astfel cum este prevăzut la articolul 8 din Cartă. Deși directiva a fost abrogată și un nou instrument juridic - Regulamentul general privind protecția datelor - este în vigoare, această jurisprudență preexistentă rămâne relevantă și valabilă pentru interpretarea și aplicarea principiilor UE privind protecția datelor, în măsura în care principiile și conceptele de bază ale Directivei privind protecția datelor au fost păstrate în RGPD.

1.2. Limitările dreptului la protecţia datelor

Puncte-cheie

- Dreptul la protecţia datelor nu este un drept absolut; acesta poate fi limitat dacă este necesar pentru un obiectiv de interes general sau pentru a proteja drepturile şi libertăţile altora.

- Condițiile de limitare a drepturilor la respectarea vieții private și la protecția datelor cu caracter personal sunt enumerate în articolul 8 din CEDO și în articolul 52 alineatul (1) din Cartă. Acestea au fost dezvoltate și interpretate prin jurisprudența Curții Europene a Drepturilor Omului și a CJUE.
- În conformitate cu legea privind protecţia datelor CoE, prelucrarea datelor cu caracter personal constituie o interferenţă legală cu dreptul la respectarea vieţii private şi poate fi efectuată doar dacă:
  - este în conformitate cu legea;
  - urmăreşte un scop legitim;
  - respectă esenţa drepturilor şi libertăţilor fundamentale;
  - este necesară şi proporţională într-o societate democratică pentru a atinge un scop legitim.
- Ordinea juridică a UE plasează condiții similare pentru limitarea exercitării drepturilor fundamentale protejate prin Cartă. Orice limitare a oricărui drept fundamental, inclusiv protecția datelor cu caracter personal, poate fi legală numai dacă:
  - este în conformitate cu legea;
  - respectă esenţa dreptului;
  - este supus principiului proporţionalităţii; şi
  - urmăreşte un obiectiv de inters general recunoscut de UE sau necesitatea de a proteja drepturile altora.

Dreptul fundamental la protecția datelor cu caracter personal în temeiul articolului 8 din Cartă nu este un drept absolut", ci trebuie să fie luat în considerare în funcție de funcția sa în societate".[40] Prin urmare, articolul 52 alineatul (1) din Cartă recunoaște că pot fi impuse restricții asupra exercitării unor drepturi precum cele prevăzute la articolele 7 și 8 din Cartă, atât timp cât aceste limitări sunt prevăzute de lege, respectă esența acestor drepturi și libertăți și, respectând principiul proporționalității, sunt necesare și îndeplinesc într-adevăr obiectivele de interes general recunoscute de UE sau necesitatea de a proteja drepturile și libertățile altora.[41] În mod similar, în sistemul CEDO, protecția datelor este garantată de articolul 8, iar exercitarea acestui drept poate fi limitată în cazul în care este necesar să se urmărească un scop legitim. Această secțiune se referă la condițiile de intervenție în temeiul CEDO, astfel cum au fost interpretate de jurisprudența CEDO, precum și condițiile pentru limitările legale prevăzute la articolul 52 din Cartă.

40 A se vedea, de exemplu,hotărârea CEDO încauzele conexate C-92/09 şi C-93/09 din 9 noiembrie 2010, *Volker und Markus Schecke GbR and Hartmut Eifert/ Land Hessa*, punctul 48.

41 *Ibidem*, punctul 50.

1.2.1. Cerinţele CEDO privind interferenţa justificată

Prelucrarea datelor cu caracter personal poate constitui o interferență cu dreptul persoanei vizate la respectarea vieții private, protejat de articolul 8 din CEDO.[42] După cum s-a explicat mai sus (a se vedea Secțiunea 1.1.1 și Secțiunea 1.1.4), contrar ordinii juridice a UE, CEDO nu afirmă protecția datelor cu caracter personal drept un drept fundamental distinct. Mai degrabă, protecția datelor cu caracter personal face parte din drepturile protejate în temeiul dreptului la respectarea vieții private. Astfel, nici o operațiune care implică prelucrarea datelor cu caracter personal nu ar putea intra sub incidența articolului 8 din CEDO. Pentru ca articolul 8 să fie declanșat, trebuie să se stabilească mai întâi dacă un interes privat sau viața privată a unei persoane au fost compromise. Prin jurisprudența sa, CEDO a tratat noțiunea de "viață privată" ca un concept larg, care acoperă chiar și aspecte ale vieții profesionale și ale comportamentului public. De asemenea, aceasta a decis că protecția datelor cu caracter personal reprezintă o parte importantă a dreptului la respectarea vieții private. Cu toate acestea, în ciuda interpretării ample a vieții private, nu toate tipurile de prelucrare ar compromite în sine drepturile protejate în temeiul articolului 8.

În cazul în care CEDO consideră că operațiunea de prelucrare în cauză afectează dreptul particularilor la respectarea vieții private, va examina dacă interferența este justificată. Dreptul la respectarea vieții private nu este un drept absolut, ci trebuie să fie echilibrat și reconciliat cu alte interese și drepturi legitime, fie că este vorba de alte persoane (interese private) sau de societate în ansamblu (interese publice).

Condiţiile cumulative în care o interferenţă ar putea fi justificată sunt:

Să fie în conformitate cu legea

Conform jurisprudenței Curții Europene a Drepturilor Omului, o interferență este conformă cu legea dacă se bazează pe o dispoziție de drept intern care are anumite calități. Legea trebuie să fie "accesibilă persoanelor în cauză și previzibilă cu privire la efectele lor".[43] O regulă este previzibilă "dacă este formu-

42 Hotărârea CtEDO nr. 30562/04 și 30566/04 din 8 decembrie 2008, în cauza *S. și Marper/ Regatul Unit*, punctul 67.

43 Hotărârea CtEDO nr. 27798/95 din 16 februarie 2000, în cauza *Amann/ Elveţia*, punctul 50; a se vedea şi hotărârea CtEDO nr. 23224/94 din 25 martie 1998, în cauza *Kopp/Elveţia*, punctul 55 şi hotărârea CtEDO nr. 25198/02 din10 februarie 2009, în cauza *Iordachi şi alţii/ Moldova*, punctul 50.

44 Hotărârea CtEDO nr. 27798/95 din 16 februarie 2000, în cauza *Amann/ Elveţia*, punctul 56; a se vedea şi hotărârea CtEDO nr. 8691/79 din 2 august 1984, în cauza *Malone/ Regatul Unit*, punctul 66; hotărârea CtEDO nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 din 25 martie, în cauza *Silver şi alţii/ Regatul Unit*, 1983, punctul 88.

lată cu suficientă precizie pentru a permite oricărei persoane - dacă este necesar, cu consiliere adecvată - să-și reglementeze conduita".[44] Mai mult, "gradul de precizie cerut de'lege' în acest sens va depinde de obiectul particular".[45]

Exemple: În cauza *Rotaru/România*,[46] reclamantul a pretins o încălcare a dreptului său la respectarea vieții private din cauza deținerii și utilizării de către Serviciul Român de Informații a unui dosar care conținea informațiile sale personale. CtEDO a constatat că, deși legea națională permite colectarea, înregistrarea și arhivarea în fișiere secrete a informațiilor care afectează securitatea națională, aceasta nu prevedea nici o limitare a exercitării acestor competențe, care a rămas la discreția autorităților. De exemplu, dreptul intern nu a definit tipul de informații care ar putea fi prelucrate, categoriile de persoane împotriva cărora ar putea fi luate măsuri de supraveghere, circumstanțele în care ar putea fi luate astfel de măsuri sau procedura care trebuie urmată. Prin urmare, Curtea a concluzionat că legea națională nu a respectat cerința de previzibilitate prevăzută la articolul 8 din CEDO și că acest articol a fost încălcat.

În cauza *Taylor-Sabori/Regatul Unit*,[47] reclamantul a fost ținta supravegherii poliției. Folosind o "clonă" a pagerului reclamantului, poliția a reușit să intercepteze mesajele trimise către el. Reclamantul a fost arestat și acuzat de conspirație pentru furnizarea unui medicament controlat. Partea cauzei procuraturii împotriva lui a constat din notele actuale scrise ale mesajelor pe pager, pe care poliția le-a transcris. Cu toate acestea, în momentul procesului reclamantului, în legislația britanică nu exista nici o prevedere care să reglementeze interceptarea comunicațiilor transmise prin intermediul unui sistem privat de telecomunicații. Interferența cu drepturile sale nu a fost, prin urmare, "în conformitate cu legea". CtEDO a concluzionat că aceasta a încălcat articolul 8 din CEDO.

45 Hotărârea CtEDO nr .6538/74 din 26 aprilie 1979, în cauza *TheSundayTimes/Regatul Unit*, punctul 49; a se vedea şi hotărârea CtEDO nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 din 25 martie 1983 în cauza *Silver și alții/ Regatul Unit*, punctul 88.

46 Hotărârea CtEDO nr. 28341/95 din 4 mai2000, în cauza *Rotaru/ România*, punctul 57; a se vedea şi hotărârea CtEDO nr. 62540/00 din 28 iunie 2007, în cauza *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev/ Bulgaria*; hotărârea CtEDO nr. 30194/09 din 21 iunie 2011, în cauza *Shimovolos/ Rusia*; şi hotărârea CtEDO nr. 59842/00 din 31 mai 2005, în cauza *Vetter/ Franța*.

47 Hotărârea CtEDO nr. 47114/99 din 22 octombrie 2002, în cauza *Taylor-Sabori/ Regatul Unit*.

Cauza *Vukota-Bojić/Elveției*[48] viza supravegherea secretă a unui reclamant de asigurări sociale de către anchetatori privați, comandat de compania de asigurări. CtEDO a considerat că, deși măsura de supraveghere în cauză a fost dispusă de o societate privată de asigurări, societatea respectivă a primit dreptul statului de a acorda beneficii provenite din asigurarea medicală obligatorie și de a colecta prime de asigurare. Un stat nu s-a putut abate de la responsabilitate în cadrul convenției prin delegarea obligațiilor sale la organisme sau persoane particulare. Legislația internă a trebuit să ofere garanții suficiente împotriva abuzului de a interfera cu drepturile prevăzute în articolul 8 din CEDO ca fiind "în conformitate cu legea". În acest caz, CEDO a concluzionat că a avut loc o încălcare a articolului 8 din CEDO, deoarece legislația națională nu a indicat cu suficientă claritate domeniului de aplicare și modului de exercitare a puterii de apreciere conferite societăților de asigurare care acționează ca autorități publice în domeniul asigurărilor de a efectua supravegherea secretă a unei persoane asigurate. În special, nu a inclus garanții suficiente împotriva abuzurilor.

Să urmărească un scop legitim

Scopul legitim poate fi unul dintre interesele publice menționate sau protecția drepturilor și libertăților celorlalți. Obiectivele legitime care ar putea justifica o intervenție sunt, în conformitate cu articolul 8 alineatul (2) din CEDO, interesele securității naționale, siguranței publice sau bunăstării economice a unei țări, prevenirea neregulilor sau a infracțiunilor, protecţia sănătăţii sau a principiilor morale și protecția drepturilor și libertăților altor persoane.

Exemplu: În cauza *Peck/Regatul Unit*,[49] reclamantul a încercat să se sinucidă pe stradă prin tăierea încheieturilor, fără să știe că o cameră TVCI îl filmase. Poliția, care urmărea camerele TVCI, l-a salvat și, ulterior, a transmis materialul TVCI către mass-media, care a publicat-o fără a ascunde fața reclamantului. CtEDO a constatat că nu există motive relevante sau suficiente care să justifice divulgarea directă a materialelor de către autorități către public, fără a fi obținut consimțământul solicitantului sau mascarea identității sale. Curtea a concluzionat că a avut loc o încălcare a articolului 8 din CEDO.

48 Hotărârea CtEDO Nr. 61838/10,18 octombrie 2016, în cauza *Vukota-Bojić/ Elveţia*, punctul 77.

49 Hotărârea CtEDO Nr. 44647/98, 28 ianuarie 2003, în cauza *Peck/ Regatul Unit*, punctul 85.

Să fie necesară într-o societate democratică

CtEDO a afirmat că "noțiunea de necesitate implică faptul că ingerința corespunde unei nevoi sociale presante și, mai ales, că este proporțională cu scopul legitim urmărit".[50] Pentru a evalua dacă o măsură este necesară pentru a răspunde unei nevoi sociale presante, CtEDO examinează relevanța și adecvarea acestuia în raport cu scopul urmărit. În acest scop, ea poate lua în considerare dacă ingerința încearcă să abordeze o problemă care, dacă nu este abordată, ar putea avea un efect negativ asupra societății, dacă există dovezi că intervenția poate atenua acest efect negativ și viziunile mai generale ale societății cu privire la problema în cauză.[51] De exemplu, colectarea și stocarea datelor cu caracter personal de către serviciile de securitate ale anumitor persoane despre care se constată că au legături cu mișcările teroriste ar constitui o interferenţă cu dreptul particularilor la respectarea vieții private, care, totuși, servește unei nevoi sociale: securitatea națională și lupta împotriva terorismului. Pentru a face față testului de necesitate, interferența va trebui, de asemenea, să fie proporțională. În jurisprudența CEDO, proporționalitatea este abordată în cadrul conceptului de necesitate. Proporționalitatea impune ca o ingerință în drepturile protejate prin CEDO să nu depășească ceea ce este necesar pentru îndeplinirea obiectivului legitim urmărit. Factorii importanți care trebuie luați în considerare la efectuarea testului de proporționalitate sunt domeniile de intervenţie, în special numărul de persoane afectate și garanțiile sau restricțiile puse în aplicare pentru a limita domeniul său de aplicare sau efectele dăunătoare asupra drepturilor persoanelor.[52]

Exemplu: În cauza *Khelili/Elveția*,[53] în timpul unei verificări a poliției, aceasta a descoperit că reclamanta a publicat anunţuri cu textul: "Femeie frumoasă, în vârstă de treizeci de ani, vreau să întâlnesc un bărbat să bem împreună sau să ieșim din când în când. Număr de telefon [...]“. Reclamanta a afirmat că, după această descoperire, poliția a introdus numele ei în evidențele lor ca prostituată, o ocupație pe care ea a negat-o în mod constant. Reclamanta a solicitat ștergerea cuvântului "prostituată" din înregistrările calculatorului poliției. CtEDO a recunoscut, în principiu, că păstrarea datelor personale ale unui individ pe motiv că persoana respectivă ar putea comite o altă infracțiune poate fi, în anumite circumstanţe, propor ţională. Cu toate aces-

50 Hotărârea CtEDO nr. 9248/81din 26martie 1987 în cauza *Leander/Suedia*, punctul 58.

5 Grupul de lucru pentru protecţia datelor Articolul 29(2014), *Aviz privind aplicarea conceptelor de necesitate şi proporţionalitate şi a protecţiei datelor în cadrul sectorului de aplicare a legii*, 211, Bruxelles, 27 februarie 2014, pagina 7–8.

52 *Ibidem*, pagina 9–11.

53 Hotărârea CtEDO nr.16188/07 din 18 octombrie 2011, în cauza Khelili/ Elveţia.

tea, în cazul reclamantei, afirmația de prostituție ilegală a fost prea vagă și generală, nu a fost susținută de fapte concrete, deoarece ea nu a fost niciodată condamnată pentru prostituție ilegală și, prin urmare, nu putea fi considerată ca întrunită "nevoia socială urgentă" în sensul articolului 8 din CEDO. Privind-o ca pe o problemă a autorităților de a dovedi exactitatea datelor stocate despre reclamantă și având în vedere gravitatea interferenţei cu drepturile reclamantei, Curtea a hotărât că păstrarea termenului de "prostituată" în dosarele poliției de ani de zile nu a fost necesară într-o societate democratică. Curtea a concluzionat că a avut loc o încălcare a articolului 8 din CEDO.

Exemplu: În cauza *S. și Marper/Regatul Unit*,[54] cei doi reclamanți au fost arestați și acuzați de infracțiuni. Poliția le-a luat amprentele digitale și probele ADN, conform prevederilor din Legea privind poliția și dovezile penale. Reclamanții nu au fost niciodată condamnați pentru infracțiuni: unul a fost achitat în instanță, iar procedura penală împotriva celui de-al doilea reclamant a fost întreruptă. Cu toate acestea, amprentele, profilele ADN și probele celulare au fost păstrate și stocate de poliție într-o bază de date, iar legislația națională a autorizat păstrarea acestora fără o limită de timp aplicabilă. În timp ce Regatul Unit a susținut că reținerea a contribuit la identificarea viitorilor infractori și, astfel, a urmărit scopul legitim de prevenire și detectare a criminalității, CtEDO a considerat că interferența cu dreptul reclamanților la respectarea vieții private este nejustificată. Aceasta a reamintit că principiile fundamentale ale protecției datelor impun ca reținerea datelor cu caracter personal să fie proporțională cu scopul de colectare și că perioadele de păstrare trebuie să fie limitate. Curtea a acceptat faptul că extinderea bazei de date pentru a include profilurile ADN nu numai pentru persoanele condamnate, ci și pentru toate persoanele care au fost bănuite, dar nu au fost condamnate, ar fi putut contribui la detectarea și prevenirea infracțiunilor în Regatul Unit.[55]

Având în vedere bogăția informațiilor genetice și de sănătate conținute în probele celulare, interferența cu dreptul reclamanților la viața privată a fost deosebit de invazivă. Amprentele și eșantioanele ar putea fi luate de la persoanele arestate și reținute pe termen nelimitat în baza de date a poliției, indiferent de natura și gravitatea infracțiunii și chiar de infracțiunile minore care nu pot fi pedepsite cu închisoare. În plus, posibilităţile persoanelor priva-

54 Hotărârea CtEDO nr. 30562/04 şi 30566/04 din 4 decembrie 2008 în cauza *S. și Marper/ Regatul Unit*.

55 *Ibidem*, punctul 119.

te achitate de a-şi scoate datele din baza de date au fost limitate. În cele din urmă, CtEDO a acordat o atenție deosebită faptului că un reclamant avea 11 ani de când a fost arestat. Păstrarea datelor cu caracter personal ale unui minor care nu este condamnat poate fi deosebit de dăunătoare, având în vedere vulnerabilitatea și importanța dezvoltării și integrării lor în societate.[56] Curtea a considerat în unanimitate că reținerea a constituit o interferenţă disproporționată cu dreptul la viața privată care nu poate fi considerată necesară într-o societate democratică.

Exemplu: În cauza *Leander/Suedia*[57], CtEDO a hotărât că controlul secret al persoanelor care solicită angajarea în posturi de importanță pentru securitatea națională nu este, în sine, contrar cerinței de a fi necesară într-o societate democratică. Garanțiile speciale prevăzute în legislația națională pentru protejarea intereselor persoanei vizate - de exemplu, controalele exercitate de parlament și de cancelarul justiției - au condus la concluzia CEDO că sistemul suedez de control al personalului a îndeplinit cerințele articolului 8 alineatul (2) din CEDO. Având în vedere marja largă de apreciere pe care o are la dispoziție, statul pârât a avut dreptul să considere că, în cazul reclamantului, interesele securității naționale au predominat asupra celor individuale. Curtea a concluzionat că nu a existat o încălcare a articolului 8 din CEDO.

1.2.2. Condiţii privind limitările legale conform Cartei Uniunii Europene a drepturilor fundamentale

Structura și formularea Cartei sunt diferite de cele ale CEDO. Carta nu folosește noțiunea de interferență cu drepturi garantate, ci conține o dispoziție privind limitarea (limitele) exercitării drepturilor și libertăților recunoscute de Cartă.

În conformitate cu articolul 52 alineatul (1), limitările exercitării drepturilor și libertăților recunoscute în Cartă și, în consecință, asupra exercitării dreptului la protecția datelor cu caracter personal sunt admisibile numai dacă:

- sunt prevăzute de lege; şi

56 *Ibidem*, punctul 124.

57 Hotărârea CtEDO nr. 9248/81 din 26 martie 1987, în cauza *Leander/ Suedia*, punctele 59 şi 67.

- respectă esenţa dreptului la protecţia datelor; şi
- se supun principiului proportionalităţii;[58] şi
- îndeplinesc obiective de interes general recunoscute de Uniune sau necesită protejarea drepturilor şi libertăţilor altora.

Întrucât protecția datelor cu caracter personal este un drept fundamental distinct și autonom în ordinea juridică comunitară protejată în temeiul articolului 8 din Cartă, orice prelucrare a datelor cu caracter personal constituie, prin ea însăși, o interferență cu acest drept. Nu este relevant dacă datele personale în cauză se referă la viața privată a unui individ, sunt sensibile sau dacă persoanele vizate au fost incomodate în vreun fel. Pentru a fi legal, interferența trebuie să respecte toate condițiile enumerate la articolul 52 alineatul (1) din Cartă.

Prevăzute de lege

Limitările privind dreptul la protecția datelor cu caracter personal trebuie să fie prevăzute de lege. Această cerință implică faptul că limitările trebuie să se bazeze pe o bază legală care este suficient de accesibilă și previzibilă și formulată cu suficientă precizie pentru a permite persoanelor să-și înțeleagă obligațiile și să-și adapteze comportamentul. Temeiul juridic trebuie să definească în mod clar domeniul de aplicare și modul de exercitare a puterii de către autoritățile competente pentru a proteja persoanele împotriva unei interferențe arbitrare. Această interpretare seamănă cu cerința unei "interferențe legale" în jurisprudența Curții Europene a Drepturilor Omului[59] și s-a susținut că sensul expresiei "prevăzut de lege" folosit în Cartă ar trebui să fie același cu cel care i-a fost atribuit în legătură cu Curtea Europeană a Drepturilor Omului.[60] Jurisprudența Curții Europene a Drepturilor Omului, în special conceptul de "calitate a legii" pe care a dezvoltat-o de-a lungul anilor, este o considerație relevantă care trebuie luată în considerare de CJUE în interpretarea domeniului de aplicare al articolului 52 alineatul (1) din Cartă.[61]

58 Cu privire la evaluarea necesităţii măsurilor care limitează dreptul fundamental la protecţia datelor cu caracter personal, a se vedea: AEPD(2017), *Set de instrumente pentru necesități*, Bruxelles, din 11 aprilie 2017.

59 AEPD(2017), *Set de intrumente pentru necesități*, Bruxelles, 11 aprilie 2017, pagina 4; a se vedea, de asemenea hotărârea CJUE, *Avizul1/15 al Curţii(Camera Mare)*, din 26 iulie 2017.

60 Hotărârea CJUE în cauzele conexate C-203/15 şi iC-698/15, *Tele2SverigeAB/Post-ochtelestyrelsen şi Secretarul de stat pentru Departamentul Local/ Tom Watson, Peter Brice, Geoffrey Lewis*, *Opinia avocatului general SaugmandsgaardØe*, din data de 19 iulie 2016, punctul 140.

61 Hotărârea CJUEdin14aprilie2011, în cauza C-70/10, Scarlet Extended SA/ Société belge des auteurs compositeurs et éditeurs (SABAM), *Opinia avocatului general Cruz Villalón*, punctul 100.

Respectă esenţa dreptului

În legislaţia UE, orice limitare a drepturilor fundamentale protejate de Cartă trebuie să respecte esența acestor drepturi. Acest lucru înseamnă că limitările care sunt atât de extinse și intruzive încât poate lipsi un drept fundamental de conținutului său de bază, nu pot fi justificate. Dacă esența dreptului este compromisă, limitarea trebuie considerată ilegală, fără a fi nevoie să se evalueze în continuare dacă îndeplinește un obiectiv de interes general și satisface criteriile de necesitate și proporționalitate.

Exemplu: Cauza *Schrems*[62] s-a referit la protecția persoanelor cu privire la transferul datelor cu caracter personal către țări terțe - în acest caz, Statele Unite. Schrems, cetățean austriac, care a fost utilizator Facebook de câțiva ani, a depus o plângere la autoritatea irlandeză de supraveghere a protecției datelor pentru a denunța transferul datelor sale personale de la filiala irlandeză Facebook către Facebook Inc. și la serverele din SUA, unde au fost prelucrate. El a susținut că, în lumina dezvăluirilor din 2013 de către Edward Snowden, un avertizor american, cu privire la activitățile de supraveghere ale serviciilor de supraveghere din SUA, legea și practica SUA nu oferă o protecție suficientă datelor personale transferate pe teritoriul SUA. Snowden a dezvăluit că Agenția Națională de Securitate a accesat direct serverele firmelor, cum ar fi Facebook, și putea citi conținutul chat-urilor și mesajelor private.

Transferurile de date către SUA s-au bazat pe o decizie a Comisiei privind compatibilitatea, adoptată în 2000, care permitea transferuri companiilor americane care au garantau că ar proteja datele personale transferate din UE și ar respecta așa-numitele "principii Safe Harbor". Atunci când cauza a fost introdusă în CJUE, aceasta a examinat validitatea deciziei Comisiei în lumina Cartei. Aceasta a reamintit că protecția drepturilor fundamentale în UE necesită derogări și limitări ale acestor drepturi pentru a se aplica numai în măsura în care acest lucru este strict necesar. CJUE a examinat legislația care permite autorităților publice să acceseze, în general, conținutul comunicațiilor electronice, "compromițând esența dreptului fundamental la respectarea vieții private, garantat de articolul 7 din Cartă". Dreptul ar deveni lipsit de sens dacă autoritățile publice americane au fost autorizate să acceseze comunicările ocazional, fără o justifi-

62 Hotărârea CJUE din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/ Comisarul pentru protecția datelor.*

care obiectivă bazată pe considerente concrete de securitate națională sau de prevenire a criminalității care sunt specifice fiecărei persoane și fără ca aceste practici de supraveghere să fie însoțite de garanții adecvate împotriva abuzului de putere.

Mai mult, CJUE a observat că "legislația care nu prevede posibilitatea unei persoane de a urmări căi de atac pentru a avea acces la datele cu caracter personal care o privesc sau pentru a obține rectificarea sau ștergerea acestor date" este incompatibilă cu dreptul fundamental de protecție judecătorească eficientă (articolul 47 din Cartă). Astfel, decizia "Safe Harbor" nu a reușit să asigure un nivel de protecție a drepturilor fundamentale acordat de SUA esențial echivalent cu cel garantat în cadrul UE în temeiul directivei, interpretat în lumina Cartei. Ca urmare, CJUE a anulat decizia.[63]

Exemplu: În cauza *Drepturi digitale Irlanda*,[64] CJUE a examinat compatibilitatea Directivei 2006/24/CE (Directiva privind păstrarea datelor) cu articolele 7 și 8 din Cartă. Directiva a obligat furnizorii de servicii de comunicații electronice să păstreze datele privind traficul și localizarea timp de cel puțin șase luni, până la 24 de luni și să permită autorităților naționale competente accesul la aceste date în scopul prevenirii, investigării, depistării și urmăririi penale a infracțiunilor grave. Directiva nu permite conservarea conținutului comunica-țiilor electronice. CJUE a constatat că datele pe care furnizorii au trebuit să le păstreze în conformitate cu directiva au inclus date necesare pentru urmărirea și identificarea sursei și destinației unei comunicări, data, ora și durata unei comunicări, numărul apelantului, numerele apelate și adresele IP. Aceste date "luate în ansamblul lor pot permite să se tragă concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, cum ar fi obiceiurile de zi cu zi, locurile de ședere permanente sau temporare, mișcările zilnice sau de altă natură, activitățile desfășurate, relațiile sociale ale acelor persoane și mediile sociale frecventate de acestea".

63 Decizia CJUE de anulare a Deciziei 520/2000/CE a Comisiei s-a bazat și pe alte motive care vor fi examinate în alte secțiuni ale acestui manual. În special, CJUE a considerat că decizia a limitat în mod ilegal competențele autorităților naționale de supraveghere a protecției datelor. În plus, în cadrul regimului Safe Harbor nu existau căi de atac pentru persoanele fizice în cazul în care acestea doresc să acceseze datele cu caracter personal care le privesc și/sau să obțină rectificarea sau ștergerea acestora. Astfel, esența dreptului fundamental la protecție jurisdicțională efectivă, consacrată în articolul 47 din Cartă, a fost, de asemenea, compromisă.

64 Hotărârea CJUE din 8 aprilie 2014, în cauzele conexate C-293/12 şi C-594/12, *Drepturi digitale Irlanda Ltd/ Ministerul Comunicaţiilor, Marinei şi a Resurselor Naturale şi alţii şi Kärntner Landesregierung şi alţii*.

Astfel, păstrarea datelor cu caracter personal în conformitate cu directiva a reprezentat o interferență deosebit de gravă a drepturilor la viața privată și la protecția datelor cu caracter personal. Cu toate acestea, CJUE a considerat că interferența nu a afectat în mod deosebit esența acestor drepturi. În ceea ce privește dreptul la viață privată, esența sa nu a fost compromisă deoarece directiva nu permitea dobândirea de cunoștințe despre conținutul comunicațiilor electronice ca atare. În mod similar, esența dreptului la protecția datelor cu caracter personal nu a fost compromisă, deoarece directiva impunea furnizorilor de servicii de comunicații electronice să respecte anumite principii privind protecția și securitatea datelor și să pună în aplicare măsuri tehnice și organizatorice adecvate în acest scop.

Necesitate şi proporţionalitate

Articolul 52 alineatul (1) din Cartă prevede că, sub rezerva principiului proporționalității, limitările exercitării drepturilor și libertăților fundamentale recunoscute de Cartă se pot face numai dacă sunt necesare.

O limitare poate fi **necesară** dacă trebuie să se adopte măsuri pentru obiectivul de interes public urmărit - dar necesitatea, astfel cum a fost interpretată de CJUE, presupune de asemenea ca măsurile să fie mai puțin invazive în comparație cu alte opțiuni pentru atingerea aceluiași obiectiv. În ceea ce privește limitarea drepturilor la respectarea vieții private și protecția datelor cu caracter personal, CJUE aplică un test strict de necesitate, considerând că "derogațiile și limitările trebuie să se aplice numai în măsura în care sunt strict necesare". Dacă o limitare este considerată strict necesară, trebuie să se evalueze dacă este proporțională.

Proporţionalitatea înseamnă că avantajele care rezultă din limitare ar trebui să depășească dezavantajele pe care aceasta din urmă le provoacă în exercitarea drepturilor fundamentale în cauză.[65] Pentru a reduce dezavantajele și riscurile pentru exercitarea drepturilor la confidențialitate și la protecția datelor, este important ca limitările să conțină garanții potrivite.

65 AEPD (2017), *Set de instrumente pentru necesități*, pagina 5.

Exemplu: În cauza *Volker und Markus Schecke*[66], CJUE a concluzionat că, prin impunerea obligației de a publica date cu caracter personal referitoare la fiecare persoană fizică care a beneficiat de un ajutor din partea anumitor fonduri agricole, fără a face o distincție pe baza unor criterii relevante, cum ar fi perioadele în care au primit acel ajutoar, frecvența sau natura unui astfel de ajutor și valoarea acestuia, Consiliul și Comisia au depășit limitele impuse de principiul proporționalității.

Prin urmare, CJUE a considerat necesar să declare invalide anumite dispoziții ale Regulamentului (CE) nr. 1290/2005 al Consiliului și să declare că Regulamentul nr. 259/2008 este nevalid în întregime.[67]

Exemplu: În cauza *Drepturi digitale Irlanda*,[68] CJUE a considerat că interferența cu dreptul la confidențialitate cauzată de Directiva privind păstrarea datelor nu a compromis esența acestui drept, deoarece interzice păstrarea conținutului comunicațiilor electronice. Cu toate acestea, Comisia a concluzionat că directiva era incompatibilă cu articolele 7 și 8 din Cartă și a declarat că este nevalidă. Datorită faptului că datele privind traficul și localizarea, reunite și luate în ansamblu, ar putea fi analizate și ar descrie o imagine detaliată a vieții private a persoanelor, aceasta a reprezentat o interferență gravă a acestor drepturi. CJUE a luat în considerare faptul că directiva a impus menținerea tuturor metadatelor privind telefonia fixă, telefonia mobilă, accesul la internet, e-mailul prin internet și telefonia prin internet, care se aplică tuturor mijloacelor de comunicare electronică - a căror utilizare este foarte răspândită în viața de zi cu zi a oamenilor. Practic, a constituit o interferență care a afectat întreaga populație europeană. Având în vedere amploarea și gravitatea acestei interferențe, păstrarea datelor privind traficul și localizarea datelor ar putea fi, în opinia CJUE, justificată doar în scopul combaterii infracțiunilor grave. În plus, directiva nu a stabilit criterii obiective care să garanteze că accesul autorităților naționale competente la datele păstrate este limitat la ceea ce este strict necesar.

66 Hotărârea CJUE din 9 noiembrie2010, în cauzele conexate C-92/09 şi C-93/09, *Volkerund Markus Schecke GbR şi Hartmut Eifert/ Hessa*, punctele 89 şi 86.

67 Regulamentul Consiliului(CE) nr. 1290/2005 din 21 iunie 2005 privind finanțarea politicii agricole comune, MO L 209, 2005; Regulamentul Comisiei (CE) nr. 259/2008 din 18 martie 2008 de stabilire a normelor de aplicare a Regulamentului Consiliului (CE) nr. 1290/2005 în ceea ce privește publicarea informațiilor referitoare la beneficiarii fondurilor provenind din Fondul European de Garantare Agricolă (FEGA) și Fondul european agricol pentru dezvoltare rurală (FEADR), MO 2008 L76.

68 Hotărârea CJUE din 8 aprilie 2014, în cauzele conexate C-293/12 şi C-594/12, *Drepturi digitale Irlanda Ltd/ Ministerul Comunicaţiilor, Marineişi a Resurselor Naturale şi alţii şi Kärntner Landesregierung şi alţii*, punctul 39.

În plus, aceasta nu conținea condiții materiale și proceduri care să reglementeze accesul și utilizarea datelor reținute de autoritățile naționale, care nu au făcut obiectul unei revizuiri prealabile a unei instanțe sau a unui alt organism independent.

CJUE a ajuns la o concluzie similară cauzelor conexate *Tele2 Sverige AB/Post-och telestryrelsen şi Secretarul de stat/Tom Watson şi alţii*.[69] Acestea au vizat păstrarea datelor privind traficul și localizarea "tuturor abonaților și utilizatorilor înregistrați și toate mijloacele de comunicații electronice, precum și metadatele "fără" o diferențiere, o limitare sau o excepție în funcție de obiectivul urmărit".[70] În cazul de față, dacă o persoană a fost sau nu legată direct sau indirect de infracțiuni grave, sau dacă comunicările sale erau sau nu relevante pentru securitatea națională, nu era o condiție pentru păstrarea datelor lor. Având în vedere absența unei legături necesare între datele păstrate și o amenințare la adresa siguranței publice, a restricțiilor de timp sau de zonă geografică, CJUE a concluzionat că legislația națională a depășit limitele a ceea ce era strict necesar pentru combaterea criminalităţii.[71]

O abordare similară, în ceea ce privește necesitatea, este luată de Autoritatea Europeană pentru Protecția Datelor în *Setul de instrumente pentru necesități*.[72] Setul de instrumente își propune să contribuie la evaluarea conformității măsurilor propuse cu legislația UE privind protecția datelor. Acesta a fost dezvoltat pentru a dota mai bine pe factorii de decizie din UE și pe legislatorii responsabili cu pregătirea sau controlul măsurilor care implică prelucrarea datelor cu caracter personal și limitarea dreptului la protecția datelor cu caracter personal și a altor drepturi și libertăți stabilite în Cartă.

Obiective de interes general

Pentru a fi justificată, orice limitare a exercitării drepturilor recunoscute de Cartă trebuie, de asemenea, să respecte cu adevărat obiectivele de interes general recunoscute de Uniune sau necesitatea de a proteja drepturile și libertățile altor persoane. În ceea ce privește necesitatea de a proteja drepturile și libertățile celorlalți, dreptul la protecție a datelor personale interacționează adesea cu alte drepturi fundamentale. Secțiunea 1.3 oferă o analiză detaliată a acestor interacțiuni. În ceea ce privește obiectivele de interes general, acestea includ

69 Hotărârea CJUE din 21 decembrie 2016, în cauzele conexate C-203/15 şi C-698/15, *Tele2 Sverige AB/ Post-ochtelestryrelsen şi Secretarul de Stat al Departamentului Local/ Tom Watson şi alţii*, punctele 105–106.

70 *Ibidem*, punctul 105.

71 *Ibidem*, punctul 107.

72 AEPD (2017), *Set de instrumente pentru necesități*, Bruxelles,11 aprilie 2017.

obiectivele generale ale UE conform articolului 3 din Tratatul privind Uniunea Europeană (TUE), cum ar fi promovarea păcii și a bunăstării statelor, justiția și protecția socială și stabilirea unui spațiu de libertate, securitatea și justiția în care se asigură libera circulație a persoanelor, împreună cu măsurile adecvate de prevenire și combatere a criminalității, precum și alte obiective și interese protejate prin dispoziții specifice ale tratatului.[73] Regulamentul general privind protecția datelor specifică în continuare articolul 52 alineatul 1) din Cartă în această privință: articolul 23 alineatul (1) din regulament enumeră o serie de obiective de interes general considerate legitime pentru limitarea drepturilor persoanelor, cu condiția ca această limitare să respecte esența dreptului la protecția datelor cu caracter personal, să fie necesară și proporțională. Securitatea și apărarea națională, prevenirea criminalității, protejarea intereselor economice și financiare importante ale UE sau ale statelor membre, sănătatea publică și securitatea socială se numără printre obiectivele de interes public menționate în cuprinsul acestuia.

Este important să se definească și să se explice suficient de detaliat obiectivul de interes general urmărit de limitare, deoarece necesitatea limitării va fi evaluată în acest context. O descriere clară și detaliată a obiectivului limitării și a măsurilor propuse este esențială pentru a permite evaluarea necesității acesteia.[74] Obiectivul urmărit, necesitatea și proporționalitatea limitării sunt strâns legate.

Exemplu: Cauza *Schwarz/Stadt Bochum*[75] se referă la limitările privind dreptul la respectarea vieții private și dreptul la protecția datelor cu caracter personal care rezultă din preluarea și stocarea amprentelor digitale atunci când autoritățile statului membru emite pașapoarte.[76] Reclamantul a solicitat Stadt Bochum un pașaport, dar a refuzat să-și dea amprentele; după aceasta, Stadt Bochum a refuzat cererea sa de emitere a pașaportului. Apoi a introdus o acțiune în fața unei instanțe germane pentru a obține un pașaport eliberat fără ca amprentele să fie luate. Instanța germană a sesizat CJUE cu privire la întrebarea dacă articolul 1 alineatul (2) din Regulamentul 2252/2004 privind standardele pentru elementele de securitate și biometrice din pașapoarte și documente de călătorie emise de statele membre trebuie considerate valabile.

73 Explicaţii referitoare la Carta Drepturilor Fundamentale (2007/C303/02), JO2007, nr. C303, pagina 17–35.

74 AEPD (2017), *Set de instrumente pentru necesități*, Bruxelles, 11 aprilie 2017, pagina 4.

75 Hotărârea CJUE din 17 octombrie 2013, în cauza C-291/12, *Michael Schwarz/ Stadt Bochum*.

76 *Ibidem*, punctele 33–36.

CJUE a subliniat faptul că amprentele digitale constituie date cu caracter personal, deoarece conțin obiecte unice despre persoane care le permite să fie identificate cu precizie, în timp ce luarea și stocarea amprentelor digitale constituie prelucrare. Această prelucrare, care este reglementată de articolul 1 alineatul (2) din Regulamentul nr. 2252/2004, constituie o amenințare la adresa respectării vieții private și a protecției datelor personale.[77] Cu toate acestea, articolul 52 alineatul (1) din Cartă permite limitările exercitării acestor drepturi, atât timp cât aceste limitări sunt prevăzute de lege, respectă esența acestor drepturi și, în conformitate cu principiul proporționalității, sunt necesare și întrunesc cu adevărat obiectivele de interes general recunoscute de Uniune sau trebuie să protejeze drepturile și libertățile celorlalți.

În cazul de față, CJUE a constatat mai întâi că limitarea care rezultă din preluarea și stocarea amprentelor digitale la eliberarea pașapoartelor trebuie să fie considerată prevăzută de lege, deoarece aceste operațiuni sunt prevăzute în articolul 1 alineatul (2) din Regulamentul nr. 2252/2004. În al doilea rând, ultimul regulament a fost conceput pentru a împiedica falsificarea pașapoartelor și utilizarea lor frauduloasă. Astfel, articolul 1 alineatul (2) este prevăzut pentru a împiedica, printre altele, intrarea ilegală în UE, urmărind astfel un obiectiv de interes general recunoscut de Uniune. În al treilea rând, din elementele de probă aflate la dispoziția CJUE nu s-a evidențiat și nici nu s-a afirmat că limitările în exercitarea acestor drepturi în cazul de față nu au respectat esența acestor drepturi. În al patrulea rând, stocarea amprentelor pe un mediu de stocare extrem de sigur, astfel cum este prevăzut de această dispoziție, necesită o tehnologie sofisticată. O astfel de depozitare ar putea reduce riscul de falsificare a pașapoartelor și ar facilita activitatea autorităților responsabile de verificare a autenticității pașapoartelor la frontierele UE. Faptul că metoda nu este pe deplin fiabilă, nu este decisivă. Deși metoda nu împiedică acceptarea tuturor persoanelor neautorizate, este suficient să reducă în mod semnificativ probabilitatea unei astfel de acceptări. În lumina celor de mai sus, CJUE a constatat că preluarea și stocarea amprentelor digitale menționate la articolul 1 alineatul (2) din Regulamentul nr. 2252/2004 a fost adecvată pentru atingerea obiectivelor urmărite de regulamentul menționat și, prin extindere, a obiectivului de prevenire a intrării ilegale în UE.[78]

În continuare, CJUE a evaluat necesitatea unei astfel de prelucrări, menționând că acțiunea în cauză nu implică decât imprimarea a două dege-

77 *Ibidem*, punctele 27–30.

78 *Ibidem*, punctele 35–45.

te, care, în plus, pot fi văzute de alții, astfel încât aceasta să nu fie o operație de natură intimă. Imprimarea nu provoacă nici un disconfort fizic sau mental deosebit persoanei implicate decât atunci când este luată imaginea facială a acesteia. De asemenea, trebuie remarcat faptul că singura alternativă reală la luarea amprentelor digitale în cursul procedurii în fața CJUE a fost o scanare a irisului. Nimic din dosarul prezentat CJUE nu a sugerat că procedura din urmă ar interveni mai puțin în drepturile recunoscute prin articolele 7 și 8 din Cartă decât în cazul luării amprentelor digitale. În plus, în ceea ce privește eficacitatea acestor două metode, este cert că tehnologia de recunoaștere a irisului nu este încă la fel de avansată ca cea de recunoaștere a amprentelor digitale, este în prezent semnificativ mai costisitoare decât procedura de comparare a amprentelor digitale și, din acest motiv, mai puțin potrivită pentru uz general. În consecință, CJUE nu a fost informată cu privire la măsurile care ar fi suficient de eficiente pentru a contribui la atingerea obiectivului de protecție împotriva utilizării frauduloase a pașapoartelor și mai puțin la adresa unei amenințări a drepturilor recunoscute prin articolele 7 și 8 din Cartă decât măsurile care decurg din metoda bazată pe utilizarea amprentelor digitale.[79]

CJUE a constatat că articolul 4 alineatul (3) din Regulamentul nr. 2252/2004 prevede în mod explicit că amprentele digitale pot fi utilizate numai pentru verificarea autenticității unui pașaport și a identității titularului acestuia, în timp ce articolul 1 alineatul (2) din regulament nu prevede stocarea amprentelor digitale, cu excepția pașaportului propriu-zis, care aparține titularului. Astfel, regulamentul nu a constituit un temei juridic pentru stocarea centralizată a datelor colectate în temeiul acestora sau pentru utilizarea acestor date în alte scopuri decât cele de prevenire a intrării ilegale în UE.[80] Având în vedere toate considerațiile de mai sus, CJUE a concluzionat că examinarea întrebării preliminare nu a evidențiat că ar putea afecta validitatea articolului 1 alineatul (2) din Regulamentul nr. 2252/2004.

Relaţia dintre Cartă şi CEDO

În ciuda implicării diferitelor formulare, condițiile de limitare legală a drepturilor prevăzute la articolul 52 alineatul (1) din Cartă amintesc de articolul 8 alineatul (2) din CEDO privind dreptul la respectarea vieții private. În jurisprudența lor, CJUE și CEDO se referă adesea la hotărârile celorlalți, ca parte a dialogului constant dintre cele două instanțe de a căuta o interpretare armonioasă a normelor privind protecția datelor. Articolul 52 (3) alineatul (3) din Cartă preve-

79 Hotărea CJUE din 17 octombrie 2013 în cauza C-291/12, *Michael Schwarz/Stadt Bochum*, punctele46–53.

80 *Ibidem*, punctele 56–61.

de că "în măsura în care această Cartă conține drepturi care corespund drepturilor garantate de Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, semnificația și domeniul de aplicare a acestor drepturi sunt la fel ca cele prevăzute de convenția menționată ". Cu toate acestea, articolul 8 din Cartă nu corespunde în mod direct unui articol din CEDO.[81] Articolul 52 alineatul (3) din Cartă se referă mai degrabă la conținutul și domeniul de aplicare a drepturilor protejate de fiecare ordine juridică decât la condițiile de limitare a acestora. Cu toate acestea, având în vedere contextul mai larg al dialogului și cooperării dintre cele două instanțe, CJUE poate lua în considerare în analizele sale criteriile de limitare legală în temeiul articolului 8 din CEDO, astfel cum au fost interpretate de CEDO. Este posibil, de asemenea, scenariul opus, prin care Curtea Europeană a Drepturilor Omului se poate referi la condițiile de limitare legală din cadrul Cartei. În orice caz, trebuie de asemenea să se țină seama de faptul că în CEDO nu există un echivalent perfect al articolului 8 din Cartă, care se referă la protecția datelor cu caracter personal și, în special, la drepturile persoanei vizate, la motivele legale de prelucrare și supraveghere de către o autoritate independentă. Unele componente ale articolului 8 din Cartă pot fi întemeiate în jurisprudența Curții Europene de Justiție elaborată în temeiul articolului 8 din CEDO și referitoare la Convenția 108.[82] Această legătură asigură existența unei inspirații reciproce între CJUE și CEDO în chestiuni legate de protecția datelor.

1.3. Interacţiunea cu alte drepturi şi interese legitime

Puncte-cheie

- Dreptul la protecția datelor interacționează adesea cu alte drepturi, cum ar fi libertatea de exprimare și dreptul de a primi și de a transmite informații.
- Această interacțiune este adesea ambivalentă: în timp ce există situații în care dreptul la protecția datelor personale este în conflict cu un anumit drept, există, de asemenea, situații în care dreptul la protecția datelor cu caracter personal asigură în mod efectiv respectarea aceluiași drept specific. De exemplu, acesta este cazul libertății de exprimare, dat fiind faptul că secretul profesional este o componentă a dreptului la respectarea vieții private.
- Necesitatea de a proteja drepturile și libertățile celorlalți este unul dintre criteriile utilizate pentru evaluarea limitării legale a dreptului la protecția datelor cu caracter personal.

81 AEPD (2017), *Set de instrumente pentru necesități*, Bruxelles,11 aprilie 2017, pagina 6.

82 Explicaţii referitoare la Carta Drepturilor Fundamentale (2007/C303/02), articolul 8.

- Atunci când sunt în joc diferite drepturi, instanțele trebuie să efectueze un exercițiu de echilibrare pentru a le reconcilia.
- Regulamentul general privind protecția datelor solicită statelor membre să echilibreze dreptul la protecția datelor cu caracter personal cu libertatea de exprimare și de informare.
- Statele membre pot, de asemenea, să adopte norme specifice în legislația națională pentru a echilibra dreptul la protecția datelor cu caracter personal cu accesul public la documentele și obligaţiile oficiale ale secretului profesional.

Dreptul la protecția datelor cu caracter personal nu este un drept absolut; condițiile de limitare legală ale acestui drept au fost detaliate mai sus. Unul dintre criteriile pentru limitările legale ale drepturilor, recunoscute atât în cadrul CoE, cât și al legislației UE, este că interferența cu protecția datelor este necesară pentru protejarea drepturilor și libertăților celorlalți. În cazul în care protecția datelor interacționează cu alte drepturi, atât CEDO, cât și CJUE au declarat în mod repetat că un exercițiu de echilibrare cu alte drepturi este necesar atunci când se aplică și interpretează articolul 8 din CEDO și articolul 8 din Cartă.[83] Mai multe exemple importante vor ilustra modul în care echilibrul este atins.

Pe lângă exercițiul de echilibrare efectuat de aceste instanțe, statele pot, dacă este necesar, să adopte o legislație care să reconcilieze dreptul la protecția datelor cu caracter personal cu alte drepturi. Din acest motiv, Regulamentul general privind protecția datelor furnizează o serie de domenii de derogare naționale.

În ceea ce privește libertatea de exprimare, RGPD cere statelor membre să reconcilieze, prin lege, "dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament cu dreptul la libertatea de exprimare și de informare, inclusiv prelucrarea în scopuri jurnalistice și academice, artistice sau literare"[84]. Statele membre pot, de asemenea, să adopte legi pentru a reconcilia protecția datelor cu accesul publicului la documentele și obligațiile oficiale privind secretul profesional protejate ca o formă a dreptului la respectarea vieții private.[85]

83 Hotărârea CtEDO nr. 40660/08 şi 60641/08, din 7 februarie 2012, în cauza *VonHannover/ Germania (nr.2)*; Hotărârea CJUE din 24 noiembrie 2011, în cauzele conexate C-468/10 şi C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) şi Federación de Comercio Electrónico y Marketing Directo(FECEMD)/ Administración del Estado*, punctul 48; Hotărârea CJUE din 29 ianuarie 2008, în cauza C-275/06, *Productores de Música de España(Promusicae)/ Telefónica de España SAU*, punctul 68.

84 Regulamentul general privind protecţia datelor, articolul 85.

85 *Ibidem*, articolele 86 şi 90.

1.3.1. Libertatea de exprimare

Unul din drepturile care interacționează cel mai mult cu dreptul la protecția datelor este dreptul la libertatea de exprimare.

Libertatea de exprimare este protejată de articolul 11 din Cartă ("Libertatea de exprimare și de informare"). Acest drept include "libertatea de a avea opinii, de a primi și de a transmite informații și idei fără ca autoritatea publică să intervină și indiferent de limitări". Conform articolului 11 din Cartă și articolului 10 din CEDO, libertatea de informare protejează atât dreptul de a transmite, cât și de a primi informații.

Limitările privind libertatea de exprimare trebuie să respecte criteriile prevăzute la articolul 52 alineatul (1) din Cartă, descrise mai sus. În plus, articolul 11 corespunde articolului 10 din CEDO. În conformitate cu articolul 52 alineatul (3) din Cartă, în măsura în care conține drepturi care corespund drepturilor garantate de CEDO, "semnificația și domeniul de aplicare al acestor drepturi sunt aceleași cu cele prevăzute de convenția menționată". Așadar, limitările care pot fi impuse în mod legal asupra dreptului garantat de articolul 11 din Cartă nu pot să depășească cele prevăzute la articolul 10 alineatul (2) din CEDO, adică trebuie să fie prevăzute de lege și să fie necesare într-o societatea democratică "pentru protecția [...] reputaţiei sau a drepturilor altora". Aceste drepturi cuprind, în special, dreptul la respectarea vieții private și la protecția datelor cu caracter personal.

Relația dintre protecția datelor cu caracter personal și libertatea de exprimare este reglementată de articolul 85 din Regulamentul general privind protecția datelor, intitulat "Prelucrarea și libertatea de exprimare și de informare". În conformitate cu acest articol, statele membre trebuie să echilibreze dreptul la protecția datelor cu caracter personal cu dreptul la libertatea de exprimare și de informare. Exceptările și derogările din capitolele specifice ale Regulamentului general privind protecția datelor se fac în special în scopuri juralistice sau în scopuri de exprimare academică, artistică sau literară, în măsura în care acestea sunt necesare pentru a reconcilia dreptul la protecția datelor personale cu libertatea de exprimare și de informare.

Exemplu: În cauza *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy și Satamedia Oy*[86], CJUE i s-a cerut să definească relația dintre protecția datelor

86 Hotărârea CJUE din 16 decembrie 2008, în cauza C-73/07, *Tietosuojavaltuutettu/ Satakunnan Markkinapörssi Oy și Satamedia Oy*, punctele 56, 61 şi 62.

și libertatea presei.[87] CJUE a trebuit să examineze difuzarea, printr-un serviciu SMS, a datelor a aproximativ 1,2 milioane de persoane fizice, obținute în mod legal de la autoritățile fiscale finlandeze. Autoritatea de supraveghere a protecției datelor finlandeze a emis o decizie prin care solicită companiei să oprească difuzarea acestor date. Compania a contestat această decizie într-o instanță națională, care a solicitat clarificări din partea CJUE privind interpretarea directivei asupra protecției datelor. CJUE a trebuit să verifice dacă prelucrarea datelor cu caracter personal, pe care autoritățile fiscale le-a pus la dispoziție pentru a permite utilizatorilor de telefonie mobilă să primească date fiscale referitoare la alte persoane fizice, trebuie considerată o activitate desfășurată exclusiv în scopuri jurnalistice. După ce a concluzionat că activitățile societății erau "prelucrarea datelor cu caracter personal" în sensul articolului 3 alineatul (1) din Directiva privind protecția datelor, CJUE a analizat articolul 9 din directivă (privind prelucrarea datelor cu caracter personal și libertatea de exprimare). Aceasta a remarcat mai întâi importanța dreptului la libertatea de exprimare în fiecare societate democratică și a considerat că noțiunile legate de această libertate, cum ar fi jurnalismul, ar trebui interpretate pe larg. Apoi, a observat că, pentru a realiza un echilibru între cele două drepturi fundamentale, derogările și limitările dreptului la protecția datelor trebuie să se aplice numai în măsura în care acest lucru este absolut necesar. În aceste condiții, CJUE a considerat că activități precum cele desfășurate de societățile în litigiu referitoare la date din documente care aparțin domeniului public în temeiul legislației naționale pot fi clasificate drept "activități jurnalistice" în cazul în care obiectivul lor este divulgarea către public de informații, opinii sau idei, indiferent de mediul folosit pentru a le transmite. De asemenea, a hotărât că aceste activități nu se limitează la întreprinderile media și pot fi întreprinse în scopuri profitabile. Cu toate acestea, CJUE a lăsat la alegerea instanței naționale să decidă verdictul final.

Același caz a fost examinat de CEDO, după ce instanța națională a decis, pe baza îndrumărilor CJUE, că ordinul autorității de supraveghere de a întrerupe publicarea tuturor informațiilor fiscale a constituit o interferență justificată a libertății de exprimare a companiei. CEDO a susținut această abordare.[88] Aceasta a constatat că, deși a existat o interferență a dreptului societății de a transmite informații, interferenţa

87 Cazul viza interpretarea Directivei privind protecția datelor, art. 9 - înlocuit acum de art. 85 din regulamentul general privind protecția datelor - care prevede: "Statele membre prevăd scutiri sau derogări de la dispozițiile prezentului capitol, capitolul IV și capitolul VI, privind prelucrarea datelor cu caracter personal efectuate exclusiv în scopuri jurnalistice sau în scopuri artistice sau exprimare literară numai dacă acestea sunt necesare pentru a concilia dreptul la viață privată cu regulile care reglementează libertatea de exprimare".

88 Hotărârea CtEDO nr. 931/13 din 27 iunie 2017, în cauza *Satakunnan Markkinapörssi Oy și Satamedia Oy/ Finlanda*.

era în conformitate cu legea, urmărea un scop legitim şi era necesară într-o societate democratică.

Curtea a reamintit criteriile de jurisprudență care ar trebui să ghideze autoritățile naționale și chiar CEDO, atunci când echilibrează libertatea de exprimare cu dreptul la respectarea vieții private. Atunci când sunt în joc discursul politic sau o dezbatere cu privire la o chestiune de interes public, există puține posibilități de restricționare a dreptului de a primi și de a transmite informații, întrucât publicul are dreptul de a fi informat, "acesta fiind un drept esențial într-o societate democratică".[89] Cu toate acestea, se poate considera că articolele de presă destinate exclusiv satisfacerii curiozității unui anumit cititor în privința detaliilor vieții private a unei persoane contribuie la o dezbatere de interes public. Derogarea de la normele de protecție a datelor în scopuri jurnalistice urmărește să permită jurnaliștilor să acceseze, să colecteze și să prelucreze date pentru a-şi putea desfășura activitățile. Astfel, a existat întradevăr un interes public de a oferi acces și de a permite societăților reclamante să colecteze și să proceseze cantități mari de date fiscale. În schimb, Curtea a constatat că nu există niciun interes public pentru difuzarea în masă a unor astfel de date brute de către presă, sub formă nemodificată și fără o contribuție analitică. Informațiile despre impozitare ar fi permis membrilor curioși ai publicului să clasifice indivizii în funcție de statutul lor economic și să satisfacă setea publicului pentru informații despre viața privată a altor persoane. Acest lucru nu poate fi considerat că ar contribui la o dezbatere de interes public.

Exemplu: În cauza *Google Spania*,[90] CJUE a analizat dacă Google ar putea fi obligat să şteargă informațiile depășite cu privire la dificultățile financiare ale solicitantului din rezultatele listei de căutare. Atunci când a fost efectuată o căutare pe motorul de căutare Google folosind numele solicitantului, rezultatele căutării au furnizat legături către articole vechi din ziare care menționează legătura sa cu procedura de faliment. Reclamantul a considerat că aceasta este o încălcare a drepturilor sale la respectarea vieții private și a protecției datelor cu caracter personal, deoarece procedurile au fost încheiate cu ani în urmă, făcând astfel de referințe irelevante.

CJUE a clarificat mai întâi dacă motoarele de căutare pe internet și rezultatele căutării care furnizează date cu caracter personal pot stabili un profil detaliat al unui individ. În lumina unei societăți din ce în ce mai digitiza-

89 *Ibidem*, punctul 169.

90 Hotărârea CJUE din 13 mai 2014, în cauza C-131/12, *Google Spain SL,Google Inc./ Agencia Española de Protección de Datos(AEPD), Mario Costeja González*, punctele 81-83.

te, cerința ca datele cu caracter personalsă fie exacte și publicarea acestora să nu depășească ceea ce este necesar, de exemplu să ofere informații publicului, este esențială pentru asigurarea unui nivel ridicat de protecție a datelor pentru persoane fizice. "În ceea ce privește prelucrarea respectivă, inspectorul trebuie să asigure, prin natura responsabilităților sale, competențe și capacități, astfel încât prelucrarea să respecte cerințele" legislaţiei UE, pentru ca garanțiile juridice stabilite să aibă efect deplin. Aceasta înseamnă că dreptul de a șterge datele cu caracter personal atunci când procesarea nu mai este necesară sau învechită acoperă și motoarele de căutare care s-au dovedit a fi inspectori, nu doar procesatori (a se vedea Secțiunea 2.3.1).

La examinarea faptului dacă Google ar fi obligat să elimine legăturile legate de solicitant, CJUE a afirmat că, în anumite condiții, indivizii au dreptul să obțină ștergerea datelor lor personale din rezultatele căutării unui motor de căutare pe internet. Acest drept poate fi invocat în cazul în care informațiile referitoare la o persoană sunt inexacte, inadecvate, irelevante sau excesive în scopul prelucrării datelor. CJUE a recunoscut că acest drept nu este absolut; trebuie să fie echilibrat cu alte drepturi, în special cu interesul și dreptul publicului larg de a avea acces la informații. Fiecare cerere de ștergere necesită o evaluare de la caz la caz pentru a găsi un echilibru între drepturile fundamentale la protecția datelor cu caracter personal și viața privată a persoanei vizate, pe de o parte, și interesele legitime ale tuturor utilizatorilor de internet, pe de altă parte. CJUE a furnizat îndrumări cu privire la factorii care trebuie luați în considerare în timpul exercițiului de echilibrare. Natura informațiilor în cauză este un factor deosebit de important. Dacă informațiile fac referire la viața privată a persoanei și în cazul în care nu există niciun interes public în ceea ce privește disponibilitatea informațiilor, protecția datelor și viața privată ar depăși dreptul publicului larg de a avea acces la informații. Dimpotrivă, în cazul în care se pare că persoana vizată este o persoană publică sau că informațiile sunt de natură să justifice acordarea accesului publicului larg la astfel de informații, interferența cu drepturile fundamentale la protecția datelor și la viața privată este justificată.

Ca urmare a hotărârii, grupul de lucru în temeiul Articolului 29 a adoptat îndrumări privind punerea în aplicare a hotărârii CJUE. Îndrumările includ o listă de criterii comune care trebuie utilizate de autoritățile de supraveghere atunci când se ocupă de reclamațiile legate de cererile de eliminare ale persoanelor fizice și de a le îndruma în acest exercițiu de echilibrare a drepturilor.[91]

91 Grupul de lucru Articolul 29 (2014), *Îndrumări privind punerea în aplicare a hotărârii CJUE în cauza "Google Spain şi Inc/ Agencia Española de Protección de Datos (AEPD) şi Mario Costeja González" C-131/12*, WP225, Bruxelles, 26 noiembrie 2014.

În ceea ce privește reconcilierea dreptului la protecția datelor cu dreptul la libertatea de exprimare, CEDO a emis mai multe hotărâri punctuale.

Exemplu: În cauza *Axel Springer AG/ Germania*,[92] CEDO a considerat că o interdicție care împiedică societatea reclamantă să publice un articol privind arestarea și condamnarea unui actor binecunoscut a încălcat articolul 10 al CEDO. CEDO a reiterat criteriile care trebuie luate în considerare la echilibrarea dreptului la libertatea de exprimare împotriva dreptului la respectarea vieții private, astfel cum este stabilit în jurisprudența sa:

- dacă publicarea articolului în cauză a fost de interes general;
- dacă persoana în cauză a fost o persoană publică; și
- modul în care au fost obținute informațiile și dacă acestea au fost de încredere.

CEDO a constatat că arestarea și condamnarea actorului a fost un fapt judiciar public și, prin urmare, era de interes public; actorul era suficient de bine cunoscut pentru a se califica drept o figură publică; informațiile au fost furnizate de procuratură și acuratețea acestora nu a fost contestată de părți. Prin urmare, restricțiile de publicare impuse societății nu au fost în mod rezonabil proporționale cu scopul legitim de a proteja viața privată a reclamantului. Curtea a concluzionat că a avut loc o încălcare a articolului 10 din CEDO.

Exemplu: Cauza *Coudec și Hachette Filipacchi Associés/ Franța*[93] a vizat publicarea de către o revistă săptămânală franceză a unui interviu cu doamna Coste, care a susținut că prințul Albert al Monacoului era tatăl fiului ei. Interviul a descris și relația doamnei Coste cu acesta și modul în care a reacționat la nașterea copilului, aducând şi fotografii ale prinţului cu copilul. Prințul Albert a introdus o acțiune împotriva companiei de publicare pentru încălcarea dreptului său la protecția vieții private. Instanțele franceze au afirmat că publicarea articolului a cauzat pagube ireversibile prințului Albert și a obligat editorul să plătească despăgubiri și să publice detaliile hotărârii pe coperta din față a revistei.

92 Hotărârea CtEDO nr. 39954/08 din 7 februarie 2012, în cauza *Axel Springer AG/ Germania*, punctele 90 şi 91.

93 Hotărârea CtEDO nr. 40454/07 din 10 noiembrie 2015, în cauza *Coudec și Hachette Filipacchi Associés/ Franța*.

Editorii revistei au introdus cauza la CEDO, susținând că hotărârea instanțelor franceze a intervenit în mod nejustificat cu dreptul la libertatea de exprimare. CEDO a trebuit să confrunte dreptul prințului Albert de a respecta viața privată cu dreptul de exprimare al editorului și dreptul publicului larg de a avea informațiile. Dreptul doamnei Coste de a-și împărtăși povestea cu publicul și interesul copilului de a avea o relație oficială cu tatăl său au fost, de asemenea, considerate importante.

CEDO a susținut că publicarea interviului a constituit o interferenţă în viața privată a prințului și a continuat să examineze dacă era necesară. Aceasta a considerat că publicația s-a referit la o figură publică și la o chestiune de interes public, deoarece cetățenii din Monaco aveau interesul să afle despre existența unui copil al prinţului, deoarece viitorul unei monarhii ereditare este "legat în mod intrinsec de existența de descendenți" și, astfel, o problemă de interes pentru public.[94] De asemenea, Curtea a remarcat că articolul permitea doamnei Coste și copilului ei să-și exercite dreptul la libertatea de exprimare. Instanțele naționale nu au acordat atenția cuvenită principiilor și criteriilor elaborate prin jurisprudența CEDO pentru echilibrarea dreptului la respectarea vieții private și a dreptului la libertatea de exprimare. Aceasta a concluzionat că Franța a încălcat articolul 10 din CEDO privind libertatea de exprimare.

În jurisprudența CEDO, unul dintre criteriile esențiale privind echilibrarea acestor drepturi este dacă expresia în cauză contribuie sau nu la o dezbatere de interes public general.

Exemplu: În cauza *Mosley/Regatul Unit*,[95] un ziar săptămânal național a publicat fotografii intime ale reclamantului, o figură binecunoscută care ulterior a adus cu succes o acțiune civilă împotriva editorului și i s-au acordat daune. În ciuda compensației monetare acordate, el s-a plâns că a rămas victima unei încălcări a dreptului său la viață privată, deoarece i s-a refuzat posibilitatea de a cere o interdicție înainte de publicarea fotografiilor în cauză datorită absenței unui temei legal pentru ziar de a da o notificare prealabilă a publicării.

94 *Ibidem*, punctele 104–116.

95 Hotărârea CtEDO nr. 48009/08 din10 mai 2011, în cauza *Mosley/ RegatulUnit*, punctele 129 şi 130.

CEDO a remarcat că, deși difuzarea unor astfel de materiale a fost în general în scopuri de divertisment, mai degrabă decât de educație, ea a beneficiat, fără îndoială, de protecția articolului 10 din CEDO, care s-ar putea conforma cerințelor articolului 8 din CEDO, în care informaţia era de natură privată și intimă și nu exista nici un interes public în difuzarea sa. Cu toate acestea, o atenție deosebită trebuia acordată în examinarea constrângerilor care ar putea funcționa ca o formă de cenzură înainte de publicare. Având în vedere efectul de răcire care ar putea genera o cerință de notificare prealabilă, îndoielile cu privire la eficacitatea acesteia și marja largă de apreciere în acest domeniu, CEDO a concluzionat că nu era necesară existența unei obligații prealabile din punct de vedere juridic în conformitate cu articolul 8. Prin urmare, Curtea a concluzionat că nu a existat o încălcare a articolului 8.

Exemplu: În cauza *Bohlen/ Germania*,[96] reclamantul, un renumit cântăreț și producător artistic, publicase o carte autobiografică și, ulterior, a fost forțat să îndepărteze unele pasaje în urma hotărârilor judecătorești. Povestea a fost distribuită pe scară largă în mass-media națională, iar o companie de tutun a lansat o campanie publicitară plină de umor referitoare la acest eveniment, folosind numele producătorului fără consimțământul său. Reclamantul a solicitat fără greșeală despăgubiri de la societatea de publicitate, întemeiat pe o încălcare a drepturilor sale în temeiul articolului 8 din CEDO. CEDO a reiterat criteriile care ghidează echilibrul dintre dreptul la respectarea vieții private și dreptul la libertatea de exprimare și a afirmat că nu a existat nicio încălcare a articolului 8. Reclamantul era o persoană publică și campania publicitară nu se referea la detalii din viața sa privată, ci la un eveniment public care a fost deja distribuit de mass-media și a făcut parte dintr-o dezbatere publică. În plus, reclama a avut un caracter plin de umor și nu conținea nimic degradant sau negativ în ceea ce privește reclamantul.

Exemplu: În *cauza Biriuk/ Lituania*[97], reclamantul a susținut în fața CEDO că Lituania nu și-a îndeplinit obligația de a-i respecta dreptul la viața privată, deoarece, deși o încălcare gravă a vieții private a fost comisă de un ziar important, ea a primit o sumă derizorie de daune pecuniare de la instanțele naționale care au examinat cazul. La acordarea despăgubirilor morale, instanțele naționale au solicitat dispoziţiile legii privind informarea publicului,

96 Hotărârea CtEDO nr. 53495/09 din 19 februarie 2015, în cauza *Bohlen/ Germania*, punctele 45–60.

97 Hotărârea CtEDO nr. 23373/03 din 25 noiembrie 2008, în cauza *Biriuk/ Lituania*.

care au impus un plafon redus pentru compensarea prejudiciului moral cauzat de difuzarea ilegală de către mass-media a informațiilor despre viața privată a unei persoane. Cazul a constat în publicarea pe prima pagină de către mai mare ziar lituanian a unui articol care dezvăluia faptul că reclamantul avea HIV pozitiv. Articolul a criticat de asemenea comportamentul reclamantului și i-a pus sub semnul întrebării standardele morale.

CEDO a reamintit că protecția datelor cu caracter personal, nu în ultimul rând datele medicale, au o importanță fundamentală pentru dreptul la respectarea vieții private în cadrul CEDO. Confidențialitatea datelor privind sănătatea este deosebit de importantă, deoarece divulgarea datelor medicale (statutul HIV al reclamantului în acest caz) poate afecta în mod dramatic viața privată și familială a persoanei, situația ocupării forței de muncă și includerea în societate. Curtea a acordat o importanță deosebită faptului că, conform raportului din ziar, personalul medical al spitalului a furnizat informații cu privire la statutul HIV al solicitantului, în mod evident, prin încălcarea obligației de păstrare a secretului medical. Astfel, nu a existat o interferenţă legitimă în dreptul reclamantului la viața privată.

Articolul a fost publicat de presă, iar libertatea de exprimare este, de asemenea, un drept fundamental în cadrul CEDO. Cu toate acestea, atunci când a examinat dacă existența unui interes public a justificat publicarea acestui tip de informații despre reclamant, Curtea a constatat că scopul principal al publicației a fost de a spori vânzările ziarului prin satisfacerea curiozității cititorului. Un astfel de scop nu ar putea fi considerat a contribui la orice dezbatere de interes general pentru societate. Deoarece acesta a fost un caz de "abuz imoral al libertății presei", limitările severe în redresarea prejudiciului și suma redusă a daunelor morale prevăzute de legislația națională au însemnat că Lituania nu și-a îndeplinit obligația de a proteja dreptul reclamantului la viaţa privată. CEDO a constatat că a avut loc o încălcare a articolului 8 din CEDO.

Dreptul la libertatea de exprimare și dreptul la protecția datelor cu caracter personal nu sunt întotdeauna în conflict. Există situații în care protecția eficientă a datelor cu caracter personal garantează libertatea de exprimare.

Exemplu: În cauza *Tele2 Sverige,* CJUE a declarat că interferența cauzată de Directiva 2006/24 (Directiva privind păstrarea datelor) cu drepturile fundamentale prevăzute la articolele 7 și 8 din Cartă este

„amplă şi trebuie să fie considerată deosebit de gravă. Mai mult, faptul că datele sunt păstrate și utilizate ulterior fără ca abonatul sau utilizatorul înregistrat să fie informați poate genera în mintea persoanelor în cauză sentimentul că viața lor privată face obiectul unei supravegheri constante". CJUE a constatat, de asemenea, că păstrarea generalizată a datelor privind traficul și localizarea ar putea avea un efect asupra utilizării comunicațiilor electronice și "în consecință, asupra exercitării de către utilizatori a libertății de exprimare garantate de articolul 11 din Cartă".[98] În acest sens, prin impunerea unor garanții stricte pentru ca păstrarea datelor să nu fie efectuată în mod generalizat, normele privind protecția datelor contribuie, în cele din urmă, la exercitarea libertății de exprimare.

În ceea ce privește dreptul de a primi informații, care, de asemenea, face parte din libertatea de exprimare, există o conștientizare din ce în ce mai mare a importanței transparenței guvernului pentru funcționarea unei societăți democratice. Transparența este un obiectiv de interes general care ar putea astfel justifica o interferență cu dreptul la protecția datelor, dacă este necesar și proporțional, așa cum se explică în Secțiunea 1.2. În ultimele două decenii, în consecință, dreptul de acces la documentele deținute de autoritățile publice a fost recunoscut ca un drept important al fiecărui cetățean al UE și al oricărei persoane fizice sau juridice care are reședința sau sediul social într-un stat membru.

În conformitate cu legea CoE, se pot face referiri la principiile consacrate în Recomandarea privind accesul la documentele oficiale, care a inspirat elaboratorii Convenției privind accesul la documentele oficiale (Convenția 205).[99]

În conformitate cu legislația UE, dreptul de acces la documente este garantat de Regulamentul 1049/2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (Regulamentul privind accesul la documente).[100] Articolul 42 din Cartă și articolul 15 alineatul (3) din TFUE au extins acest drept de acces "la documentele instituțiilor, organelor, oficiilor și agențiilor Uniunii, indiferent de forma lor".

98 Hotărârea CJUE din 21 decembrie 2016, în cauzele conexate C-203/15 şi C-698/15, *Tele2 Sverige AB/ Post-ochtelestyrelsen şi Secretaul de Stat pentru Departamentul Local/ Tom Watson şi alţii*, punctele 37 şi 101; hotărârea CJUE din 8 aprilie 2014, în cauzele conexate C-293/12 şi C-594/12, *Drepturi digitale Irlanda Ltd/ Ministrul Comunicaţiilor, Marinei şi Resurselor Naturale şi alţii şi Kärntner Landesregierung şi alţii*, punctul 28.

99 Consiliul Europei, Comitetul de Miniştri (2002), Recomandarea Rec (81) 19 şi Recomandarea Rec (2002) 2 către statele membre cu privire la accesul la documente, 21 februarie 2002; Consiliul Europei, Convenţia privind accesul la documentele oficiale, CETS nr. 205, 18 iunie 2009. Convenţia nu a intrat încă în vigoare.

100 Regulamentul (CE) nr.1049/2001 al Parlamentului şi al Consiliului European din 30 mai 2001 privind accesul public la documentele Parlamentului, Consiliului şi Comisiei Europene, MO 2001 L145.

Acest drept poate intra în conflict cu dreptul la protecția datelor dacă accesul la un document ar dezvălui datele personale ale altor persoane. Articolul 86 din Regulamentul general privind protecția datelor prevede în mod clar că datele cu caracter personal din documentele oficiale deținute de autoritățile și organismele publice pot fi divulgate de către autoritatea sau organismul în cauză în conformitate cu legislația Uniunii[101] sau cu legislația statelor membre pentru a reconcilia accesul publicului la documentele oficiale cu dreptul la protecția datelor în conformitate cu regulamentul.

Prin urmare, cererile de acces la documente sau informații deținute de autoritățile publice pot necesita echilibrarea cu dreptul la protecția datelor persoanelor ale căror date figurează în documentele solicitate.

Exemplu: În cauza *Volker und Markus Schecke și Hartmut Eifert/ Land Hessen*,[102] CJUE a trebuit să judece proporționalitatea publicării, cerută de legislația UE, a numelor beneficiarilor subvențiilor agricole UE și a sumelor pe care le-au primit. Publicația a vizat creșterea transparenței și contribuția la controlul public al utilizării adecvate a fondurilor publice de către administrație. Mai mulți beneficiari au contestat proporționalitatea acestei publicații.

Observând că dreptul la protecția datelor nu este absolut, CJUE a susținut că publicarea pe site a unor date care desemnează beneficiarii a două fonduri UE de ajutor agricol și sumele precise primite constituie o ingerință în viața privată în general și cu protecția datelor lor personale, în special.

CJUE a constatat că o astfel de ingerință la articolele 7 și 8 din Cartă a fost prevăzută de lege și a îndeplinit un obiectiv de interes general recunoscut de UE - și anume, creșterea transparenței utilizării fondurilor comunitare. Cu toate acestea, CJUE a considerat că publicarea numelor persoanelor fizice care beneficiază de ajutor agricol de la UE din aceste două fonduri și sumele exacte primite a constituit o măsură disproporționată și nu a fost justificată având în vedere articolul 52 alineatul (1) din Cartă. Aceasta a recunoscut importanța, într-o societate democratică, de informare a contribuabililor cu

101 Articolul 42 din Cartă, articolul 15 alin. (3) din TFUE şi Regulamentul 1049/2009.

102 Hotărârea CJUE din 9 noiembrie 2010, în cauzele conexate C-92/09 şi C-93/09, *Volker und Markus Schecke GbR şi Hartmut Eifert/ Hessa*, punctele 47–52, 58, 66–67, 75, 86 şi 92.

privire la utilizarea fondurilor publice. Cu toate acestea, întrucât "nu se poate conferi o prioritate automată a obiectivului de transparență în ceea ce privește dreptul la protecția datelor cu caracter personal",[103] instituțiile UE au fost obligate să echilibreze interesul Uniunii în ceea ce privește transparența cu limitarea exercitării drepturilor la confidențialitate și protecția datelor pe care beneficiarii le-a suferit ca urmare a publicării.

CJUE a considerat că instituțiile UE nu au efectuat în mod corespunzător acest exercițiu de echilibrare, deoarece a fost posibil să se ia în considerare măsuri care ar afecta mai puțin negativ drepturile fundamentale ale persoanelor, contribuind, în același timp, la obiectivul de transparență urmărit de publicație. De exemplu, în loc de o publicare generală care afectează toți beneficiarii, indicând numele lor și sumele precise primite de fiecare dintre aceştia, s-ar putea face o distincție pe baza unor criterii relevante, cum ar fi perioadele în care aceste persoane au primit ajutorul, frecvența ajutorului sau valoarea și natura acestuia[104]. Astfel, CJUE a declarat parțial invalidă legislația UE privind publicarea informațiilor referitoare la beneficiarii fondurilor agricole europene.

Exemplu: În cauza *Rechnungshof/ Österreichischer Rundfunk și alții*[105], CJUE a examinat compatibilitatea anumitor legislații austriece cu legislația UE privind protecția datelor. Legislația a cerut unui organism de stat să colecteze și să transmită date privind veniturile în scopul publicării numelui și veniturilor angajaților diferitelor entități publice într-un raport anual pus la dispoziția publicului larg. Unele persoane au refuzat să comunice datele lor pe baza protecției datelor.

În avizul său, CJUE s-a bazat pe protecția drepturilor fundamentale ca principiu general al dreptului UE și la articolul 8 din CEDO, reamintind că Carta nu era obligatorie la momentul respectiv. Acesta a considerat că colectarea datelor privind veniturile profesionale ale unui particular, în special comunicarea acestuia unor terți, intră în domeniul de aplicare al dreptului la respectarea vieții private și constituie o încălcare a acestui drept. Ingerința ar putea fi justificată dacă ar fi fost în conformitate cu legea, ar urmări un scop legitim și ar fi fost necesară într-o societate de-

103 *Ibidem*, punctul 85.

104 *Ibidem*, punctul 89.

105 Hotărârea CJUE din 20 mai 2003, în cauzele C-465/00, C-138/01 şi C-139/09, *Rechnungshof/ Österreichischer Rundfunk şi alţiişi Christa Neukomm şi Jospeh Lauermann/ ÖsterreichischerRundfunk*.

mocratică pentru a atinge acest scop. CJUE a constatat că legislația austriacă urmărea un scop legitim, având în vedere că obiectivul său era de a menține salariile funcționarilor publici în limite rezonabile - o considerație care se referă și la bunăstarea economică a țării. Cu toate acestea, interesul Austriei de a asigura cea mai bună utilizare a fondurilor publice a trebuit să fie echilibrat în raport cu gravitatea intervenției în dreptul persoanelor în cauză de a-și respecta viața privată.

În timp ce, lăsând la latitudinea instanței naționale să verifice dacă publicarea datelor privind veniturile persoanelor era necesară și proporțională cu obiectivul urmărit de legislație, CJUE solicita instanței naționale să examineze dacă un astfel de scop nu ar fi putut fi atins în mod egal și eficient prin mijloace mai puțin invazive. Un exemplu ar fi transmiterea datelor cu caracter personal numai organismelor publice de monitorizare și nu publicului larg.

În cazurile ulterioare, a devenit evident că echilibrarea dintre protecția datelor și accesul la documente necesită o analiză detaliată, de la caz la caz. Nici un drept nu poate suprascrie automat celălalt. CJUE a avut ocazia să interpreteze dreptul de acces la documentele care conțin date cu caracter personal în două cazuri.

Exemplu: În cauza *Comisia Europeană/Bavarian Lager*,[106] CJUE a definit domeniul de aplicare al protecției datelor cu caracter personal în contextul accesului la documentele instituțiilor UE și relația dintre Regulamentul nr. 1049/2001 (Regulamentul privind accesul la documente) și Regulamentul nr. 45/2001 (Regulamentul instituțiilor UE privind protecția datelor). Bavarian Lager, înființată în 1992, importă bere germană în Marea Britanie, în principal pentru localuri și baruri publice. Cu toate acestea, a întâmpinat dificultăți, deoarece legislația britanică a favorizat producătorii naționali de facto. Ca răspuns la plângerea Bavarian Lager, Comisia Europeană a intentat o acțiune împotriva Regatului Unit pentru neîndeplinirea obligațiilor sale, ceea ce i-a determinat să modifice dispozițiile în litigiu și să le alinieze la legislația UE. Bavarian Lager a solicitat apoi Comisiei, printre alte documente, o copie a procesului-verbal al unei întâlniri la care au participat reprezentanți ai Comisiei, ai autorităților britanice și Confederation des Brasseurs du Marché Commun (CBMC). Comisia a fost de acord să dezvăluie anumite documente referitoare la reuniune, însă a șters cinci nume care figurează în procesul-verbal - două persoane care au obiectat în

106 Hotărârea CJUE din 29 iunie 2010, în cauza C-28/08P, *ComisiaEuropeană/ TheBavarian Lager Co.Ltd.*

mod expres la dezvăluirea identității lor, iar Comisia nu a putut să contacteze celelalte trei. Prin decizia din 18 martie 2004, Comisia a respins o nouă cerere a Bavarian Lager pentru a obține procesul-verbal complet al reuniunii, invocând, în special, protecția vieții private a acestor persoane, aşa cum este garantată de Regulamentul privind protecția datelor instituțiilor UE.

Întrucât nu a fost mulțumit de această poziție, Bavarian Lager a introdus o acțiune în fața Tribunalului de Primă Instanță. Această instanță a anulat decizia Comisiei prin Hotărârea din 8 noiembrie 2007 (cauza T-194/04, *The Bavarian Lager Co. Ltd/ Comisia Comunităților Europene*), constatând că simpla înscriere a numelor persoanelor în cauză pe lista persoanelor care participă la o întâlnire în numele organismului pe care l-au reprezentat nu a subminat viața privată și nu a pus viața privată a acestor persoane în pericol.

În apelul Comisiei, CJUE a anulat hotărârea Tribunalului de Primă Instanță. CJUE a considerat că Regulamentul privind accesul la documente stabilește "un sistem specific și consolidat de protecție a persoanei ale cărei date cu caracter personal ar putea fi, în anumite cazuri, comunicate publicului". Potrivit CJUE, cererea bazată pe Regulamentul privind accesul la documente urmărește astfel obținerea accesului la documente care conțin date cu caracter personal, astfel dispozițiile regulamentului UE privind protecția datelor devin aplicabile în întregime. Ulterior, CJUE a concluzionat că Comisia a respins corect cererea de acces la procesul-verbal complet al reuniunii din octombrie 1996. În absența consimțământului celor cinci participanți la această reuniune, Comisia s-a conformat în mod suficient cu obligația de deschidere prin eliberarea unei versiuni a documentului în cauză, cu numele lor desprinse.

În plus, potrivit CJUE, "întrucât Bavarian Lager nu a furnizat nici o justificare explicită și legitimă sau nici un argument convingător pentru a demonstra necesitatea transferării acestor date cu caracter personal, Comisia nu a putut să cântărească diversele interese ale părților interesate. De asemenea, nu a putut verifica dacă există vreun motiv pentru a presupune că interesele legitime ale persoanelor vizate ar putea fi prejudiciate", în conformitate cu Regulamentul UE privind protecția datelor instituțiilor UE.

Exemplu: În cauza *Client Earth și PAN Europe/ EFSA*[107], CJUE a examinat dacă decizia Autorității Europene pentru Siguranță Alimentară (AESA) de a refuza solicitanţilor accesul deplin la documente era necesar

107 Hotărârea CJUE din 16 iulie 2015, în cauza C-615/13P, *ClientEarth, Pesticide Action Network Europe(PANEurope)/ Autoritatea Europeană pentru Siguranţă Alimentară(AESA),Comisia Europeană*.

pentru a proteja drepturile de confidențialitate și protecția datelor persoanelor cărora le-au fost adresate documentele. Documentele au vizat un raport de orientare elaborat de un grup de lucru al AESA în colaborare cu experți externi privind plasarea pe piață a produselor fitosanitare. Inițial, AESA a acordat accesul parțial solicitanților, refuzând accesul la unele versiuni de lucru ale documentului. Ulterior, a acordat acces la o versiune a proiectului care a inclus comentariile individuale ale experților externi. Cu toate acestea, a redactat numele experților, invocând articolul 4 alineatul (1) litera (b) din Regulamentul 45/2001 privind prelucrarea datelor cu caracter personal de către instituțiile și organele UE și necesitatea de a proteja confidențialitatea experților externi. În primă instanță, Tribunalul a confirmat decizia AESA.

În apelul reclamanților, CJUE a anulat hotărârea pronunțată în primă instanță. Aceasta a concluzionat că transferul de date cu caracter personal în acest caz a fost necesar pentru a stabili imparțialitatea fiecăruia dintre experții externi în îndeplinirea sarcinilor lor de cercetători și pentru a asigura transparența procesului de luare a deciziilor în cadrul AESA. Potrivit CJUE, AESA nu a precizat cum dezvăluirea numelor experților externi care au făcut observații specifice cu privire la proiect ar aduce atingere intereselor legitime ale experților. Un argument general potrivit căruia divulgarea poate submina confidențialitatea nu este suficient dacă nu este susținut de dovezi specifice fiecărui caz.

Conform acestor hotărâri, interferența cu dreptul la protecția datelor în contextul accesului la documente necesită un motiv specific și justificat. Dreptul de acces la documente nu poate anula în mod automat dreptul la protecția datelor.[108]

Această abordare este similară celei a CEDO în ceea ce privește confidențialitatea și accesul la documente, după cum demonstrează următoarea hotărâre. În hotărârea *Magyar Helsinki*, CEDO a declarat că articolul 10 nu conferă persoanei dreptul de acces la informațiile deținute de o autoritate publică sau obligă guvernul să transmită aceste informații individului. Cu toate acestea, un astfel de drept sau obligație ar putea apărea - în primul rând, în cazul în care divulgarea informațiilor este impusă printr-o ordonanță judecătorească care a dobândit putere juridică; în al doilea rând, în cazul în care accesul la informații este esențial pentru exercitarea de către un individ a dreptului său la libertatea de exprimare - în special a libertății de a primi și de a transmite informații - și în care refuzul acestuia ar fi în conflict cu acest

108 A se vedea, totuși, deliberările detaliate din AEPD (2011), *Accesul public la documentele care conţin date cu caracter personal după hotărârea din cauza Bavarian Lager*, Bruxelles, 24 martie 2011.

drept.[109] Dacă și în ce măsură negarea accesului la informații constituie o ingerință în libertatea de exprimare a unui reclamant, trebuie evaluată în fiecare caz în parte și ținând seama de circumstanțele sale specifice, printre care: (i) scopul cererii de informații; (ii) natura informațiilor solicitate; (iii) rolul solicitantului; și (iv) dacă informațiile au fost pregătite și disponibile.

Exemplu: În cauza *Magyar Helsinki Bizottság/Ungaria*,[110] reclamantul, un ONG pentru drepturile omului, a solicitat informații de la poliție cu privire la activitatea consilierului de apărare *din oficiu*, pentru a finaliza un studiu privind funcționarea sistemului apărătorilor publici din Ungaria. Poliția a refuzat să furnizeze informațiile, argumentând că acestea constituie date cu caracter personal care nu sunt supuse dezvăluirii. Aplicând criteriile de mai sus, CEDO a considerat că a intervenit un drept protejat în temeiul articolului 10. Mai exact, solicitantul a dorit să-și exercite dreptul de a transmite informații cu privire la o chestiune de interes public, a căutat accesul la informații în acest scop, iar informațiile au fost necesare pentru exercitarea dreptului de liberă exprimare al reclamantului. Informațiile privind numirea apărătorilor publici au fost de interes pentru public. Nu exista nici un motiv de îndoială că ancheta în cauză conținea informații pe care reclamantul s-a angajat să le transmită publicului, care avea dreptul să le primească. Prin urmare, Curtea a constatat că accesul la informațiile solicitate era necesar pentru ca solicitantul să-și îndeplinească sarcina. În cele din urmă, informațiile au fost pregătite și disponibile.

CtEDO a concluzionat că refuzul accesului la informații în acest caz a afectat însăși substanța libertății de a primi informații. Pentru a ajunge la această concluzie, aceasta a examinat în special scopul informațiilor solicitate și contribuția lor la o dezbatere publică importantă, natura informațiilor solicitate, caracterul de interes public și rolul jucat în societate de către reclamantul în cauză.

În raționamentul său, Curtea a remarcat că studiul realizat de ONG vizează funcționarea justiției și dreptul la un proces echitabil, care este un drept de o importanță capitală în cadrul CEDO. Întrucât informațiile solicitate nu au implicat date în afara domeniului public, drepturile de confidențialitate ale persoanelor vizate în cauză (apărătorii publici din

109 Hotărârea CtEDO nr.18030/11 din 8 noiembrie 2016, în cauza *Magyar Helsinki Bizottság/ Ungaria*, punctul 148.

110 *Ibidem*, punctele 181, 187–200.

oficiu) nu ar fi compromise dacă poliția a dat acces la informații solicitantului. Informațiile solicitate au fost de natură statistică, referitoare la de câte ori au fost numiți avocații din oficiu pentru a reprezenta inculpații în procedurile penale publice.

Pentru Curte, având în vedere că studiul a avut ca scop să contribuie la o dezbatere importantă pe o chestiune de interes general, orice restricție asupra publicării propuse de ONG ar fi trebuit să fie supusă unui control riguros. Informațiile în cauză au fost de interes public, deoarece interesul public acoperă "chestiuni care pot crea controverse considerabile, care privesc o problemă socială importantă sau care implică o problemă pe care publicul ar avea interesul să o cunoască".[111] Astfel, cu siguranță ar fi vorba despre o discuție privind conduita justiției și procesele echitabile, care face obiectul studiului reclamantului. Prin echilibrarea diferitelor drepturi în cauză și aplicarea principiului proporționalității, CtEDO a considerat că a avut loc o încălcare nejustificată a drepturilor reclamantului în temeiul articolului 10 din CEDO.

1.3.2. Secretul profesional

În conformitate cu legislația națională, anumite comunicări pot face obiectul secretului profesional. Secretul profesional poate fi înțeles ca o datorie etică specială care implică o obligație legală inerentă anumitor profesii și funcții care se bazează pe credință și încredere. Persoanele și instituțiile care îndeplinesc aceste funcții sunt obligate să nu dezvăluie informațiile confidențiale pe care le primesc în timpul îndeplinirii îndatoririlor lor. Secretul profesional se aplică în mod deosebit profesiei medicale și privilegiului avocat-client, multe jurisdicții recunoscând, de asemenea, obligația secretului profesional privind sectorul financiar. Secretul profesional nu este un drept fundamental, ci este protejat ca o formă a dreptului la respectarea vieții private. De exemplu, CJUE a hotărât că, în anumite cazuri, "ar putea fi necesar să se interzică divulgarea anumitor informații care sunt clasificate ca fiind confidențiale, pentru a proteja dreptul fundamental al unei întreprinderi de a-și respecta viața privată, consacrat la articolul 8 din CEDO și articolul 7 din Cartă".[112] CtEDO a fost, de asemenea, chemată să se pronunțe asupra faptului dacă restricțiile privind secretul profesional constituie o încălcare a articolului 8 din CEDO, după cum se arată în exemplele evidențiate.

111 *Ibidem*, punctul 156.

112 Hotărârea CJUE din 11martie 2013, în cauza T-462/12R, *PilkingtonGroupLtd/Comisia Europeană*, Ordonanţa Preşedintelui Curţii Generale, punctul 44.

Exemplu: În cauza *Pruteanu/România*,[113] reclamantul a acționat ca avocat al unei societăți comerciale, căreia i s-a interzis să efectueze tranzacții bancare ca urmare a unor acuzații de fraudă. În timpul investigării cazului, instanțele române au autorizat autoritățile de urmărire penală să intercepteze și să înregistreze convorbirile telefonice ale unui partener al companiei pe o anumită perioadă. Înregistrările și intercepțiile au inclus comunicarea cu avocatul său.

Domnul Pruteanu a susținut că acest lucru a interferat cu dreptul său la respectarea vieții private și a corespondenței sale. În hotărârea sa, CEDO a subliniat statutul și importanța relației avocatului cu clientul său. Interceptarea conversațiilor avocatului cu clientul său a încălcat, fără îndoială, secretul profesional, care a stat la baza relației dintre acești doi oameni. Într-un astfel de caz, avocatul ar putea, de asemenea, să se plângă de o interferență cu dreptul său la respectarea vieții private și a corespondenței. CJUE a susținut că a avut loc o violare a articolului 8 din CEDO.

Exemplu: În cauza *Brito Ferrinho Bexiga Villa-Nova/ Portugalia*,[114] reclamanta, avocat, a refuzat să-și dezvăluie declarațiile personale ale băncii autorităților fiscale din motive de confidențialitate profesională și secret de bancă. Procuratura a deschis o anchetă privind fraudarea fiscală și a solicitat suspendarea autorizării confidențialității profesionale. Instanțele naționale au dispus suspendarea regulilor de confidențialitate și secretul bancar, constatând că interesul public ar trebui să prevaleze asupra intereselor private ale reclamantului.

Atunci când cauza a ajuns la Curtea Europeană a Drepturilor Omului, Curtea a statuat că accesarea declarațiilor bancare ale reclamantei a constituit o ingerință în dreptul său la respectarea confidențialității profesionale, care intră în sfera vieții private. Interferența a avut un temei juridic, deoarece se baza pe codul de procedură penală și urmărea un scop legitim. Cu toate acestea, examinând necesitatea și proporționalitatea ingerinței, CEDO a subliniat faptul că procedurile de ridicare a confidențialității au fost efectuate fără participarea sau cunoștințele solicitantului. Prin urmare, reclamanta nu a putut să își prezinte argumentele. În plus, chiar dacă legea națională a susţinut că asociaţia de avocaţi trebuia să fie consultată în astfel de proce-

113 Hotărârea CtEDO nr. 30181/05 din 3 februarie 2015, în cauza *Pruteanu/ România*.

114 Hotărârea CtEDO nr. 69436/10 din1 decembrie 2015, în cauza *Brito Ferrinho Bexiga Villa-Nova/ Portugalia*.

duri, asociația nu fusese consultată. În cele din urmă, reclamantul nu a avut opțiunea de a contesta în mod efectiv ridicarea confidențialității și nici de a remedia măsura. Din cauza lipsei garanțiilor procedurale și a controlului jurisdicțional efectiv asupra măsurii de suspendare a obligației de confidențialitate, CEDO a concluzionat că a avut loc o încălcare a articolului 8 din CEDO.

Interacțiunea dintre secretul profesional și protecția datelor este adesea ambivalentă. Pe de o parte, normele și garanțiile de protecție a datelor stabilite în legislație contribuie la asigurarea secretului profesional. De exemplu, normele care impun inspectorilor și procesatorilor să implementeze măsuri robuste de securitate a datelor încearcă să prevină, printre altele, pierderea confidențialității datelor cu caracter personal protejate prin secretul profesional. În plus, Regulamentul general al UE privind protecția a datelor permite prelucrarea datelor privind sănătatea, care constituie categorii speciale de date cu caracter personal care merită o protecție mai mare, dar care face obiectul existenței unor măsuri adecvate și specifice pentru a proteja drepturile persoanelor vizate, în special a secretului profesional.[115]

Pe de altă parte, obligațiile privind secretul profesional impuse inspectorilor și operatorilor cu privire la anumite date cu caracter personal pot limita drepturile persoanelor vizate, în special dreptul de a primi informații. Chiar dacă regulamentul general privind protecția datelor conține o listă extinsă cu informații care, în principiu, trebuie furnizate persoanei vizate în cazul în care datele cu caracter personal nu au fost obținute de la el sau ea, această cerință de dezvăluire nu se aplică atunci când datele cu caracter personal trebuie să rămână confidențiale datorită obligației de păstrare a secretului profesional solicitată fie de legislația națională, fie de legislația UE.[116]

Regulamentul general privind protecția datelor (RGPD) prevede posibilitatea ca statele membre să adopte de drept norme specifice pentru a proteja obligațiile profesionale sau alte obligații de secretizare și pentru a reconcilia dreptul la protecția datelor cu caracter personal cu obligația de păstrare a secretului profesional.[117]

RGPD prevede că statele membre pot adopta norme specifice privind competențele autorităților de supraveghere în ceea ce privește inspectorii sau operatorii care sunt supuși obligației de păstrare a secretului profesional. Aceste reguli specifice se referă la posibilitatea de a obține accesul la datele unui inspector

115 Regulamentul general privind protecţia datelor, articolul 9 alin. (2) lit. (h) şi alin. (3).

116 *Ibidem*, articolul 14 alin. (5) lit. (d).

117 *Ibidem*, Relatarea 164 şi articolul 90.

sau operator, a echipamentului său de prelucrare a datelor și a datelor cu caracter personal deținute, în cazul în care aceste date cu caracter personal au fost primite în cursul unei activități care face obiectul obligației de păstrare a secretului. Astfel, autoritățile de supraveghere cărora le-a fost încredințată protecția datelor trebuie să respecte obligațiile privind secretul profesional care unesc inspectorii și operatorii. Mai mult, membrii autorităților de supraveghere înşişi sunt, de asemenea, supuși obligației de păstrare a secretului profesional în timpul și după perioada de mandat. În timpul exercitării sarcinilor lor, membrii și personalul autorităților de supraveghere pot dobândi cunoștințe despre informațiile confidențiale. Articolul 54 alineatul (2) din regulament prevede clar că aceştia au obligația de a păstra secretul profesional cu privire la astfel de informații confidențiale.

RGPD cere ca statele membre să notifice Comisiei normele pe care le adoptă pentru a reconcilia protecția datelor și principiile stabilite în regulament cu obligația de păstrare a secretului profesional.

1.3.3. Libertatea la religie şi credinţă

Libertatea la religie și credință este protejată în temeiul articolului 9 din CEDO (libertatea de gândire, conștiință și religie) și al articolului 10 din Carta Drepturilor Fundamentale a UE. Datele personale care dezvăluie convingeri religioase sau filozofice sunt considerate "date sensibile" atât în temeiul legislației UE, cât și în cea a CoE, iar prelucrarea și utilizarea acestora este supusă unei protecții sporite.

Exemplu: Reclamantul din cauza *Sinak Isik/ Turcia*[118] a fost membru al comunității religioase Alevi, a cărei credință este influențată de sufism și alte credințe pre-Islamice și este considerată de unii cărturari ca o religie separată și de alții ca parte a religiei islamice. Reclamantul s-a plâns că, împotriva dorințelor sale, cartea sa de identitate conținea o căsuță care indica religia sa ca "Islam", mai degrabă decât "Alevi". Curțile interne au respins cererea sa de a schimba cartea de identitate la "Alevi" pe motiv că acest cuvânt a desemnat un subgrup de Islam și nu o religie separată. El s-a plâns apoi în fața CEDO că a fost obligat să-și dezvăluie credința fără consimțământul său, deoarece era obligatoriu să indice religia unei persoane pe cartea de identitate și că acest lucru încalcă dreptul său la libertatea religioasă și a conștiinței, dat fiind că desemnarea "Islamului" pe cartea sa de identitate era incorectă.

118 Hotărârea CtEDO nr. 21924/05 din 2 februarie 2010, în cauza *Sinan Işık/ Turcia*.

CtEDO a reiterat faptul că libertatea la religie presupune libertatea de a manifesta religia unei persoane în comunitate cu ceilalți, în public și în cercul persoanelor care împărtășesc aceeași credință, dar și în sine și în particular. Legislația internă aplicabilă în acel moment a obligat persoanele să poarte un buletin de identitate, un document care trebuia prezentat la cererea oricărei autorități publice sau a unor întreprinderi private, indicând religia lor. Această obligație nu a recunoscut că dreptul de a-și manifesta religia a conferit și reversul, adică dreptul de a nu fi obligat să-și dezvăluie credința. Chiar dacă guvernul a susținut că legislația națională a fost modificată astfel încât persoanele să poată solicita ca religia să nu fie completată în cărțile de identitate, în opinia Curții, simplul fapt de a cere să fie eliminată religia ar putea constitui o divulgare a informațiilor cu privire atitudinile lor față de religie. În plus, atunci când cărțile de identitate au o casetă pentru religie, lăsând-o goală are o conotație specială, deoarece deținătorii unui buletin de identitate fără informații despre religie ar ieși în evidenţă faţă de cei la care este indicată religia lor. CtEDO a concluzionat că legislația internă încalcă articolul 9 din CEDO.

Cu toate acestea, funcționarea bisericilor și a asociațiilor sau comunităților religioase poate necesita prelucrarea informațiilor personale, pentru a permite comunicarea și organizarea activităților în cadrul congregației. Astfel, bisericile și asociațiile religioase au pus de multe ori în aplicare norme privind prelucrarea datelor cu caracter personal. În conformitate cu articolul 91 din Regulamentul general privind protecția datelor, în cazul în care aceste norme sunt exhaustive, acestea pot fi în continuare valabile, cu condiția ca acestea să fie conforme cu dispozițiile regulamentului. Bisericile și asociațiile religioase care au astfel de reguli trebuie să facă obiectul supravegherii unei autorități independente de supraveghere, care ar putea fi specifică pentru ele, cu condiția să îndeplinească cerințele Regulamentului general privind protecția datelor pentru astfel de autorități.[119]

Organizațiile religioase pot prelua prelucrarea datelor personale din mai multe motive - de exemplu, pentru a menține contactul cu congregația lor sau pentru a comunica informații despre evenimente religioase sau caritabile și festivități organizate. În anumite state, bisericile trebuie să păstreze registrele membrilor lor din motive fiscale, deoarece apartenența la instituțiile religioase poate avea un impact asupra impozitelor plătibile de către persoane fizice. În orice caz, în conformitate cu legislația europeană, datele care dezvăluie convingerile religioase sunt date sensibile, iar bisericile trebuie să fie responsabile pentru manipularea și prelucrarea acestor date, mai ales că informaţiile prelucrate de

119 Regulamentul general privind protecţia datelor, articolul 91 alin. (2).

organizaţiile religioase se referă adesea la copii, vârstnici sau alţi membri vulnerabili ai societăţii.

1.3.4. Libertatea artelor şi ştiinţelor

Un alt drept la echilibru împotriva drepturilor la respectarea vieții private și la protecția datelor este libertatea artelor și a științelor, protejată în mod explicit în temeiul articolului 13 din Carta drepturilor fundamentale a UE. Acest drept este dedus în primul rând din dreptul la libertatea de gândire și exprimare și trebuie exercitat în conformitate cu articolul 1 din Cartă (demnitatea umană). CtEDO consideră că libertatea artelor este protejată în temeiul articolului 10 din CEDO.[120] Dreptul garantat de articolul 13 din Cartă poate fi, de asemenea, supus limitărilor, în conformitate cu articolul 52 alineatul (1) din Cartă, care poate fi, de asemenea, interpretat în conformitate cu articolul 10 alineatul (2) din CEDO.[121]

Exemplu: În cauza *Vereinigung bildender Künstler/ Austria*[122], instanțele austriece au interzis asociației reclamante să continue să prezinte un tablou care conținea fotografii ale șefilor diferitelor personalități publice în poziții sexuale. Un parlamentar austriac, a cărui fotografie a fost folosită în tablou, a intentat o acțiune împotriva asociației reclamante, solicitând o interdicție care îi interzicea să prezinte pictura. Instanța națională a emis o interdicție. CEDO a reiterat faptul că articolul 10 din CEDO se extinde la comunicarea ideilor care ofensează, șochează sau perturbă statul sau orice parte a populației. Cei care creează, interpretează, distribuie sau expun opere de artă contribuie la schimbul de idei și opinii, iar statul are obligația de a nu încălca în mod nejustificat libertatea de exprimare. Având în vedere că tabloul era un colaj și că folosea doar fotografii ale șefilor de persoane și că trupurile lor erau pictate într-o manieră nerealistă și exagerată, care, evident, nu vizează reflectarea sau chiar sugerarea realității, CEDO a mai spus că "pictura cu greu poate fi înțeleasă că abordează detalii despre viața privată a lui [descris], ci mai degrabă legată de poziția sa publică de politician "și că" în această calitate [imaginea] trebuia să afișeze o toleranță mai largă în ceea ce privește critica". Cântărind diferitele interese în joc, CEDO a constatat că interdicția nelimitată împotriva expunerii în continuare a tabloului a fost disproporționată. Curtea a concluzionat că a avut loc o încălcare a articolului 10 din CEDO.

120 Hotărârea CtEDO nr. 10737/84 din 24 mai 1988, în cauza *Müllerşi alţii/ Elveţia*.

121 Explicaţii privind Carta Drepturilor Fundamentale, MO 2007 C303.

122 Hotărârea CtEDO nr. 68345/01 din 25 ianuarie 2007, în cauza *Vereinigung bildender Künstler/ Austria*, punctele 26 şi 34.

Legea europeană privind protecția datelor recunoaște, de asemenea, valoarea specială a științei pentru societate. Regulamentul general privind protecția datelor și Convenția modernizată 108 permit păstrarea datelor pentru perioade mai lungi, în măsura în care datele cu caracter personal vor fi prelucrate exclusiv în scopuri științifice sau istorice de cercetare. În plus, indiferent de scopul inițial al unei activități de prelucrare specifice, utilizarea ulterioară a datelor cu caracter personal pentru cercetarea științifică nu este considerată un scop incompatibil.[123] În același timp, trebuie puse în aplicare garanții adecvate pentru o astfel de prelucrare pentru a proteja drepturile și libertățile persoanelor vizate. Legislația UE sau a statelor membre poate prevedea derogări de la drepturile persoanei vizate, cum ar fi de exemplu dreptul de acces, rectificare, restricționarea prelucrării și de a se opune prelucrării datelor cu caracter personal în scopuri științifice, istorice sau statistice (a se vedea de asemenea Secțiunea 6.1 și Secțiunea 9.4).

1.3.5. Protecţia proprietăţii intelectuale

Dreptul la protecția proprietății este consacrat în articolul 1 din primul Protocol al CEDO și în articolul 17 alineatul (1) din Carta Drepturilor Fundamentale a UE. Un aspect important al dreptului la proprietate, care este deosebit de relevant pentru protecția datelor, este protecția proprietății intelectuale, menționată explicit la articolul 17 alineatul (2) din cartă. Mai multe directive din ordinea juridică comunitară vizează protejarea eficientă a proprietății intelectuale, în special a dreptului de autor. Proprietatea intelectuală acoperă nu numai proprietatea literară și artistică, ci și brevetul, marca comercială și drepturile conexe.

După cum a clarificat jurisprudența Curții Europene de Justiție, protecția dreptului fundamental la proprietate trebuie să fie echilibrată cu protecția altor drepturi fundamentale, în special a dreptului la protecție a datelor[124]. Au existat cazuri în care instituțiile de protecție a drepturilor de autor au solicitat furnizorilor de acces la internet să dezvăluie identitatea utilizatorilor platformelor de partajare a fișierelor pe internet. Astfel de platforme permit adesea utilizatorilor de internet să descarce înregistrări muzicale gratuit, chiar dacă acestea titluri sunt protejate prin drepturi de autor.

> Exemplu: Cauza *Promusicae/ Telefónica de España*[125] se referea la refuzul unui furnizor spaniol de acces la internet, Telefónica, de a dezvălui Promusicae, o organizație non-profit a producătorilor și editorilor de muzică și

123 Regulamentul general privind protecţia datelor, art.5 alin. (1) lit. (b) şi Convenţia modernizată 108, art. 5 alin. (4) lit. (b).

124 Hotărârea CJUE din 29 ianuarie 2008, în cauza C-275/06, *Productores de Música de España (Promusicae)/ Telefónica de España SAU*, punctele 62–68.

125 *Ibidem*, punctele 54 şi 60.

înregistrări audio-vizuale, datele personale ale anumitor persoane cărora le-a furnizat servicii de acces la internet. Promusicae a solicitat divulgarea informațiilor astfel încât să poată iniția proceduri civile împotriva acelor persoane, despre care a spus că foloseau un program de schimb de fișiere care permitea accesul la fonograme ale căror drepturi de exploatare erau deținute de membrii Promusicae.

Instanța spaniolă a sesizat CJUE cu privire la întrebarea dacă aceste date cu caracter personal trebuie să fie comunicate, în conformitate cu dreptul comunitar, în cadrul procedurilor civile pentru a asigura protecția eficientă a drepturilor de autor. El a făcut trimitere la Directivele 2000/31, 2001/29 și 2004/48, citite și în lumina articolelor 17 și 47 din Cartă. CJUE a concluzionat că aceste trei directive, precum și Directiva privind confidențialitatea 2002/58, nu împiedică statele membre să prevadă obligația de divulgare a datelor cu caracter personal în cadrul procedurilor civile pentru a asigura protecția eficientă a drepturilor de autor.

CJUE a subliniat că, prin urmare, cauza ridică problema necesității de a reconcilia cerințele protecției diferitelor drepturi fundamentale - și anume dreptul la respectarea vieții private cu dreptul la protecția proprietății și la o cale de atac eficientă.

Aceasta a concluzionat că "statele membre trebuie să se prevaleze, atunci când transpun directivele menționate anterior, de o interpretare a acestor directive care să permită stabilirea unui echilibru echitabil între diferitele drepturi fundamentale protejate de ordinea juridică comunitară. În plus, atunci când pun în aplicare măsurile de transpunere a acestor directive, autoritățile și instanțele statelor membre trebuie nu numai să interpreteze legislația lor națională într-o manieră compatibilă cu aceste directive, ci și să se asigure că nu se bazează pe o interpretare a acestora care ar fi în conflict cu aceste drepturi fundamentale sau cu celelalte principii generale ale dreptului comunitar, cum ar fi principiul proporționalității".[126]

Exemplu: Cauza *Bonnier Audio AB și alții/ Perfect Communication Suedia AB*[127] se referea la echilibrul dintre drepturile de proprietate intelectuală și protecția datelor cu caracter personal. Reclamanții - cinci societăți editoriale care dețin drepturi de autor asupra a 27 audiobook-uri - au introdus o acțiune în fața instanței suedeze, susţinând că aceste drepturi de autor au

126 *Ibidem*, punctele 65 și 68; a se vedea, de asemenea, hotărârea CJUE din16 februarie 2012, în cauza C-360/10, *Belgische Vereniging van Auteurs,Componistenen Uitgevers CVBA(SABAM)/Netlog NV*.

127 Hotărârea CJUE din 19 aprilie 2012, în cauza C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB/ Perfect Communication Suedia AB*.

fost încălcate prin intermediul unui server FTP (un protocol de transfer de fișiere care permite partajarea de fișiere și transferul de date prin internet). Solicitanții au cerut furnizorului de servicii de internet (ISP) să dezvăluie numele și adresa persoanei care utilizează adresa IP din care au fost trimise fișierele. ISP, ePhone, au contestat cererea, întemeiată pe încălcarea Directivei 2006/24 (Directiva privind păstrarea datelor - invalidată în 2014).

Instanța suedeză a sesizat CJUE, întrebând dacă Directiva 2006/24 se opune aplicării unei dispoziții naționale în temeiul articolului 8 din Directiva 2004/48 (Directiva privind executarea drepturilor de proprietate intelectuală), care permite emiterea unei interdicții care impune ISP să transmită drepturile deținătorilor de drepturi de autor despre acei abonați ale căror adrese IP se presupune că au fost utilizate în caz de încălcare. Întrebarea s-a bazat pe ipoteza că reclamantul a prezentat dovezi clare privind încălcarea unui anumit drept de autor și că măsura este proporțională.

CJUE a subliniat că Directiva 2006/24 se referea exclusiv la tratarea și păstrarea datelor generate de furnizorii de servicii de comunicații electronice în scopul anchetării, depistării și urmăririi penale a infracțiunilor grave și comunicarea acestora autorităților naționale competente. Astfel, o dispoziție națională care transpune Directiva privind aplicarea drepturilor de proprietate intelectuală nu intră în domeniul de aplicare al Directivei 2006/24 și, prin urmare, nu este exclusă de aceasta.[128]

În ceea ce privește comunicarea numelui și adresei în cauză, solicitate de reclamanți, CJUE a considerat că o astfel de acțiune constituie prelucrarea datelor cu caracter personal și intră în domeniul de aplicare al Directivei 2002/58 (Directiva privind confidențialitatea). De asemenea, aceasta a constatat că comunicarea acestor date a fost solicitată în cadrul procedurilor civile în beneficiul titularului dreptului de autor pentru a asigura protecția eficientă a dreptului de autor și, prin urmare, intră în sfera de aplicare a Directivei 2004/48.[129]

CJUE a concluzionat că Directivele 2002/58 și 2004/48 trebuie interpretate în sensul că nu se opun unei reglementări naționale precum cea în cauză în acțiunea principală, în măsura în care această legislație permite instanței naționale sesizate printr-o cerere de ordonare a divulgării datelor cu carac-

128 *Ibidem*, punctele 40–41.

129 *Ibidem*, punctele 52–54. A se vedea şi hotărârea CJUE din 29 ianuarie 2008, în cauza C-275/06, *Productores de Música de España (Promusicae)/ Telefónica de España*, punctul 58.

ter personal pentru a evalua interesele conflictuale implicate, pe baza faptelor fiecărui caz și ținând seama în mod corespunzător de cerințele principiului proporționalității.

1.3.6. Protecţia datelor şi interesele economice

În era digitală, datele au fost descrise drept "noul petrol" al economiei pentru stimularea inovației și a creativității.[130] Multe companii au construit modele robuste de afaceri în domeniul procesării datelor și o astfel de prelucrare implică adesea date cu caracter personal. Anumite societăți ar putea crede că norme specifice legate de protecția datelor cu caracter personal pot duce, în practică, la obligații excesive care ar putea afecta interesele lor economice. Astfel, se pune întrebarea dacă interesele economice ale ispectorilor și operatorilor sau ale publicului larg ar putea justifica limitarea dreptului la protecție a datelor.

Exemplu: În cauza *Google Spania*[131], CJUE a considerat că, în anumite condiții, persoanele au dreptul să solicite motoarelor de căutare să elimine rezultatele căutării din indexul lor de căutare. În raționamentul său, CJUE a subliniat faptul că utilizarea motoarelor de căutare și rezultatele căutării afișate poate stabili un profil detaliat al unui individ. Aceste informații se pot referi la un aspect vast al vieții private al unui individ și nu ar fi putut fi găsite cu ușurință sau interconectate fără un motor de căutare. Aceasta a constituit astfel o interferență potențial gravă cu drepturile fundamentale ale persoanelor vizate asupra vieții private și a protecției datelor cu caracter personal.

CJUE a examinat apoi dacă interferența ar putea fi justificată. În ceea ce privește interesul economic al societății motorului de căutare în efectuarea procesării, CJUE a declarat că "este evident că [ingerința] nu poate fi justificată doar de interesul economic pe care îl are operatorul unui astfel de motor în prelucrare" și "ca regulă", drepturile fundamentale prevăzute la articolele 7 și 8 din Cartă au prioritate față de interesul economic și interesul publicului larg în găsirea informațiilor în urma unei căutări referitoare la numele persoanei vizate.[132]

130 A se vedea, de exemplu, publicaţia din 16 noiembrie 2016 a *Financial Times*(2016), “Datele sunt noul petrol... cine le va deține?”.

131 Hotărârea CJUE din 13 mai 2014, în cauza C-131/12, *Google Spain SL, Google Inc./ Agencia Española de Protección de Datos(AEPD), Mario Costeja González*.

132 *Ibidem*, punctele 81 şi 97.

Unul dintre principalele considerente ale legislației europene privind protecția datelor este acela de a le oferi persoanelor mai mult control asupra datelor lor personale. În special în era digitală, există un dezechilibru între puterea entităților economice care procesează și au acces la cantități mari de date cu caracter personal și la puterea persoanelor cărora le aparțin datele personale pentru a le controla informațiile. CJUE adoptă o abordare de la caz la caz atunci când echilibrează protecția datelor și interesele economice - cum ar fi interesele terților în ceea ce privește societățile pe acțiuni și societățile cu răspundere limitată, după cum se arată în hotărârea Manni.

Exemplu: Cauza *Manni*[133] se referea la includerea datelor personale ale unui particular într-un registru comercial public. Domnul Manni a solicitat Camerei de Comerț din Lecce să șteargă datele sale personale din registrul respectiv, după ce a descoperit că potențialii clienți ar recurge la registru și ar vedea că acesta a fost administratorul unei societăți care a fost declarată în stare de faliment cu mai mult de un deceniu înainte. Această informație prejudiciază potențialii clienți și ar putea avea un impact negativ asupra intereselor sale comerciale.

CJUE a fost chemată să stabilească dacă legea UE recunoaște dreptul de ștergere în acest caz. Pentru a ajunge la concluzia sa, a echilibrat normele UE privind protecția datelor și interesul comercial al d-lui Manni de a elimina informațiile despre falimentul fostei sale societăți, cu interesul public pentru accesul la informații. A luat act de faptul că divulgarea în registrul public al societăților comerciale a fost prevăzută de lege și, în special, de o directivă a UE menită să faciliteze accesul terților la informațiile despre întreprinderi. Dezvăluirea a fost importantă pentru protejarea intereselor terților care ar putea dori să desfășoare o afacere cu o anumită companie, deoarece singurele garanții oferite de societățile pe acțiuni și societățile cu răspundere limitată terților sunt activele lor. Prin urmare, "documentele de bază ale societății în cauză ar trebui să fie dezvăluite pentru ca terții să poată afla conținutul lor și alte informații referitoare la societate, în special particularitățile persoanelor care sunt autorizate să unească societatea".[134]

Având în vedere importanţa scopului legitim urmărit de registru, CJUE a considerat că domnul Manni nu avea dreptul să obţină ştergerea datelor

133 Hotărârea CJUE din 9 martie 2017, în cauza C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/ Salvatore Manni*.

134 *Ibidem*, punctul 49.

cu caracter personal, deoarece necesitatea de a proteja interesele terților în ceea ce privește societățile pe acțiuni și societățile cu răspundere limitată și pentru a asigura certitudinea juridică, comerțul echitabil și, prin urmare, buna funcționare a pieței interne au avut prioritate față de drepturile sale în materie de protecție a datelor. Acest lucru s-a întâmplat în special în contextul în care persoanele care aleg să participe la tranzacții printr-o societate pe acțiuni sau o societate cu răspundere limitată sunt conștiente că sunt obligate să dezvăluie informații referitoare la identitatea și funcțiile lor.

Deși a constatat că nu există motive pentru a obține ștergerea în acest caz, CJUE a recunoscut existența unui drept de opoziție față de prelucrare, menționând: "nu poate fi exclus [...] că pot exista situații specifice în care principalele motive legitime referitoare la cazul specific al persoanei în cauză justifică în mod excepțional că accesul la datele cu caracter personal înscrise în registru este limitat la expirarea unei perioade suficient de lungi [...] care demonstrează un interes specific în consultarea lor".[135]

CJUE a precizat că este de competența instanțelor naționale să evalueze fiecare caz având în vedere toate circumstanțele pertinente ale persoanei respective, existența sau absența unor motive legitime și imperative care ar putea justifica în mod excepțional restricționarea accesului terților la datele personale conținute în registrele societăților. Cu toate acestea, CJUE a precizat că, în cazul lui Manni, simplul fapt că divulgarea datelor sale personale în registru ar fi afectat clientela sa nu putea fi considerată un astfel de motiv legitim și imperativ. Clienții potențiali ai dlui Manni au un interes legitim de a cunoaște informațiile privind falimentul companiei sale anterioare.

Interferența cu drepturile fundamentale ale domnului Manni și ale altor persoane înscrise în registru privind respectarea vieții private și protecția datelor cu caracter personal garantate de articolele 7 și 8 din Cartă a servit unui obiectiv de interes general și a fost necesară și proporțională.

Prin urmare, în cauza Manni, CJUE a considerat că drepturile la protecția datelor și la viața privată nu au fost dominate de interesul terților de a accesa informațiile din registrul societăților în ceea ce privește societățile pe acțiuni și societățile cu răspundere limitată.

135 *Ibidem*, punctul 60.