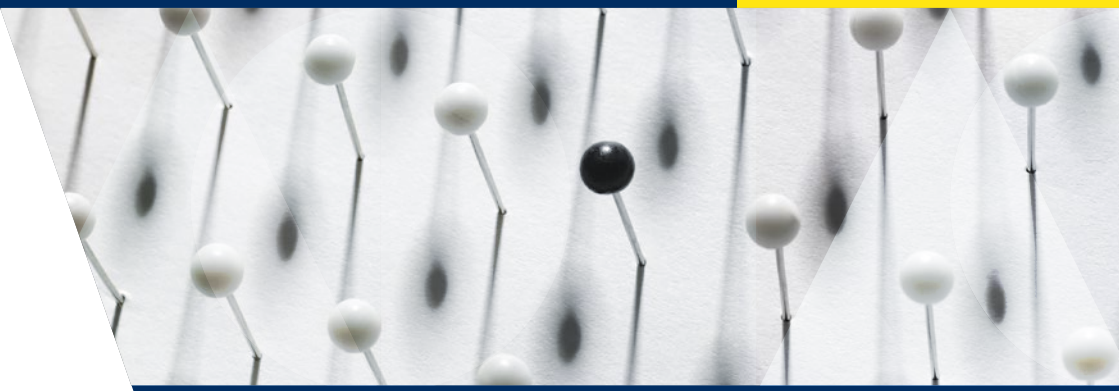
MANUAL



Manual de legislație europeană privind protecția datelor

Ediția 2018

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Manuscrisul prezentului manual a fost finalizat în luna aprilie 2018.

Actualizările vor fi disponibile pe site-ul FRA, la adresa fra.europa.eu, pe site-ul Consiliului Europei, la adresa coe.int/dataprotection, pe site-ul Curții Europene a Drepturilor Omului, la adresa echr.coe.int, în meniul Case-Law (Jurisprudență) și pe site-ul Autorității Europene pentru Protecția Datelor, la adresa edps.europa.eu.

Credit fotografie (copertă și interior): © iStockphoto

© Agenția pentru Drepturi Fundamentale a Uniunii Europene și Consiliul Europei, 2020

Reproducerea este autorizată cu condiția menționării sursei.

Pentru orice utilizare sau reproducere a fotografiilor sau a altor materiale care nu se află sub dreptul de autor al Agenției pentru Drepturi Fundamentale a Uniunii Europene/Consiliului Europei, trebuie să se solicite direct permisiunea deținătorilor drepturilor de autor.

Nici Agenția pentru Drepturi Fundamentale a Uniunii Europene/Consiliul Europei și nicio persoană care acționează în numele Agenției pentru Drepturi Fundamentale a Uniunii Europene/Consiliului Europei nu sunt responsabile pentru utilizarea informațiilor din prezentul manual.

Numeroase alte informații despre Uniunea Europeană sunt disponibile pe internet pe serverul Europa (http://europa.eu).

Luxemburg: Oficiul pentru Publicații al Uniunii Europene, 2020

Consiliul Europei:	ISBN 978-92-871-9824-2		
FRA – Print:	ISBN 978-92-9474-791-4	doi:10.2811/332079	TK-05-17-225-RO-C
FRA – PDF:	ISBN 978-92-9474-787-7	doi:10.2811/582023	TK-05-17-225-RO-N

Prezentul manual a fost redactat în limba engleză. Consiliul Europei (CoE) și Curtea Europeană a Drepturilor Omului (CEDO) nu răspund pentru calitatea traducerii în și din alte limbi. Opiniile exprimate în prezentul manual nu atrag răspunderea CoE și CEDO. Manualul conține o selecție de comentarii și ghiduri. CoE și CEDO nu răspund pentru conținutul acestora. De asemenea, enumerarea acestora în conținutul manualului nu echivalează cu nicio formă de andosare a acestor publicații. Publicațiile ulterioare sunt enumerate pe paginile de internet ale bibliotecii CEDO la adresa echr.coe.int/Library.

Conținutul prezentului manual nu reprezintă o poziție oficială a Autorității Europene pentru Protecția Datelor (AEPD) și nu are caracter obligatoriu pentru AEPD în cadrul exercitării competențelor sale. AEPD nu își asumă responsabilitatea pentru calitatea traducerilor în alte limbi decât engleza.

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Manual de legislație europeană privind protecția datelor

Ediția 2018

Cuvânt-înainte

Societățile noastre devin din ce în ce mai digitalizate. Date fiind aceste transformări, fiecare dintre noi este afectat zilnic și sub diferite forme de ritmul evoluțiilor tehnologice și de modul în care sunt prelucrate datele cu caracter personal. Cadrele juridice ale Uniunii Europene (UE) și ale Consiliului Europei care asigură protecția vieții private și a datelor cu caracter personal au fost revizuite recent.

Europa se află în avangarda protecției datelor la nivel mondial. Standardele UE în materie de protecție a datelor se bazează pe Convenția 108 a Consiliului Europei, pe instrumentele UE – inclusiv Regulamentul general privind protecția datelor și Directiva privind protecția datelor pentru autoritățile polițienești și judiciare din sectorul penal – și pe jurisprudența Curții Europene a Drepturilor Omului și a Curții de Justiție a Uniunii Europene.

Reformele în domeniul protecției datelor realizate de UE și de Consiliul Europei sunt ample și uneori complexe, cu nenumărate beneficii și impact semnificativ asupra persoanelor și întreprinderilor. Prezentul manual urmărește creșterea gradului de conștientizare și îmbunătățirea cunoștințelor privind normele de protecție a datelor, în special în rândul practicienilor nespecializați din domeniul juridic care se confruntă în activitatea lor cu aspecte legate de protecția datelor.

Manualul a fost redactat de Agenția pentru Drepturi Fundamentale a Uniunii Europene (FRA), în colaborare cu Consiliul Europei (alături de Grefa Curții Europene a Drepturilor Omului) și cu Autoritatea Europeană pentru Protecția Datelor. Acesta actualizează ediția din 2014 și face parte dintr-o serie de manuale juridice întocmite în colaborare de FRA și Consiliul Europei.

Mulțumim autorităților de protecție a datelor din Belgia, Elveția, Estonia, Franța, Georgia, Irlanda, Italia, Monaco, Regatul Unit și Ungaria pentru observațiile utile transmise pe marginea versiunii provizorii a manualului. De asemenea, dorim să ne exprimăm aprecierea față de Unitatea pentru protecția datelor a Comisiei Europene și față de unitatea Fluxurile internaționale de date și protecția datelor. Mulțumim Curții de Justiție a Uniunii Europene pentru sprijinul documentar furnizat în timpul lucrărilor de redactare a prezentului manual.

Pe final, am dori să ne exprimăm recunoștința față de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal pentru sprijinul acordat în revizuirea versiunii în limba română a acestui manual.

Christos Giakoumopoulos

Director pentru Drepturile omului și statul de drept, Consiliul Europei

Giovanni Buttarelli

Autoritatea Europeană pentru Protecția Datelor

Michael O'Flaherty

Director al Agenției pentru Drepturi Fundamentale a Uniunii Europene

Cuprins

Abrevieri și acronime

AELS	Asociația Europeană a Liberului Schimb
AEPD	Autoritatea Europeană pentru Protecția Datelor
APD	Autoritate pentru protecția datelor
BCR	Reguli corporatiste obligatorii
Carta	Carta drepturilor fundamentale a Uniunii Europene
CE	Comunitatea Europeană
CEaDO	Convenția europeană a drepturilor omului
CEDO	Curtea Europeană a Drepturilor Omului
CEPD	Comitetul European pentru Protecția Datelor
CETS	Seria de tratate ale Consiliului Europei
CJUE	Curtea de Justiție a Uniunii Europene (înainte de decembrie 2009, denumită Curtea Europeană de Justiție, CEJ)
CoE	Consiliul Europei
Convenția 108	Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Consiliul Europei) Protocolul de modificare (CETS nr. 223) a Convenției 108 („Convenția 108 modernizată") a fost adoptat cu ocazia celei de a 128-a reuniuni a Comitetului de Miniștri al Consiliului Europei, care a avut loc la Elsinore, Danemarca (17-18 mai 2018). Trimiterile la „Convenția 108 modernizată" se referă la convenția modificată prin Protocolul CETS nr. 223.
CRM	Gestionarea relațiilor cu clienții
C-SIS	Sistemul Central de Informații Schengen
DUDO	Declarația universală a drepturilor omului
EFSA	Autoritatea Europeană pentru Siguranța Alimentară
ENISA	Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor
EPPO	Parchetul European
ESMA	Autoritatea Europeană pentru Valori Mobiliare și Piețe
eTEN	Rețele de telecomunicații transeuropene

eu-LISA	Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție
EuroPriSe	Marca europeană de protecție a vieții private
FRA	Agenția pentru Drepturi Fundamentale a Uniunii Europene
GCS	Grupul de coordonare a supravegherii
GPS	Sistem de poziționare globală
ISP	Furnizor de servicii de internet
JO	Jurnalul Oficial
MEA	Mandat european de arestare
N-SIS	Sistemul Național de Informații Schengen
OCDE	Organizația pentru Cooperare și Dezvoltare Economică
OCS	Organism comun de supraveghere
ONG	Organizație neguvernamentală
ONU	Organizația Națiunilor Unite
PIDCP	Pactul internațional cu privire la drepturile civile și politice
PIN	Număr personal de identificare
PNR	Registrul cu numele pasagerilor
RGPD	Regulamentul general privind protecția datelor
RPD	Responsabil cu protecția datelor
SEE	Spațiul Economic European
SEPA	Zona unică de plăți în euro
SIS	Sistemul de informații Schengen
SIV	Sistemul de informații al vămilor
SWIFT	Societatea pentru Telecomunicații Financiare Interbancare Mondiale
TFUE	Tratatul privind funcționarea Uniunii Europene
TIC	Tehnologia informației și comunicațiilor
TUE	Tratatul privind Uniunea Europeană
TVCI	Televiziune cu circuit închis
UE	Uniunea Europeană
UNE	Unitate națională Europol
VIS	Sistemul de informații privind vizele

Cum se utilizează acest manual

Manualul prezintă standardele juridice aplicabile în domeniul protecției datelor, stabilite de Uniunea Europeană (UE) și de Consiliul Europei (CoE). Este conceput astfel încât să ajute practicienii în domeniul dreptului care nu sunt specializați în domeniul protecției datelor, inclusiv avocați, judecători sau alți practicieni în domeniul dreptului, precum și persoanele care lucrează pentru alte organisme, cum ar fi organizații neguvernamentale (ONG-uri), care se pot confrunta cu chestiuni juridice legate de protecția datelor.

Manualul servește ca prim punct de referință pentru legislația UE relevantă și pentru Convenția europeană a drepturilor omului (CEaDO), precum și pentru Convenția CoE pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108) și alte instrumente ale CoE.

Fiecare capitol începe cu un tabel care evidențiază dispozițiile legale relevante pentru subiectele abordate în capitolul respectiv. Tabelele fac trimitere atât la legislația CoE, cât și la dreptul Uniunii, și cuprind selecții din jurisprudența Curții Europene a Drepturilor Omului (CEDO) și a Curții de Justiție a Uniunii Europene (CJUE). Legislația relevantă a celor două ordini juridice europene aplicabilă subiectelor specifice abordate este prezentată apoi succesiv. Acest lucru permite cititorului să observe punctele de convergență ale celor două sisteme juridice și aspectele în care acestea diferă. De asemenea, acest lucru trebuie să ajute utilizatorii să găsească informațiile esențiale referitoare la propria situație, în special dacă se află exclusiv sub incidența legislației CoE. În unele capitole, în cazul în care acest lucru ajută la prezentarea concisă a conținutului, ordinea subiectelor din tabele poate fi puțin diferită față de ordinea din capitolul propriu-zis. Manualul oferă, de asemenea, o scurtă trecere în revistă a cadrului Organizației Națiunilor Unite.

Practicienii din statele care nu sunt membre ale UE, dar sunt membre ale CoE și părți la Convenția europeană a drepturilor omului și la Convenția 108 pot accesa informațiile relevante pentru țara lor prin consultarea directă a secțiunilor privind CoE. Practicienii din statele care nu sunt membre ale UE trebuie să țină cont și de faptul că, de la adoptarea Regulamentului general privind protecția datelor al UE, normele Uniunii în materie de protecție a datelor se aplică organizațiilor și altor entități care nu sunt stabilite în UE dacă prelucrează date cu caracter personal și furnizează produse și servicii persoanelor vizate din Uniune sau monitorizează comportamentul acestor persoane vizate.

Practicienii din statele membre ale UE vor trebui să consulte ambele secțiuni, întrucât aceste state se află sub incidența ambelor ordini juridice. Trebuie remarcat faptul că reformele și modernizarea normelor de protecție a datelor în Europa, întreprinse atât în cadrul Consiliului Europei (Convenția 108 modernizată, astfel cum a fost modificată prin Protocolul CETS nr. 223), cât și în cadrul UE [adoptarea Regulamentului general privind protecția datelor și a Directivei (UE) 2016/680] au fost realizate în paralel. Autoritățile de reglementare din ambele sisteme juridice au depus eforturi consistente pentru a asigura coerența și compatibilitatea între cele două cadre juridice. Astfel, reformele au contribuit la un grad mai mare de armonizare între legislațiile CoE și UE în materie de protecție a datelor. Persoanele care au nevoie de informații suplimentare despre un anumit aspect au la dispoziție o listă de materiale mai specializate în secțiunea „Lecturi suplimentare". Pentru informații referitoare la dispozițiile Convenției 108 și ale protocolului adițional la aceasta din 2001, care continuă să se aplice până la intrarea în vigoare a protocolului de modificare, cititorii trebuie să consulte ediția din 2014 a manualului.

Legislația CoE este prezentată prin scurte trimiteri la o selecție de cauze ale CEDO. Acestea au fost alese dintr-un număr mare de hotărâri și decizii CEDO existente cu privire la aspecte legate de protecția datelor.

Legislația relevantă a UE cuprinde măsurile legislative adoptate, dispozițiile relevante ale tratatelor și ale Cartei drepturilor fundamentale a Uniunii Europene, astfel cum sunt interpretate în jurisprudența CJUE. În plus, manualul prezintă avize și orientări adoptate de Grupul de lucru „Articolul 29", organismul consultativ însărcinat, în temeiul Directivei privind protecția datelor, cu furnizarea de consultanță de specialitate statelor membre ale UE și care va fi înlocuit de Comitetul European pentru Protecția Datelor (CEPD) începând cu 25 mai 2018. Manualul cuprinde, de asemenea, avize ale Autorității Europene pentru Protecția Datelor, care oferă la rândul lor contribuții importante privind interpretarea dreptului UE.

Cauzele descrise sau citate în prezentul manual oferă exemple care ilustrează un corpus semnificativ din jurisprudența CEDO și a CJUE. Orientările de la sfârșitul manualului sunt destinate să ajute cititorii în căutarea online a jurisprudenței. Jurisprudența CJUE prezentată se referă la fosta Directivă privind protecția datelor. Cu toate acestea, interpretările CJUE continuă să se aplice drepturilor și obligațiilor corespunzătoare stabilite de Regulamentul general privind protecția datelor.

În plus, se oferă exemple practice cu scenarii ipotetice în casetele de text cu fundal albastru. Acestea ilustrează și mai bine aplicarea concretă a normelor europene de

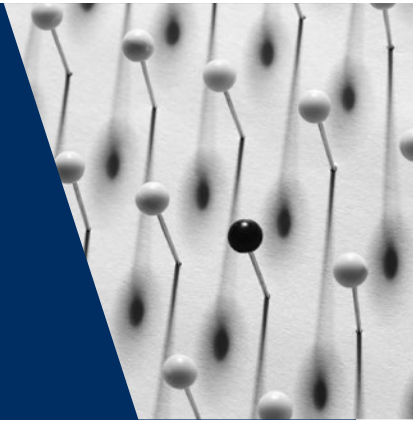
protecție a datelor, în special în cazuri în care nu există o jurisprudență specifică relevantă a CEDO sau a CJUE. Alte casete de text – cele cu fundal gri – oferă exemple preluate din alte surse decât jurisprudența CEDO și a CJUE, cum ar fi legislația și avizele emise de Grupul de lucru „Articolul 29".

Manualul începe cu o scurtă descriere a rolului celor două sisteme juridice, rol stabilit prin legislația UE și a Convenției europene a drepturilor omului (capitolul 1). Capitolele 2-10 tratează următoarele aspecte:

- terminologia în domeniul protecției datelor;
- principiile-cheie ale legislației europene privind protecția datelor;
- normele legislației europene privind protecția datelor;
- supravegherea independentă;
- drepturile persoanelor vizate și aplicarea acestora;
- transferurile și fluxurile transfrontaliere de date cu caracter personal;
- protecția datelor în contextul poliției și justiției penale;
- alte norme europene de protecție a datelor în domenii specifice;
- provocările moderne legate de protecția datelor cu caracter personal.

1

Contextul și cadrul legislației europene privind protecția datelor



UE	Aspecte vizate	CoE
Dreptul la protecția datelor		
Tratatul privind funcționarea Uniunii Europene, articolul 16 Carta drepturilor fundamentale a Uniunii Europene (Carta), articolul 8 (dreptul la protecția datelor cu caracter personal) Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (Directiva privind protecția datelor), JO 1995 L 281 (în vigoare până în mai 2018) Decizia-cadru 2008/977/JAI a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, JO 2008 L 350 (în vigoare până în mai 2018) Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), JO 2016 L 119		Convenția europeană a drepturilor omului, articolul 8 (dreptul la respectarea vieții private și de familie, a domiciliului și a corespondenței) Convenția modernizată pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108 modernizată)

UE	Aspecte vizate	CoE
Directiva (UE) 2016/680 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (Directiva privind protecția datelor destinată autorităților polițienești și judiciare), JO 2016 L 119 Directiva 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), JO 2002 L 201 Regulamentul (CE) nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (Regulamentul privind protecția datelor de către instituțiile europene), JO 2001 L 8		
Limitări ale dreptului la protecția datelor cu caracter personal		
Carta, articolul 52 alineatul (1) Regulamentul general privind protecția datelor, articolul 23 Hotărârea CJUE [MC] în cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*, 2010		Convenția europeană a drepturilor omului, articolul 8 alineatul (2) Convenția 108 modernizată, articolul 11 Hotărârea CEDO [MC] în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04, 2008
Echilibrarea drepturilor		
Hotărârea CJUE [MC] în cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*, 2010	**Generalități**	

UE	Aspecte vizate	CoE
Hotărârea CJUE [MC] în cauza C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy și Satamedia Oy*, 2008 Hotărârea CJUE [MC] în cauza C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 2014	**Libertatea de exprimare**	Hotărârea CEDO [MC] în cauza *Axel Springer AG/Germania*, nr. 39954/08, 2012 Hotărârea CEDO în cauza *Mosley/Regatul Unit*, nr. 48009/08, 2011 Hotărârea CEDO în cauza *Bohlen/Germania*, nr. 53495/09, 2015
Hotărârea CJUE [MC] în cauza C-28/08 P, *Comisia Europeană/The Bavarian Lager Co. Ltd.*, 2010 Hotărârea CJUE în cauza C-615/13 P, *ClientEarth, PAN Europe/EFSA*, 2015	**Dreptul de acces la documente**	Hotărârea CEDO [MC] în cauza *Magyar Helsinki Bizottság/Ungaria*, nr. 18030/11, 2016
Regulamentul general privind protecția datelor, articolul 90	**Secretul profesional**	Hotărârea CEDO în cauza *Pruteanu/România*, nr. 30181/05, 2015
Regulamentul general privind protecția datelor, articolul 91	**Libertatea religioasă sau de convingeri**	
	Libertatea artelor și științelor	Hotărârea CEDO în cauza *Vereinigung bildender Künstler/Austria*, nr. 68354/01, 2007
Hotărârea CJUE [MC] în cauza C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, 2008	**Protecția proprietății**	
Hotărârea CJUE [MC] în cauza C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 2014 Hotărârea CJUE în cauza C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 2017	**Drepturi economice**	

1.1. Dreptul la protecția datelor cu caracter personal

Principalele elemente

- În conformitate cu articolul 8 din Convenția europeană a drepturilor omului, dreptul unei persoane 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 deocamdată singurul – instrument internațional obligatoriu din punct de vedere juridic care tratează protecția datelor. Convenția a trecut printr-un proces de modernizare, finalizat prin adoptarea Protocolului de modificare CETS nr. 223.
- În dreptul UE, protecția datelor a fost recunoscută ca drept fundamental distinct. Acesta este consacrat la articolul 16 din Tratatul privind funcționarea UE, precum și la articolul 8 din Carta drepturilor fundamentale a UE.
- În dreptul UE, protecția datelor a fost reglementată pentru prima dată în 1995, prin Directiva privind protecția datelor.
- Având în vedere progresele tehnologice rapide, UE a adoptat o nouă legislație în 2016 pentru a adapta normele de protecție a datelor la epoca digitală. Regulamentul general privind protecția datelor a devenit aplicabil în mai 2018, abrogând Directiva privind protecția datelor.
- Pe lângă Regulamentul general privind protecția datelor, UE a adoptat acte legislative privind prelucrarea datelor cu caracter personal de către autoritățile de stat în scopul aplicării legii. Directiva (UE) 2016/680 stabilește normele și principiile de protecție a datelor care reglementează prelucrarea datelor cu caracter personal în scopul prevenirii, investigării, depistării și urmăririi penale a infracțiunilor sau în scopul executării sancțiunilor penale.

1.1.1. Dreptul la respectarea vieții private și dreptul la protecția datelor cu caracter personal: scurtă introducere

Deși strâns legate, dreptul la respectarea vieții private și dreptul la protecția datelor cu caracter personal sunt drepturi distincte. Dreptul la viață privată – menționat în legislația europeană ca drept la respectarea vieții private – a fost consacrat în dreptul internațional al drepturilor omului prin Declarația universală a drepturilor omului

(DUDO) adoptată în 1948, ca unul dintre drepturile fundamentale protejate ale omului. La scurt timp după adoptarea DUDO, Europa a consacrat la rândul său acest drept în Convenția europeană a drepturilor omului (CEaDO), un tratat obligatoriu din punct de vedere juridic pentru părțile contractante, care a fost elaborat în 1950. Convenția europeană a drepturilor omului prevede că orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului și a corespondenței. Atingerea adusă acestui drept de o autoritate publică este interzisă, cu excepția cazurilor în care intervenția este în conformitate cu legea, urmărește interese publice importante și legitime și este necesară într-o societate democratică.

DUDO și Convenția europeană a drepturilor omului au fost adoptate cu mult înainte de apariția computerelor și a internetului și de ascensiunea societății informaționale. Aceste evoluții au oferit beneficii considerabile persoanelor și societății, îmbunătățind calitatea vieții, eficiența și productivitatea. În același timp, totuși, au creat noi riscuri în ceea ce privește dreptul la respectarea vieții private. Ca răspuns la necesitatea unor norme specifice care să reglementeze colectarea și utilizarea de informații cu caracter personal, a apărut un nou concept al vieții private, cunoscut în unele jurisdicții drept „confidențialitatea informațiilor", iar în altele ca „dreptul la autodeterminare informațională"[1]. Acest concept a dus la elaborarea de reglementări juridice speciale care să asigure protecția datelor cu caracter personal.

Protecția datelor în Europa a început în anii 1970, odată cu adoptarea – de către unele state – a unor acte legislative care vizau gestionarea prelucrării informațiilor cu caracter personal de către autoritățile publice și întreprinderile mari[2]. Ulterior, s-au instituit instrumente de protecție a datelor la nivel european[3] și, de-a lungul anilor, protecția datelor a devenit o valoare distinctă, care nu este subsumată dreptului la respectarea vieții private. În ordinea juridică a Uniunii, protecția datelor este

1 Curtea Constituțională Federală a Germaniei a consacrat un drept la autodeterminare informațională în hotărârea din 1983 pronunțată în cauza *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. Curtea a considerat că autodeterminarea informațională derivă din dreptul fundamental la respectarea personalității, protejat în Constituția Germaniei. CEDO a recunoscut într-o hotărâre din 2017 că articolul 8 din Convenția europeană a drepturilor omului „prevede dreptul la o formă de autodeterminare informațională". Vezi Hotărârea CEDO [MC] din 27 iunie 2017 în cauza *Satakunnan Markkinapörssi Oy și Satamedia Oy/Finlanda*, nr. 931/13, punctul 137.

2 Landul Hessa a adoptat în 1970 prima lege privind protecția datelor, care s-a aplicat doar în acest land. În 1973, Suedia a adoptat prima lege națională privind protecția datelor. Până la sfârșitul anilor 1980, mai multe state europene (Franța, Germania, Regatul Unit și Țările de Jos) au adoptat, de asemenea, acte legislative privind protecția datelor.

3 Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată 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.

recunoscută ca 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 vizează protejarea unor valori similare, respectiv autonomia și demnitatea umană a indivizilor, asigurându-le o sferă personală în care aceștia să își poată dezvolta personalitatea, să poată gândi și să își poată forma opinii în mod liber. Aceste drepturi sunt, așadar, o condiție esențială pentru exercițiul altor libertăți fundamentale, precum libertatea de exprimare, libertatea de întrunire și de asociere pașnică și libertatea religioasă.

Cele două drepturi diferă în ceea ce privește formularea și domeniul de aplicare. Dreptul la respectarea vieții private constă în interzicerea generală a ingerințelor, sub rezerva anumitor criterii de interes public care pot justifica intervenția în anumite cazuri. Protecția datelor cu caracter personal este privită ca fiind un drept modern și activ[4], care instituie un sistem de ponderi și contraponderi pentru a proteja indivizii în orice situație în care le sunt prelucrate datele cu caracter personal. Prelucrarea acestor date trebuie să respecte elementele esențiale ale protecției datelor cu caracter personal, și anume supravegherea independentă și respectarea drepturilor persoanelor vizate[5].

Articolul 8 din Carta Drepturilor Fundamentale a Uniunii Europene (Carta) consacră nu doar dreptul la protecția datelor cu caracter personal, ci și valorile fundamentale asociate acestui drept. Acesta prevede că asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Persoanele fizice trebuie să aibă dreptul de acces la datele lor cu caracter personal și dreptul de a obține rectificarea acestora, iar respectarea acestui drept trebuie să facă obiectul controlului exercitat de o autoritate independentă.

4 Avocatul general Sharpston a descris situația ca implicând două drepturi distincte: dreptul „clasic" la protecția vieții private și un drept mai „modern", și anume dreptul la protecția datelor. Vezi Hotărârea CJUE din 17 iunie 2010 în cauzele conexate C-92/09 și C-93/02, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*, și *Concluziile avocatului general Sharpston*, punctul 71.

5 Hustinx, P., *EDPS Speeches & Articles* (Discursuri și articole ale AEPD), *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation* (Legislația UE în materie de protecție a datelor: revizuirea Directivei 95/46/CE și propunerea de regulament general privind protecția datelor), iulie 2013.

Dreptul la protecția datelor cu caracter personal se aplică ori de câte ori sunt prelucrate date cu caracter personal; astfel, are un domeniu de aplicare mai larg decât dreptul la respectarea vieții private. Orice operațiune de prelucrare a datelor cu caracter personal intră sub incidența protecției adecvate. Protecția datelor se referă la toate tipurile de date cu caracter personal și de prelucrări de date cu caracter personal, indiferent de legătura acestora cu viața privată și de impactul asupra acesteia. Prelucrarea datelor cu caracter personal poate, de asemenea, să încalce dreptul la viață privată, după cum se arată în exemplele de mai jos. Cu toate acestea, nu este necesar să se demonstreze o încălcare a dreptului la respectarea vieții private pentru ca normele de protecție a datelor să fie aplicate.

Dreptul la viață privată se referă la situațiile în care a fost compromis(ă) un interes privat sau „intimitatea" unei persoane. Astfel cum se arată în acest manual, conceptul de „viață privată" a fost interpretat în sens larg în jurisprudență ca aplicându-se unor situații intime, informații sensibile sau confidențiale, informații care ar putea aduce atingere percepției publice despre o persoană și chiar aspecte care țin de viața profesională și de comportamentul public. Cu toate acestea, aprecierea dacă există sau nu există sau dacă a existat sau nu a existat o ingerință în „viața privată" depinde de contextul și de faptele fiecărui caz.

În schimb, orice operațiune care implică prelucrarea datelor cu caracter personal poate intra sub incidența normelor de protecție a datelor și poate face obiectul dreptului la protecția datelor cu caracter personal. De exemplu, în cazul în care un angajator înregistrează informații referitoare la numele și remunerația plătită angajaților, simpla înregistrare a acestor informații nu poate fi considerată ca fiind o ingerință în viața privată. O astfel de ingerință ar putea fi însă invocată dacă, de exemplu, angajatorul a transferat informațiile cu caracter personal ale angajaților către părți terțe. Angajatorii trebuie să respecte în orice situație normele de protecție a datelor, deoarece înregistrarea informațiilor despre angajați constituie o operațiune de prelucrare a datelor.

Exemplu: În cauza *Digital Rights Ireland*[6], CJUE a fost sesizată să se pronunțe cu privire la valabilitatea Directivei 2006/24/CE în ceea ce privește drepturile fundamentale la protecție a datelor cu caracter personal și la respectarea vieții private, consacrate în Carta drepturilor fundamentale a UE. Directiva

6 Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții și Kärntner Landesregierung și alții*.

impunea furnizorilor de servicii de comunicații electronice destinate publicului sau rețelelor publice de comunicații să păstreze datele din telecomunicații ale cetățenilor pe o perioadă de până la doi ani, pentru a se asigura disponibilitatea datelor în scopul prevenirii, investigării și urmăririi penale a infracțiunilor grave. Măsura viza numai metadatele, datele de localizare și datele necesare identificării abonatului sau a utilizatorului, fără a se aplica conținutului comunicațiilor electronice.

CJUE a considerat că directiva aduce atingere dreptului fundamental la protecția datelor cu caracter personal „întrucât prevede o prelucrare a datelor cu caracter personal”[7]. În plus, Curtea a constatat că directiva aduce atingere dreptului la respectarea vieții private[8]. Luate în ansamblu, datele cu caracter personal păstrate în temeiul directivei și la care puteau avea acces autoritățile competente ar fi putut permite „deducerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, precum obiceiurile din viața cotidiană, locurile de ședere permanente sau temporare, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele”[9]. Cele două drepturi au fost încălcate în mod global și deosebit de grav.

CJUE a declarat Directiva 2006/24/CE nulă, constatând că, deși aceasta urmărea un scop legitim, încălcarea drepturilor 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 internațional: Organizația Națiunilor Unite

Cadrul ONU nu recunoaște protecția datelor cu caracter personal ca pe un drept fundamental, cu toate că dreptul la respectarea vieții private este un drept fundamental stabilit de mult timp în ordinea juridică internațională. Articolul 12 din DUDO privind respectarea vieții private și de familie[10] a marcat prima ocazie în care

7 *Ibidem*, punctul 36.

8 *Ibidem*, punctele 32-35.

9 *Ibidem*, punctul 27.

10 Organizația Națiunilor Unite (ONU), Declarația Universală a Drepturilor Omului (DUDO), 10 decembrie 1948.

un instrument internațional stabilea dreptul unei persoane la protecția sferei sale private împotriva imixtiunii altora, în special împotriva intervenției statului. Deși este o declarație fără caracter obligatoriu, DUDO are un statut semnificativ ca instrument fundamental al dreptului internațional al drepturilor omului și a influențat elaborarea altor instrumente de protecție a drepturilor omului în Europa. Pactul internațional cu privire la drepturile civile și politice (PIDCP) a intrat în vigoare în 1976. Acesta prevede că nimeni nu poate fi supus la imixtiuni arbitrare sau ilegale în viața privată, în domiciliul sau corespondența sa și nimănui nu i se pot leza ilegal onoarea și reputația. PIDCP este un tratat internațional prin care cele 169 de părți se angajează să respecte și să asigure exercițiul drepturilor civile ale persoanelor, inclusiv dreptul la viață privată.

După 2013, ONU a adoptat două rezoluții referitoare la aspecte legate de viața privată ale căror titluri includ „dreptul la viață privată în era digitală”[11], ca răspuns la dezvoltarea de noi tehnologii și la dezvăluirile privind supravegherea în masă desfășurată în unele state (dezvăluirile lui Snowden). Aceste rezoluții 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 asupra libertății de exprimare, precum și asupra funcționării unei societăți dinamice și democratice. Deși nu au caracter obligatoriu din punct de vedere juridic, acestea au dat naștere unei dezbateri politice importante la nivel înalt și la scară internațională pe tema vieții private, a noilor tehnologii și a supravegherii. De asemenea, au dus la instituirea unui raportor special pentru dreptul la viață privată, care are mandatul de a promova și de a proteja acest drept. Sarcinile specifice ale raportorului includ culegerea de informații privind practicile și experiențele naționale în materie de respectare a vieții private și provocările create de noile tehnologii, schimbul și promovarea de bune practici și identificarea eventualelor obstacole.

În timp ce rezoluțiile anterioare s-au concentrat asupra efectelor negative ale supravegherii în masă și asupra responsabilității statelor de a limita prerogativele serviciilor de informații, rezoluțiile mai recente reflectă o evoluție esențială a dezbaterii privind aspectele legate de viața privată în cadrul Organizației Națiunilor Unite[12]. Rezoluțiile adoptate în 2016 și 2017 reafirmă necesitatea de a limita prerogativele

11 Vezi Adunarea Generală a ONU, Rezoluția privind dreptul la viață privată în era digitală, A/RES/68/167, New York, 18 decembrie 2013, și Adunarea Generală a ONU, Proiect de rezoluție revizuită privind dreptul la viață privată în era digitală, A/C.3/69/L.26/Rev. 1, New York, 19 noiembrie 2014.

12 Adunarea Generală a ONU, Proiect de rezoluție revizuită privind dreptul la viață privată în era digitală, A/C.3/71/L.39/Rev. 1, New York, 16 noiembrie 2016; ONU, Consiliul pentru Drepturile Omului, Dreptul la viață privată în era digitală, A/HRC/34/L.7/Rev. 1, 22 martie 2017.

agențiilor de informații și de a condamna supravegherea în masă. Cu toate acestea, ele afirmă în mod explicit că „posibilitățile tot mai mari ale întreprinderilor de a colecta, de a prelucra și de a utiliza date cu caracter personal pot constitui un risc pentru exercitarea dreptului la viață privată în era digitală". Astfel, pe lângă responsabilitatea autorităților de stat, rezoluțiile menționează și responsabilitatea sectorului privat de a respecta drepturile omului și solicită întreprinderilor să informeze utilizatorii cu privire la colectarea, utilizarea, partajarea și păstrarea datelor cu caracter personal ale acestora și să adopte politici de prelucrare transparente.

1.1.3. Convenția europeană a drepturilor omului

Consiliul Europei a luat ființă imediat după cel de al Doilea Război Mondial pentru a reuni statele Europei în vederea promovării principiului statului de drept, democrației, drepturilor omului și dezvoltării sociale. În acest sens, a adoptat în 1950 Convenția Europeană a Drepturilor Omului, care a intrat în vigoare în 1953.

Părțile contractante au obligația internațională de a respecta Convenția europeană a drepturilor omului. Toate statele membre ale CoE au integrat sau au aplicat deja Convenția europeană a drepturilor omului în legislația lor națională, fapt care le obligă să acționeze în conformitate cu dispozițiile convenției. Părțile contractante trebuie să respecte drepturile prevăzute de convenție atunci când exercită o activitate sau o prerogativă. Aici se includ activitățile întreprinse în sfera securității naționale. Hotărârile de referință ale Curții Europene a Drepturilor Omului (CEDO) au avut ca obiect activități ale statelor în domeniile sensibile ale legislației și practicii în materia securității naționale[13]. Curtea nu a ezitat să afirme că activitățile de supraveghere constituie o încălcare a dreptului la respectarea vieții private[14].

Pentru a garanta respectarea de către părțile contractante a obligațiilor ce le revin în conformitate cu Convenția europeană a drepturilor omului, în anul 1959 a fost înființată la Strasbourg, în Franța, CEDO. CEDO se asigură că statele își respectă obligațiile ce le revin în conformitate cu convenția, prin tratarea plângerilor formulate de persoane fizice, grupuri de persoane, ONG-uri sau persoane juridice, care invocă încălcări ale convenției. CEDO poate examina și cauzele interstatale introduse de unul sau mai multe state membre ale CoE împotriva unui alt stat membru.

13 Vezi, de exemplu: Hotărârea CEDO din 6 septembrie 1978 în cauza *Klass și alții/Germania*, nr. 5029/71; Hotărârea CEDO [MC] din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95, și Hotărârea CEDO din 12 ianuarie 2016 în cauza *Szabó și Vissy/Ungaria*, nr. 37138/14.

14 *Ibidem.*

Din 2018, Consiliul Europei are 47 de părți contractante, 28 dintre acestea fiind și state membre ale UE. Nu este obligatoriu ca un reclamant care sesizează CEDO să fie cetățean al uneia dintre părțile contractante, deși presupusele încălcări trebuie să fi avut loc în jurisdicția uneia dintre părțile contractante.

Dreptul la protecția datelor cu caracter personal se numără printre drepturile protejate în temeiul articolului 8 din Convenția europeană a drepturilor omului, care garantează dreptul la respectarea vieții private și de familie, a domiciliului și a corespondenței și stabilește condițiile în baza cărora sunt permise limitări ale acestui drept[15].

CEDO a examinat multe situații care implică probleme de protecție a datelor. Printre acestea se numără interceptarea comunicărilor[16], diferite forme de supraveghere atât din sectorul privat, cât și în cel public[17], precum și protecția împotriva stocării datelor cu caracter personal de autoritățile publice[18]. Respectarea vieții private nu este un drept absolut, întrucât exercițiul dreptului la viață privată ar putea aduce atingere altor drepturi, cum ar fi libertatea de exprimare și accesul la informații și invers. Prin urmare, Curtea încearcă să găsească un echilibru între diferitele drepturi concurente. Aceasta a clarificat faptul că articolul 8 din Convenția europeană a drepturilor omului nu numai că obligă statele să nu întreprindă acțiuni care ar putea încălca dreptul prevăzut de convenție, ci prevede și că acestea sunt supuse, în anumite împrejurări, obligațiilor pozitive de a asigura în mod activ respectarea efectivă a vieții private și de familie[19]. Capitolele corespunzătoare descriu multe dintre aceste cazuri în detaliu.

1.1.4. Convenția 108 a Consiliului Europei

Odată cu apariția tehnologiei informației în anii 1960, a crescut tot mai mult necesitatea unor norme mai detaliate pentru protecția persoanelor fizice prin protejarea datelor lor cu caracter personal. Până la mijlocul anilor 1970, Comitetul de

15 Consiliul Europei, Convenția Europeană a Drepturilor Omului, CETS nr. 005, 1950.

16 Vezi, de exemplu: Hotărârea CEDO din 2 august 1984 în cauza *Malone/Regatul Unit*, nr. 8691/79; Hotărârea CEDO din 3 aprilie 2007 în cauza *Copland/Regatul Unit*, nr. 62617/00, sau Hotărârea CEDO din 18 iulie 2017 în cauza *Mustafa Sezgin Tanrıkulu/Turcia*, nr. 27473/06.

17 Vezi, de exemplu: Hotărârea CEDO din 6 septembrie 1978 în cauza *Klass și alții/Germania*, nr. 5029/71; Hotărârea CEDO din 2 septembrie 2010 în cauza *Uzun/Germania*, nr. 35623/05.

18 Vezi, de exemplu: Hotărârea CEDO [MC] din 4 decembrie 2015 în cauza *Roman Zakharov/Rusia*, nr. 47143/06; Hotărârea CEDO din 12 ianuarie 2016 în cauza *Szabó și Vissy/Ungaria*, nr. 37138/14.

19 Vezi, de exemplu: Hotărârea CEDO din 17 iulie 2008 în cauza *I/Finlanda*, nr. 20511/03; Hotărârea CEDO din 2 decembrie 2008 în cauza *K.U./Finlanda*, nr. 2872/02.

Miniștri al Consiliului Europei a adoptat diferite rezoluții privind protecția datelor cu caracter personal, cu referire la articolul 8 din Convenția europeană a drepturilor omului[20]. În 1981 a fost deschisă pentru semnare Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108)[21]. Convenția 108 a fost, și rămâne încă, singurul instrument internațional obligatoriu din punct de vedere juridic în domeniul protecției datelor.

Convenția 108 se aplică tuturor operațiunilor de prelucrare a datelor efectuate de sectorul privat și cel public, inclusiv prelucrării datelor de către autoritățile judiciare și autoritățile de aplicare a legii. Aceasta protejează persoanele împotriva abuzurilor care pot însoți prelucrarea datelor cu caracter personal și, totodată, urmărește să reglementeze fluxurile transfrontaliere de date cu caracter personal. În ceea ce privește prelucrarea datelor cu caracter personal, principiile prevăzute de convenție privesc, în special, culegerea și prelucrarea automatizată corecte și legale ale datelor, în scopurile legitime precizate. Aceasta înseamnă că datele nu trebuie utilizate în moduri incompatibile cu aceste scopuri și nu trebuie păstrate mai mult decât este necesar. Principiile vizează, de asemenea, calitatea datelor, în special caracterul lor oportun, relevant și neexcesiv (proporțional), precum și exact.

Pe lângă faptul că oferă garanții pentru prelucrarea datelor cu caracter personal și prevede obligații în materie de securitate a datelor, convenția scoate în afara legii, în absența unor garanții juridice adecvate, prelucrarea datelor „sensibile", precum cele referitoare la rasă, opinii politice, starea de sănătate, convingeri religioase, viață sexuală sau cazier judiciar.

Convenția consacră, de asemenea, dreptul unei persoane fizice de a fi informată cu privire la stocarea informațiilor sale cu caracter personal și, dacă este cazul, de a solicita corectarea acestora. Limitarea drepturilor prevăzute în convenție este posibilă numai atunci când sunt în joc interese prioritare, cum ar fi securitatea statului sau apărarea. În plus, convenția prevede fluxul liber al datelor cu caracter personal între părțile sale contractante și impune anumite restricții asupra fluxurilor către state în care cadrul juridic nu oferă o protecție echivalentă.

20 Consiliul Europei, Comitetul de Miniștri (1973), Rezoluția (73)22 privind protejarea vieții private a persoanelor în ceea ce privește bazele de date electronice din sectorul privat, 26 septembrie 1973; Consiliul Europei, Comitetul de Miniștri (1974), Rezoluția (74)29 privind protecția vieții private a persoanelor în ceea ce privește bazele de date electronice din sectorul public, 20 septembrie 1974.

21 Consiliul Europei, Convenția pentru protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal, CETS nr. 108, 1981.

Trebuie remarcat faptul că Convenția 108 are caracter obligatoriu pentru statele care au ratificat-o. Nu este supusă controlului jurisdicțional al CEDO, dar a fost luată în considerare în jurisprudența CEDO în contextul articolului 8 din Convenția europeană a drepturilor omului. De-a lungul anilor, Curtea a statuat că protecția datelor cu caracter personal este o parte importantă a dreptului la respectarea vieții private (articolul 8) și s-a ghidat după principiile Convenției 108 pentru a determina dacă acest drept fundamental a fost sau nu a fost încălcat[22].

Pentru a elabora în continuare principiile generale și normele prevăzute de Convenția 108, Comitetul Miniștrilor CoE a adoptat o serie de recomandări fără caracter obligatoriu din punct de vedere juridic. Aceste recomandări au influențat elaborarea legislației privind protecția datelor în Europa. De exemplu, de mai mulți ani, singurul instrument european care oferă îndrumări cu privire la utilizarea datelor cu caracter personal în sectorul polițienesc a fost Recomandarea privind sectorul polițienesc[23]. Principiile cuprinse în recomandare, cum ar fi mijloacele de păstrare a fișierelor de date și necesitatea de a pune în aplicare norme clare privind persoanele care au acces la aceste fișiere, au fost dezvoltate în continuare și se reflectă în legislația UE ulterioară[24]. Recomandările mai recente încearcă să abordeze provocările erei digitale – de exemplu, prelucrarea datelor în contextul ocupării forței 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 la aceasta, dar respectivele amendamente nu au mai intrat în vigoare[25]. În 2001 s-a adoptat un protocol adițional la Convenția 108. Acesta a introdus dispoziții privind fluxurile transfrontaliere de date către țări care nu sunt parte la convenție, așa-numitele țări terțe, și cu privire la înființarea obligatorie a autorităților naționale de supraveghere a protecției datelor[26].

22 Vezi, de exemplu: Hotărârea CEDO din 25 februarie 1997 în cauza *Z./Finlanda*, nr. 22009/93.

23 Recomandarea Rec(87)15 din 17 septembrie 1987 a Comitetului de Miniștri al Consiliului Europei către statele membre privind reglementarea utilizării datelor cu caracter personal în sectorul polițienesc.

24 Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, JO 1995 L 281.

25 Consiliul Europei, Amendamente la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), adoptate de Comitetul de Miniștri la Strasbourg, la 15 iunie 1999.

26 Consiliul Europei, Protocol adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor, CETS nr. 181, 2001. Odată cu modernizarea Convenției 108, acest protocol nu mai este aplicabil, întrucât dispozițiile sale au fost actualizate și integrate în Convenția 108 modernizată.

Convenția 108 este deschisă pentru aderarea părților necontractante la CoE. Potențialul convenției ca standard universal și caracterul său deschis pot servi drept bază pentru promovarea protecției datelor la nivel mondial. Până în prezent, 51 de țări sunt părți la Convenția 108. Acestea includ toate statele membre ale Consiliului Europei (47 de țări), Uruguay, prima țară din afara Europei care a aderat (în august 2013), și Mauritius, Senegal și Tunisia, care au aderat în 2016 și 2017.

Convenția a trecut recent printr-un proces de modernizare. O consultare publică desfășurată în 2011 a confirmat cele două obiective principale ale acestei lucrări: sporirea protecției vieții private în domeniul digital și consolidarea mecanismului de urmărire al convenției. Procesul de modernizare s-a axat pe aceste obiective și s-a încheiat prin adoptarea unui protocol de modificare a Convenției 108 (Protocolul CETS nr. 223). Activitatea s-a desfășurat în paralel cu alte reforme ale instrumentelor internaționale de protecție a datelor și alături de reforma normelor UE în materie de protecție a datelor, lansată în 2012. Autoritățile de reglementare din cadrul Consiliului Europei și al UE au depus eforturi considerabile pentru a asigura coerența și compatibilitatea între cele două cadre juridice. Modernizarea păstrează caracterul general și flexibil al convenției și consolidează potențialul acesteia de instrument universal al legislației privind protecția datelor. Aceasta reafirmă și stabilește principii importante și consacră noi drepturi pentru persoanele fizice, extinzând totodată responsabilitățile entităților care prelucrează datele cu caracter personal și asigurând un grad mai mare de asumare a răspunderii. De exemplu, persoanele ale căror date cu caracter personal sunt prelucrate au dreptul de a cunoaște raționamentul prelucrării acestor date și dreptul de a se opune prelucrării respective. Pentru a contracara utilizarea sporită a creării de profiluri în mediul online, convenția stabilește, de asemenea, dreptul persoanei de a nu face obiectul unor decizii bazate exclusiv pe prelucrarea automată, fără a se lua în considerare opiniile sale. Aplicarea eficientă a normelor de protecție a datelor de către autoritățile de supraveghere independente din cadrul părților contractante este considerată esențială pentru punerea concretă în aplicare a convenției. În acest scop, convenția modernizată subliniază necesitatea ca autoritățile de supraveghere să dețină competențe și funcții eficace și să beneficieze de o independență reală în îndeplinirea misiunii lor.

1.1.5. Legislația Uniunii Europene privind protecția datelor

Dreptul UE este format din legislație primară și secundară a Uniunii. Tratatele, și anume Tratatul privind Uniunea Europeană (TUE) și Tratatul privind funcționarea Uniunii Europene (TFUE), au fost ratificate de toate statele membre ale Uniunii și reprezintă „legislația primară a UE". Regulamentele, directivele și deciziile UE au fost adoptate de instituțiile Uniunii care au primit această autoritate în baza tratatelor și constituie „legislația secundară a UE".

Protecția datelor în legislația primară a UE

Tratatele inițiale ale Comunităților Europene nu conțineau referiri la drepturile omului sau la protecția acestora, întrucât Comunitatea Economică Europeană a fost inițial gândită ca o organizație regională axată pe integrarea economică și pe crearea unei piețe comune. Un principiu fundamental care a stat la baza constituirii și dezvoltării Comunităților Europene – și care rămâne valabil și astăzi – este principiul de atribuire a competențelor. Potrivit acestui principiu, UE acționează numai în limitele competențelor care îi sunt atribuite de statele membre, astfel cum se reflectă în tratatele UE. Spre deosebire de Consiliul Europei, tratatele UE nu prevăd competențe explicite în materie de drepturi fundamentale.

Cu toate acestea, pe măsură ce CJUE a fost sesizată cu cauze având ca obiect presupuse încălcări ale drepturilor omului în domenii care intră sub incidența legislației UE, CJUE a oferit o interpretare importantă a tratatelor. Pentru a oferi protecție persoanelor fizice, a inclus drepturile fundamentale în așa-numitele principii generale de drept european. Conform CJUE, aceste principii generale reflectă conținutul protecției drepturilor omului în constituțiile naționale și tratatele privind drepturile omului, în special în Convenția europeană a drepturilor omului. CJUE a declarat că va asigura conformitatea dreptului european cu aceste principii.

Recunoscând faptul că politicile sale pot avea impact asupra drepturilor omului și într-un efort de a face cetățenii să se simtă „mai aproape" de UE, în anul 2000 UE a proclamat Carta drepturilor fundamentale a Uniunii Europene (Carta). Aceasta încorporează întreaga gamă de drepturi civile, politice, economice și sociale ale cetățenilor europeni, sintetizând tradițiile constituționale și obligațiile internaționale comune statelor membre. Drepturile descrise în Cartă se împart în șase secțiuni: demnitate, libertate, egalitate, solidaritate, drepturile cetățenilor și justiție.

Deși inițial a fost doar un document politic, Carta a dobândit caracter juridic obligatoriu[27] ca legislație primară a UE [vezi articolul 6 alineatul (1) din TUE)] odată cu intrarea în vigoare a Tratatului de la Lisabona la 1 decembrie 2009[28]. Dispozițiile Cartei sunt adresate instituțiilor și organismelor UE, impunându-le obligația de a respecta drepturile enumerate în aceasta în cadrul exercitării atribuțiilor lor. De asemenea, dispozițiile Cartei creează obligații pentru statele membre în cazul în care acestea pun în aplicare dreptul Uniunii.

Carta nu numai că garantează respectarea vieții private și a vieții de familie (articolul 7), ci stabilește și dreptul la protecția datelor cu caracter personal (articolul 8). Carta ridică în mod explicit nivelul acestei protecții la cel de drept fundamental în cadrul legislației UE. Instituțiile și organismele UE trebuie să respecte și să garanteze acest drept, precum și statele membre în cazul în care acestea pun în aplicare dreptul Uniunii (articolul 51 din Cartă). Formulat la câțiva ani după Directiva privind protecția datelor, articolul 8 din Cartă trebuie înțeles ca încorporând legislația europeană preexistentă cu privire la protecția datelor. Prin urmare, Carta nu numai că menționează explicit dreptul la protecția datelor la articolul 8 alineatul (1), dar face referire și la principiile-cheie privind protecția datelor la articolul 8 alineatul (2). În sfârșit, articolul 8 alineatul (3) din Cartă solicită unei autorități independente să controleze respectarea acestor principii.

Adoptarea Tratatului de la Lisabona este un punct de reper pentru elaborarea legislației privind protecția datelor, nu doar pentru că a ridicat Carta la statut de act juridic cu caracter obligatoriu, la nivel de drept primar, ci și pentru că acest tratat consacră dreptul la protecția datelor cu caracter personal. Acest drept este prevăzut în mod specific la articolul 16 din TFUE, în partea din tratat dedicată principiilor generale ale UE. Articolul 16 creează și un nou temei juridic, conferind 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 – s-au bazat inițial pe temeiul juridic al pieței interne și pe necesitatea de a armoniza legislațiile naționale astfel încât să nu fie împiedicată libera circulație a datelor în cadrul UE. Articolul 16 din TFUE oferă acum un temei juridic independent pentru o abordare modernă și cuprinzătoare a protecției datelor, care se aplică tuturor domeniilor de competență ale UE, inclusiv cooperarea polițienească și judiciară în materie penală. Articolul 16 din TFUE afirmă, de asemenea, că respectarea

27 UE (2012), Carta drepturilor fundamentale a Uniunii Europene, JO 2012 C 326.

28 Vezi versiunea consolidată a Comunităților Europene (2012), Tratatul privind Uniunea Europeană, JO 2012 C 326, și versiunea consolidată a Comunităților Europene (2012), TFUE, JO 2012 C 326.

normelor de protecție a datelor adoptate în temeiul acestuia trebuie să facă obiectul controlului unor autorități independente de supraveghere. Articolul 16 a servit drept temei juridic pentru adoptarea reformei cuprinzătoare a normelor de protecție a datelor în 2016, și anume Regulamentul general privind protecția datelor și Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale (vezi mai jos).

Regulamentul general privind protecția datelor

Din 1995 și până în mai 2018, principalul instrument juridic al UE pentru 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 circulație a acestor date (Directiva privind protecția datelor)[29]. A fost adoptată în 1995, după ce mai multe state membre adoptaseră deja legi naționale privind protecția datelor[30], ca răspuns la necesitatea de a armoniza aceste legi pentru a asigura un nivel ridicat de protecție și fluxul liber al datelor cu caracter personal între diferitele state membre. Libera circulație a mărfurilor, capitalurilor, serviciilor și persoanelor în cadrul pieței interne necesita un flux liber de date, care nu se putea realiza dacă statele membre nu se puteau baza pe un nivel uniform ridicat de protecție a datelor.

Directiva privind protecția datelor a reflectat principiile de protecție a datelor deja cuprinse în legile naționale și în Convenția 108, extinzându-le în multe cazuri. S-a sprijinit pe posibilitatea, prevăzută la articolul 11 din Convenția 108, de adăugare a unor instrumente de protecție. În special, introducerea în directivă a supravegherii independente ca instrument de îmbunătățire a conformității cu normele privind protecția datelor s-a dovedit a fi o contribuție importantă la funcționarea eficace a legislației europene privind protecția datelor. În consecință, această caracteristică a fost integrată în legislația CoE în 2001, prin Protocolul adițional la Convenția 108. Acest lucru ilustrează interacțiunea strânsă și influența reciprocă pozitivă a celor două instrumente de-a lungul anilor.

29 Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, JO 1995 L 281.

30 Landul Hessa a adoptat în 1970 prima lege privind protecția datelor din lume, care s-a aplicat doar în acest land. Suedia a adoptat *Datalagen* în 1973, Germania a adoptat *Bundesdatenschutzgesetz* în 1976, iar Franța a adoptat *Loi relative à l'informatique, aux fichiers et aux libertés* în 1977. În Regatul Unit, legea Data Protection Act a fost adoptată în 1984. În sfârșit, Țările de Jos au adoptat *Wet Persoonregistraties* în 1989.

Directiva privind protecția datelor a instituit un sistem detaliat și cuprinzător de protecție a datelor în UE. Cu toate acestea, conform sistemului juridic al UE, directivele nu se aplică direct și trebuie transpuse în dreptul național al statelor membre. În mod inevitabil, statele membre dispun de o marjă de apreciere în ceea ce privește transpunerea dispozițiilor directivei. Deși 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. Ca urmare, au fost stabilite norme diverse de protecție a datelor în UE, cu definiții și reguli interpretate diferit în legislațiile naționale. De asemenea, nivelurile de aplicare și severitatea sancțiunilor au variat de la un stat membru la altul. În sfârșit, de la redactarea directivei la mijlocul anilor 1990 au avut loc schimbări semnificative în tehnologia informației. 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 mai mulți ani de dezbateri intense. Dezbaterile privind necesitatea modernizării normelor UE de protecție a 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. Comisia a publicat propunerea de regulament în ianuarie 2012, dând startul unui îndelungat proces legislativ de negocieri între Parlamentul European și Consiliul UE. Regulamentul general privind protecția datelor prevede o perioadă de tranziție de doi ani după adoptare. Regulamentul a devenit aplicabil pe deplin la 25 mai 2018, când Directiva privind protecția datelor a fost abrogată.

Adoptarea, în 2016, a Regulamentului general privind protecția datelor a modernizat legislația UE în materie de protecție a datelor, făcând-o adecvată pentru protejarea drepturilor fundamentale în contextul provocărilor economice și sociale ale erei digitale. RGPD menține și dezvoltă principiile și drepturile fundamentale ale persoanei vizate prevăzute de Directiva privind protecția datelor. În plus, a introdus noi obligații care impun organizațiilor să pună în aplicare protecția datelor din faza de proiectare și protecția implicită a datelor, să numească un responsabil cu protecția datelor în anumite circumstanțe, să respecte un nou drept la portabilitatea datelor și să respecte principiul responsabilității. Conform legislației UE, regulamentele sunt aplicabile în mod direct, nu este necesară punerea în aplicare la nivel național. Astfel, Regulamentul general privind protecția datelor stabilește un set unic de norme de protecție a datelor în întreaga UE. Acest fapt generează norme coerente de protecție

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

a datelor în întreaga UE, creând un mediu de securitate juridică de care pot beneficia operatorii economici și persoanele fizice în calitate de „persoane vizate".

Cu toate acestea, deși Regulamentul general privind protecția datelor este aplicabil în mod direct, statele membre trebuie să își actualizeze legislațiile naționale în materie de protecție a datelor pentru a le alinia pe deplin la regulament, păstrând totodată o marjă de apreciere pentru dispoziții specifice, astfel cum se menționează la considerentul 10. Principalele norme și principii stabilite în regulament și drepturile solide pe care le conferă acesta persoanelor fizice formează o parte importantă a prezentului manual și sunt prezentate în capitolele următoare. Regulamentul conține norme cuprinzătoare privind domeniul de aplicare teritorial. Acesta se aplică întreprinderilor stabilite în UE, precum și operatorilor și persoanelor împuternicite de aceștia care nu sunt stabiliți în UE, dar care furnizează produse sau servicii persoanelor vizate din UE sau le monitorizează comportamentul. Dat fiind faptul că mai multe societăți din domeniul tehnologiei din afara continentului dețin o cotă esențială pe piața europeană și au milioane de clienți în UE, impunerea obligației acestor organizații de a respecta normele UE de protecție a datelor este importantă pentru a asigura protecția persoanelor și pentru a asigura condiții de concurență echitabile.

Protecția datelor în cadrul aplicării legii – Directiva (UE) 2016/680

Directiva privind protecția datelor abrogată a instituit un regim cuprinzător de protecție a datelor. Acest regim a fost îmbunătățit acum prin adoptarea Regulamentului general privind protecția datelor. Deși Directiva privind protecția datelor abrogată era cuprinzătoare, domeniul său de aplicare se limita la activitățile aferente pieței interne și la activitățile autorităților publice, altele decât cele de aplicare a legii. Prin urmare, era necesară adoptarea unor instrumente speciale pentru a obține claritatea și echilibrul necesare între protecția datelor și alte interese legitime și pentru a răspunde unor provocări deosebit de pertinente din sectoare specifice. Acesta este cazul normelor care reglementează prelucrarea datelor cu caracter personal de către autoritățile de aplicare a legii.

Primul instrument juridic al UE care a reglementat acest domeniu 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 acesteia se aplicau doar datelor polițienești și judiciare care făceau obiectul unui schimb între statele membre. Prelucrarea la nivel național a datelor cu caracter personal de către autoritățile de aplicare a legii era exclusă din domeniul său de aplicare.

Directiva (UE) 2016/680 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date[32], denumită și Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale, a rectificat această situație. Adoptată în paralel cu Regulamentul general privind protecția datelor, directiva a abrogat Decizia-cadru 2008/977/JAI și a instituit un sistem cuprinzător de protecție a datelor cu caracter personal în contextul aplicării legii, recunoscând în același timp particularitățile prelucrării datelor în domeniul securității publice. În timp ce Regulamentul general privind protecția datelor stabilește norme generale pentru a proteja persoanele fizice în ceea ce privește prelucrarea datelor lor cu caracter personal și pentru a asigura libera circulație a acestor date în UE, directiva stabilește norme specifice de protecție a datelor în domeniul cooperării judiciare în materie penală și al cooperării polițienești. Atunci când o autoritate competentă prelucrează date cu caracter personal în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor, se aplică Directiva (UE) 2016/680. În cazul în care autoritățile competente prelucrează date cu caracter personal în alte scopuri decât cele menționate anterior, se aplică regimul general prevăzut de Regulamentul general privind protecția datelor. Spre deosebire de predecesoarea sa (Decizia-cadru 2008/977/JAI a Consiliului), domeniul de aplicare al Directivei (UE) 2016/680 se extinde la prelucrarea la nivel național a datelor cu caracter personal de către autoritățile de aplicare a legii, fără a se limita la schimburile de astfel de date între statele membre. În plus, directiva încearcă să realizeze un echilibru între drepturile persoanelor și obiectivele legitime ale prelucrării datelor în domeniul securității.

În acest scop, directiva consacră dreptul la protecția datelor cu caracter personal și principiile de bază care trebuie să reglementeze prelucrarea datelor, respectând cu strictețe normele și principiile prevăzute de Regulamentul general privind protecția datelor. Drepturile persoanelor fizice și obligațiile impuse operatorilor – de exemplu, în ceea ce privește securitatea datelor, protecția datelor din faza de proiectare și protecția implicită a datelor și notificările în cazul încălcării securității datelor – sunt similare drepturilor și obligațiilor prevăzute de Regulamentul general privind protecția datelor. De asemenea, directiva ia în considerare și încearcă să abordeze provocările tehnologice emergente problematice, care pot avea un impact deosebit de grav asupra persoanelor, cum ar fi utilizarea tehnicilor de creare de profiluri de către

32 Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date, JO L 119, 4 mai 2016.

autoritățile de aplicare a legii. În principiu, deciziile întemeiate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, trebuie interzise[33]. În plus, aceste decizii 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 aibă ca rezultat discriminarea împotriva vreunei persoane[34].

Directiva prevede, de asemenea, norme care să asigure responsabilitatea operatorilor. Aceștia trebuie să desemneze un responsabil cu protecția datelor care să monitorizeze respectarea normelor de protecție a datelor, să informeze și să ofere consultanță entității și angajaților care efectuează prelucrarea cu privire la obligațiile lor și să coopereze cu autoritatea de supraveghere. Prelucrarea datelor cu caracter personal în sectorul polițienesc și al justiției penale face în prezent obiectul supravegherii din partea autorităților de supraveghere independente. Atât regimul juridic general privind protecția datelor, cât și regimul special de protecție a datelor în contextul aplicării legii și al justiției penale trebuie să respecte în egală măsură cerințele Cartei drepturilor fundamentale a UE.

Regimul special pentru prelucrarea datelor în contextul cooperării polițienești și judiciare instituit prin Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale este descris în detaliu la capitolul 8.

Directiva asupra confidențialității și comunicațiilor electronice

De asemenea, s-a considerat necesar să se stabilească norme speciale de protecție a datelor în sectorul comunicațiilor electronice. Odată cu dezvoltarea internetului, a telefoniei fixe și a telefoniei mobile, a fost important să se asigure respectarea drepturilor utilizatorilor la viață privată și la confidențialitate. Directiva 2002/58/CE[35] privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) stabilește norme privind securitatea datelor cu caracter personal în aceste rețele, notificarea în cazul încălcării securității datelor și confidențialitatea comunicațiilor.

33 Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale, articolul 11 alineatul (1).

34 *Ibidem*, articolul 11 alineatele (2) și (3).

35 Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice, JO L 201 (Directiva asupra confidențialității și comunicațiilor electronice).

În ceea ce privește securitatea, operatorii serviciilor 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 preveni distrugerea, pierderea sau deteriorarea accidentală a datelor cu caracter personal[36]. În cazul în care există un risc deosebit de încălcare a securității rețelei publice de comunicații, operatorii trebuie să informeze abonații cu privire la acest risc[37]. Dacă, în pofida măsurilor de securitate puse în aplicare, se produce o încălcare a securității, operatorii trebuie să notifice încălcarea securității datelor cu caracter personal autorității naționale competente însărcinate cu punerea în aplicare și asigurarea respectării directivei. În unele situații, operatorii au obligația de a notifica, de asemenea, persoanelor fizice încălcarea securității datelor cu caracter personal, și anume atunci când încălcarea ar putea să le afecteze în mod negativ datele personale sau viața privată[38]. Confidențialitatea comunicațiilor necesită interzicerea, în principiu, a ascultării, interceptării, stocării sau a oricărui tip de supraveghere sau interceptare a comunicațiilor și a metadatelor. De asemenea, directiva interzice comunicațiile nesolicitate (denumite adesea „spam"), cu excepția cazului în care utilizatorii și-au dat acordul pentru primirea acestora, și conține norme privind stocarea modulelor „cookie" pe computere și dispozitive. Aceste obligații negative fundamentale indică în mod clar că confidențialitatea comunicațiilor este legată în mod semnificativ de protecția dreptului la respectarea vieții private consacrat la 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 asupra confidențialității și comunicațiilor electronice. Reforma urmărește să alinieze normele care reglementează comunicațiile electronice la noul regim de protecție a datelor instituit în temeiul Regulamentului general privind protecția datelor. Noul regulament va fi direct aplicabil în întreaga UE; toate persoanele fizice se vor bucura de același nivel de protecție a comunicațiilor lor electronice, iar operatorii și întreprinderile de telecomunicații vor beneficia de claritate, de securitate juridică și de 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 intră în domeniul de aplicare al Directivei asupra confidențialității și comunicațiilor electronice. Aceasta se referea doar la furnizorii tradiționali de servicii de telecomunicații.

36 Directiva asupra confidențialității și comunicațiilor electronice, articolul 4 alineatul (1).

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

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

Având în vedere utilizarea masivă a serviciilor de tipul Skype, WhatsApp, Facebook Messenger și Viber pentru a trimite mesaje sau pentru a efectua apeluri telefonice, aceste servicii OTT vor intra de acum în domeniul de aplicare al regulamentului și vor trebui să respecte cerințele acestuia cu privire la protecția datelor, respectarea vieții private și securitatea datelor. La data publicării prezentului manual, procesul legislativ având ca obiect normele de confidențialitate a comunicațiilor electronice era încă în desfășurare.

Regulamentul (CE) nr. 45/2001

Având în vedere că Directiva privind protecția datelor se aplica numai statelor membre ale UE, era necesar un instrument juridic suplimentar pentru a stabili protecția datelor pentru prelucrarea datelor cu caracter personal de către instituțiile și organismele UE. Regulamentul (CE) nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date[39] (Regulamentul privind protecția datelor de către instituțiile europene) îndeplinește această atribuție.

Regulamentul (CE) nr. 45/2001 urmează îndeaproape principiile regimului general al UE de protecție a datelor și aplică aceste principii prelucrării datelor de către instituțiile și organismele UE în exercitarea atribuțiilor lor. În plus, instituie o autoritate independentă de supraveghere pentru a monitoriza aplicarea dispozițiilor sale, Autoritatea Europeană pentru Protecția Datelor (AEPD). AEPD este învestită cu competențe de supraveghere și are sarcina de a monitoriza prelucrarea datelor cu caracter personal în instituțiile și organismele UE și de a audia și investiga plângerile având ca obiect presupuse încălcări ale normelor privind protecția datelor. De asemenea, oferă consiliere instituțiilor și organismelor UE cu privire la toate aspectele legate de protecția datelor cu caracter personal, de la propuneri de noi acte legislative până la elaborarea de norme interne privind prelucrarea datelor.

În ianuarie 2017, Comisia Europeană a prezentat o propunere pentru un nou regulament privind prelucrarea datelor de către instituțiile UE, care va abroga actualul regulament. Ca și în cazul reformei Directivei asupra confidențialității și comunicațiilor electronice, reforma Regulamentului (CE) nr. 45/2001 va moderniza și alinia normele acestuia la noul regim de protecție a datelor instituit prin Regulamentul general privind protecția datelor.

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

Rolul CJUE

CJUE are competența de a stabili dacă un stat membru și-a îndeplinit sau nu obligațiile care îi revin în temeiul legislației UE privind protecția datelor și de a interpreta legislația UE pentru a asigura aplicarea eficace și uniformă a acesteia în toate statele membre. De la adoptarea Directivei privind protecția datelor în 1995, s-a acumulat un corpus considerabil de jurisprudență, care clarifică domeniul de aplicare și înțelesul principiilor privind protecția datelor și ale dreptului fundamental la protecția datelor cu caracter personal, astfel cum este consacrat la articolul 8 din Cartă. Deși directiva a fost abrogată și acum este în vigoare un nou instrument juridic, Regulamentul general privind protecția datelor, 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. Limitări ale dreptului la protecția datelor cu caracter personal

Principalele elemente

- Dreptul la protecția datelor cu caracter personal nu este un drept absolut; dacă este necesar, acesta poate fi restrâns în favoarea unui obiectiv de interes general sau pentru a proteja drepturile și libertățile celorlalți.
- Condițiile care pot limita dreptul la respectarea vieții private și dreptul la protecția datelor cu caracter personal sunt enumerate la articolul 8 din Convenția europeană a drepturilor omului și la articolul 52 alineatul (1) din Cartă. Acestea au fost dezvoltate și interpretate prin jurisprudența CEDO și a CJUE.
- În conformitate cu legislația CoE privind protecția datelor, prelucrarea datelor cu caracter personal constituie o intervenție legală în dreptul la respectarea vieții private și nu poate fi efectuată decât dacă:
  - este în conformitate cu legea;
  - urmărește un scop legitim;
  - respectă substanța drepturilor și libertăților fundamentale;
  - este necesară și proporțională într-o societate democratică pentru atingerea unui scop legitim.

- Ordinea juridică a UE stabilește condiții similare pentru limitarea exercițiului drepturilor fundamentale protejate prin Cartă. Orice limitare a oricărui drept fundamental, inclusiv a dreptului la protecția datelor cu caracter personal, poate fi legală doar dacă:
  - este în conformitate cu legea;
  - respectă substanța dreptului în cauză;
  - în acord cu principiul proporționalității, este necesară; și
  - urmărește un obiectiv de interes general recunoscut de UE sau necesitatea protejării drepturilor celorlalți.

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 raport cu funcția sa în societate”[40]. Articolul 52 alineatul (1) din Cartă recunoaște, astfel, că pot fi impuse limitări ale exercițiului unor drepturi, precum cele consacrate la articolele 7 și 8 din aceasta, în măsura în care aceste limitări sunt prevăzute de lege, respectă substanța acestor drepturi și libertăți și, în acord cu principiul proporționalității, sunt necesare și răspund efectiv obiectivelor de interes general recunoscute de UE sau necesității protejării drepturilor și libertăților celorlalți[41]. În mod similar, în sistemul Convenției europene a drepturilor omului, protecția datelor este garantată de articolul 8, iar exercițiul acestui drept poate fi limitat, dacă este necesar, în vederea urmăririi unui scop legitim. Prezenta secțiune se referă la condițiile stabilite pentru intervenție în cadrul Convenției europene a drepturilor omului, astfel cum sunt interpretate de jurisprudența CEDO, și la condițiile stabilite pentru limitările legale în temeiul articolului 52 din Cartă.

1.2.1. Cerințe privind intervenția legitimă în temeiul Convenției europene a drepturilor omului

Prelucrarea datelor cu caracter personal poate constitui o intervenție în dreptul persoanei vizate la respectarea vieții private, protejat de articolul 8 din Convenția europeană a drepturilor omului[42]. Astfel cum s-a explicat mai sus (vezi secțiunea 1.1.1 și secțiunea 1.1.4), contrar ordinii juridice a UE, Convenția europeană

40 Vezi, de exemplu, Hotărârea CJUE [MC] din 9 noiembrie 2010 în cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR* și *Hartmut Eifert/Land Hessen*, punctul 48.

41 *Ibidem*, punctul 50.

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

a drepturilor omului nu consacră protecția datelor cu caracter personal drept un drept fundamental distinct. În schimb, protecția datelor cu caracter personal face parte din drepturile protejate în cadrul dreptului la respectarea vieții private. Astfel, nicio operațiune care implică prelucrarea datelor cu caracter personal nu poate intra sub incidența articolului 8 din Convenția europeană a drepturilor omului. Pentru ca articolul 8 să devină aplicabil, trebuie să se stabilească mai întâi dacă a fost compromis un interes privat sau viața privată a unei persoane. În cadrul jurisprudenței sale, CEDO a tratat conceptul de „viață privată" ca pe un concept larg, aplicabil chiar și unor aspecte care țin de viața profesională și de comportamentul public. De asemenea, a statuat că protecția datelor cu caracter personal constituie o parte importantă a dreptului la respectarea vieții private. Cu toate acestea, în pofida sensului larg conferit conceptului de viață privată, nu toate tipurile de prelucrare ar compromite propriu-zis drepturile protejate în temeiul articolului 8.

Atunci când CEDO consideră că operațiunea de prelucrare în cauză afectează dreptul persoanelor fizice la respectarea vieții private, va examina dacă intervenția este justificată. Dreptul la respectarea vieții private nu este totuși un drept absolut, ci trebuie echilibrat și conciliat cu alte drepturi și interese legitime, fie ale altor persoane (interese particulare), fie ale societății în ansamblu (interese publice).

Condițiile cumulative în care o intervenție ar putea fi justificată sunt următoarele:

Conformitatea cu legea

Potrivit jurisprudenței CEDO, o intervenție este în conformitate cu legea dacă se bazează pe o prevedere a dreptului intern care prezintă anumite calități. Legea trebuie să fie „accesibilă persoanelor în cauză și previzibilă în ceea ce privește efectele sale"[43]. O normă este previzibilă „atunci când este redactată cu suficientă precizie, în așa fel încât să permită oricărei persoane – care, la nevoie, poate apela la consultanță de specialitate – să își corecteze conduita"[44]. De asemenea, „[g]radul de precizie impus «legii» în legătură cu acest aspect va depinde de finalitatea specifică"[45].

43 Hotărârea CEDO [MC] din 16 februarie 2000 în cauza *Amann/Elveția*, nr. 27798/95, punctul 50; vezi, de asemenea, Hotărârea CEDO din 25 martie 1998 în cauza *Kopp/Elveția*, nr. 23224/94, punctul 55, și Hotărârea CEDO din 10 februarie 2009 în cauza *Iordachi și alții/Moldova*, nr. 25198/02, punctul 50.

44 Hotărârea CEDO [MC] din 16 februarie 2000 în cauza *Amann/Elveția*, nr. 27798/95, punctul 56; vezi, de asemenea, Hotărârea CEDO din 2 august 1984 în cauza *Malone/Regatul Unit*, nr. 8691/79, punctul 66; Hotărârea CEDO din 25 martie 1983 în cauza *Silver și alții/Regatul Unit*, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, punctul 88.

45 Hotărârea CEDO din 26 aprilie 1979 în cauza *The Sunday Times/Regatul Unit*, nr. 6538/74, punctul 49; vezi, de asemenea, Hotărârea CEDO din 25 martie 1983 în cauza *Silver și alții/Regatul Unit*, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, punctul 88.

Exemple: În cauza *Rotaru/România*[46], reclamantul a susținut că îi fusese încălcat dreptul la respectarea vieții private prin deținerea și utilizarea de către Serviciul Român de Informații a unui dosar care conținea informațiile sale cu caracter personal. CEDO a constatat că legislația internă permitea colectarea, înregistrarea și arhivarea în fișiere secrete a informațiilor care afectează securitatea națională, dar nu stabilea nicio limitare a exercitării acestor competențe, care rămâneau la aprecierea autorităților. De exemplu, legislația internă nu definea tipul de informații care puteau fi prelucrate, categoriile de persoane împotriva cărora se puteau lua măsuri de supraveghere, circumstanțele în care aceste măsuri puteau fi adoptate sau procedura care trebuia urmată. Prin urmare, Curtea a concluzionat că legislația internă nu respecta cerința de previzibilitate de la articolul 8 din Convenția europeană a drepturilor omului și că acest articol a fost încălcat.

În cauza *Taylor-Sabori/Regatul Unit*[47], reclamantul fusese ținta măsurilor de supraveghere ale poliției. Utilizând o „clonă" a pagerului acestuia, poliția a putut intercepta mesajele care îi erau trimise. Reclamantul a fost arestat și acuzat de conspirație la trafic de substanțe controlate. O parte a dosarului de acuzare a constat în note scrise contemporane din mesajele primite pe pager, care fuseseră transcrise de poliție. Cu toate acestea, la data procesului reclamantului, legislația britanică nu conținea nicio dispoziție care să reglementeze interceptarea comunicațiilor transmise prin intermediul unui sistem privat de telecomunicații. Prin urmare, intervenția asupra drepturilor sale nu a fost „în conformitate cu legea". CEDO a concluzionat că aceasta a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Cauza *Vukota-Bojić/Elveția*[48] a avut ca obiect supravegherea în secret a unui solicitant de asigurări sociale de către anchetatori privați, comandată de compania de asigurări a reclamantei. CEDO a considerat că, deși măsura de supraveghere care făcea obiectul plângerii fusese dispusă de o societate privată de asigurări, societatea respectivă primise din partea statului dreptul de a oferi beneficii provenite din asigurarea medicală obligatorie și de a colecta prime de asigurare. Un stat nu poate fi exonerat de responsabilitate în temeiul

46 Hotărârea CEDO [MC] din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95, punctul 57; vezi, de asemenea, Hotărârea CEDO din 28 iunie 2007 în cauza *Association for European Integration and Human Rights (Asociația pentru integrare europeană și drepturile omului) și Ekimdzhiev/Bulgaria*, nr. 62540/00; Hotărârea CEDO din 21 iunie 2011 în cauza *Shimovolos/Rusia*, nr. 30194/09; și Hotărârea CEDO din 31 mai 2005 în cauza *Vetter/Franța*, nr. 59842/00.

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

48 Hotărârea CEDO din 18 octombrie 2016 în cauza *Vukota-Bojić/Elveția*, nr. 61838/10, punctul 77.

convenției prin faptul că își deleagă obligațiile unor organisme private sau unor persoane fizice. Legislația internă trebuia să ofere garanții suficiente împotriva abuzului pentru ca intervenția asupra drepturilor prevăzute la articolul 8 din Convenția europeană a drepturilor omului să poată fi considerată „în conformitate cu legea". În cazul menționat, CEDO a concluzionat că a avut loc o încălcare a articolului 8 din Convenția europeană a drepturilor omului deoarece legislația internă nu a indicat cu suficientă claritate domeniul de aplicare și modalitatea de exercitare a marjei de apreciere conferite companiilor de asigurări care acționează ca autorități publice în domeniul litigiilor în materie de asigurări și efectuează supravegherea în secret a unei persoane asigurate. În special, legislația internă nu a inclus garanții suficiente împotriva abuzurilor.

Urmărirea unui scop legitim

Scopul legitim poate fi oricare dintre interesele publice numite sau protejarea drepturilor și libertăților celorlalți. Scopurile legitime care ar putea justifica o intervenție sunt, potrivit articolului 8 alineatul (2) din Convenția europeană a drepturilor omului, interesele securității naționale, siguranței publice sau bunăstării economice a unei țări, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei și protecția drepturilor și libertăților altor persoane.

Exemplu: În cauza *Peck/Regatul Unit*[49], reclamantul a încercat să se sinucidă pe stradă tăindu-și venele de la mâini, neștiind că o cameră TVCI îl filmase în timpul tentativei. După ce poliția, care urmărea camerele TVCI, l-a salvat, a transmis înregistrarea camerei TVCI către mass-media, care a publicat-o fără să ascundă fața reclamantului. CEDO a constatat că nu există motive relevante sau suficiente care să justifice dezvăluirea directă către public a înregistrării autorităților fără obținerea consimțământului reclamantului sau ascunderea identității acestuia. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Necesitatea într-o societate democratică

CEDO a stabilit că „noțiunea de necesitate presupune ca intervenția să corespundă unei nevoi sociale presante și, în special, să fie proporțională cu scopul legitim

49 Hotărârea CEDO din 28 ianuarie 2003 în cauza *Peck/Regatul Unit*, nr. 44647/98, punctul 85.

urmărit"[50]. Atunci când evaluează dacă o măsură este necesară pentru a răspunde unei nevoi sociale presante, CEDO examinează relevanța și adecvarea acesteia în raport cu obiectivul urmărit. În acest scop, Curtea poate lua în considerare dacă intervenția încearcă să abordeze o problemă care, dacă nu ar fi abordată, ar putea avea un efect negativ asupra societății, dacă există dovezi că intervenția ar putea atenua acest efect negativ și care este opinia publică la scară largă cu privire la problema în cauză[51]. De exemplu, colectarea și stocarea de către serviciile de securitate a datelor cu caracter personal ale anumitor persoane fizice despre care s-a descoperit că au legături cu mișcările teroriste ar constitui o intervenție asupra dreptului persoanelor fizice la respectarea vieții private, dar corespund totuși unei nevoi sociale majore și presante: securitatea națională și combaterea terorismului. Pentru a trece testul necesității, intervenția trebuie să fie, de asemenea, proporțională. În jurisprudența CEDO, proporționalitatea este abordată în cadrul conceptului de necesitate. Proporționalitatea impune ca o intervenție asupra drepturilor protejate prin Convenția europeană a drepturilor omului să nu depășească ceea ce este necesar pentru atingerea scopului legitim urmărit. Factorii importanți care trebuie luați în considerare la efectuarea testului de proporționalitate sunt domeniul de aplicare a intervenției, în special numărul de persoane afectate, și garanțiile sau avertismentele instituite pentru a restrânge domeniul de aplicare sau efectele negative asupra drepturilor persoanelor[52].

Exemplu: În cauza *Khelili/Elveția*[53], în timpul unui control, poliția a constatat că reclamanta avea asupra sa cărți de vizită pe care scria: „Plăcută, atractivă, spre 40 de ani, doresc să cunosc un domn pentru ieșiri ocazionale în oraș. Telefon [...]". Reclamanta a pretins că, în urma acestei descoperiri, poliția i-a introdus numele în evidențele sale sub titulatura de prostituată, ocupație pe care aceasta a negat-o constant. Reclamanta a solicitat ștergerea cuvântului „prostituată" din evidențele computerizate ale poliției. CEDO a confirmat, în principiu, că păstrarea datelor cu caracter personal ale unei persoane, pe motiv că acea persoană ar putea comite o altă infracțiune, ar putea fi în anumite circumstanțe proporțională. Cu toate acestea, în cazul reclamantei, acuzația de prostituție ilegală părea a fi prea vagă și generală,

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

51 Grupul de lucru „Articolul 29" pentru protecția datelor (Grupul de lucru „Articolul 29") (2014), Opinion on the application of the necessity and proportionality concepts and data protection within the law enforcement sector (Aviz privind aplicarea conceptelor de necesitate și proporționalitate și protecția datelor în sectorul de aplicare a legii), WP 211, Bruxelles, 27 februarie 2014, pp. 7-8.

52 *Ibidem*, pp. 9-11.

53 Hotărârea CEDO din 18 octombrie 2011 în cauza *Khelili/Elveția*, nr. 16188/07.

nu era susținută prin fapte concrete, întrucât aceasta nu fusese condamnată niciodată pentru prostituție ilegală și, prin urmare, nu se putea considera că îndeplinește „o nevoie socială presantă" în sensul articolului 8 din Convenția europeană a drepturilor omului. Considerând că este de competența autorităților să dovedească exactitatea datelor stocate cu privire la reclamantă și având în vedere seriozitatea atingerii asupra drepturilor reclamantei, Curtea a hotărât că reținerea cuvântului „prostituată" în evidențele polițienești o perioadă îndelungată nu este necesară într-o societate democratică. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Exemplu: În cauza *S. și Marper/Regatul Unit*[54], cei doi reclamanți au fost arestați și acuzați de săvârșirea unor infracțiuni. Poliția le-a prelevat amprentele digitale și probe de ADN, conform prevederilor din Police and Criminal Evidence Act (Legea privind probele prelevate de autoritățile polițienești și judiciare penale). Reclamanții nu au fost condamnați pentru presupusele infracțiuni: unul a fost achitat în instanță, iar procedura penală împotriva celui de al doilea a fost suspendată. Cu toate acestea, amprentele digitale, profilurile ADN și probele celulare ale acestora au fost păstrate și stocate de poliție într-o bază de date, iar legislația națională a autorizat păstrarea acestora fără a se aplica vreo limită de timp. Deși Regatul Unit a susținut că păstrarea probelor a contribuit la identificarea unor viitori infractori și, astfel, a urmărit scopul legitim al prevenirii și depistării infracțiunilor, CEDO a considerat că intervenția asupra dreptului reclamanților la respectarea vieții private era nejustificată. Curtea a reamintit că principiile de bază ale protecției datelor impun ca păstrarea datelor cu caracter personal să fie proporțională cu scopul colectării și ca perioadele de păstrare să fie limitate. Curtea a acceptat că extinderea bazei de date pentru a include profilurile ADN nu doar pentru persoanele condamnate, ci și pentru toate persoanele suspectate, dar care nu au fost condamnate, ar fi putut contribui la depistarea și prevenirea infracțiunilor în Regatul Unit. Cu toate acestea, a fost „uimită de caracterul general și nediferențiat al puterii de păstrare"[55] a datelor.

Având în vedere amploarea informațiilor genetice și privind sănătatea conținute în probele celulare, intervenția asupra dreptului reclamanților la respectarea vieții private a fost deosebit de invazivă. Se puteau preleva de la

54 Hotărârea CEDO [MC] din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04.

55 *Ibidem*, punctul 119.

persoanele arestate amprente și probe care puteau fi păstrate pe o perioadă nedeterminată în baza de date a poliției, indiferent de caracterul și de gravitatea infracțiunii și chiar în cazul unor infracțiuni minore, pentru care nu se dispun pedepse cu închisoarea. În plus, persoanele achitate aveau posibilități limitate de a obține ștergerea datelor lor din baza de date. În sfârșit, CEDO a acordat o atenție deosebită faptului că unul dintre reclamanți avea 11 ani la momentul arestării. Păstrarea datelor cu caracter personal ale unui minor care nu este condamnat poate fi deosebit de dăunătoare, având în vedere vulnerabilitatea minorilor și importanța dezvoltării și a integrării acestora în societate[56]. Curtea a statuat, în unanimitate, că păstrarea datelor a constituit o atingere disproporționată adusă dreptului la viață privată, care nu putea fi considerată necesară într-o societate democratică.

Exemplu: În cauza *Leander/Suedia*[57], CEDO a hotărât că un control în secret al candidaților la funcții importante pentru securitatea națională nu contravine, în sine, cerinței de necesitate într-o societate democratică. Garanțiile speciale prevăzute în legislația națională pentru protejarea intereselor persoanelor vizate – de exemplu, controale efectuate de Parlament și de Cancelarul Justiției – au determinat CEDO să concluzioneze că sistemul suedez de control al personalului respectă dispozițiile articolului 8 alineatul (2) din Convenția europeană a drepturilor omului. Având în vedere marja largă de apreciere de care dispunea, statul respondent a fost îndreptățit să considere că, în cazul reclamantului, interesele de securitate națională au prevalat asupra celor individuale. Curtea a concluzionat că nu a existat nicio încălcare a articolului 8 din Convenția europeană a drepturilor omului.

1.2.2. Condițiile limitărilor legale în temeiul Cartei drepturilor fundamentale a UE

Structura și modul de redactare a Cartei sunt diferite de cele ale Convenției europene a drepturilor omului. Carta nu folosește noțiunea de atingere adusă drepturilor garantate, însă conține o dispoziție privind restrângerea (restrângerile) exercițiului drepturilor și libertăților recunoscute de Cartă.

56 *Ibidem*, punctul 124.

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

În conformitate cu articolul 52 alineatul (1), restrângerea exercițiului drepturilor și libertăților recunoscute de Cartă și, în consecință, a exercițiului dreptului la protecția datelor cu caracter personal, este admisibilă numai dacă:

- este prevăzută de lege;
- respectă substanța dreptului la protecția datelor;
- respectă principiul proporționalității, este necesară[58]; și
- îndeplinește obiective de interes general recunoscute de Uniune sau necesitatea protejării drepturilor și libertăților celorlalți.

Întrucât protecția datelor cu caracter personal este un drept fundamental distinct și de sine stătător în ordinea juridică a UE, protejat în temeiul articolului 8 din Cartă, orice prelucrare a datelor cu caracter personal constituie, în sine, o atingere adusă acestui drept. Nu este relevant dacă datele cu caracter personal în cauză se referă la viața privată a unei persoane, dacă sunt sensibile sau dacă persoanele vizate au avut de suferit în vreun fel. Pentru a fi legală, atingerea trebuie să respecte toate condițiile enumerate la articolul 52 alineatul (1) din Cartă.

Prevăzută de lege

Restrângerea exercițiului dreptului la protecția datelor cu caracter personal trebuie să fie prevăzută de lege. Această cerință implică faptul că limitările trebuie să se bazeze pe un temei juridic accesibil și previzibil într-o măsură adecvată și care să fie formulat cu suficientă precizie pentru a permite persoanelor să înțeleagă obligațiile care le revin și să își corecteze comportamentul. De asemenea, 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 unui amestec arbitrar. Această interpretare este similară cu cerința privind „intervenția legală" din jurisprudența CEDO[59] și s-a susținut că sensul expresiei „prevăzut de lege" folosite în Cartă trebuie să fie același cu cel pe care îl implică această expresie în

58 În ceea ce privește evaluarea necesității măsurilor care restrâng dreptul fundamental la protecția datelor cu caracter personal, vezi: AEPD (2017), *Necessity Toolkit* (*Set de instrumente privind necesitatea*), Bruxelles, 11 aprilie 2017.

59 AEPD (2017), *Set de instrumente privind necesitatea*, Bruxelles, 11 aprilie 2017, p. 4; vezi, de asemenea, CJUE, *Avizul 1/15 din 26 iulie 2017 al Curții (Marea Cameră)*.

contextul Convenției europene a drepturilor omului[60]. Jurisprudența CEDO și, în special, conceptul de „calitate a legii" pe care l-a elaborat de-a lungul anilor reprezintă un aspect relevant care trebuie luat în considerare de CJUE în interpretarea domeniului de aplicare al articolului 52 alineatul (1) din Cartă[61].

Respectarea substanței dreptului

În ordinea juridică a Uniunii, orice limitare a drepturilor fundamentale protejate prin Cartă trebuie să respecte substanța drepturilor în cauză. Aceasta înseamnă că limitările care sunt atât de ample și de invazive încât golesc un drept fundamental de conținutul său de bază nu pot fi justificate. În cazul în care substanța dreptului este compromisă, limitarea trebuie considerată ilegală, fără a mai fi nevoie să se evalueze dacă acesta îndeplinește un obiectiv de interes general și satisface criteriile de necesitate și proporționalitate.

Exemplu: Cauza *Schrems*[62] a vizat protecția persoanelor cu privire la transferul datelor lor cu caracter personal către țări terțe – în acest caz, către Statele Unite. Domnul Schrems, un cetățean austriac care era de mai mulți ani utilizator al platformei Facebook, a depus o plângere la autoritatea irlandeză de supraveghere a protecției datelor pentru a denunța transferul datelor sale cu caracter personal de la filiala irlandeză Facebook către Facebook Inc. și serverele din SUA, unde datele în cauză au fost prelucrate. Reclamantul a susținut că, având în vedere dezvăluirile din 2013 ale lui Edward Snowden, un avertizor de integritate american, privind activitățile de supraveghere ale serviciilor de supraveghere din SUA, legea și practica din SUA nu oferă o protecție suficientă a datelor cu caracter personal transferate pe teritoriul SUA. Snowden dezvăluise că National Security Agency (Agenția Națională de Securitate) a obținut acces direct la serverele unor societăți precum Facebook și a putut citi conținutul chatului și al mesajelor private.

60 Hotărârea CJUE [MC] în cauzele conexate C-203/15 și C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen și Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*, și Concluziile avocatului general Saugmandsgaard Øe prezentate la 19 iulie 2016, punctul 140.

61 Hotărârea CJUE în cauza C-70/10, *Scarlet Extended SA/Société belge des auteurs compositeurs et éditeurs (SABAM)*, și Concluziile avocatului general Cruz Villalón prezentate la 14 aprilie 2011, punctul 100.

62 Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*.

Transferurile de date către SUA se bazau pe o decizie a Comisiei privind adecvarea, adoptată în 2000, care permitea transferuri către societăți din SUA care declaraseră pe propria răspundere că vor proteja datele cu caracter personal transferate din UE și vor respecta așa-numitele principii ale „sferei de siguranță". Atunci când cauza a ajuns în fața CJUE, aceasta a examinat valabilitatea deciziei Comisiei în lumina Cartei. Curtea a reamintit că protecția drepturilor fundamentale în UE impune ca derogările și limitările acestor drepturi să se aplice numai în măsura în care acest lucru este strict necesar. CJUE a considerat că o reglementare care permite autorităților publice să acceadă în mod generalizat la conținutul comunicărilor electronice „aduce atingere substanței dreptului fundamental la respectarea vieții private, astfel cum este garantat la articolul 7 din [C]artă". Dreptul ar deveni lipsit de sens dacă autoritățile publice din SUA ar fi autorizate să acceadă la comunicări în mod uzual, fără o justificare obiectivă bazată pe considerente concrete de securitate națională sau de prevenire a infracțiunilor care să fie specifice pentru persoana vizată și fără ca aceste practici de supraveghere să fie însoțite de garanții adecvate împotriva abuzului de putere.

De asemenea, CJUE a constatat că „[o] reglementare care nu prevede nicio posibilitate a justițiabilului de a exercita căi legale pentru a avea acces la date cu caracter personal care îl privesc sau pentru a obține rectificarea sau ștergerea unor astfel de date" este incompatibilă cu dreptul fundamental la o protecție jurisdicțională efectivă (articolul 47 din Cartă). Astfel, Decizia privind „sfera de siguranță" nu a reușit să asigure un nivel de protecție a drepturilor fundamentale de către SUA echivalent în esență cu cel garantat în cadrul UE în temeiul directivei interpretate în lumina Cartei. În consecință, CJUE a anulat decizia[63].

Exemplu: În cauza *Digital Rights Ireland*[64], CJUE a examinat compatibilitatea Directivei 2006/24/CE (Directiva privind păstrarea datelor) cu articolele 7 și 8 din Cartă. Directiva impunea furnizorilor de servicii de comunicații electronice

63 Hotărârea 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 prezentului manual. În special, CJUE a considerat că decizia limita în mod ilegal competențele autorităților naționale de supraveghere a protecției datelor. În plus, în cadrul regimului privind „sfera de siguranță" persoanele fizice nu dispuneau de căi de atac în cazul în care doreau să acceadă la datele cu caracter personal care le privesc și/sau să obțină rectificarea sau ștergerea acestora. Astfel, a fost compromisă și substanța dreptului fundamental la o protecție jurisdicțională efectivă consacrat la articolul 47 din Cartă.

64 Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții* și *Kärntner Landesregierung și alții*.

să păstreze datele privind traficul și localizarea timp de cel puțin șase luni și 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 permitea păstrarea conținutului comunicațiilor electronice. CJUE a arătat că datele pe care furnizorii trebuiau să le păstreze în conformitate cu directiva includeau datele necesare pentru urmărirea și identificarea sursei și destinației unei comunicări, data, ora și durata unei comunicări, numărul de la care se inițiază apelul, numerele apelate și adresele IP. Aceste date, „[c]onsiderate în ansamblu, [...] pot permite deducerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, precum obiceiurile din viața cotidiană, locurile de ședere permanente sau temporare, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele".

Astfel, păstrarea datelor cu caracter personal în temeiul directivei a constituit o intervenție deosebit de gravă asupra drepturilor la respectarea vieții private și la protecția datelor cu caracter personal. Cu toate acestea, CJUE a considerat că intervenția în cauză nu a afectat negativ substanța acestor drepturi. În ceea ce privește dreptul la respectarea vieții private, substanța acestuia nu a fost compromisă, întrucât directiva nu permitea accesul la conținutul comunicațiilor electronice în sine. În mod similar, substanța dreptului la protecția datelor cu caracter personal nu a fost compromisă, întrucât directiva impunea furnizorilor de servicii de comunicații electronice să respecte anumite principii de protecție a datelor și de securitate a datelor și să pună în aplicare măsurile tehnice și organizatorice adecvate în acest scop.

Necesitatea și proporționalitatea

Articolul 52 alineatul (1) din Cartă prevede că, sub rezerva principiului proporționalității, exercițiul drepturilor și libertăților fundamentale recunoscute de Cartă poate fi restrâns numai dacă acest lucru este necesar.

Poate fi **necesară** o limitare în cazul în care trebuie adoptate măsuri în vederea atingerii unui obiectiv public, dar necesitatea, astfel cum a fost interpretată de CJUE, implică și faptul că măsurile adoptate trebuie să fie mai puțin invazive decât alte metode prin care se poate atinge același obiectiv. În ceea ce privește limitările drepturilor la respectarea vieții private și la protecția datelor cu caracter personal, CJUE aplică un test al necesității stricte, considerând că „derogările de la protecția datelor

cu caracter personal și limitările acesteia [trebuie] să fie efectuate în limitele strictului necesar". Dacă o limitare este considerată strict necesară, trebuie să se evalueze, de asemenea, dacă este proporțională.

Proporționalitatea înseamnă că avantajele care rezultă din limitare trebuie să depășească dezavantajele pe care aceasta le creează în ceea ce privește exercițiul drepturilor fundamentale în cauză[65]. Pentru a reduce dezavantajele și riscurile la adresa exercițiului drepturilor la respectarea vieții private și la protecția datelor, este important ca limitările să fie însoțite de garanții adecvate.

Exemplu: În cauza *Volker und Markus Schecke*[66], CJUE a concluzionat că prin impunerea unei obligații de publicare a datelor cu caracter personal ale fiecărei persoane fizice care a beneficiat de ajutor de la anumite fonduri agricole fără a face distincție în funcție de criterii relevante, cum ar fi perioadele în care acele persoane au primit un astfel de ajutor, frecvența acestui ajutor sau natura și valoarea acestuia, Consiliul și Comisia au depășit limitele pe care le impune respectarea principiului proporționalității.

Prin urmare, CJUE a considerat necesar să declare nule anumite dispoziții ale Regulamentului (CE) nr. 1290/2005 al Consiliului și să declare Regulamentul (CE) nr. 259/2008 nul în totalitate[67].

Exemplu: În cauza *Digital Rights Ireland*[68], CJUE a constatat că intervenția asupra dreptului la respectarea vieții private generată de Directiva privind păstrarea datelor nu a compromis substanța acestui drept, întrucât interzice păstrarea conținutului comunicărilor electronice. Cu toate acestea, Curtea a concluzionat că directiva era incompatibilă cu articolele 7 și 8 din Cartă și a declarat-o nulă. Având în vedere că datele privind traficul și localizarea, agregate și luate în ansamblu, pot fi analizate și pot reda o imagine detaliată

65 AEPD (2017), *Necessity Toolkit* (Set de instrumente privind necesitatea), p. 5.

66 Hotărârea CJUE [MC] din 9 noiembrie 2010 în cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*, punctele 89 și 86.

67 Regulamentul (CE) nr. 1290/2005 al Consiliului din 21 iunie 2005 privind finanțarea politicii agricole comune, JO 2005 L 209; Regulamentul (CE) nr. 259/2008 al Comisiei din 18 martie 2008 de stabilire a normelor de aplicare a Regulamentului (CE) nr. 1290/2005 al Consiliului în ceea ce privește publicarea informațiilor referitoare la beneficiarii fondurilor provenite din Fondul European de Garantare Agricolă (FEGA) și Fondul European Agricol pentru Dezvoltare Rurală (FEADR), JO 2008 L 76.

68 Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții și Kärntner Landesregierung și alții*, punctul 39.

a vieții private a persoanelor, acest fapt a reprezentat o intervenție gravă asupra acestor drepturi. CJUE a ținut seama de faptul că directiva a impus păstrarea tuturor metadatelor privind telefonia fixă, telefonia mobilă, accesul la internet, e-mailul prin internet și telefonia prin internet, aplicându-se tuturor mijloacelor de comunicare electronică, a căror utilizare este foarte răspândită în viața de zi cu zi a oamenilor. Practic, directiva constituia o ingerință care afecta întreaga populație europeană. Având în vedere amploarea și gravitatea acestei ingerințe, păstrarea datelor privind traficul și localizarea ar putea fi justificată, în opinia CJUE, 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 se limitează la ceea ce este strict necesar. De asemenea, aceasta nu prevedea condiții de fond și de procedură care să reglementeze accesul la datele păstrate de autoritățile naționale și utilizarea acestor date și care să facă obiectul unei examinări prealabile de către o instanță sau alt organism independent.

CJUE a ajuns la o concluzie similară în cauzele conexate *Tele2 Sverige AB/Post- och telestyrelsen* și *Secretary of State for the Home Department/Tom Watson și alții*[69]. Acestea au vizat păstrarea datelor de trafic și de localizare ale „[tuturor abonaților și utilizatorilor] înregistrați și [priveau] toate mijloacele de comunicare electronică, precum și toate datele de transfer" fără „nicio diferențiere, limitare sau excepție în funcție de obiectivul urmărit"[70]. În cazul în speță, aspectul dacă o persoană avea sau nu vreo legătură directă sau indirectă cu infracțiuni grave sau dacă comunicările sale erau sau nu relevante pentru securitatea națională nu constituia o condiție pentru păstrarea datelor sale. Având în vedere lipsa atât a unei legături necesare între datele păstrate și o amenințare la adresa siguranței publice, cât și a limitării păstrării datelor la o perioadă sau la o zonă geografică, CJUE a concluzionat că legislația națională a depășit limitele a ceea ce era strict necesar pentru combaterea infracțiunilor grave[71].

69 Hotărârea CJUE [MC] din 21 decembrie 2016 în cauzele conexate C-203/15 și C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen și Secretary of State for the Home Department/Tom Watson și alții*, punctele 105-106.

70 *Ibidem*, punctul 105.

71 *Ibidem*, punctul 107.

Autoritatea Europeană pentru Protecția Datelor a adoptat o abordare similară în ceea ce privește necesitatea în cadrul *Setului de instrumente privind necesitatea*[72]. Setul de instrumente are scopul de a contribui la evaluarea conformității măsurilor propuse cu legislația UE privind protecția datelor. Acesta a fost elaborat pentru a îmbunătăți formarea factorilor de decizie și a legiuitorilor din UE responsabili cu pregătirea sau examinarea măsurilor care implică prelucrarea datelor cu caracter personal și care restrâng dreptul la protecția datelor cu caracter personal și alte drepturi și libertăți consacrate de Cartă.

Obiective de interes general

Pentru a fi justificată, orice limitare a exercițiului drepturilor recunoscute de Cartă trebuie, de asemenea, să îndeplinească efectiv obiectivele de interes general recunoscute de Uniune sau necesitatea protejării drepturilor și libertăților altor persoane. În ceea ce privește necesitatea protejării drepturilor și libertăților celorlalți, dreptul la protecția datelor cu caracter personal interacționează adesea cu alte drepturi fundamentale. Secțiunea 1.3 prezintă o analiză detaliată a acestor interacțiuni. În ceea ce privește obiectivele de interes general, acestea includ obiectivele generale ale UE descrise la articolul 3 din Tratatul privind Uniunea Europeană (TUE), cum ar fi promovarea păcii și a bunăstării popoarelor Uniunii, justiția și protecția sociale, precum și crearea unui spațiu de libertate, securitate și justiție în interiorul căruia este asigurată libera circulație a persoanelor, în corelare cu măsuri adecvate privind prevenirea criminalității și combaterea acestui fenomen, precum și alte obiective și interese protejate de dispozițiile specifice ale tratatelor[73]. Regulamentul general privind protecția datelor elaborează dispozițiile articolului 52 alineatul (1) din Cartă în acest sens: articolul 23 alineatul (1) din regulament enumeră o serie de obiective de interes general considerate ca reprezentând motive legitime pentru limitarea drepturilor persoanelor, cu condiția ca limitarea să respecte substanța dreptului la protecția datelor cu caracter personal și să fie necesară și proporțională. Securitatea și apărarea națională, prevenirea infracțiunilor, 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 regulament.

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 contextul acestuia. Descrierea clară și detaliată a obiectivului limitării și a măsurilor

72 AEPD (2017), *Set de instrumente privind necesitatea*, Bruxelles, 11 aprilie 2017.

73 Explicații cu privire la Carta drepturilor fundamentale (2007/C 303/02), JO 2007 C 303, p. 17.

propuse este esențială pentru a permite evaluarea necesității acestuia[74]. Obiectivul urmărit și necesitatea și proporționalitatea limitării sunt strâns legate.

Exemplu: Cauza *Schwarz/Stadt Bochum*[75] a vizat unele limitări ale dreptului la respectarea vieții private și ale dreptului la protecția datelor cu caracter personal care rezultă din prelevarea și stocarea amprentelor digitale în cadrul eliberării de pașapoarte de către autoritățile statelor membre[76]. Reclamantul a solicitat orașului Bochum un pașaport, dar a refuzat prelevarea amprentelor digitale; în consecință, autoritățile orașului Bochum i-au respins cererea de eliberare a pașaportului. Ulterior, reclamantul a introdus o acțiune în fața unei instanțe germane pentru a obține eliberarea pașaportului fără prelevarea amprentelor. Instanța germană a sesizat CJUE cu această cauză, adresând întrebarea dacă articolul 1 alineatul (2) din Regulamentul (CE) nr. 2252/2004 privind standardele pentru elementele de securitate și elementele biometrice integrate în pașapoarte și în documente de călătorie emise de statele membre trebuie considerat valabil.

CJUE a subliniat că amprentele digitale **constituie date cu caracter personal** din moment ce conțin în mod obiectiv informații unice privind persoane fizice și permit identificarea lor precisă, iar prelevarea și stocarea amprentelor digitale constituie prelucrare. Această prelucrare, reglementată de articolul 1 alineatul (2) din Regulamentul (CE) nr. 2252/2004, constituie o amenințare la adresa respectării vieții private și a protecției datelor cu caracter personal[77]. Totuși, articolul 52 alineatul (1) din Cartă admite restrângeri ale exercițiului acestor drepturi, cu condiția ca aceste restrângeri să fie prevăzute de lege, să respecte substanța acestor drepturi și, cu respectarea principiului proporționalității, să fie necesare și să răspundă efectiv unor obiective de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

În speță, CJUE a arătat, în primul rând, că restrângerea care rezultă din prelevarea și din stocarea amprentelor digitale în cadrul eliberării pașapoartelor trebuie considerată ca fiind **prevăzută de lege** din moment ce articolul 1 alineatul (2) din Regulamentul (CE) nr. 2252/2004 prevede aceste

74 AEPD (2017), *Set de instrumente privind necesitatea*, Bruxelles, 11 aprilie 2017, p. 4.

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

76 *Ibidem*, punctele 33-36.

77 *Ibidem*, punctele 27-30.

operațiuni. În al doilea rând, acest regulament avea ca scop să prevină falsificarea pașapoartelor și utilizarea lor frauduloasă. Astfel, articolul 1 alineatul (2) are ca scop, printre altele, să împiedice intrarea ilegală în UE, urmărind astfel un obiectiv de interes general recunoscut de Uniune. În al treilea rând, din diferitele elemente de care dispunea CJUE nu reiese și de altfel nu s-a susținut că restrângerile exercițiului drepturilor în speță nu ar respecta substanța acestor drepturi. În al patrulea rând, stocarea amprentelor digitale pe un suport de stocare de înaltă securitate, prevăzută de dispoziția menționată anterior, implică un anumit grad de sofisticare tehnică. Această stocare poate reduce riscul de falsificare a pașapoartelor și poate facilita munca autorităților însărcinate cu examinarea la frontierele UE a autenticității lor. Nu este hotărâtor faptul că metoda menționată nu este pe deplin fiabilă. Deși aceasta nu exclude complet acceptările de persoane neautorizate, este suficient să reducă în mod considerabil riscul unor astfel de acceptări. Având în vedere considerațiile care precedă, CJUE a constatat că prelevarea și stocarea amprentelor digitale, prevăzute la articolul 1 alineatul (2) din Regulamentul (CE) nr. 2252/2004, sunt apte să atingă obiectivele urmărite de acest regulament și, prin urmare, obiectivul de prevenire a intrării ilegale de persoane pe teritoriul UE[78].

În continuare, CJUE a evaluat **necesitatea** unei astfel de prelucrări, menționând că acțiunea în cauză implică doar prelevarea amprentei a două degete, care sunt de altfel în mod normal expuse vederii celorlalți, astfel încât nu este vorba despre o operațiune cu caracter intim. Aceasta nu implică nicio neplăcere fizică sau psihică specială pentru persoana interesată, la fel ca în cazul fotografierii feței. De asemenea, este necesar să se arate că unica alternativă reală la prelevarea amprentelor digitale evocată în cursul procedurii în fața CJUE constă în înregistrarea unei imagini a irisului. Nimic din dosarul prezentat CJUE nu arată că acest din urmă procedeu ar afecta drepturile recunoscute de articolele 7 și 8 din Cartă mai puțin decât prelevarea amprentelor digitale. În plus, în ceea ce privește eficacitatea acestor două ultime metode, nu se contestă că nivelul de maturitate tehnologică al celei întemeiate pe recunoașterea irisului nu atinge nivelul celei întemeiate pe amprentele digitale, este un procedeu mult mai oneros la ora actuală decât cel al comparării amprentelor digitale și, astfel, mai puțin adaptat unei utilizări generalizate. În aceste condiții, este necesar să se constate că nu s-a adus la cunoștința CJUE existența unor măsuri apte să contribuie destul de eficient la atingerea obiectivului privind protecția pașapoartelor împotriva

78 *Ibidem*, punctele 35-45.

utilizării lor frauduloase, aducând totodată atingeri mai puțin semnificative drepturilor recunoscute la articolele 7 și 8 din Cartă decât cele determinate de metoda întemeiată pe amprentele digitale[79].

CJUE a arătat că articolul 4 alineatul (3) din Regulamentul (CE) nr. 2252/2004 precizează în mod expres că amprentele digitale pot fi utilizate numai pentru a verifica autenticitatea pașaportului și identitatea titularului său, iar articolul 1 alineatul (2) din acest regulament nu prevede stocarea amprentelor digitale decât în pașaport, care rămâne în posesia exclusivă a titularului său. Prin urmare, regulamentul nu a furnizat un temei juridic unei eventuale centralizări a datelor colectate pe baza acestuia sau unei utilizări a acestora din urmă în alte scopuri decât cel prin care se urmărește prevenirea intrării ilegale de persoane pe teritoriul UE[80]. Având în vedere considerațiile care precedă, CJUE a concluzionat că analiza întrebării cu care a fost sesizată nu a pus în evidență niciun element în măsură să afecteze valabilitatea articolului 1 alineatul (2) din Regulamentul (CE) nr. 2252/2004.

Comparație între Cartă și Convenția europeană a drepturilor omului

Deși prezintă un mod de redactare diferit, condițiile pentru limitarea legală a drepturilor prevăzute la articolul 52 alineatul (1) din Cartă sunt similare cu dispozițiile articolului 8 alineatul (2) din Convenția europeană a drepturilor omului privind dreptul la respectarea vieții private. În jurisprudența lor, CJUE și CEDO își citează adesea reciproc hotărârile, într-un dialog constant între cele două instanțe care urmărește o interpretare armonioasă a normelor de protecție a datelor. Articolul 52 alineatul (3) din Cartă prevede că, „[î]n măsura în care prezenta [C]artă conține drepturi ce corespund unor drepturi garantate prin Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, înțelesul și întinderea lor sunt aceleași ca și cele prevăzute de convenția menționată". Cu toate acestea, articolul 8 din Cartă nu corespunde în mod direct unui articol din Convenția europeană a drepturilor omului[81]. Articolul 52 alineatul (3) din Cartă privește mai degrabă conținutul și domeniul de aplicare al drepturilor protejate de fiecare ordine juridică decât condițiile de limitare a acestora. Totuși, 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 prevăzute la articolul 8 din Convenția europeană a drepturilor

79 Hotărârea CJUE din 17 octombrie 2013 în cauza C-291/12, *Michael Schwarz/Stadt Bochum*, punctele 46-53.

80 *Ibidem*, punctele 56-61.

81 AEPD (2017), *Set de instrumente privind necesitatea*, Bruxelles, 11 aprilie 2017, p. 6.

omului, astfel cum au fost interpretate de CEDO. Scenariul opus, în care CEDO poate face trimitere la condițiile de limitare legală în temeiul Cartei, este, de asemenea, posibil. În orice caz, trebuie să se țină seama și de faptul că în Convenția europeană a drepturilor omului nu există un echivalent perfect al articolului 8 din Cartă, care privește protecția datelor cu caracter personal și, în special, drepturile persoanei vizate, motivele legitime de prelucrare a datelor și supravegherea de către o autoritate independentă. Unele elemente ale articolului 8 din Cartă se pot regăsi în jurisprudența CEDO, elaborată în temeiul articolului 8 din Convenția europeană a drepturilor omului și coroborată cu Convenția 108[82]. Această legătură garantează faptul că CJUE și CEDO se inspiră una de la cealaltă în ceea ce privește aspectele legate de protecția datelor.

1.3. Interacțiunea cu alte drepturi și interese legitime

Principalele elemente

- 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: deși există situații în care dreptul la protecția datelor cu caracter personal concurează cu un drept specific, alteori dreptul la protecția datelor cu caracter personal asigură în mod eficace respectarea aceluiași drept specific. De exemplu, acesta este cazul libertății de exprimare, dat fiind că secretul profesional este o componentă a dreptului la respectarea vieții private.
- Necesitatea protejării drepturilor și libertăților celorlalți este unul dintre criteriile utilizate pentru a evalua legalitatea limitării dreptului la protecția datelor cu caracter personal.
- În situațiile în care interacționează diferite drepturi, instanțele trebuie să realizeze un exercițiu de echilibrare pentru a le concilia.
- Regulamentul general privind protecția datelor solicită statelor membre să stabilească un echilibru între dreptul la protecția datelor cu caracter personal și libertatea de exprimare și de informare.
- Statele membre pot, de asemenea, să adopte norme specifice în legislația națională pentru a stabili un echilibru între dreptul la protecția datelor cu caracter personal și accesul publicului la documentele oficiale și obligațiile privind secretul profesional.

82 Explicații cu privire la Carta drepturilor fundamentale a UE (2007/C 303/02), articolul 8.

Dreptul la protecția datelor cu caracter personal nu este un drept absolut; condițiile de limitare legală a acestui drept au fost detaliate mai sus. Unul dintre criteriile pentru limitările legale ale drepturilor, recunoscut atât în legislația CoE, cât și a UE, este faptul că intervenția asupra dreptului la protecția datelor este necesară pentru protejarea drepturilor și libertăților celorlalți. În situațiile în care protecția datelor interacționează cu alte drepturi, atât CEDO, cât și CJUE au statuat în repetate rânduri că este necesar un exercițiu de echilibrare cu alte drepturi în momentul aplicării și interpretării articolului 8 din Convenția europeană a drepturilor omului și a articolului 8 din Cartă[83]. Mai multe exemple sugestive vor ilustra modul în care se realizează acest echilibru.

Pe lângă exercițiul de echilibrare efectuat de aceste instanțe, statele pot adopta, dacă este necesar, o legislație care să stabilească un echilibru între dreptul la protecția datelor cu caracter personal și alte drepturi. Din acest motiv, Regulamentul general privind protecția datelor prevede o serie de domenii de derogare națională.

În ceea ce privește libertatea de exprimare, RGPD cere statelor membre să asigure, prin intermediul dreptului intern, un echilibru între „dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament și dreptul la libertatea de exprimare și de informare, inclusiv prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare”[84]. Statele membre pot, de asemenea, să adopte legi pentru a stabili un echilibru între protecția datelor și accesul public la documente oficiale, pe de o parte, și obligațiile privind secretul profesional protejat ca formă a dreptului la respectarea vieții private, pe de altă parte[85].

1.3.1. Libertatea de exprimare

Unul dintre drepturile care interacționează în modul cel mai semnificativ cu dreptul la protecția datelor este dreptul la libertatea de exprimare.

Libertatea de exprimare este protejată prin articolul 11 din Cartă („Libertatea de exprimare și de informare”). Acest drept cuprinde „libertatea de opinie și libertatea

83 Hotărârea CEDO [MC] din 7 februarie 2012 în cauza *Von Hannover/Germania (nr. 2)*, nr. 40660/08 și 60641/08; Hotărârea CJUE din 24 noiembrie 2011 în cauzele conexate C-468/10 și C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* și *Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, punctul 48; Hotărârea CJUE [MC] 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 protecția datelor, articolul 85.

85 *Ibidem*, articolele 86 și 90.

de a primi sau de a transmite informații sau idei fără amestecul autorităților publice și fără a ține seama de frontiere". În conformitate cu articolul 11 din Cartă și articolul 10 din Convenția europeană a drepturilor omului, libertatea de informare protejează nu numai dreptul de a transmite, ci și dreptul de a *primi* informații.

Limitările libertății 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 Convenția europeană a drepturilor omului. În conformitate cu articolul 52 alineatul (3) din Cartă, în măsura în care Carta conține drepturi ce corespund unor drepturi garantate prin Convenția europeană a drepturilor omului, „înțelesul și întinderea lor sunt aceleași ca și cele prevăzute de convenția menționată". Prin urmare, limitările care pot fi impuse legal asupra dreptului garantat prin articolul 11 din Cartă nu pot depăși limitările prevăzute la articolul 10 alineatul (2) din Convenția europeană a drepturilor omului, adică trebuie să fie prevăzute de lege și să constituie, într-o societate democratică, o măsură necesară „pentru protecția [...] reputației sau a drepturilor altora". Aceste drepturi includ, în special, dreptul la respectarea vieții private și dreptul la protecția datelor cu caracter personal.

Raportul dintre protecția datelor cu caracter personal și libertatea de exprimare este reglementat de articolul 85 din Regulamentul general privind protecția datelor, denumit „Prelucrarea și libertatea de exprimare și de informare". În conformitate cu acest articol, statele membre asigură un echilibru între dreptul la protecția datelor cu caracter personal și dreptul la libertatea de exprimare și de informare. În special, se prevăd scutiri și derogări de la capitole specifice ale Regulamentului general privind protecția datelor în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare, în măsura în care acestea sunt necesare pentru a stabili un echilibru între dreptul la protecția datelor cu caracter personal și libertatea de exprimare și de informare.

Exemplu: În cauza *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy și Satamedia Oy*[86], CJUE a fost sesizată cu solicitarea de a defini raportul dintre protecția datelor și libertatea presei[87]. Curtea a trebuit să examineze diseminarea de către o societate, prin intermediul unui serviciu de SMS, a datelor fiscale aparținând unui număr de aproximativ 1,2 milioane de persoane fizice, obținute legal de la autoritățile fiscale finlandeze. Autoritatea finlandeză de supraveghere a protecției datelor a emis o decizie prin care a solicitat societății să pună capăt diseminării acestor date. Societatea a contestat această decizie la o instanță națională, care a solicitat clarificări din partea CJUE cu privire la interpretarea Directivei privind protecția datelor. În special, Curtea a trebuit să verifice dacă prelucrarea datelor cu caracter personal puse la dispoziție de autoritățile fiscale pentru a permite utilizatorilor de telefonie mobilă să primească datele fiscale ale altor persoane fizice trebuie să fie considerată ca fiind o activitate întreprinsă numai în scopuri jurnalistice. După ce a concluzionat că activitățile societății reprezentau „prelucrare de date 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). Curtea a remarcat, în primul rând, importanța dreptului la libertatea de exprimare în fiecare societate democratică și a considerat că noțiunile legate de această libertate, cum ar fi jurnalismul, trebuie interpretate în sens larg. Apoi a observat că, pentru a se obține un echilibru între cele două drepturi fundamentale, derogările și limitările protecției datelor trebuie să fie efectuate în limitele strictului necesar. În aceste situații, CJUE a considerat că activități precum cele întreprinse de societățile în cauză privind date provenite din documente publice potrivit legislației naționale pot fi calificate drept „activități de jurnalism" în cazul în care au ca scop aducerea la cunoștința publicului a unor informații, opinii sau idei, indiferent de mijlocul de transmitere a acestora. Curtea a hotărât, de asemenea, că aceste activități nu sunt rezervate întreprinderilor din sectorul mijloacelor de comunicare în masă și pot avea un scop lucrativ. Cu toate acestea, CJUE a lăsat la aprecierea instanței naționale să stabilească dacă faptele specifice în speță se încadrau în aceste criterii.

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

87 Cauza viza interpretarea Directivei privind protecția datelor, mai exact a articolului 9 – înlocuit acum de articolul 85 din Regulamentul general privind protecția datelor – care prevede: „[s]tatele membre prevăd exonerări și derogări de la dispozițiile prezentului capitol, ale capitolului IV și ale capitolului VI pentru prelucrarea datelor cu caracter personal efectuată numai în scopuri jurnalistice, artistice sau literare, în măsura în care se dovedesc necesare pentru a pune dreptul la viață privată în acord cu normele care reglementează libertatea de exprimare".

Aceeași cauză a fost examinată și de CEDO, după ce instanța națională a decis, pe baza orientărilor CJUE, că ordinul autorității de supraveghere de a suspenda publicarea tuturor informațiilor fiscale constituia o intervenție justificată în libertatea de exprimare a societății. CEDO a susținut această abordare[88]. Curtea a constatat că, deși a existat o intervenție asupra dreptului societăților de a transmite informații, aceasta era în conformitate cu legea, urmărea un scop legitim și era necesară într-o societate democratică.

Curtea a reamintit criteriile de jurisprudență care ar trebui să ghideze autoritățile naționale și chiar CEDO atunci când stabilesc un echilibru între libertatea de exprimare și dreptul la respectarea vieții private. Atunci când este vorba despre un discurs politic sau o dezbatere pe teme de interes public, există puține posibilități legitime de restrângere a dreptului de a primi și de a transmite informații, deoarece publicul are dreptul de a fi informat, „iar acesta este un drept esențial într-o societate democratică"[89]. Cu toate acestea, nu se poate considera că articolele de presă destinate exclusiv satisfacerii curiozității unui anumit public cu privire la detaliile vieții private a unei persoane ar contribui la o dezbatere de interes public. Derogarea de la normele de protecție a datelor în scopuri jurnalistice urmărește să permită jurnaliștilor accesul la date și colectarea și prelucrarea acestora în vederea desfășurării activității lor jurnalistice. Astfel, în cazul în speță a existat, într-adevăr, un interes public de a oferi societăților reclamante acces la cantitățile mari de date fiscale în cauză și de a permite acestor societăți să colecteze și să prelucreze respectivele date. În schimb, Curtea a constatat că nu există niciun interes public pentru diseminarea în bloc a unor astfel de date brute de către ziare, în formă nemodificată și fără nicio contribuție analitică. Informațiile fiscale ar fi permis membrilor curioși ai publicului să clasifice persoanele după statutul lor economic și ar fi satisfăcut setea publicului pentru informații despre viața privată a altora. Acest lucru nu poate fi considerat ca fiind o contribuție la o dezbatere de interes public.

Exemplu: În cauza *Google Spain*[90], CJUE a analizat dacă Google avea obligația de a elimina din rezultatele căutării informații perimate despre dificultățile financiare ale reclamantului. La efectuarea unei căutări în motorul de căutare

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

89 *Ibidem*, punctul 169.

90 Hotărârea CJUE [MC] 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.

Google după numele reclamantului, rezultatele căutării au furnizat linkuri către articole vechi din ziare care menționau legătura reclamantului cu o procedură de executare silită. Reclamantul a considerat că aceasta constituie o încălcare a dreptului său la respectarea vieții private și la protecția datelor cu caracter personal, deoarece procedura se finalizase în urmă cu mai mulți ani și menționarea acesteia era lipsită de relevanță.

CJUE a clarificat mai întâi că motoarele de căutare pe internet și rezultatele căutării care furnizează date cu caracter personal pot stabili un profil detaliat al unei persoane. Într-o societate din ce în ce mai digitizată, cerința ca datele cu caracter personal să fie corecte și ca publicarea acestora să nu depășească ceea ce este necesar, adică să furnizeze informații publicului, este esențială pentru asigurarea unui nivel ridicat de protecție a datelor cu caracter personal. „[Operatorul] prelucrării respective trebuie să asigure, în cadrul responsabilităților, al competențelor și al posibilităților sale, că aceasta îndeplinește cerințele" legislației UE, pentru ca garanțiile juridice stabilite să își producă efectul deplin. Aceasta înseamnă că dreptul de a obține ștergerea datelor cu caracter personal atunci când prelucrarea nu mai este necesară sau datele sunt perimate privește și motoarele de căutare, despre care s-a constatat că sunt operatori, nu doar persoane împuternicite de operatori (vezi secțiunea 2.3.1).

Examinând dacă Google avea obligația de a elimina linkurile legate de reclamant, CJUE a considerat că, în anumite condiții, persoanele au dreptul să obțină ștergerea datelor lor cu caracter personal din rezultatele căutării unui motor de căutare pe internet. Acest drept poate fi invocat atunci când informațiile referitoare la o persoană sunt incorecte, inadecvate, irelevante sau excesive în ceea ce privește scopurile prelucrării datelor. CJUE a recunoscut că acest drept nu este absolut; trebuie stabilit un echilibru între acesta și alte drepturi, în special interesul și dreptul publicului larg de a avea acces la informații. Fiecare solicitare de ștergere a datelor necesită o evaluare de la caz la caz pentru a se găsi un echilibru între drepturile fundamentale la protecția datelor cu caracter personal și la respectarea vieții private ale persoanei vizate, pe de o parte, și interesele legitime ale tuturor utilizatorilor de internet, pe de altă parte. CJUE a oferit orientări 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 sunt sensibile în ceea ce privește viața privată a persoanei vizate și nu există un interes public de a pune la dispoziție informațiile în cauză, protecția

datelor și respectarea vieții private prevalează asupra dreptului publicului larg de a avea acces la informații. Dimpotrivă, dacă persoana vizată pare să fie o personalitate publică sau dacă informațiile sunt de natură să justifice acordarea accesului publicului larg la acestea, intervenția asupra drepturilor fundamentale la protecția datelor și la respectarea vieții private este justificată.

Ca urmare a pronunțării acestei hotărâri, Grupul de lucru „Articolul 29" a adoptat orientări privind punerea în aplicare a hotărârii CJUE. Orientările cuprind o listă de criterii comune care să fie utilizate de autoritățile de supraveghere atunci când analizează plângeri legate de cereri ale persoanelor fizice de eliminare a datelor și care să ghideze aceste autorități în cadrul exercițiului de echilibrare a drepturilor[91].

În ceea ce privește stabilirea unui echilibru între dreptul la protecția datelor și dreptul la libertatea de exprimare, CEDO a emis o serie de hotărâri de referință.

Exemplu: În cauza *Axel Springer AG/Germania*[92], CEDO a considerat că un ordin de încetare impus societății reclamante care dorea să publice un articol cu privire la arestarea și condamnarea unui actor cunoscut încălca dispozițiile articolului 10 din Convenția europeană a drepturilor omului. CEDO a reiterat criteriile care trebuie luate în considerare la stabilirea unui echilibru între dreptul la libertatea de exprimare și dreptul la respectarea vieții private, astfel cum sunt stabilite în jurisprudența sa:

- dacă evenimentul care face obiectul articolului publicat este de interes general;
- dacă persoana vizată este o personalitate publică; și
- modul în care au fost obținute informațiile și dacă acestea sunt corecte.

91 Grupul de lucru „Articolul 29" (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12* [Orientări privind punerea în aplicare a hotărârii CJUE în cauza *Google Spain și Google Inc./ Agencia Española de Protección de Datos (AEPD) și Mario Costeja González*, C-131/12], WP 225, Bruxelles, 26 noiembrie 2014.

92 Hotărârea CEDO [MC] din 7 februarie 2012 în cauza *Axel Springer AG/Germania*, nr. 39954/08, punctele 90 și 91.

CEDO a constatat că arestarea și condamnarea actorului era un fapt judiciar public și că, prin urmare, era de interes public, că actorul era suficient de bine cunoscut pentru a fi calificat drept o personalitate publică și că informațiile fuseseră furnizate de procuratură, iar exactitatea lor nu a fost contestată de părți. Prin urmare, restricțiile de publicare impuse societății nu au fost proporționale în mod rezonabil cu scopul legitim de protejare a vieții private a reclamantului. Curtea a concluzionat că s-a încălcat articolul 10 din Convenția europeană a drepturilor omului.

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 de Monaco este tatăl fiului ei. Interviul a descris, de asemenea, relația doamnei Coste cu prințul și modul în care a reacționat acesta la nașterea copilului, textul fiind însoțit de fotografii ale prințului cu copilul. Prințul Albert a introdus o acțiune în instanță împotriva editurii pentru încălcarea dreptului său la protecția vieții private. Instanțele franceze au considerat că publicarea articolului a provocat daune ireversibile prințului Albert și a impus editorului să plătească despăgubiri și să publice detaliile hotărârii judecătorești pe coperta din față a revistei.

Editorii revistei au prezentat cauza în fața CEDO, susținând că hotărârea instanțelor franceze a intervenit în mod nejustificat în dreptul lor la libertatea de exprimare. CEDO a trebuit să stabilească un echilibru între dreptul prințului Albert la respectarea vieții private, pe de o parte, și dreptul la libertatea de exprimare al editorului și dreptul publicului larg la informare, pe de altă parte. Dreptul doamnei Coste de a-și împărtăși povestea publicului și interesul copilului ca relația între tată și copil să fie stabilită în mod oficial au fost, de asemenea, considerente importante.

CEDO a statuat că publicarea interviului a constituit o ingerință în viața privată a prințului și a examinat în continuare dacă ingerința era necesară. Curtea a considerat că interviul publicat a vizat o personalitate publică și un subiect de interes public, deoarece cetățenii din Monaco aveau interesul să știe despre existența unui copil al prințului, întrucât viitorul unei monarhii ereditare este „legat în mod intrinsec de existența urmașilor”, aceasta fiind,

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

astfel, o temă de interes public[94]. Curtea a arătat, de asemenea, că articolul permitea doamnei Coste și copilului ei să își exercite dreptul la libertatea de exprimare. Instanțele naționale nu au acordat atenția cuvenită principiilor și criteriilor elaborate prin jurisprudența CEDO pentru stabilirea unui echilibru între dreptul la respectarea vieții private și dreptul la libertatea de exprimare. Curtea a concluzionat că Franța a încălcat articolul 10 din Convenția europeană a drepturilor omului privind libertatea de exprimare.

În jurisprudența CEDO, unul dintre criteriile esențiale de stabilire a unui echilibru între aceste drepturi se referă la măsura în care exprimarea în speță 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 personalitate publică bine-cunoscută care ulterior a introdus în instanță o acțiune civilă împotriva editorului și a avut câștig de cauză, acordându-i-se despăgubiri. În pofida compensației monetare acordate, reclamantul a obiectat că rămânea în continuare victima unei încălcări a dreptului său la respectarea vieții private, deoarece i s-a refuzat posibilitatea de a cere în instanță un ordin de încetare înainte de publicarea fotografiilor în cauză prin faptul că nu exista nicio cerință legală pentru ziar să notifice în prealabil publicarea.

CEDO a arătat că, deși difuzarea acestui material a avut, în general, scop de divertisment, și nu educațional, a beneficiat fără îndoială de protecția articolului 10 din Convenția europeană a drepturilor omului, care poate ceda în fața cerințelor articolului 8 din Convenția europeană a drepturilor omului, în cazul în care informațiile sunt personale, cu caracter intim și nu există niciun interes public în difuzarea acestora. Cu toate acestea, s-a acordat o atenție deosebită examinării constrângerilor care ar putea funcționa ca formă de cenzură anterior publicării. Având în vedere efectul de intimidare pe care l-ar putea genera cerința de notificare prealabilă, incertitudinile legate de eficacitatea acesteia și marja largă de apreciere în acest domeniu, CEDO a concluzionat că nu este obligatorie existența unei condiții legale de notificare prealabilă în temeiul articolului 8. Astfel, Curtea a concluzionat că nu a fost încălcat articolul 8 din Convenția europeană a drepturilor omului.

94 *Ibidem*, punctele 104-116.

95 Hotărârea CEDO din 10 mai 2011 în cauza *Mosley/Regatul Unit*, nr. 48009/08, punctele 129 și 130.

Exemplu: În cauza *Bohlen/Germania*[96], reclamantul, un renumit cântăreț și producător artistic, publicase o carte autobiografică și, ulterior, a fost obligat să înlăture unele pasaje în urma hotărârilor judecătorești. Subiectul a fost prezentat pe larg în mass-media națională, iar o societate din sectorul tutunului a lansat o campanie publicitară umoristică referitor la acest eveniment, folosind prenumele reclamantului fără consimțământul său. Reclamantul a solicitat despăgubiri de la compania de publicitate susținând că i-au fost încălcate drepturile garantate de articolul 8 din Convenția europeană a drepturilor omului, dar nu a avut câștig de cauză. CEDO a reiterat criteriile care ghidează stabilirea echilibrului între dreptul la respectarea vieții private și dreptul la libertatea de exprimare și a statuat că nu existase o încălcare a articolului 8. Reclamantul era o personalitate publică, iar reclama nu s-a referit la detalii din viața sa privată, ci la un eveniment public care fusese deja prezentat de mass-media și a făcut obiectul unei dezbateri publice. În plus, reclama a avut un caracter umoristic și nu conținea niciun element degradant sau negativ la adresa reclamantului.

Exemplu: În cauza *Biriuk/Lituania*[97], reclamanta a susținut în fața CEDO că Lituania nu și-a îndeplinit obligația de a-i proteja dreptul la respectarea vieții private, întrucât, deși un ziar important a săvârșit o încălcare gravă a acestui drept al său, instanțele naționale care au examinat cauza i-au acordat despăgubiri pentru repararea prejudiciului material într-un cuantum derizoriu. La acordarea despăgubirilor pentru repararea prejudiciului moral, instanțele naționale au aplicat dispozițiile din legislația națională privind furnizarea de informații publicului, care impuneau un plafon redus pentru repararea prejudiciului moral cauzat de difuzarea ilegală de către mass-media către public a unor informații despre viața privată a unei persoane. Cauza privea publicarea pe prima pagină a celui mai mare cotidian lituanian a unui articol care raporta că reclamanta era seropozitivă. De asemenea, articolul critica comportamentul reclamantei și i-a pus sub semnul întrebării standardele morale.

CEDO a reamintit că protecția datelor cu caracter personal, și nu în ultimul rând a datelor medicale, este de o importanță fundamentală pentru dreptul la respectarea vieții private în temeiul Convenției europene a drepturilor omului. Confidențialitatea datelor medicale personale este deosebit de importantă,

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

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

deoarece divulgarea acestora (în speță, infectarea cu HIV a reclamantei) poate afecta în mod dramatic viața privată și de familie a persoanei, situația încadrării sale în muncă și incluziunea în societate. Curtea a atribuit o semnificație deosebită faptului că, potrivit relatării cotidianului, personalul medical al unui spital a oferit informații cu privire la infectarea cu HIV a reclamantei, aceasta constituind o încălcare evidentă a obligației de a păstra secretul medical. Astfel, nu a existat o intervenție legitimă asupra dreptului reclamantei la respectarea vieții private.

Articolul a fost publicat de presă, iar libertatea de exprimare este, de asemenea, un drept fundamental în temeiul Convenției europene a drepturilor omului. Cu toate acestea, atunci când a examinat dacă existența unui interes public justifică publicarea acestui tip de informații despre reclamantă, Curtea a constatat că scopul principal al publicației a fost acela de a mări vânzările ziarului prin satisfacerea curiozității cititorilor. Un astfel de scop nu poate fi considerat o contribuție la o dezbatere de interes general pentru societate. Întrucât a fost vorba despre un „abuz scandalos de libertate a presei", limitările severe în repararea prejudiciului și cuantumul redus al daunelor morale acordate în temeiul legislației naționale au însemnat că Lituania nu și-a îndeplinit obligația pozitivă de a proteja dreptul reclamantei la respectarea vieții private. CEDO a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

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

Exemplu: În cauza *Tele2 Sverige*, CJUE a stabilit că ingerința pe care o implică Directiva 2006/24/CE (Directiva privind păstrarea datelor) în drepturile fundamentale consacrate la articolele 7 și 8 din Cartă este „de o mare amploare și trebuie considerată deosebit de gravă". În plus, „[î]mprejurarea că păstrarea datelor este efectuată fără ca utilizatorii serviciilor de comunicații electronice să fie informați cu privire la aceasta este susceptibilă să genereze în mintea persoanelor vizate sentimentul că viața lor privată face obiectul unei supravegheri constante". CJUE a constatat, de asemenea, că păstrarea generalizată a datelor de transfer și a datelor de localizare ar putea avea totuși o incidență asupra utilizării mijloacelor de comunicații electronice și, „în consecință, asupra exercitării de către utilizatori a acestor mijloace ale

libertății lor de exprimare, garantată la articolul 11 din [C]artă”[98]. În acest sens, prin impunerea unor măsuri stricte care să garanteze că păstrarea datelor nu se efectuează în mod generalizat, normele de protecție a datelor contribuie, în fapt, la exercițiul libertății de exprimare.

În ceea ce privește dreptul la a primi informații, care face parte și din libertatea de exprimare, se constată din ce în ce mai mult importanța unei guvernări transparente în vederea funcționării unei societăți democratice. Transparența este un obiectiv de interes general care ar putea astfel justifica o intervenție asupra dreptului la protecția datelor, dacă este necesară și proporțională, astfel cum se explică în secțiunea 1.2. În consecință, în ultimele două decenii, dreptul de acces la documentele deținute de autoritățile publice a fost recunoscut ca drept important al fiecărui cetățean al UE și al oricărei persoane fizice sau juridice cu domiciliul sau sediul social într-un stat membru.

În temeiul legislației CoE, se poate face trimitere la principiile consacrate în Recomandarea privind accesul la documentele oficiale, care a inspirat autorii Convenției privind accesul la documentele oficiale (Convenția 205)[99].

În temeiul legislației UE, dreptul de acces la documentele oficiale este garantat de Regulamentul (CE) nr. 1049/2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei[100] (Regulamentul privind accesul la documente). 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 suportul pe care se află aceste documente”.

Acest drept poate intra în conflict cu dreptul la protecția datelor în cazul în care accesul la un document ar dezvălui datele cu caracter personal ale altora. Articolul 86 din Regulamentul general privind protecția datelor prevede în mod clar

98 Hotărârea CJUE [MC] din 21 decembrie 2016 în cauzele conexate C-203/15 și C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen* și *Secretary of State for the Home Department/Tom Watson și alții*, punctele 37 și 101; Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții* și *Kärntner Landesregierung și alții*, punctul 28.

99 Recomandarea Rec(81)19 din 2002 și Recomandarea Rec(2002)2 din 21 februarie 2002 a Comitetului de Miniștri al Consiliului Europei către statele membre privind accesul la documentele oficiale; Convenția din 18 iunie 2009 a Consiliul Europei privind accesul la documentele oficiale, CETS nr. 205. Convenția nu a intrat încă în vigoare.

100 Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei, JO 2001 L 145.

că datele cu caracter personal din documentele oficiale deținute de autoritățile și organismele publice pot fi divulgate de autoritatea sau organismul în cauză, în conformitate cu legislația Uniunii[101] sau a statului membru, pentru a stabili un echilibru între accesul public la documente oficiale și dreptul la protecția datelor în conformitate cu regulamentul.

Prin urmare, este posibil ca solicitările de acces la documentele sau informațiile deținute de autoritățile publice să presupună echilibrarea cu dreptul la protecția datelor persoanelor ale căror date sunt cuprinse în documentele solicitate.

Exemplu: În cauzele conexate *Volker und Markus Schecke și Hartmut Eifert/Land Hessen*[102], CJUE a trebuit să se pronunțe asupra proporționalității publicării, impusă de legislația UE, a numelor beneficiarilor subvențiilor agricole ale UE și a sumelor pe care aceștia le-au primit. Publicarea urmărea creșterea transparenței și contribuția la controlul public al utilizării adecvate a fondurilor publice de către administrație. Mai mulți beneficiari au contestat proporționalitatea acestei publicări.

Remarcând faptul că dreptul la protecția datelor nu este absolut, CJUE a argumentat că publicarea pe un site a datelor nominale ale beneficiarilor a două fonduri ale UE de ajutoare pentru agricultură și a sumelor exacte primite constituie o ingerință în viața privată, la nivel general, și în protecția datelor cu caracter personal ale acestora, la nivel particular.

CJUE a constatat că o astfel de atingere adusă articolelor 7 și 8 din Cartă este prevăzută de lege și răspunde unui obiectiv de interes general recunoscut de UE, și anume consolidarea transparenței în ceea ce privește utilizarea fondurilor comunitare. Cu toate acestea, CJUE a considerat că publicarea numelor persoanelor fizice care beneficiază de ajutor pentru agricultură din partea UE în cadrul acestor două fonduri și a sumelor exacte primite constituie o măsură disproporționată și nejustificată în conformitate cu articolul 52 alineatul (1) din Cartă. Curtea a recunoscut că, într-o societate democratică, este important ca contribuabilii să fie informați cu privire la utilizarea fondurilor publice. Cu toate acestea, întrucât „nu se poate recunoaște obiectivului transparenței nicio superioritate automată asupra dreptului la protecția datelor cu caracter

101 Articolul 42 din Cartă, articolul 15 alineatul (3) din TFUE și Regulamentul (CE) nr. 1049/2001.

102 Hotărârea CJUE [MC] din 9 noiembrie 2010 în cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*, punctele 47-52, 58, 66-67, 75, 86 și 92.

personal”[103], instituțiile UE aveau obligația de a stabili un echilibru între interesul Uniunii în ceea ce privește transparența, pe de o parte, și limitarea exercițiului drepturilor la respectarea vieții private și la protecția datelor care le fusese impusă beneficiarilor ca rezultat al publicării, pe de altă parte.

CJUE a considerat că instituțiile UE nu au efectuat corect acest exercițiu de echilibrare, întrucât era posibil să fie concepute măsuri prin care se aduc atingeri mai puțin grave drepturilor fundamentale ale persoanelor, astfel încât să contribuie în același timp în mod eficient la obiectivul transparenței urmărit de publicare. De exemplu, în locul unei publicări generale care afectează toți beneficiarii, indicând numele acestora și sumele exacte primite de fiecare dintre ei, se putea face o distincție în funcție de criterii relevante, precum perioadele în care aceste persoane au primit astfel de fonduri, frecvența sau tipul și valoarea acestora[104]. Astfel, CJUE a declarat parțial nulă legislația UE privind publicarea informațiilor referitoare la beneficiarii fondurilor UE pentru agricultură.

Exemplu: În cauza *Rechnungshof/Österreichischer Rundfunk și alții*[105], CJUE a examinat compatibilitatea anumitor acte legislative interne ale Austriei cu legislația UE privind protecția datelor. Legislația austriacă impunea unui organism de stat să colecteze și să transmită date privind veniturile în scopul publicării numelor și veniturilor angajaților diferitelor entități publice într-un raport anual pus la dispoziția publicului larg. Unele persoane au refuzat să comunice datele care le priveau, invocând dreptul la protecția datelor.

În avizul său, CJUE s-a bazat pe protecția drepturilor fundamentale ca principiu general al dreptului UE și pe articolul 8 din Convenția europeană a drepturilor omului, reamintind că Carta nu avea caracter juridic obligatoriu la momentul respectiv. Curtea a considerat că colectarea datelor privind veniturile profesionale ale unei persoane și în special comunicarea acestor date către părți terțe 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 în conformitate cu legea, ar urmări un scop legitim și ar fi necesară într-o societate democratică pentru atingerea acestui scop. CJUE a arătat

103 *Ibidem*, punctul 85.

104 *Ibidem*, punctul 89.

105 Hotărârea CJUE din 20 mai 2003 în cauzele conexate C-465/00, C-138/01 și C-139/01, *Rechnungshof/Österreichischer Rundfunk și alții și Christa Neukomm și Joseph Lauermann/Österreichischer Rundfunk*.

că legislația austriacă urmărea un scop legitim, întrucât obiectivul său era de a menține salariile angajaților din sectorul public în limite rezonabile, un considerent care este legat, de asemenea, de bunăstarea economică a țării. Cu toate acestea, interesul Austriei de a asigura cea mai bună utilizare a fondurilor publice trebuia să fie echilibrat cu amploarea ingerinței în dreptul persoanelor în cauză la respectarea vieții private.

Lăsând instanței naționale sarcina de a determina dacă publicarea datelor privind veniturile persoanelor era necesară și proporțională cu obiectivul urmărit de legislație, CJUE a solicitat instanței naționale să examineze dacă scopul în cauză nu ar fi putut fi atins în mod la fel de eficient prin mijloace mai puțin invazive. Spre exemplu, datele cu caracter personal ar fi putut să fie comunicate doar organismelor publice de monitorizare, iar nu publicului larg.

În cauzele ulterioare, a devenit evident că stabilirea unui echilibru între protecția datelor și accesul la documentele oficiale necesită o analiză detaliată, de la caz la caz. Niciunul dintre cele două drepturi nu îl poate anula în mod automat pe celălalt. CJUE a avut ocazia să interpreteze dreptul de acces la documente oficiale 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 raportul între Regulamentul (CE) nr. 1049/2001 (Regulamentul privind accesul la documente) și Regulamentul (CE) nr. 45/2001 (Regulamentul privind protecția datelor de către instituțiile europene). Bavarian Lager, înființată în anul 1992, importă bere germană îmbuteliată în Regatul Unit, în principal pentru puburi și baruri. Cu toate acestea, a întâmpinat dificultăți, întrucât legislația britanică *de facto* favorizează producătorii naționali. Ca răspuns la plângerea introdusă de Bavarian Lager, Comisia Europeană a introdus o acțiune împotriva Regatului Unit pentru neîndeplinirea obligațiilor, care a condus la modificarea dispozițiilor contestate și la alinierea acestora la dreptul UE. Ulterior, Bavarian Lager a solicitat Comisiei, printre alte documente, o copie a procesului-verbal al reuniunii la care au participat reprezentanți ai Comisiei, ai autorităților britanice și ai *Confédération des Brasseurs du Marché Commun* (CBMC). Comisia a fost de acord să divulge anumite documente cu privire la reuniune, însă a șters cinci nume care apăreau în procesul-verbal, două persoane obiectând în mod expres

106 Hotărârea CJUE [MC] din 29 iunie 2010 în cauza C-28/08 P, *Comisia Europeană/The Bavarian Lager Co. Ltd.*

față de publicarea identității lor, iar celelalte trei neputând fi contactate de către Comisie. Prin decizia din 18 martie 2004, Comisia a respins din nou cererea Bavarian Lager privind obținerea procesului-verbal integral al reuniunii, citând, în special, protecția vieții private a acelor persoane, astfel cum este garantată prin Regulamentul privind protecția datelor de către instituțiile europene.

Întrucât nu a fost mulțumită de această poziție, Bavarian Lager a introdus o acțiune înaintea Tribunalului de Primă Instanță. Acesta a anulat decizia Comisiei prin hotărârea din 8 noiembrie 2007 (cauza T-194/04, *The Bavarian Lager Co. Ltd./Comisia Comunităților Europene*), considerând, în speță, că simpla includere a numelor persoanelor în cauză pe lista persoanelor care au participat la reuniune în numele organismului pe care îl reprezintă nu constituie o subminare a vieții private și nu periclitează în niciun fel viețile private ale acelor persoane.

În cadrul judecării recursului introdus de Comisie, CJUE a anulat hotărârea Tribunalului de Primă Instanță. CJUE a considerat că Regulamentul privind accesul la documente instituie „un regim specific și consolidat de protecție a unei persoane ale cărei date cu caracter personal ar putea, eventual, să fie comunicate public". Potrivit CJUE, în cazul în care o cerere în conformitate cu Regulamentul privind accesul la documente urmărește să obțină acces la documente care includ date cu caracter personal, dispozițiile Regulamentului privind protecția datelor de către instituțiile europene devin aplicabile în toate elementele lor. Potrivit concluziilor ulterioare ale CJUE, Comisia a fost îndreptățită să respingă solicitarea de acces la procesul-verbal integral al reuniunii din luna octombrie 1996. În absența consimțământului celor cinci participanți la reuniune, Comisia și-a respectat suficient îndatorirea de deschidere prin eliberarea unei versiuni a documentului în cauză în care numele acestora erau șterse.

În plus, potrivit CJUE, „[î]ntrucât Bavarian Lager nu a oferit nicio motivare expresă și legitimă și niciun argument convingător pentru a demonstra necesitatea transferului acestor date personale, Comisia nu a putut să compare diferitele interese ale părților în cauză. Aceasta nu putea nici să verifice dacă nu exista niciun motiv să se presupună că acest transfer ar putea aduce atingere intereselor legitime ale persoanelor vizate", astfel precum prevede Regulamentul privind protecția datelor de către instituțiile europene.

Exemplu: În cauza *ClientEarth și PAN Europe/EFSA*[107], CJUE a examinat dacă decizia Autorității Europene pentru Siguranța Alimentară (EFSA) de a refuza reclamanților accesul deplin la documente a fost necesară pentru a proteja drepturile la respectarea vieții private și la protecția datelor persoanelor la care se refereau documentele în cauză. Documentele au vizat un proiect de raport de orientare elaborat de un grup de lucru al EFSA în colaborare cu experți externi privind introducerea pe piață a produselor fitosanitare. Inițial, EFSA a acordat reclamanților accesul parțial la documente, refuzând accesul la anumite versiuni de lucru ale documentului de orientare. Ulterior, a acordat acces la versiunea de proiect care includea observațiile individuale ale experților externi. Cu toate acestea, a omis numele experților, invocând articolul 4 alineatul (1) litera (b) din Regulamentul (CE) nr. 45/2001 privind prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și necesitatea de a proteja viața privată a experților externi. În primă instanță, Tribunalul UE a confirmat decizia EFSA.

În cadrul judecării recursului introdus de reclamanți, CJUE a anulat hotărârea Tribunalului de Primă Instanță. CJUE a concluzionat că transferul de date cu caracter personal în acest caz era 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 EFSA. Potrivit CJUE, EFSA nu a specificat în ce mod dezvăluirea numelor experților externi care au făcut observații specifice cu privire la proiectul de document de orientare ar aduce atingere intereselor legitime ale experților. Argumentul general potrivit căruia divulgarea ar putea submina viața privată nu este suficient dacă nu este susținut de probe specifice fiecărui caz.

Potrivit acestor hotărâri, atingerea adusă dreptului la protejarea datelor în contextul accesului la documente necesită o motivare precisă și întemeiată. Dreptul de acces la documente nu poate anula în mod automat dreptul la protecția datelor[108].

Această abordare a raportului dintre respectarea vieții private și accesul la documente este similară celei adoptate de CEDO, după cum demonstrează hotărârea descrisă în continuare. În hotărârea *Magyar Helsinki*, CEDO a stabilit că articolul 10 nu

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

108 Vezi totuși dezbaterile detaliate ale Autorității Europene pentru Protecția Datelor (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling* (Accesul public la documente care conțin date cu caracter personal în urma hotărârii din cauza *Bavarian Lager*), Bruxelles, 24 martie 2011.

conferă unei persoane fizice dreptul de acces la informațiile deținute de o autoritate publică și nu obligă guvernul să comunice aceste informații persoanelor fizice. Cu toate acestea, ar putea apărea un astfel de drept sau obligație în următoarele situații: în primul rând, în cazul în care divulgarea informațiilor este impusă printr-un ordin judecătoresc care a dobândit o forță juridică; în al doilea rând, în cazul în care accesul la informații este esențial pentru exercitarea de către o persoană a dreptului său la libertatea de exprimare – în special a libertății de a primi și de a transmite informații – și dacă refuzarea accesului ar aduce atingere acestui drept[109]. Aspectul dacă refuzarea accesului la informații constituie o ingerință în libertatea de exprimare a unui solicitant și amploarea acestei ingerințe trebuie să fie evaluate de la caz la caz și în funcție de circumstanțele specifice, printre care: (i) scopul cererii de informații; (ii) natura informațiilor solicitate; (iii) rolul solicitantului; și (iv) aspectul dacă informațiile sunt pregătite și disponibile.

Exemplu: În cauza *Magyar Helsinki Bizottság/Ungaria*[110], reclamantul, un ONG din domeniul drepturilor omului, a solicitat autorității polițienești informații cu privire la activitatea avocatului apărării *ex officio*, în scopul realizării unui studiu despre funcționarea sistemului apărătorilor publici din Ungaria. Poliția a refuzat să furnizeze informațiile, argumentând că acestea constituie date cu caracter personal care nu pot fi divulgate. Aplicând criteriile de mai sus, CEDO a considerat că a existat o intervenție asupra unui drept protejat în temeiul articolului 10. Mai exact, reclamantul a dorit să își exercite dreptul de a transmite informații cu privire la un subiect de interes public, a solicitat acces la informații în acest scop, iar informațiile erau necesare pentru exercițiul dreptului la libertate de exprimare al reclamantului. Informațiile privind numirea apărătorilor publici erau informații de interes public. Nu a existat niciun motiv pentru a pune la îndoială faptul că studiul în cauză conținea informații pe care reclamantul s-a angajat să le transmită publicului și pe care publicul avea dreptul să le primească. Astfel, Curtea a confirmat că accesul la informațiile solicitate era necesar pentru îndeplinirea sarcinii reclamantului. În sfârșit, informațiile erau pregătite și disponibile.

CEDO a concluzionat că refuzarea accesului la informații în speță a afectat însăși substanța libertății de a primi informații. În stabilirea concluziei sale, Curtea a examinat în special scopul informațiilor solicitate și contribuția lor

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

110 *Ibidem*, punctele 181, 187-200.

la o dezbatere publică importantă, natura informațiilor solicitate, caracterul de interes public al acestora și rolul jucat în societate de către reclamantul în cauză.

În raționamentul său, Curtea a arătat că studiul realizat de ONG-ul în cauză viza funcționarea justiției și dreptul la un proces echitabil, care constituie un drept de o importanță capitală în temeiul Convenției europene a drepturilor omului. Întrucât informațiile solicitate nu conțineau date din afara domeniului public, drepturile la respectarea vieții private ale persoanelor vizate în cauză (apărătorii publici *ex officio*) nu ar fi fost compromise dacă autoritatea polițienească ar fi acordat reclamantului acces la informații. Informațiile solicitate de reclamant erau de natură statistică, fiind legate de numărul de cazuri în care fuseseră numiți avocați *ex officio* pentru a reprezenta inculpații în proceduri penale publice.

În opinia Curții, având în vedere că studiul a avut ca scop să contribuie la o dezbatere importantă pe o temă de interes general, orice restricții privind publicarea propusă de ONG trebuiau să fie supuse unei examinări foarte atente. Informațiile în cauză erau de interes public, întrucât interesul public vizează „aspecte care pot crea controverse semnificative, care privesc o problemă socială importantă sau care implică o problemă în legătură cu care publicul ar avea interesul să fie informat”[111]. Prin urmare, interesul public ar viza, cu siguranță, o dezbatere privind funcționarea justiției și procesul echitabil, care făcea obiectul studiului reclamantului. Stabilind un echilibru între diferitele drepturi în cauză și aplicând principiul proporționalității, CEDO a considerat că a avut loc o încălcare nejustificată a drepturilor reclamantului prevăzute de articolul 10 din Convenția europeană a drepturilor omului.

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 juridică inerentă anumitor profesii și funcții care se bazează pe încredere. Persoanele și instituțiile care îndeplinesc aceste funcții au obligația de a nu divulga informațiile confidențiale pe care le primesc în cursul îndeplinirii îndatoririlor lor. Secretul profesional se aplică în mod deosebit profesiei de medic și celei

111 *Ibidem*, punctul 156.

de avocat, multe jurisdicții recunoscând, de asemenea, o obligație a secretului profesional în sectorul financiar. Secretul profesional nu este un drept fundamental, dar este protejat ca o formă a dreptului la respectarea vieții private. De exemplu, CJUE a statuat că, în anumite cazuri, „interzicerea divulgării anumitor informații calificate drept confidențiale poate fi necesară pentru a garanta dreptul fundamental al unei întreprinderi la respectarea vieții private, prevăzut la articolul 8 din [Convenția europeană a drepturilor omului] [...] și la articolul 7 din [C]artă"[112]. Și CEDO a fost sesizată cu solicitarea de a se pronunța asupra faptului dacă restricțiile legate de secretul profesional constituie o încălcare a articolului 8 din Convenția europeană a drepturilor omului, după cum se arată la exemplele de mai jos.

Exemplu: În cauza *Pruteanu/România*[113], reclamantul a acționat în calitate de avocat al unei societăți comerciale căreia i s-a interzis să efectueze tranzacții bancare ca urmare a unor acuzații de fraudă. În cadrul examinării cauzei, instanțele române au autorizat autoritățile de urmărire penală să intercepteze și să înregistreze convorbirile telefonice ale unui partener de afaceri al societății în cauză pentru o anumită perioadă. Înregistrările și interceptările au inclus comunicările cu avocatul său.

Domnul Pruteanu a susținut că acest lucru a adus atingere dreptului său la respectarea vieții private și a corespondenței. În hotărârea sa, CEDO a subliniat statutul și importanța relației dintre avocat și client. Interceptarea conversațiilor avocatului cu clientul său a încălcat fără îndoială secretul profesional, pe care se întemeia relația dintre aceste două persoane. Într-un astfel de caz, avocatul ar putea, de asemenea, să acuze o ingerință în dreptul său la respectarea vieții private și a corespondenței. CJUE a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Exemplu: În cauza *Brito Ferrinho Bexiga Villa-Nova/Portugalia*[114], reclamanta, de profesie avocat, a refuzat să își divulge extrasele de cont personale autorităților fiscale, invocând secretul profesional și secretul bancar. Procuratura a deschis o anchetă de fraudă fiscală și a solicitat autorizația de a suspenda

112 Hotărârea CJUE din 11 martie 2013 în cauza T-462/12 R, *Pilkington Group Ltd/Comisia Europeană*, Ordonanța președintelui Tribunalului, punctul 44.

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

114 Hotărârea CEDO din 1 decembrie 2015 în cauza *Brito Ferrinho Bexiga Villa-Nova/Portugalia*, nr. 69436/10.

secretul profesional. Instanțele naționale au dispus suspendarea normelor privind secretul profesional și secretul bancar, considerând că interesul public ar trebui să prevaleze asupra intereselor private ale reclamantei.

Când a fost sesizată cu această cauză, CEDO a considerat că accesul la extrasele de cont ale reclamantei constituia o intervenție asupra dreptului său la respectarea secretului profesional, care intră în sfera vieții private. Intervenția a avut un temei juridic, deoarece se baza pe codul de procedură penală, și a urmărit un scop legitim. Cu toate acestea, examinând necesitatea și proporționalitatea intervenției, CEDO a subliniat faptul că procedurile de suspendare a confidențialității au fost efectuate fără participarea reclamantei și fără să îi fie aduse la cunoștință. Prin urmare, reclamanta nu a avut posibilitatea să își prezinte argumentele. În plus, chiar dacă dreptul intern prevedea că asociația de avocați trebuia să fie consultată în astfel de proceduri, asociația nu fusese consultată. În sfârșit, reclamanta nu a avut opțiunea de a contesta în mod eficace suspendarea confidențialității și nici nu a avut la dispoziție vreo cale de atac prin care să conteste măsura. Având în vedere lipsa garanțiilor procedurale și a controlului judiciar efectiv asupra măsurii de suspendare a obligației de confidențialitate, CEDO a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

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 operatorilor și persoanelor împuternicite de operatori 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 privind protecția datelor al UE permite prelucrarea datelor medicale, care constituie categorii speciale de date cu caracter personal și necesită o protecție mai puternică, dar condiționează această prelucrare de existența unor măsuri adecvate și specifice de protecție a drepturilor persoanelor vizate, în special obligația de păstrare a secretului profesional[115].

Pe de altă parte, obligațiile de păstrare a secretului profesional impuse operatorilor și persoanelor împuternicite de operatori cu privire la anumite date cu caracter personal pot restrânge drepturile persoanelor vizate, în special dreptul de a primi

115 Regulamentul general privind protecția datelor, articolul 9 alineatul (2) litera (h) și articolul 9 alineatul (3).

informații. Deși Regulamentul general privind protecția datelor conține o listă cuprinzătoare de informații care, în principiu, trebuie furnizate persoanei vizate în cazul în care datele cu caracter personal nu au fost obținute de la persoana în cauză, această cerință de divulgare nu se aplică atunci când datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern[116].

Regulamentul general privind protecția datelor (RGPD) prevede posibilitatea ca statele membre să adopte prin lege norme specifice pentru a proteja obligația de a păstra secretul profesional sau alte obligații echivalente de confidențialitate și pentru a stabili un echilibru între dreptul la protecția datelor cu caracter personal și obligația păstrării secretului profesional[117].

RGPD prevede că statele membre pot adopta norme specifice privind competențele autorităților de supraveghere în legătură cu operatori sau cu persoane împuternicite de operatori care au obligația de a păstra secretul profesional. Aceste norme specifice se referă la prerogativa de a obține acces la sediul unui operator sau al unei persoane împuternicite de operator, la echipamentele de prelucrare a datelor ale acestora și la datele 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 însărcinate cu protecția datelor trebuie să respecte obligațiile privind secretul profesional care sunt obligatorii pentru operatori și persoanele împuternicite de operatori. Mai mult, membrii autorităților de supraveghere înșiși au obligația de a păstra secretul profesional în timpul mandatului lor și după încheierea acestuia. În cursul exercitării atribuțiilor, membrii și personalul autorităților de supraveghere pot să dobândească acces la informații confidențiale. Articolul 54 alineatul (2) din regulament prevede în mod clar că aceștia au obligația de a păstra secretul profesional cu privire la astfel de informații confidențiale.

RGPD impune ca statele membre să notifice Comisiei normele pe care le adoptă pentru a stabili un echilibru între protecția datelor și principiile stabilite în regulament, pe de o parte, și obligația de păstrare a secretului profesional, pe de altă parte.

116 *Ibidem*, articolul 14 alineatul (5) litera (d).

117 *Ibidem*, considerentul 164 și articolul 90.

1.3.3. Libertatea religioasă și de convingeri

Libertatea religioasă și de convingeri este protejată în temeiul articolului 9 din Convenția europeană a drepturilor omului (libertatea de gândire, de conștiință și de religie) și al articolului 10 din Carta drepturilor fundamentale a UE. Datele cu caracter personal care dezvăluie convingeri religioase sau filosofice sunt considerate „date sensibile" atât în temeiul legislației UE, cât și al legislației CoE, iar prelucrarea și utilizarea acestora fac obiectul unei protecții sporite.

Exemplu: Reclamantul din cauza *Sinan Işık/Turcia*[118] era membru al comunității religioase Alevi, a cărei credință este influențată de sufism și de alte credințe pre-islamice și care este considerată de unii cercetători ca fiind o religie separată, iar de alții ca făcând parte din religia islamică. Reclamantul a denunțat faptul că, împotriva voinței sale, cartea sa de identitate conține o casetă care indică religia sa drept „Islam", iar nu „Alevi". Instanțele interne i-au respins cererea de a i se înlocui mențiunea de pe cartea de identitate cu „Alevi" pentru motivul că acest cuvânt desemna un subgrup al islamului, iar nu o religie separată. Ulterior, reclamantul a susținut în fața CEDO că a fost obligat să își dezvăluie credința fără consimțământul său, deoarece era obligatoriu să se indice religia unei persoane pe cartea de identitate, și că acest lucru îi încălca dreptul la libertatea de religie și de conștiință, cu atât mai mult cu cât mențiunea „islam" pe cartea sa de identitate era incorectă.

CEDO a reiterat faptul că libertatea religioasă presupune libertatea unei persoane de a-și manifesta religia în comunitate cu alte persoane, în public și în cercul persoanelor care împărtășesc aceeași credință, dar și în solitudine și în particular. Legislația internă aplicabilă la momentul respectiv impunea persoanelor să poarte la ele o carte de identitate, un document care trebuia prezentat la cererea oricărei autorități publice sau a unor întreprinderi private, iar cartea de identitate indica religia titularului. Această obligație a ignorat faptul că dreptul unei persoane de a-și manifesta religia garantează și posibilitatea inversă, și anume dreptul unei persoane de a nu fi obligate să își dezvăluie convingerile. Deși guvernul a susținut că legislația națională a fost modificată astfel încât persoanele să poată solicita necompletarea casetei destinate religiei de pe cartea de identitate, Curtea consideră că simplul fapt de a solicita să nu se menționeze religia ar putea constitui o divulgare de informații privind atitudinea față de religie a unei persoane. În plus,

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

în condițiile în care cărțile de identitate conțin o casetă destinată religiei, necompletarea acesteia are o conotație specială, întrucât titularii unei cărți de identitate fără informații despre religie ar ieși în evidență în raport cu cei care au o carte de identitate pe care se indică religia. CEDO a concluzionat că s-a încălcat articolul 9 din Convenția europeană a drepturilor omului.

Cu toate acestea, funcționarea bisericilor și a asociațiilor sau comunităților religioase poate necesita prelucrarea informațiilor cu caracter personal ale membrilor lor, pentru a permite comunicarea și organizarea activităților în cadrul congregației. Astfel, bisericile și asociațiile religioase au pus adesea 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 cuprinzătoare, ele pot continua să se aplice, cu condiția să fie aliniate la dispozițiile regulamentului. Bisericile și asociațiile religioase care aplică astfel de norme trebuie să fie supuse supravegherii unei autorități de supraveghere independente care poate fi specifică, cu condiția să îndeplinească cerințele Regulamentului general privind protecția datelor aplicabile unor astfel de autorități[119].

Organizațiile religioase pot prelucra date cu caracter personal din diverse motive – de exemplu, pentru a păstra contactul cu congregația sau pentru a comunica informații despre evenimentele religioase sau caritabile și festivitățile organizate. În anumite state, bisericile trebuie să păstreze registre cu membrii lor pentru motive fiscale, deoarece apartenența la instituțiile religioase poate avea un impact asupra impozitelor datorate de către persoanele fizice. În orice caz, în temeiul dreptului european, datele care divulgă convingerile religioase sunt considerate date sensibile, iar bisericile trebuie să fie responsabile pentru gestionarea și prelucrarea acestor date, cu atât mai mult cu cât informațiile prelucrate de organizațiile religioase se referă adesea la copii, vârstnici sau alți membri vulnerabili ai societății.

1.3.4. Libertatea artelor și științelor

Un alt drept care trebuie să fie echilibrat cu dreptul la respectarea vieții private și cu dreptul la protecția datelor este libertatea artelor și științelor, protejată în mod explicit în temeiul articolului 13 din Carta drepturilor fundamentale a UE. Acest drept decurge în principal din libertatea de gândire și de exprimare și se exercită cu respectarea articolului 1 din Cartă („Demnitatea umană"). CEDO consideră că libertatea

119 Regulamentul general privind protecția datelor, articolul 91 alineatul (2).

artelor este protejată prin articolul 10 din Convenția europeană a drepturilor omului[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 Convenția europeană a drepturilor omului[121].

Exemplu: În cauza *Vereinigung bildender Künstler/Austria*[122], instanțele austriece au interzis asociației reclamante să continue expunerea unei picturi care conținea fotografii ale capetelor mai multor personalități în poziții sexuale. Un parlamentar austriac, a cărui fotografie fusese folosită în tablou, a formulat o acțiune împotriva asociației reclamante, solicitând un ordin de încetare care să îi interzică acesteia să expună tabloul. Instanța națională a emis un ordin de încetare. CEDO a reiterat că articolul 10 din Convenția europeană a drepturilor omului este aplicabil și în cazul transmiterii unor idei care insultă, șochează sau perturbă statul sau orice parte a populației. Acele persoane care creează, realizează, distribuie sau expun lucrări de artă contribuie la schimbul de idei și opinii, iar statul are obligația de a nu atenta în mod nejustificat la libertatea lor de exprimare. Având în vedere că tabloul era un colaj și folosea fotografii înfățișând numai capetele persoanelor, corpurile fiind pictate într-o manieră nerealistă și exagerată, care, în mod evident, nu avea ca scop reflectarea sau chiar sugerarea realității, CEDO a stabilit în continuare că „tabloul nu putea fi înțeles ca vizând detalii din viața privată a [persoanei descrise], ci, mai degrabă, asociate figurii sale publice de politician" și că „în această calitate [persoana descrisă] trebuie să afișeze o mai mare toleranță în ceea ce privește dezaprobarea". Cântărind diferitele interese în cauză, CEDO a constatat că interzicerea pe termen nelimitat a expunerii tabloului este disproporționată. Curtea a concluzionat că s-a încălcat articolul 10 din Convenția europeană a drepturilor omului.

Legislația europeană privind protecția datelor recunoaște, de asemenea, valoarea specială a științei pentru societate. Regulamentul general privind protecția datelor și Convenția 108 modernizată permit păstrarea datelor pentru perioade mai lungi în măsura în care datele cu caracter personal vor fi prelucrate numai în scopuri de

120 Hotărârea CEDO din 24 mai 1988 în cauza *Müller și alții/Elveția*, nr. 10737/84.

121 Explicații cu privire la Carta drepturilor fundamentale, JO 2007 C 303.

122 Hotărârea CEDO din 25 ianuarie 2007 în cauza *Vereinigung bildender Künstler/Austria*, nr. 68354/01, punctele 26 și 34.

cercetare științifică sau istorică. Mai mult, și indiferent de scopul inițial al unei activități specifice de prelucrare, utilizarea ulterioară a datelor cu caracter personal pentru cercetarea științifică nu este considerată a fi 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 a obține accesul la prelucrare sau rectificarea ori restricționarea acesteia și de a obiecta în ceea ce privește prelucrarea datelor cu caracter personal în scopuri științifice, istorice sau statistice (vezi, de asemenea, secțiunea 6.1 și secțiunea 9.4).

1.3.5. Protejarea proprietății intelectuale

Dreptul la protejarea proprietății este consacrat la articolul 1 din Primul protocol la Convenția europeană a drepturilor omului și la articolul 17 alineatul (1) din Carta drepturilor fundamentale a UE. Un aspect important legat de dreptul la proprietate care prezintă o relevanță deosebită din perspectiva protecției datelor este protecția proprietății intelectuale, menționată în mod explicit la articolul 17 alineatul (2) din Cartă. Mai multe directive din ordinea juridică a UE vizează protejarea eficientă a proprietății intelectuale, în special a dreptului de autor. Proprietatea intelectuală desemnează nu numai proprietatea literară sau artistică, ci și brevetele, mărcile și drepturile asociate.

Astfel cum se clarifică prin jurisprudența CJUE, protecția dreptului fundamental la proprietate trebuie echilibrată cu protecția altor drepturi fundamentale, în special cu dreptul la protecția datelor[124]. Au existat cazuri în care unele instituții responsabile pentru protejarea dreptului de autor au solicitat furnizorilor de internet să publice identitatea utilizatorilor platformelor de partajare de fișiere prin internet. Aceste platforme oferă deseori posibilitatea utilizatorilor de internet să descarce gratuit melodii, chiar dacă acestea sunt protejate prin drepturi de autor.

> Exemplu: Cauza *Promusicae/Telefónica de España*[125] se referă la refuzul unui furnizor spaniol de acces la internet, Telefónica, de a face cunoscute către Promusicae, o organizație nonprofit de producători muzicali și editori de

123 Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (b) și Convenția 108 modernizată, articolul 5 alineatul (4) litera (b).

124 Hotărârea CJUE [MC] 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 și 60.

înregistrări muzicale și audiovizuale, datele cu caracter personal ale anumitor persoane cărora le furnizase servicii de acces la internet. Promusicae a solicitat publicarea informațiilor astfel încât să poată iniția un proces civil împotriva acelor persoane, despre care a declarat că utilizau un program de schimb de fișiere care oferea acces la fonograme ale căror drepturi de exploatare erau deținute de membrii Promusicae.

Instanța spaniolă a trimis cauza CJUE, întrebând dacă aceste date cu caracter personal trebuie comunicate, în temeiul dreptului comunitar, în contextul unui proces civil pentru a asigura protecția eficace a dreptului de autor. Instanța spaniolă a făcut referire la Directivele 2000/31/CE, 2001/29/CE și 2004/48/CE, interpretate și din perspectiva articolelor 17 și 47 din Cartă. CJUE a concluzionat că aceste trei directive, precum și Directiva asupra confidențialității și comunicațiilor electronice (Directiva 2002/58/CE), nu împiedică statele membre să stabilească o obligație de publicare a datelor cu caracter personal în contextul unui proces civil pentru a asigura protecția eficace a dreptului de autor.

CJUE a subliniat faptul că această cauză a ridicat, astfel, întrebarea cu privire la necesitatea de a stabili un echilibru între cerințele legate de protecția diferitor drepturi fundamentale, și anume între dreptul la respectarea vieții private, pe de o parte, și dreptul la protecția proprietății și dreptul de acces la o cale de atac eficientă, pe de altă parte.

Curtea a concluzionat că „revine statelor membre ca, la transpunerea directivelor menționate, să se asigure că se întemeiază pe o interpretare a directivelor care poate asigura un just echilibru între diferitele drepturi fundamentale protejate de ordinea juridică comunitară. Pe lângă aceasta, la punerea în aplicare a măsurilor de transpunere a acestor directive, incumbă autorităților și instanțelor din statele membre nu numai să interpreteze dreptul lor național într-un mod conform directivelor menționate, ci și să se asigure că nu se vor întemeia pe o interpretare a acestora care ar intra în conflict cu drepturile fundamentale respective sau cu alte principii generale ale dreptului comunitar, precum principiul proporționalității”[126].

126 *Ibidem*, punctele 65 și 68; vezi, de asemenea, Hotărârea CJUE din 16 februarie 2012 în cauza C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/Netlog NV*.

Exemplu: Cauza *Bonnier Audio AB și alții/Perfect Communication Sweden AB*[127] a vizat echilibrul între drepturile de proprietate intelectuală și protecția datelor cu caracter personal. Reclamantele – cinci societăți editoriale care dețineau drepturile de autor pentru 27 de cărți audio – au introdus o acțiune în fața instanței suedeze, susținând că aceste drepturi de autor au fost încălcate prin intermediul unui server FTP (un protocol de transfer de fișiere care permite partajarea de fișiere și transferul de date prin internet). Reclamantele au solicitat furnizorului de servicii internet (ISP) să divulge numele și adresa persoanei care utilizează adresa IP de la care au fost trimise fișierele. ePhone, furnizorul de servicii internet în cauză, a contestat cererea, susținând că aceasta încalcă Directiva 2006/24/CE (Directiva privind păstrarea datelor, anulată în 2014).

Instanța suedeză a trimis cauza CJUE, întrebând dacă Directiva 2006/24/CE se opune aplicării unei dispoziții naționale în temeiul articolului 8 din Directiva 2004/48/CE (Directiva privind respectarea drepturilor de proprietate intelectuală), care permite emiterea unui ordin judecătoresc care să impună ISP să transmită deținătorilor drepturilor de autor informații despre abonații ale căror adrese IP se presupune că au fost utilizate în cadrul unor încălcări ale drepturilor în cauză. Întrebarea se baza pe premisa că reclamantele au prezentat dovezi clare privind încălcarea unui anumit drept de autor și că măsura este proporțională.

CJUE a subliniat că Directiva 2006/24/CE privește exclusiv prelucrarea și păstrarea datelor generate sau prelucrate de furnizorii de servicii de comunicații electronice în scopul utilizării în cadrul activităților de cercetare, de depistare și de urmărire a infracțiunilor grave, precum și transmiterea acestora către autoritățile naționale competente. Astfel, o dispoziție națională care transpune Directiva privind respectarea drepturilor de proprietate intelectuală nu intră sub incidența Directivei 2006/24/CE și, prin urmare, această directivă nu se opune aplicării respectivei dispoziții[128].

În ceea ce privește comunicarea numelui și adresei în cauză, solicitată de către reclamante, CJUE a considerat că o astfel de acțiune constituie prelucrare a unor date cu caracter personal și intră în domeniul de aplicare al

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 Sweden AB*.

128 *Ibidem*, punctele 40-41.

Directivei 2002/58/CE (Directiva asupra confidențialității și comunicațiilor electronice). De asemenea, Curtea a arătat că comunicarea acestor date este necesară în cadrul unei proceduri civile, în beneficiul titularului unui drept de autor, pentru a asigura protecția eficace a dreptului de autor și că, prin urmare, se încadrează prin însuși obiectul său în domeniul de aplicare al Directivei 2004/48/CE[129].

CJUE a concluzionat că Directivele 2002/58/CE și 2004/48/CE trebuie interpretate în sensul că nu se opun unei legislații naționale, precum cea în cauză în acțiunea principală, în măsura în care această legislație permite instanței naționale sesizate cu o cerere de emitere a unei somații de comunicare a datelor cu caracter personal să pondereze, în funcție de împrejurările fiecărei cauze și ținând seama în mod corespunzător de cerințele care rezultă din principiul proporționalității, interesele opuse existente.

1.3.6. Protecția datelor și interesele economice

În era digitală sau în era datelor masive, datele au fost descrise ca fiind „noul petrol" pentru economie din perspectiva stimulării inovației și a creativității[130]. Multe societăți comerciale au construit modele robuste de afaceri în domeniul prelucrării datelor și o astfel de prelucrare implică adesea date cu caracter personal. Unele societăți ar putea considera că anumite norme de protecție a datelor cu caracter personal pot conduce, în practică, la obligații excesive, care le-ar putea afecta interesele economice. Astfel, se pune întrebarea dacă interesele economice ale operatorilor și ale persoanelor împuternicite de operatori sau ale publicului larg ar putea justifica limitarea dreptului la protecția datelor.

Exemplu: În cauza *Google Spain*[131], CJUE a statuat că, în anumite condiții, persoanele au dreptul să solicite motoarelor de căutare să elimine rezultatele căutării din indexul de căutare. În raționamentul său, CJUE a subliniat faptul că utilizarea motoarelor de căutare și rezultatele afișate ale căutării pot stabili un profil detaliat al unei persoane. Aceste informații pot construi

129 *Ibidem*, punctele 52-54. Vezi, de asemenea, Hotărârea CJUE [MC] din 29 ianuarie 2008 în cauza C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, punctul 58.

130 Vezi, de exemplu, articolul publicat în 2016 de *Financial Times*, intitulat „Data is the new oil... who's going to own it?" („Datele sunt noul petrol... cine le va deține?", 16 noiembrie 2016.

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

o imagine amplă a vieții private a unei persoane și nu ar fi putut fi găsite sau interconectate cu ușurință fără un motor de căutare. Prin urmare, acest aspect constituie o posibilă ingerință gravă în drepturile fundamentale ale persoanelor vizate la respectarea vieții private și la protecția datelor cu caracter personal.

CJUE a examinat apoi dacă ingerința ar putea fi justificată. În ceea ce privește interesul economic al societății care exploatează motorul de căutare privind efectuarea prelucrării, CJUE a arătat că „trebuie să se constate că [ingerința] nu poate fi justificată doar prin interesul economic al operatorului unui astfel de motor privind prelucrarea respectivă" și că „în principiu" drepturile fundamentale prevăzute la articolele 7 și 8 din Cartă prevalează asupra interesului economic în cauză și asupra interesului publicului larg de a găsi informația în cauză cu ocazia unei căutări referitoare la numele persoanei vizate[132].

Unul dintre obiectivele principale ale legislației UE privind protecția datelor este acela de a le oferi persoanelor fizice mai mult control asupra datelor lor cu caracter personal. În special în era digitală, există un dezechilibru între puterea entităților comerciale care prelucrează și au acces la cantități mari de date cu caracter personal și puterea persoanelor fizice cărora le aparțin respectivele date cu caracter personal de a exercita controlul asupra informațiilor. CJUE adoptă o abordare de la caz la caz atunci când stabilește echilibrul între protecția datelor și interesele economice – cum ar fi interesele părților terțe în ceea ce privește societățile pe acțiuni și societățile cu răspundere limitată, după cum se arată în hotărârea *Manni*.

Exemplu: Cauza *Manni*[133] a vizat includerea datelor cu caracter personal ale unei persoane fizice într-un registru comercial public. Domnul Manni a solicitat Camerei de Comerț din Lecce să îi elimine datele cu caracter personal din registrul respectiv după ce a descoperit că potențialii clienți care ar consulta registrul ar vedea că a fost administratorul unei societăți care a fost declarată în stare de faliment cu mai mult de zece ani în urmă. Această informație crea o prejudecată în rândul clienților săi potențiali și putea să aibă un impact negativ asupra intereselor sale comerciale.

132 *Ibidem*, punctele 81 și 97.

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

CJUE a fost sesizată cu solicitarea de a stabili dacă dreptul UE recunoaște dreptul la ștergerea datelor în acest caz. În stabilirea concluziei sale, Curtea a examinat raportul dintre normele UE de protecție a datelor și interesul comercial al domnului Manni de a obține eliminarea informațiilor despre falimentul fostei sale societăți, pe de o parte, și interesul publicului de a avea acces la aceste informații, pe de altă parte. Curtea a luat în considerare, în mod corespunzător, faptul că publicarea registrului societăților comerciale este prevăzută de lege și, în special, de o directivă a UE care urmărește să faciliteze accesul terților la informațiile despre societățile comerciale. Divulgarea este importantă pentru a proteja interesele terților care ar putea dori să facă afaceri cu o anumită societate, deoarece singura garanție oferită terților de societățile pe acțiuni și de societățile cu răspundere limitată este patrimoniul lor social. Prin urmare, „publicitatea trebuie să permită terților cunoașterea actelor esențiale ale societății comerciale și alte informații privind societatea interesată, în special identitatea persoanelor care au competența să angajeze societatea”[134].

Având în vedere importanța scopului legitim urmărit de registru, CJUE a considerat că domnul Manni nu avea dreptul să obțină ștergerea datelor sale cu caracter personal, deoarece necesitatea de a proteja interesele terților în raport cu societățile pe acțiuni și cu societățile cu răspundere limitată și de a asigura securitatea juridică, loialitatea tranzacțiilor comerciale și, astfel, buna funcționare a pieței interne prevalează asupra drepturilor sale în temeiul legislației privind protecția datelor. Acest lucru era valabil cu atât mai mult cu cât persoanele care aleg să participe la comerț printr-o societate pe acțiuni sau o societate cu răspundere limitată sunt conștiente că au obligația de a divulga informații referitoare la identitatea și la funcțiile lor.

Deși a constatat că nu există motive pentru a obține ștergerea datelor în acest caz, CJUE a recunoscut totuși existența unui drept de a obiecta față de prelucrarea datelor, arătând următoarele: „nu este exclusă [...] posibilitatea existenței unor situații speciale în care motive preponderente și legitime care țin de situația concretă a persoanei interesate să justifice în mod excepțional ca accesul la datele cu caracter personal care o privesc înscrise în registru să fie limitat, la expirarea unui termen suficient de lung [...], la terții care justifică un interes specific pentru consultare”[135].

134 *Ibidem*, punctul 49.

135 *Ibidem*, punctul 60.

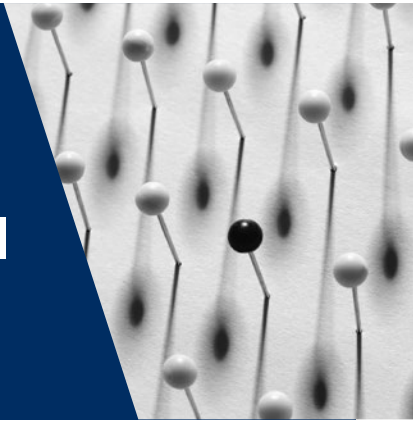
CJUE a stabilit că este de competența instanțelor naționale să evalueze, în fiecare caz și ținând seama de toate circumstanțele relevante ale situației persoanei, existența sau lipsa unor motive legitime și preponderente care ar putea justifica în mod excepțional restricționarea accesului terților la datele cu caracter personal din registrele societăților. Cu toate acestea, Curtea a precizat că, în cazul domnului Manni, simplul fapt că divulgarea datelor sale cu caracter personal în registru ar fi putut să îi afecteze clientela nu putea fi considerat un astfel de motiv legitim și preponderent. Clienții potențiali ai domnului Manni au un interes legitim de a avea acces la informațiile referitoare la falimentul societății sale anterioare.

Ingerința în drepturile fundamentale ale domnului Manni și ale altor persoane înscrise în registru la respectarea vieții private și la 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 statuat că drepturile la protecția datelor și la respectarea vieții private nu prevalau asupra interesului terților de a avea acces la informațiile din registrul societăților comerciale referitoare la societățile pe acțiuni și la societățile cu răspundere limitată.

2

Terminologia în domeniul protecției datelor



UE	Aspecte vizate	CoE
Date cu caracter personal		
Regulamentul general privind protecția datelor, articolul 4 punctul 1 Regulamentul general privind protecția datelor, articolul 4 punctul 5 și articolul 5 alineatul (1) litera (e) Regulamentul general privind protecția datelor, articolul 9 Hotărârea CJUE [MC] în cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*, 2010 Hotărârea CJUE [MC] în cauza C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, 2008 Hotărârea CJUE în cauza C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 Hotărârea CJUE în cauza C-582/14, *Patrick Breyer/Bundesrepublik Deutschland*, 2016 Hotărârea CJUE în cauzele conexate C-141/12 și C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel* și *Minister voor Immigratie, Integratie en Asiel/M și S*, 2014	**Definiția juridică a protecției datelor**	Convenția 108 modernizată, articolul 2 litera (a) Hotărârea CEDO în cauza *Bernh Larsen Holding AS și alții/Norvegia*, nr. 24117/08, 2013 Hotărârea CEDO în cauza *Uzun/Germania*, nr. 35623/05, 2010 Hotărârea CEDO [MC] în cauza *Amann/Elveția*, nr. 27798/95, 2000

UE	Aspecte vizate	CoE
Hotărârea CJUE în cauza C-101/01, *Proces penal împotriva lui Bodil Lindqvist*, 2003	**Categorii speciale de date cu caracter personal (date sensibile)**	Convenția 108 modernizată, articolul 6 alineatul (1)
Hotărârea CJUE în cauza C-434/16, *Peter Nowak/Data Protection Commissioner*, 2017	**Date cu caracter personal anonimizate și pseudonimizate**	Convenția 108 modernizată, articolul 5 alineatul (4) litera (e) Raportul explicativ privind Convenția 108 modernizată, punctul 50
Prelucrarea datelor		
Regulamentul general privind protecția datelor, articolul 4 punctul 2 Hotărârea CJUE în cauza C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 2014 Hotărârea CJUE în cauza C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/ Salvatore Manni*, 2017 Hotărârea CJUE în cauza C-101/01, *Proces penal împotriva lui Bodil Lindqvist*, 2003 Hotărârea CJUE [MC] în cauza C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 2014	**Definiții**	Convenția 108 modernizată, articolul 2 literele (b) și (c)
Utilizatorii de date		
Regulamentul general privind protecția datelor, articolul 4 punctul 7 Hotărârea CJUE în cauza C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 2014 Hotărârea CJUE [MC] în cauza C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 2014	**Operator**	Convenția 108 modernizată, articolul 2 litera (d) Recomandare privind crearea de profiluri, articolul 1 litera (g)*
Regulamentul general privind protecția datelor, articolul 4 punctul 8	**Persoana împuternicită de operator**	Convenția 108 modernizată, articolul 2 litera (f) Recomandare privind crearea de profiluri, articolul 1 litera (h)

UE	Aspecte vizate	CoE
Regulamentul general privind protecția datelor, articolul 4 punctul 9	**Destinatar**	Convenția 108 modernizată, articolul 2 litera (e)
Regulamentul general privind protecția datelor, articolul 4 punctul 10	**Parte terță**	
Consimțământ		
Regulamentul general privind protecția datelor, articolul 4 punctul 11 și articolul 7 Hotărârea CJUE în cauza C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 2011 Hotărârea CJUE în cauza C-536/15, *Tele2 (Netherlands) BV și alții/ Autoriteit Consument en Markt (ACM)*, 2017	**Definiție și cerințe privind consimțământul valabil**	Convenția 108 modernizată, articolul 5 alineatul (2) Recomandare privind datele medicale, articolul 6, și diferite recomandări ulterioare Hotărârea CEDO în cauza *Elberte/Letonia*, nr. 61243/08, 2015

*Observație: * Recomandarea Rec(2010)13 din 23 noiembrie 2010 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal în contextul creării de profiluri (Recomandarea privind crearea de profiluri).*

2.1. Date cu caracter personal

Principalele elemente

- Datele reprezintă date cu caracter personal dacă se referă la o persoană identificată sau care poate fi identificată, denumită „persoana vizată".
- Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective.
- Prin autentificare se înțelege dovedirea faptului că o anumită persoană are o anumită identitate și/sau este autorizată să desfășoare anumite activități.
- Există categorii speciale de date, așa-numitele date sensibile, prevăzute în Convenția 108 modernizată și în legislația UE privind protecția datelor, care necesită protecție sporită și, prin urmare, sunt supuse unui regim juridic special.
- Datele sunt anonimizate dacă nu se mai referă la o persoană identificată sau identificabilă.

- Pseudonimizarea este o măsură în urma căreia datele cu caracter personal nu pot fi atribuite persoanei vizate fără informații suplimentare, care sunt păstrate separat. „Cheia" care permite re-identificarea persoanelor vizate trebuie păstrată separat, în condiții de siguranță. Datele care au fost supuse unui proces de pseudonimizare rămân date cu caracter personal. Conceptul de „date pseudonimizate" nu există în legislația UE.
- Principiile și normele de protecție a datelor nu se aplică informațiilor anonimizate. Ele se aplică, în schimb, datelor pseudonimizate.

2.1.1. Aspectele principale ale conceptului de date cu caracter personal

Atât **în dreptul UE**, cât și **în legislația CoE**, „datele cu caracter personal" sunt definite ca informații referitoare la o persoană fizică identificată sau identificabilă[136]. Este vorba despre informații privind o persoană a cărei identitate este fie clară în mod evident, fie poate fi stabilită cu ajutorul unor informații suplimentare. Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective[137].

În cazul în care se prelucrează date despre o astfel de persoană, această persoană este denumită „persoană vizată".

Persoana vizată

În dreptul UE, persoanele fizice sunt singurii beneficiari ai normelor de protecție a datelor[138] și numai persoanele în viață sunt protejate în temeiul legislației UE privind protecția datelor[139]. Regulamentul general privind protecția datelor (RGPD) definește datele cu caracter personal ca fiind orice informație privind o persoană fizică identificată sau identificabilă.

136 Regulamentul general privind protecția datelor, articolul 4 punctul 1; Convenția 108 modernizată, articolul 2 litera (a).

137 Regulamentul general privind protecția datelor, considerentul 26.

138 *Ibidem*, articolul 1.

139 *Ibidem*, considerentul 27. Vezi, de asemenea, Avizul 4/2007 al Grupului de lucru „Articolul 29" privind conceptul de date cu caracter personal, WP 136, 20 iunie 2007, p. 22.

Legislația CoE, în special Convenția 108 modernizată, reglementează, de asemenea, protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Și în acest caz, datele cu caracter personal înseamnă orice informație referitoare la o persoană identificată sau identificabilă. Această „persoană fizică" sau „individ", astfel cum este numită în RGPD, respectiv în Convenția 108 modernizată, este cunoscută în legislația privind protecția datelor drept „persoana vizată".

Și persoanele juridice beneficiază de o anumită protecție. Există o jurisprudență a CEDO care se pronunță asupra cererilor entităților juridice care invocă încălcarea dreptului la protecție împotriva utilizării datelor lor, în temeiul articolului 8 din Convenția europeană a drepturilor omului. Articolul 8 din Convenția europeană a drepturilor omului vizează atât dreptul la respectarea vieții private și de familie, cât și dreptul la respectarea domiciliului și a corespondenței. Prin urmare, în ceea ce privește persoanele juridice, Curtea poate examina cauze având ca obiect acest din urmă aspect, în locul celui legat de respectarea vieții private.

Exemplu: Cauza *Bernh Larsen Holding AS și alții/Norvegia*[140] se referă la plângerea formulată de trei societăți norvegiene cu privire la decizia unei autorități fiscale prin care li se impunea să pună la dispoziția auditorilor fiscali o copie a tuturor datelor aflate pe un server informatic pe care cele trei îl utilizau în comun.

CEDO a considerat că obligația impusă societăților reclamante constituie o atingere adusă drepturilor lor la respectarea „domiciliului" și a „corespondenței" în sensul articolului 8 din Convenția europeană a drepturilor omului. Cu toate acestea, Curtea a constatat că autoritățile fiscale posedă garanții eficiente și adecvate împotriva abuzurilor: societățile reclamante au fost anunțate cu suficient timp în avans, au fost prezente și în măsură să facă observații în timpul intervenției la fața locului, iar materialul urma a fi distrus după finalizarea auditului fiscal. În aceste condiții, s-a găsit un echilibru echitabil între dreptul societăților reclamante la respectarea „domiciliului" și a „corespondenței" și interesul acestora de protejare a vieții private a persoanelor care lucrează pentru ele, pe de o parte, și interesul public de asigurare a unei inspecții eficiente în scopuri de evaluare fiscală, pe de altă parte. Prin urmare, Curtea a concluzionat că nu s-a încălcat articolul 8.

140 Hotărârea CEDO din 14 martie 2013 în cauza *Bernh Larsen Holding AS și alții/Norvegia*, nr. 24117/08. Vezi totuși și Hotărârea CEDO din 1 iulie 2008 în cauza *Liberty și alții/Regatul Unit*, nr. 58243/00.

Conform Convenției 108 modernizate, protecția datelor vizează, în principal, protecția persoanelor fizice; cu toate acestea, părțile contractante pot extinde, în dreptul intern, protecția datelor la persoanele juridice, cum ar fi societățile comerciale și asociațiile. Raportul explicativ privind Convenția 108 modernizată precizează că dreptul național poate proteja interesele legitime ale persoanelor juridice prin extinderea domeniului de aplicare al convenției la acești actori[141]. **Legislația UE privind protecția datelor** nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice[142]. Cu toate acestea, Directiva asupra confidențialității și comunicațiilor electronice protejează confidențialitatea comunicărilor și interesele legitime ale persoanelor juridice în ceea ce privește capacitățile în creștere de stocare automată și de prelucrare a datelor referitoare la abonați și utilizatori[143]. În mod similar, proiectul de regulament privind confidențialitatea comunicațiilor electronice extinde protecția la persoanele juridice.

Exemplu: În cauzele conexate *Volker und Markus Schecke și Hartmut Eifert/Land Hessen*[144], făcând referire la publicarea datelor cu caracter personal ale beneficiarilor de ajutoare pentru agricultură, CJUE a considerat că „persoanele juridice nu se pot prevala de protecția articolelor 7 și 8 din [C]artă față de o astfel de identificare decât în măsura în care denumirea persoanei juridice identifică una sau mai multe persoane fizice. [...] [R]espectarea dreptului la viață privată în raport cu prelucrarea datelor cu caracter personal, recunoscută prin articolele 7 și 8 din [C]artă, se raportează la orice informație privind o persoană fizică identificată sau identificabilă [...]”[145].

Ponderând interesul UE de a asigura transparența în alocarea ajutorului, pe de o parte, cu drepturile fundamentale la respectarea vieții private și la protecția datelor ale persoanelor care au beneficiat de ajutor, pe de altă parte, CJUE a considerat că intervenția asupra acestor drepturi fundamentale a fost disproporționată. Curtea a considerat că obiectivul privind transparența putea să fie atins în mod eficace prin măsuri mai puțin invazive pentru drepturile

141 Raportul explicativ privind Convenția 108 modernizată, punctul 30.

142 Regulamentul general privind protecția datelor, considerentul 14.

143 Directiva asupra confidențialității și comunicațiilor electronice, considerentul 7 și articolul 1 alineatul (2).

144 Hotărârea CJUE [MC] din 9 noiembrie 2010 în cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*, punctul 53.

145 *Ibidem*, punctele 52-53.

persoanelor în cauză. Cu toate acestea, examinând proporționalitatea publicării informațiilor referitoare la persoanele juridice care au beneficiat de ajutor, CJUE a ajuns la o concluzie diferită, statuând că această publicare nu a depășit limitele principiului proporționalității. Curtea a stabilit că „gravitatea atingerii aduse dreptului la protecția datelor cu caracter personal se prezintă în mod diferit pentru persoanele juridice și pentru persoanele fizice”[146]. Persoanele juridice erau supuse unei obligații sporite de publicare a datelor care le privesc. CJUE a considerat că obligația autorităților naționale de a examina, înainte de publicarea datelor în cauză, pentru fiecare persoană juridică beneficiară, dacă datele acesteia identifică persoane fizice asociate ar impune acestor autorități o sarcină administrativă disproporționată. Prin urmare, legislația care impunea o publicare generalizată a datelor referitoare la persoane juridice a asigurat un just echilibru între interesele concurente din speță.

Natura datelor

Orice tip de informații pot fi date cu caracter personal în măsura în care acestea se referă la o persoană identificată sau identificabilă.

Exemplu: Evaluarea performanței profesionale a unui angajat realizată de un supervizor, stocată în dosarul personal al angajatului, reprezintă date cu caracter personal ale angajatului. Acest lucru este valabil chiar dacă evaluarea în cauză reflectă, integral sau parțial, numai opinia personală a supervizorului, cum ar fi „angajatul nu este dedicat muncii sale”, iar nu fapte concrete, cum ar fi „angajatul a lipsit de la locul de muncă cinci săptămâni în ultimele șase luni”.

Datele cu caracter personal includ informațiile referitoare la viața privată a unei persoane, unde se încadrează și activitățile profesionale, precum și informațiile referitoare la viața publică a acesteia.

În cauza *Amann*[147], CEDO a interpretat că noțiunea „date cu caracter personal” nu se limitează la aspecte ale sferei private a unei persoane. Acest înțeles al termenului „date cu caracter personal” este relevant și pentru RGPD.

146 *Ibidem*, punctul 87.

147 Vezi Hotărârea CEDO din 16 februarie 2000 în cauza *Amann/Elveția*, nr. 27798/95, punctul 65.

Exemplu: În cauza *Volker und Markus Schecke și Hartmut Eifert/Land Hessen*[148], CJUE a stabilit că „[î]n această privință, este lipsit de importanță faptul că datele publicate au legătură cu activitățile profesionale [...]. Curtea Europeană a Drepturilor Omului a hotărât în această privință, referitor la interpretarea articolului 8 din [Convenția europeană a drepturilor omului], că termenii «viață privată» nu trebuie interpretați în mod restrictiv și că «niciun motiv de principiu nu permite excluderea activităților profesionale [...] din noțiunea «viață privată»".

Exemplu: În cauzele conexate *YS/Minister voor Immigratie, Integratie en Asiel* și *Minister voor Immigratie, Integratie en Asiel/M și S*[149], CJUE a stabilit că analiza juridică conținută într-un proiect de decizie a serviciului pentru imigrație și naturalizări cu privire la solicitările de permise de ședere nu constituie în sine date cu caracter personal, chiar dacă poate include astfel de date.

Jurisprudența CEDO cu privire la articolul 8 din Convenția europeană a drepturilor omului confirmă că separarea completă a aspectelor legate de viața privată și cea profesională poate fi dificilă[150].

Exemplu: În cauza *Bărbulescu/Romania*[151], reclamantul fusese concediat pentru că a folosit internetul angajatorului său în timpul orelor de lucru, încălcând reglementările interne. Angajatorul său i-a monitorizat comunicările, iar înregistrările acestora, care puneau în evidență mesaje cu caracter pur personal, au fost prezentate în cadrul procedurii în fața instanței naționale. Constatând că articolul 8 este aplicabil în speță, CEDO a lăsat deschisă întrebarea dacă reglementările restrictive ale angajatorului permiteau ca reclamantul să aibă așteptări rezonabile în ceea ce privește viața privată, dar în orice caz a considerat că instrucțiunile unui angajator nu puteau reduce la zero viața socială privată la locul de muncă. Cu privire la fond, statele contractante trebuiau să beneficieze de o marjă largă de apreciere

148 Hotărârea CJUE [MC] din 9 noiembrie 2010 în cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*, punctul 59.

149 Hotărârea CJUE din 17 iulie 2014 în cauzele conexate C-141/12 și C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel* și *Minister voor Immigratie, Integratie en Asiel/M și S*, punctul 39.

150 Vezi, de exemplu, Hotărârea CEDO [MC] din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95, punctul 43; Hotărârea CEDO din 16 decembrie 1992 în cauza *Niemitz/Germania*, nr. 13710/88, punctul 29.

151 Hotărârea CEDO [MC] din 5 septembrie 2017 în cauza *Bărbulescu/România*, nr. 61496/08, punctul 121.

pentru a evalua necesitatea stabilirii unui cadru juridic care să reglementeze condițiile în care un angajator poate reglementa comunicările de altă natură decât profesională ale angajaților săi – în format electronic sau de alt tip – la locul de muncă. Cu toate acestea, autoritățile naționale trebuiau să se asigure că introducerea de către angajator a unor măsuri de monitorizare a corespondenței și a altor comunicări, indiferent de amploarea și de durata acestor măsuri, este însoțită de garanții adecvate și suficiente împotriva abuzurilor. Proporționalitatea și garanțiile procedurale împotriva arbitrarului măsurilor sunt esențiale, iar CEDO a identificat o serie de factori relevanți în speță. Acești factori includ, de exemplu, amploarea monitorizării de către angajator a angajaților și gradul de intruziune în viața privată a acestora din urmă, consecințele pentru angajați și aspectul dacă s-au oferit garanții adecvate. În plus, autoritățile naționale trebuiau să se asigure că un angajat ale cărui comunicări fuseseră monitorizate avea acces la o cale de atac în fața unei instanțe judecătorești competente să determine, cel puțin în fond, cum au fost respectate criteriile stabilite și dacă măsurile contestate erau legale. CEDO a constatat în această speță că s-a încălcat articolul 8, deoarece autoritățile naționale nu au acordat o protecție adecvată dreptului reclamantului la respectarea vieții private și a corespondenței și, prin urmare, nu au reușit să asigure un echilibru just între interesele concurente în cauză.

În temeiul dreptului UE, precum și **în temeiul legislației CoE**, informațiile conțin date cu privire la o persoană dacă:

- o persoană fizică este identificată sau identificabilă prin aceste informații; sau
- în cazul în care o persoană fizică, deși neidentificată, poate fi individualizată prin aceste informații într-un mod care face posibilă descoperirea persoanei vizate prin efectuarea de cercetări ulterioare.

Ambele tipuri de informații sunt protejate în același mod, în conformitate cu legislația europeană privind protecția datelor. Identificarea directă sau indirectă a persoanelor necesită o evaluare continuă, „ținându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât și de dezvoltarea tehnologică”[152]. CEDO a statuat în mod repetat că noțiunea „date cu caracter personal” în conformitate cu Convenția

152 Regulamentul general privind protecția datelor, considerentul 26.

europeană a drepturilor omului este aceeași cu cea din Convenția 108, în special în ceea ce privește condiția de referire la persoane identificate sau identificabile[153].

RGPD prevede că o persoană fizică este identificabilă dacă „poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale”[154]. Prin urmare, identificarea presupune elemente care descriu o persoană într-un mod în care aceasta se poate distinge de toate celelalte persoane și poate fi recunoscută ca persoană fizică. Numele unei persoane este un prim exemplu de element de descriere și poate identifica în mod direct o persoană. În anumite cazuri, alte atribute pot avea un efect similar ca cel al numelui, făcând persoana identificabilă în mod indirect. Un număr de telefon, un număr de asigurare socială și un număr de înmatriculare al vehiculului sunt toate exemple de informații care pot face o persoană identificabilă. De asemenea, se pot utiliza anumite elemente – cum ar fi fișiere de computer, module cookie și instrumente de supraveghere a traficului web – pentru a individualiza persoanele prin identificarea comportamentului și a obiceiurilor lor. Astfel cum se explică într-un aviz al Grupului de lucru „Articolul 29”, „[c]hiar și fără a cunoaște numele și adresa unei persoane, este posibilă clasificarea acesteia după criterii socioeconomice, psihologice, filosofice sau de altă natură și i se pot atribui anumite decizii din moment ce punctul de contact al persoanei în cauză (computerul) nu îi mai solicită să își divulge identitatea în sensul strict”[155]. Definiția datelor cu caracter personal atât în legislația CoE, cât și a UE este suficient de largă pentru a acoperi toate posibilitățile de identificare (și, prin urmare, toate gradele de identificabilitate).

Exemplu: În cauza *Promusicae/Telefónica de España*[156], CJUE a arătat că „nu se contestă faptul că respectiva comunicare a numelui și a adreselor anumitor utilizatori ai [unei anumite platforme de partajare de fișiere prin internet], solicitată de Promusicae, presupune punerea la dispoziție a unor date cu caracter personal, mai precis a unor informații privind persoane fizice identificate sau identificabile, în conformitate cu definiția cuprinsă la articolul 2

153 Vezi Hotărârea CEDO [MC] din 16 februarie 2000 în cauza *Amann/Elveția*, nr. 27798/95, punctul 65.

154 Regulamentul general privind protecția datelor, articolul 4 punctul 1.

155 Avizul 4/2007 al Grupului de lucru „Articolul 29” privind conceptul de date cu caracter personal, WP 136, 20 iunie 2007, p. 15.

156 Hotărârea CJUE [MC] din 29 ianuarie 2008 în cauza C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, punctul 45.

litera (a) din Directiva 95/46/CE [în prezent, articolul 4 punctul 1 din RGPD] [...]. Această comunicare de informații care, în opinia Promusicae, sunt stocate de către Telefónica – fapt necontestat de către aceasta din urmă – constituie o prelucrare de date cu caracter personal [...]"[157].

Exemplu: Cauza *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] a vizat refuzul furnizorului de servicii internet Scarlet de a instala un sistem de filtrare a comunicațiilor electronice care utilizează software de partajare a fișierelor pentru a împiedica partajarea de fișiere care încalcă drepturile de autor protejate de SABAM, o societate de administrare care reprezintă autori, compozitori și editori. CJUE a considerat că adresele IP ale utilizatorilor „[reprezintă] date protejate cu caracter personal, deoarece permit identificarea precisă a utilizatorilor respectivi".

Deoarece multe dintre nume nu sunt unice, stabilirea identității unei persoane poate necesita atribute suplimentare pentru a garanta că o persoană nu este confundată cu o alta. Uneori, atributele directe și indirecte pot fi combinate pentru a identifica persoana la care se referă informațiile. Data și locul nașterii sunt deseori utilizate. În plus, în unele țări au fost introduse numere personalizate pentru o mai bună diferențiere a cetățenilor. Datele fiscale transferate[159], datele referitoare la un solicitant de permis de ședere conținute într-un document administrativ[160] și documentele referitoare la relații bancare și fiduciare[161] pot fi date cu caracter personal. Datele biometrice, cum ar fi amprentele, fotografiile digitale sau înregistrarea unei imagini a irisului, datele de localizare și atributele online devin din ce în ce mai importante pentru identificarea persoanelor în era tehnologică.

Cu toate acestea, în sensul aplicabilității legislației europene privind protecția datelor, nu este necesară o identificare efectivă a persoanelor vizate; este suficient ca persoana în cauză să fie identificabilă. O persoană este considerată identificabilă dacă există suficiente elemente disponibile prin care persoana poate fi identificată direct

157 Directiva 95/46/CE (abrogată), articolul 2 litera (b), acum Regulamentul general privind protecția datelor, articolul 4 punctul 2.

158 Hotărârea CJUE din 24 noiembrie 2011 în cauza C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, punctul 51.

159 Hotărârea CJUE din 1 octombrie 2015 în cauza C-201/14, *Smaranda Bara și alții/Casa Națională de Asigurări de Sănătate și alții*.

160 Hotărârea CJUE din 17 iulie 2014 în cauzele conexate C-141/12 și C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel* și *Minister voor Immigratie, Integratie en Asiel/M și S*.

161 Hotărârea CEDO din 7 iulie 2015 în cauza *M.N. și alții/San Marino*, nr. 28005/12.

sau indirect[162]. Potrivit considerentului 26 din RGPD, criteriul de referință constă în posibilitatea ca utilizatorii previzibili ai informațiilor să dispună de mijloace rezonabile de identificare și să administreze aceste mijloace; aceasta include și informații deținute de destinatarii terți (vezi secțiunea 2.3.2).

Exemplu: O autoritate locală decide să colecteze date despre mașinile care rulează cu viteză peste limita legală. Aceasta fotografiază mașinile, înregistrând automat ora și locul, pentru a transmite datele autorității competente astfel încât să poată aplica amenzi celor care depășesc limita de viteză. O persoană vizată depune o plângere, invocând faptul că autoritatea locală nu are niciun temei juridic, în conformitate cu legislația privind protecția datelor, pentru colectarea acestor date. Autoritatea locală își menține poziția conform căreia nu colectează date cu caracter personal. Aceasta susține că numerele de înmatriculare sunt anonime. Autoritatea locală nu are autoritatea juridică de a accesa registrul general al vehiculelor pentru a descoperi identitatea proprietarului sau a conducătorului mașinii.

Acest raționament nu este în conformitate cu considerentul 26 din RGPD. Având în vedere că scopul colectării datelor este în mod clar acela de a identifica și amenda vitezomanii, este previzibil faptul că se va încerca identificarea. Cu toate că autoritățile locale nu dispun de mijloace directe de identificare, acestea vor transmite datele autorității competente, poliția, care posedă astfel de mijloace. De asemenea, considerentul 26 include în mod explicit un scenariu în care este prevăzută posibilitatea ca destinatarii ulteriori ai datelor, alții decât utilizatorii imediați, să încerce să identifice persoana fizică. Din perspectiva considerentului 26, acțiunea autorității locale echivalează cu colectarea de date privind persoane identificabile și, prin urmare, necesită un temei juridic în conformitate cu legislația privind protecția datelor.

Pentru „a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace pentru identificarea persoanei fizice, ar trebui luați în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât și de dezvoltarea tehnologică”[163].

162 Regulamentul general privind protecția datelor, articolul 4 punctul 1.

163 *Ibidem*, considerentul 26.

Exemplu: În cauza *Breyer/Bundesrepublik Deutschland*[164], CJUE a luat în considerare noțiunea de identificabilitate indirectă a persoanelor vizate. Cauza a vizat adrese IP dinamice, care se modifică de fiecare dată când se stabilește o nouă conexiune la internet. Site-urile instituțiilor germane federale au înregistrat și stocat adrese IP dinamice pentru a preveni atacurile cibernetice și pentru a iniția proceduri penale acolo unde este necesar. Doar furnizorul de servicii internet pe care îl utiliza domnul Breyer deținea informațiile suplimentare necesare pentru a-l identifica.

CJUE a considerat că o adresă IP dinamică pe care un furnizor de servicii media online o înregistrează atunci când o persoană accesează un site pe care furnizorul l-a pus la dispoziția publicului constituie date cu caracter personal în măsura în care numai o parte terță – furnizorul de servicii internet în acest caz – deține datele suplimentare necesare identificării persoanei[165]. Curtea a afirmat că „nu este necesar ca toate informațiile care permit identificarea persoanei vizate să se afle în posesia unei singure persoane" pentru ca informațiile să constituie date cu caracter personal. Utilizatorii unei adrese IP dinamice înregistrate de un furnizor de servicii internet pot fi identificați în anumite situații, de exemplu în cadrul procedurilor penale inițiate în cazul unor atacuri cibernetice, cu ajutorul altor persoane[166]. Potrivit CJUE, atunci când furnizorul „dispune de mijloace legale care îi permit să identifice persoana vizată cu ajutorul informațiilor suplimentare de care dispune furnizorul de acces la internet al acestei persoane", acestea reprezintă „un mijloc care poate fi utilizat în mod rezonabil pentru a identifica persoana vizată". Prin urmare, aceste date sunt considerate date cu caracter personal.

Identificabilitatea este înțeleasă în mod similar **în cadrul legislației CoE**. Raportul explicativ privind Convenția 108 modernizată include o descriere similară: noțiunea „identificabil" nu se referă numai la identitatea civilă sau juridică a persoanei ca atare, ci și la elementele care permit „individualizarea" sau diferențierea unei persoane în raport cu altele și, prin urmare, posibilitatea aplicării unui tratament diferit. Această „individualizare" se poate realiza, de exemplu, prin referirea la persoana în

164 Hotărârea CJUE din 19 octombrie 2016 în cauza C-582/14, *Patrick Breyer/Bundesrepublik Deutschland*, punctul 47-48.

165 Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (abrogată), articolul 2 litera (a).

166 Hotărârea CJUE din 24 noiembrie 2011 în cauza C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, punctele 47-48.

cauză în mod specific sau la un dispozitiv sau o combinație de dispozitive (computer, telefon mobil, cameră web, dispozitive pentru jocuri etc.) asociate cu un număr de identificare, un pseudonim, date biometrice sau genetice, date de localizare, o adresă IP sau un alt identificator[167]. O persoană nu este considerată „identificabilă" dacă identificarea acesteia necesită timp, efort sau resurse nerezonabile. Acest lucru este valabil, de exemplu, atunci când identificarea persoanei vizate ar necesita operațiuni excesiv de complexe, lungi și costisitoare. Eventualul caracter nerezonabil al duratei, eforturilor sau resurselor trebuie să fie evaluat de la caz la caz, luând în considerare factori precum scopul prelucrării, costul și beneficiile identificării, tipul de operator și tehnologia utilizată[168].

În ceea ce privește forma în care sunt stocate sau utilizate datele cu caracter personal, este important să se precizeze că aceasta nu este relevantă pentru aplicabilitatea legislației privind protecția datelor. Comunicările scrise sau verbale pot conține date cu caracter personal, precum și imagini[169], inclusiv înregistrări video prin TVCI[170] sau sunete[171]. Informațiile înregistrate electronic și pe suport de hârtie pot fi, de asemenea, date cu caracter personal. Chiar și probele celulare de țesut uman, în care este înregistrat ADN-ul unei persoane, pot fi surse din care se pot extrage date biometrice[172], în măsura în care datele se referă la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, oferă informații unice privind fiziologia sau sănătatea persoanei respective și rezultă în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză[173].

167 Raportul explicativ privind Convenția 108 modernizată, punctul 18.

168 *Ibidem*, punctul 17.

169 Hotărârea CEDO din 24 iunie 2004 în cauza *Von Hannover/Germania*, nr. 59320/00; Hotărârea CEDO din 11 ianuarie 2005 în cauza *Sciacca/Italia*, nr. 50774/99; Hotărârea CJUE din 11 decembrie 2014 în cauza C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*.

170 Hotărârea CEDO din 28 ianuarie 2003 în cauza *Peck/Regatul Unit*, nr. 44647/98; Hotărârea CEDO din 5 octombrie 2010 în cauza *Köpke/Germania* (dec.), nr. 420/07; AEPD (2010), *The EDPS video-surveillance guidelines* (*Orientările AEPD privind supravegherea video*), 17 martie 2010.

171 Hotărârea CEDO din 25 septembrie 2001 în cauza *P.G. și J.H./Regatul Unit*, nr. 44787/98, punctele 59-60; Hotărârea CEDO din 20 decembrie 2005 în cauza *Wisse/Franța*, nr. 71611/01 (versiunea în limba franceză).

172 Vezi Avizul 4/2007 al Grupului de lucru „Articolul 29" privind conceptul de date cu caracter personal, WP136, 20 iunie 2007, p. 9; *Recomandarea Rec(2006)4 a Comitetului de Miniștri al Consiliului Europei către statele membre privind cercetarea în domeniul materialelor biologice de origine umană*, 15 martie 2006.

173 Regulamentul general privind protecția datelor, articolul 4 punctul 13.

Anonimizarea

Potrivit principiului limitărilor legate de stocare inclus atât în RGPD, cât și în Convenția 108 modernizată (și discutat în detaliu în capitolul 3), datele trebuie păstrate „într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele”[174]. În consecință, datele trebuie să fie șterse sau anonimizate în cazul în care un operator dorește să le stocheze după ce nu mai sunt necesare și nu mai servesc scopului inițial.

Procesul de anonimizare a datelor desemnează eliminarea tuturor elementelor de identificare dintr-un set de date cu caracter personal, astfel încât persoana vizată să nu mai fie identificabilă[175]. În Avizul 05/2014, Grupul de lucru „Articolul 29” analizează eficacitatea și limitele diferitelor tehnici de anonimizare[176]. Acesta recunoaște valoarea potențială a tehnicilor respective, dar subliniază că anumite tehnici nu funcționează neapărat în toate cazurile. Pentru a găsi soluția optimă într-o situație dată, procesul adecvat de anonimizare trebuie stabilit de la caz la caz. Indiferent de tehnica utilizată, identificarea trebuie să fie împiedicată în mod ireversibil. Aceasta înseamnă că, pentru ca datele să fie anonimizate, în informații nu poate fi lăsat niciun element care, prin exercitarea unui efort rezonabil, ar putea servi la reidentificarea persoanei (persoanelor) vizate[177]. Riscul de reidentificare poate fi evaluat luând în considerare „timpul, efortul sau resursele necesare având în vedere natura datelor, contextul utilizării acestora, tehnologiile de reidentificare disponibile și costurile aferente”[178].

Dacă datele au fost anonimizate cu succes, acestea nu mai sunt date cu caracter personal, iar legislația privind protecția datelor nu mai este aplicabilă în cazul lor.

RGPD prevede că persoana sau organizația care administrează prelucrarea datelor cu caracter personal nu are obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată în scopul unic al respectării

174 *Ibidem*, articolul 5 alineatul (1) litera (e); Convenția 108 modernizată, articolul 5 alineatul (4) litera (e).

175 Regulamentul general privind protecția datelor, considerentul 26.

176 Avizul 5/2014 al Grupului de lucru „Articolul 29” privind tehnicile de anonimizare, WP216, 10 aprilie 2014.

177 Regulamentul general privind protecția datelor, considerentul 26.

178 Consiliul Europei, Comitetul Convenției 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* (*Orientări privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive*), 23 ianuarie 2017, punctul 6.2.

regulamentului. Există totuși o excepție semnificativă aferentă acestei norme: ori de câte ori persoana vizată, în scopul exercitării dreptului de acces, rectificare, ștergere, restricționare a prelucrării și a portabilității datelor, oferă operatorului informații suplimentare care permit identificarea sa, datele care au fost anonimizate anterior redevin date cu caracter personal[179].

Pseudonimizarea

Informațiile cu caracter personal conțin atribute, cum ar fi numele, data nașterii, sexul, adresa sau alte elemente care ar putea duce la identificare. Procesul de pseudonimizare a datelor cu caracter personal presupune înlocuirea acestor atribute cu un pseudonim.

Legislația UE definește „pseudonimizarea" ca fiind „prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile"[180]. Spre deosebire de datele anonimizate, datele pseudonimizate rămân în continuare date cu caracter personal și, prin urmare, fac obiectul legislației privind protecția datelor. Deși pseudonimizarea poate reduce riscurile de securitate care afectează persoanele vizate, aceasta nu este exclusă din domeniul de aplicare al RGPD.

RGPD recunoaște diferite utilizări ale pseudonimizării drept măsuri tehnice adecvate pentru îmbunătățirea protecției datelor, pseudonimizarea fiind menționată în mod specific în relație cu proiectarea și securitatea prelucrării datelor pe care le asigură[181]. Aceasta constituie, de asemenea, o garanție adecvată care poate fi utilizată pentru prelucrarea datelor cu caracter personal în alte scopuri decât pentru care au fost colectate inițial[182].

Pseudonimizarea nu este menționată în mod explicit în cadrul definițiilor juridice ale Convenției 108 modernizate a **CoE**. Cu toate acestea, Raportul explicativ privind Convenția 108 modernizată arată în mod clar că „utilizarea unui pseudonim sau

179 Regulamentul general privind protecția datelor, articolul 11.

180 *Ibidem*, articolul 4 punctul 5.

181 *Ibidem*, articolul 25 alineatul (1).

182 *Ibidem*, articolul 6 alineatul (4).

a oricărui identificator digital/a oricărei identități digitale nu conduce la anonimizarea datelor deoarece persoana vizată poate fi încă identificabilă sau individualizată”[183]. O modalitate de pseudonimizare a datelor este criptarea acestora. Odată ce datele au fost pseudonimizate, legătura cu o identitate există sub forma pseudonimului plus o cheie de decriptare. Fără o astfel de cheie, este dificil să se identifice datele pseudonimizate. Cu toate acestea, pentru persoanele care au dreptul să utilizeze cheia de decriptare, reidentificarea este facilă. Trebuie create garanții speciale împotriva utilizării cheilor de criptare de către persoane neautorizate. Prin urmare, „[d]atele pseudonimizate trebuie [...] să fie considerate date cu caracter personal [...]” reglementate de Convenția 108 modernizată[184].

Autentificarea

Aceasta este o procedură prin care o persoană poate dovedi că are o anumită identitate și/sau este autorizată să întreprindă anumite acțiuni, cum ar fi să pătrundă într-o zonă de securitate sau să retragă bani dintr-un cont bancar. Autentificarea se poate realiza prin compararea datelor biometrice, cum ar fi o fotografie sau amprenta digitală într-un pașaport, cu datele cu care persoana se identifică, de exemplu, la controlul imigrației[185], prin solicitarea de informații care pot fi cunoscute numai de către persoana având o anumită identitate sau autorizare, cum ar fi un număr personal de identificare (PIN) sau o parolă sau prin solicitarea prezentării unui anumit token, care ar trebui să aparțină exclusiv persoanei cu o anumită identitate sau autorizare, cum ar fi un card inteligent sau cheia unui seif bancar. Pe lângă parole sau carduri inteligente, semnăturile electronice, utilizate uneori împreună cu PIN-ul, sunt un instrument prin care o persoană se poate identifica și autentifica foarte eficient în cadrul comunicațiilor electronice.

2.1.2. Categorii speciale de date cu caracter personal

În temeiul dreptului UE, precum și **în temeiul legislației CoE**, există categorii speciale de date cu caracter personal care, prin natura lor, pot prezenta un risc pentru persoanele vizate atunci când sunt prelucrate și, prin urmare, necesită o protecție sporită. Aceste date fac obiectul unui principiu de interdicție și există un număr limitat de circumstanțe în care o astfel de prelucrare este legitimă.

183 Raportul explicativ privind Convenția 108 modernizată, punctul 18.

184 *Ibidem*.

185 *Ibidem*, punctele 56-57.

În cadrul Convenției 108 modernizate (articolul 6) și al RGPD (articolul 9), următoarele categorii de date cu caracter personal sunt considerate date sensibile:

- date cu caracter personal referitoare la originea rasială sau etnică;
- date cu caracter personal care divulgă opinii politice, convingeri religioase sau de altă natură, inclusiv convingeri filosofice;
- date cu caracter personal care divulgă calitatea de membru al unui sindicat;
- datele genetice și datele biometrice prelucrate în scopul identificării unei persoane;
- date cu caracter personal referitoare la starea de sănătate, la viața sexuală sau la orientarea sexuală.

Exemplu: Cauza *Bodil Lindqvist*[186] a vizat referirea la diverse persoane prin menționarea numelui sau a altor atribute, cum ar fi numărul de telefon sau informații despre hobby-uri, pe o pagină web. CJUE a stabilit că „precizarea faptului că o persoană s-a rănit la picior și lucrează cu fracțiune de normă pe motive medicale constituie date cu caracter personal referitoare la starea de sănătate”[187].

Datele cu caracter personal referitoare la condamnări penale și infracțiuni

Convenția 108 modernizată include datele cu caracter personal referitoare la infracțiuni, la proceduri și condamnări penale și la măsurile de securitate conexe în lista categoriilor speciale de date cu caracter personal[188]. În cadrul RGPD, datele cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsurile de securitate conexe nu sunt menționate ca atare în lista categoriilor speciale de date, dar sunt abordate într-un articol separat. Articolul 10 din RGPD prevede că prelucrarea acestor date poate fi efectuată numai „sub controlul unei autorități de stat

186 Hotărârea CJUE din 6 noiembrie 2003 în cauza C-101/01, *Proces penal/Bodil Lindqvist*, punctul 51.

187 Directiva 95/46/CE (abrogată), articolul 8 alineatul (1), acum Regulamentul general privind protecția datelor, articolul 9 alineatul (1).

188 Convenția 108 modernizată, articolul 6 alineatul (1).

sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate". În ceea ce privește registrele cuprinzătoare care conțin informații despre condamnările penale, acestea se țin numai sub controlul autorităților de stat specifice[189]. În UE, prelucrarea datelor cu caracter personal în contextul aplicării legii este reglementată de un instrument juridic specific, Directiva (UE) 2016/680[190]. Directiva prevede norme specifice de protecție a datelor, care sunt obligatorii pentru autoritățile competente atunci când prelucrează date cu caracter personal în scopul specific al prevenirii, depistării, investigării și urmăririi penale a infracțiunilor (vezi secțiunea 8.2.1).

2.2. Prelucrarea datelor

Principalele elemente

- „Prelucrarea datelor" se referă la orice operațiune efectuată asupra datelor cu caracter personal.
- Termenul „prelucrare" include prelucrarea automată și cea neautomată.
- În temeiul dreptului UE, prin „prelucrare" se înțelege și prelucrarea manuală în sisteme de evidență structurate.
- În temeiul legislației CoE, sensul termenului „prelucrare" poate fi extins de legislația internă pentru a include prelucrarea manuală.

2.2.1. Conceptul de prelucrare a datelor

Conceptul de prelucrare a datelor cu caracter personal este cuprinzător **atât în cadrul legislației UE, cât și al legislației CoE**: „«prelucrare» [...] înseamnă orice operațiune [...] cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea,

189 Regulamentul general privind protecția datelor, articolul 10.

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

restricționarea, ștergerea sau distrugerea"[191] care se efectuează asupra datelor cu caracter personal. Convenția 108 modernizată adaugă la definiție păstrarea datelor cu caracter personal[192].

Exemplu: În cauza *František Ryneš*[193], domnul Ryneš a captat imaginea a două persoane care i-au spart ferestrele casei prin sistemul de supraveghere video TVCI pe care îl instalase pentru a-și proteja proprietatea. CJUE a stabilit că supravegherea video care implică înregistrarea și stocarea datelor cu caracter personal constituie o prelucrare automatizată a datelor care intră sub incidența legislației UE privind protecția datelor.

Exemplu: În cauza *Camera de Comercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*[194], domnul Manni a solicitat eliminarea datelor sale cu caracter personal dintr-un registru de rating al societăților comerciale care îl asocia cu lichidarea unei societăți imobiliare, având astfel un impact negativ asupra reputației sale. CJUE a considerat că „întrucât transcrie și stochează informațiile menționate în registru și le comunică, după caz, la cerere unor terți, autoritatea responsabilă cu ținerea acestui registru efectuează o «prelucrare a datelor cu caracter personal» pentru care este «responsabilă»".

Exemplu: Angajatorii colectează și prelucrează datele angajaților lor, inclusiv informațiile legate de salariile acestora. Contractele de muncă pe care le utilizează oferă temeiul juridic pentru a face acest lucru în mod legitim.

Angajatorii vor trebui să transmită autorităților fiscale datele privind salariile personalului. Această transmitere de date va constitui „prelucrare" atât în sensul acestui termen din Convenția 108 modernizată, cât și în sensul RGPD. Cu toate acestea, temeiul juridic al acestei divulgări nu se regăsește în contractele de muncă. Trebuie să existe un temei juridic suplimentar pentru operațiunile de prelucrare care au drept rezultat transmiterea datelor privind salariile de la angajator către autoritățile fiscale. Acest temei juridic este,

191 Regulamentul general privind protecția datelor, articolul 4 punctul 2. Vezi, de asemenea, Convenția 108 modernizată, articolul 2 litera (b).

192 Convenția 108 modernizată, articolul 2 litera (b).

193 Hotărârea CJUE din 11 decembrie 2014 în cauza C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, punctul 25.

194 Hotărârea CJUE din 9 martie 2017 în cauza C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, punctul 35.

de obicei, cuprins în dispozițiile legislației fiscale naționale. Fără astfel de dispoziții – și în lipsa oricărui alt motiv legitim pentru prelucrare – această transmitere a datelor cu caracter personal ar fi o prelucrare ilegitimă.

2.2.2. Prelucrarea automată a datelor

Protecția datelor în conformitate cu Convenția 108 modernizată și cu RGPD se aplică pe deplin prelucrării automate a datelor.

În temeiul **dreptului UE**, prelucrarea automată a datelor se referă la prelucrarea „datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate”[195]. Convenția 108 modernizată conține o definiție similară[196]. În sens practic, aceasta înseamnă că orice prelucrare a datelor cu caracter personal prin mijloace automatizate, de exemplu cu ajutorul unui computer, al unui dispozitiv mobil sau al unui router, este reglementată atât de normele UE, cât și de normele CoE privind protecția datelor.

Exemplu: Cauza *Bodil Lindqvist*[197] a vizat referirea la diverse persoane prin menționarea numelui sau a altor atribute, cum ar fi numărul de telefon sau informații despre hobby-uri, pe o pagină web. CJUE a constatat că „menționarea, pe o pagină web, a unor persoane și identificarea acestora după nume sau prin alte atribute, de exemplu prin furnizarea numărului de telefon al acestora sau prin furnizarea de informații referitoare la condițiile de muncă și hobby-urile persoanelor respective constituie «prelucrare de date cu caracter personal efectuată total sau parțial prin mijloace automatizate», în sensul articolului 3 alineatul (1) din Directiva 95/46/CE”[198].

Exemplu: În cauza *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[199], domnul González a solicitat eliminarea sau modificarea unui link între numele său în motorul de căutare Google și două pagini de ziar care anunță o vânzare imobiliară

195 Regulamentul general privind protecția datelor, articolul 2 alineatul (1) și articolul 4 punctul 2.

196 Convenția 108 modernizată, articolul 2 literele (b) și (c); Raportul explicativ privind Convenția 108 modernizată, punctul 21.

197 Hotărârea CJUE din 6 noiembrie 2003 în cauza C-101/01, *Proces penal/Bodil Lindqvist*, punctul 27.

198 Regulamentul general privind protecția datelor, articolul 2 alineatul (1).

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

la licitație pentru recuperarea creanțelor de asigurări sociale. CJUE a stabilit că „prin explorarea în mod automat, constant și sistematic a internetului în căutarea informațiilor publicate acolo, operatorul unui motor de căutare «colectează» astfel de date, pe care apoi le «extrage», le «înregistrează» și le «organizează» în cadrul programelor sale de indexare, le «stochează» pe serverele sale și, după caz, le «dezvăluie» și le pune la dispoziția utilizatorilor săi sub forma unor liste cu rezultatele căutărilor acestora”[200]. CJUE a ajuns la concluzia că astfel de acțiuni constituie „prelucrare”, „fiind lipsit de relevanță faptul că operatorul motorului de căutare aplică aceleași operațiuni și altor tipuri de informații și nu face distincție între acestea și datele cu caracter personal”.

2.2.3. Prelucrarea neautomată a datelor

Prelucrarea manuală a datelor necesită, de asemenea, protecția datelor.

Protecția datelor **în temeiul dreptului UE** nu se limitează în niciun caz la prelucrarea automată a datelor. În consecință, în temeiul dreptului UE, protecția datelor se aplică în cazul prelucrării datelor cu caracter personal într-un sistem de evidență manual, și anume, un dosar de hârtie structurat special[201]. Un sistem structurat de evidență este unul care clasifică un set de date cu caracter personal, făcându-le accesibile după anumite criterii. De exemplu, dacă un angajator ține un dosar de hârtie intitulat „concediile angajaților”, care conține toate detaliile referitoare la concediile luate de membrii personalului în cursul anului precedent, sortate în ordine alfabetică, dosarul va constitui un sistem de evidență manuală care face obiectul normelor UE de protecție a datelor. Motivele acestei extinderi a protecției datelor sunt următoarele:

- dosarele de hârtie pot fi structurate într-un mod care ajută la găsirea rapidă și ușoară a informațiilor;

- stocarea datelor cu caracter personal în dosare de hârtie structurate înlesnește eludarea restricțiilor prevăzute de lege pentru prelucrarea automată a datelor[202].

În temeiul **legislației CoE**, definiția prelucrării automate admite că pot fi necesare unele etape de utilizare manuală a datelor cu caracter personal între operațiunile

200 *Ibidem*, punctul 28.

201 Regulamentul general privind protecția datelor, articolul 2 alineatul (1).

202 Regulamentul general privind protecția datelor, considerentul 15.

automate[203]. Articolul 2 litera (c) din Convenția 108 modernizată prevede că „(î)n cazul în care nu se folosește prelucrarea automată, prelucrarea datelor înseamnă o operațiune sau un set de operațiuni efectuate asupra datelor cu caracter personal dintr-un set structurat de astfel de date care sunt accesibile sau care pot fi extrase în funcție de anumite criterii".

2.3. Utilizatorii datelor cu caracter personal

Principalele elemente

- Oricine stabilește mijloacele și scopul prelucrării datelor cu caracter personal ale altor persoane este un „operator" în sensul legislației privind protecția datelor; în cazul în care mai multe persoane iau această decizie împreună, acestea pot fi „operatori asociați".
- O „persoană împuternicită de operator" este o persoană fizică sau juridică a cărei sarcină este prelucrarea datelor cu caracter personal în numele operatorului.
- O persoană împuternicită de operator devine operator dacă stabilește mijloacele și scopurile prelucrării propriu-zise a datelor.
- Orice persoană căreia i se divulgă datele cu caracter personal este un „destinatar".
- „Partea terță" este o persoană fizică sau juridică, alta decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele autorizate să prelucreze datele cu caracter personal sub autoritatea directă a operatorului sau a persoanei împuternicite de operator.
- Consimțământul, ca temei juridic pentru prelucrarea datelor cu caracter personal, trebuie acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului pentru prelucrare.
- Prelucrarea categoriilor speciale de date cu caracter personal pe bază de consimțământ necesită un consimțământ explicit.

2.3.1. Operatori și persoane împuternicite de operatori

Cea mai importantă consecință a statutului de operator sau de persoană împuternicită de operator este responsabilitatea juridică pentru respectarea

203 Convenția 108 modernizată, articolul 2 literele (b) și (c).

obligațiilor în conformitate cu legislația privind protecția datelor. În sectorul privat, este vorba, de regulă, despre o persoană fizică sau juridică; în sectorul public, este în general o autoritate. Există o distincție semnificativă între un operator de date și o persoană împuternicită de operator: primul este persoana fizică sau juridică care stabilește scopurile și mijloacele de prelucrare, în timp ce aceasta din urmă este persoana fizică sau juridică care prelucrează datele în numele operatorului, urmând instrucțiuni stricte. În principiu, operatorul de date este cel care trebuie să exercite controlul asupra prelucrării și care poartă responsabilitatea pentru aceasta, inclusiv răspunderea juridică. Cu toate acestea, odată cu reformarea normelor de protecție a datelor, persoanele împuternicite de operatori au acum obligația de a respecta multe dintre cerințele aplicabile operatorilor. De exemplu, în conformitate cu RGPD, persoanele împuternicite de operatori păstrează o evidență a tuturor categoriilor de activități de prelucrare pentru a demonstra că își respectă obligațiile în temeiul regulamentului[204]. De asemenea, persoanele împuternicite de operatori trebuie să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura securitatea prelucrării[205], să desemneze un responsabil cu protecția datelor în anumite situații[206] și să notifice operatorului eventualele încălcări ale securității datelor[207].

Depinde de elementele de fapt sau de circumstanțele cazului dacă o persoană are capacitatea de a decide și de a stabili scopul și mijloacele de prelucrare. Conform definiției operatorului din RGPD, persoanele fizice, persoanele juridice sau orice alte organisme pot fi operatori. Grupul de lucru „Articolul 29" a subliniat totuși că, în interesul persoanelor fizice, pentru a asigura existența unei entități mai stabile pentru exercitarea drepturilor lor, „ar trebui să se considere, de preferință, ca operator societatea sau organismul ca atare, mai degrabă decât o anumită persoană din cadrul societății sau al organismului"[208]. De exemplu, o societate care vinde produse de îngrijire medicală practicienilor este operatorul compilării și păstrării listei de distribuție a tuturor practicienilor dintr-o anumită zonă, iar nu directorul de vânzări care utilizează și actualizează efectiv lista.

204 Regulamentul general privind protecția datelor, articolul 30 alineatul (2).

205 *Ibidem*, articolul 32.

206 *Ibidem*, articolul 37.

207 *Ibidem*, articolul 33 alineatul (2).

208 Avizul 1/2010 al Grupului de lucru „Articolul 29" privind conceptele „operator" și „persoană împuternicită de operator", WP 169, Bruxelles, 16 februarie 2010.

Exemplu: Dacă departamentul de marketing al societății Sunshine intenționează să prelucreze date pentru un studiu de piață, societatea Sunshine va fi operatorul acestei prelucrări, iar nu angajații departamentului de marketing. Departamentul de marketing nu poate fi operator, deoarece nu are identitate juridică separată.

Persoanele fizice pot fi operatori atât în conformitate cu legislația UE, cât și cu cea a CoE. Totuși, atunci când se prelucrează date despre alte persoane cu privire la o activitate pur personală sau domestică, persoanele fizice nu intră sub incidența normelor RGPD și ale Convenției 108 modernizate și nu sunt considerate operatori[209]. O persoană fizică care își gestionează corespondența, care ține un jurnal personal în care descrie întâmplări cu prieteni și colegi și dosarele medicale ale membrilor familiei poate fi scutită de aplicarea normelor de protecție a datelor, deoarece aceste activități ar putea fi pur personale sau domestice. RGPD specifică în continuare că activitățile personale sau domestice ar putea include activitățile din cadrul rețelelor sociale și activitățile online desfășurate în contextul respectivelor activități[210]. Dimpotrivă, normele de protecție a datelor se aplică pe deplin operatorilor și persoanelor împuternicite de operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activități personale sau domestice (de exemplu, platformele de socializare în rețea)[211].

Accesul cetățenilor la internet și posibilitatea utilizării platformelor de comerț electronic, a rețelelor sociale și a site-urilor de bloguri pentru a împărtăși informații personale despre ei înșiși și despre alte persoane face din ce în ce mai dificilă separarea prelucrării personale de cea care nu este personală[212]. Caracterul personal sau domestic al activităților depinde de circumstanțe[213]. Activitățile care au aspecte profesionale sau comerciale nu pot face obiectul excepției privind activitățile domestice[214]. Astfel, în cazul în care amploarea și frecvența prelucrării datelor sugerează o activitate profesională sau cu normă întreagă, persoana fizică în cauză ar putea fi

209 Regulamentul general privind protecția datelor, considerentul 18 și articolul 2 alineatul (2) litera (c); Convenția 108 modernizată, articolul 3 alineatul (2).

210 Regulamentul general privind protecția datelor, considerentul 18.

211 *Ibidem*, considerentul 18; Raportul explicativ privind Convenția 108 modernizată, punctul 29.

212 Vezi declarația Grupului de lucru „Articolul 29" privind discuțiile referitoare la pachetul de reforme privind protecția datelor, Anexa 2: Propunerile și amendamentele legate de excepția privind activitățile personale sau domestice, 27 februarie 2013.

213 Raportul explicativ privind Convenția 108 modernizată, punctul 28.

214 Vezi Regulamentul general privind protecția datelor, considerentul 18, și Raportul explicativ privind Convenția 108 modernizată, punctul 27.

considerată operator. Pe lângă caracterul profesional sau comercial al activității de prelucrare, un alt factor care trebuie luat în considerare este aspectul dacă datele cu caracter personal sunt puse la dispoziția unui număr mare de persoane care se află, în mod evident, în afara sferei private a persoanei fizice în cauză. Jurisprudența în temeiul Directivei privind protecția datelor a constatat că legislația privind protecția datelor se aplică în cazul în care o persoană fizică, în timpul utilizării internetului, publică date cu privire la alte persoane pe un site public. CJUE nu s-a pronunțat încă în legătură cu fapte similare în temeiul RGPD, care oferă mai multe îndrumări cu privire la subiectele care ar putea fi considerate ca fiind în afara domeniului de aplicare a legislației privind protecția datelor, încadrându-se în „excepția privind activitățile domestice", cum ar fi utilizarea platformelor de comunicare socială în scopuri personale.

Exemplu: Cauza *Bodil Lindqvist*[215] a vizat referirea la diverse persoane prin menționarea numelui sau a altor atribute, cum ar fi numărul de telefon sau informații despre hobby-uri, pe o pagină web. CJUE a stabilit că „menționarea, pe o pagină web, a unor persoane și identificarea acestora după nume sau prin alte atribute [...] constituie «prelucrare de date cu caracter personal efectuată total sau parțial prin mijloace automatizate»", în sensul articolului 3 alineatul (1) din Directiva privind protecția datelor[216].

Această prelucrare de date cu caracter personal nu se încadrează în activitățile exclusiv personale sau domestice, care se situează în afara domeniului de aplicare al normelor privind protecția datelor, deoarece această excepție „trebuie [...] interpretată ca fiind asociată numai activităților desfășurate în viața privată sau de familie a persoanelor, ceea ce în mod evident nu este cazul prelucrării datelor cu caracter personal care constă în publicarea pe internet astfel încât aceste date să fie accesibile unui număr nedefinit de persoane"[217].

Potrivit CJUE, înregistrările vizuale ale unei camere video de supraveghere instalate în context privat pot intra, de asemenea, sub incidența legislației UE privind protecția datelor în anumite circumstanțe.

215 Hotărârea CJUE din 6 noiembrie 2003 în cauza C-101/01, *Proces penal/Bodil Lindqvist*.

216 *Ibidem*, punctul 27; Directiva 95/46/CE (abrogată), articolul 3 alineatul (1), acum Regulamentul general privind protecția datelor, articolul 2 alineatul (1).

217 Hotărârea CJUE din 6 noiembrie 2003 în cauza C-101/01, *Proces penal/Bodil Lindqvist*, punctul 47.

Exemplu: În cauza *František Ryneš*[218], domnul Ryneš a captat imaginea a două persoane care i-au spart ferestrele casei prin sistemul de supraveghere video TVCI pe care îl instalase pentru a-și proteja proprietatea. Înregistrările au fost apoi predate poliției și au constituit probe în timpul procedurii penale.

CJUE a stabilit că „[î]n măsura în care o supraveghere video [...] se extinde, fie și parțial, la spațiul public și, în consecință, este îndreptată în afara sferei private a persoanei care efectuează prelucrarea datelor prin acest mijloc, aceasta nu poate fi considerată drept o activitate exclusiv «personală sau domestică» [...]”[219].

Operator

În dreptul UE, operatorul este definit ca fiind persoana sau entitatea care, „[singură] sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal”[220]. Decizia unui operator stabilește motivul și metoda prelucrării datelor.

În legislația CoE, Convenția 108 modernizată definește „operatorul” ca fiind „persoana fizică sau juridică, autoritatea, serviciul, agenția publică sau orice alt organism care, singur sau împreună cu altele, deține puterea de decizie în ceea ce privește prelucrarea datelor”[221]. Această putere de decizie privește scopurile și mijloacele de prelucrare, categoriile de date care urmează să fie prelucrate și accesul la date[222]. Trebuie să se decidă de la caz la caz dacă această putere derivă dintr-o desemnare legală sau din situația de fapt[223].

Exemplu: În cauza *Google Spain*[224], reclamantul este un cetățean spaniol care dorea să obțină eliminarea din rezultatele căutării pe Google a unui articol vechi de ziar care conținea informații despre antecedentele sale financiare.

218 Hotărârea CJUE din 11 decembrie 2014 în cauza C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, punctul 33.

219 Directiva 95/46/CE (abrogată), articolul 3 alineatul (2) a doua liniuță, acum Regulamentul general privind protecția datelor, articolul 2 alineatul (2) litera (c).

220 Regulamentul general privind protecția datelor, articolul 4 punctul 7.

221 Convenția 108 modernizată, articolul 2 litera (d).

222 Raportul explicativ privind Convenția 108 modernizată, punctul 22.

223 *Ibidem*.

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

CJUE i s-a solicitat să se pronunțe dacă Google, în calitate de operator al unui motor de căutare, era „operatorul" datelor în sensul articolului 2 litera (d) din Directiva privind protecția datelor[225]. CJUE a adoptat o definiție largă a noțiunii „operator" pentru a asigura „[protecția eficientă și completă] a persoanelor [vizate]"[226]. CJUE a constatat că operatorul motorului de căutare a stabilit scopurile și mijloacele activității și că a făcut datele încărcate pe paginile web de către editorii de site-uri accesibile tuturor utilizatorilor de internet care efectuează o căutare plecând de la numele persoanei vizate[227]. Prin urmare, CJUE a stabilit că Google poate fi considerat „operator"[228].

În cazul în care un operator sau o persoană împuternicită de operator este stabilit(ă) în afara UE, această societate trebuie să desemneze în scris un reprezentant în UE[229]. RGPD subliniază că reprezentantul trebuie să își aibă sediul „în unul dintre statele membre în care se află persoanele vizate ale căror date cu caracter personal sunt prelucrate în legătură cu furnizarea de bunuri și servicii sau al căror comportament este monitorizat"[230]. În cazul în care nu se desemnează un reprezentant, se pot introduce acțiuni în justiție împotriva operatorului sau a persoanei împuternicite de operator înșiși[231].

Controlul comun

RGPD prevede că, în cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt considerați operatori asociați. Înseamnă că aceștia decid împreună să prelucreze date într-un scop comun[232]. Raportul explicativ privind Convenția 108 modernizată precizează că sunt posibile, **în cadrul CoE**, asocierea operatorilor sau controlul comun[233].

225 Regulamentul general privind protecția datelor, articolul 4 punctul 7; Hotărârea CJUE [MC] din 13 mai 2014 în cauza C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, punctul 21.

226 Hotărârea CJUE [MC] din 13 mai 2014 în cauza C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, punctul 34.

227 *Ibidem*, punctele 35-40.

228 *Ibidem*, punctul 41.

229 Regulamentul general privind protecția datelor, articolul 27 alineatul (1).

230 *Ibidem*, articolul 27 alineatul (3).

231 *Ibidem*, articolul 27 alineatul (5).

232 *Ibidem*, articolul 4 punctul 7 și articolul 26.

233 Convenția 108 modernizată, articolul 2 litera (d); Raportul explicativ privind Convenția 108 modernizată, punctul 22.

Grupul de lucru „Articolul 29” subliniază că controlul comun poate lua forme diferite și că participarea diferiților operatori la activitățile de control poate fi inegală[234]. Această flexibilitate face posibilă adaptarea la realitățile din ce în ce mai complexe ale prelucrării datelor[235]. În consecință, operatorii asociați trebuie să își stabilească responsabilitățile în vederea respectării obligațiilor prevăzute de regulament printr-un acord specific[236].

Controlul comun conduce la responsabilitatea comună pentru o activitate de prelucrare[237]. În cadrul **legislației UE**, aceasta înseamnă că fiecare operator sau persoană împuternicită de operator este răspunzător (răspunzătoare) pentru întregul prejudiciu cauzat de prelucrarea în regim de control comun, pentru a asigura despăgubirea efectivă a persoanei vizate[238].

> Exemplu: O bază de date administrată în comun de mai multe instituții de credit pentru clienții lor rău platnici este un exemplu uzual de control comun. Atunci când o persoană solicită o linie de credit la una dintre băncile care este operator asociat, băncile vor consulta baza de date pentru a putea lua decizii informate cu privire la bonitatea solicitantului.

Dispozițiile legale nu menționează în mod explicit dacă un control comun presupune ca scopul comun să fie același pentru fiecare dintre operatori sau dacă este suficient ca scopurile acestora să se suprapună doar parțial. Deocamdată, nu există o jurisprudență relevantă la nivel european în acest sens. În avizul său din 2010 privind operatorii și persoanele împuternicite de operatori, Grupul de lucru „Articolul 29” afirmă că este posibil ca operatorii asociați să împărtășească toate scopurile și mijloacele de prelucrare sau să împărtășească doar anumite scopuri sau mijloace sau părți din acestea[239]. În timp ce prima posibilitate presupune o relație foarte strânsă între diferiți actori, cea din urmă indică o relație mai flexibilă.

234 Avizul 1/2010 al Grupului de lucru „Articolul 29” privind conceptele „operator” și „persoană împuternicită de operator”, WP 169, Bruxelles, 16 februarie 2010, p. 19.

235 *Ibidem*.

236 Regulamentul general privind protecția datelor, considerentul 79.

237 *Ibidem*, punctul 21.

238 *Ibidem*, articolul 82 alineatul (4).

239 Avizul 1/2010 al Grupului de lucru „Articolul 29” privind conceptele „operator” și „persoană împuternicită de operator”, WP 169, Bruxelles, 16 februarie 2010, p. 19.

Grupul de lucru „Articolul 29” susține o interpretare mai largă a conceptului de control comun, astfel încât să permite o oarecare flexibilitate necesară pentru a aborda complexitatea tot mai mare a realității actuale din domeniul prelucrării datelor[240]. Un caz care implică Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT) ilustrează poziția Grupului de lucru.

Exemplu: În așa-numitul caz SWIFT, instituțiile bancare europene au angajat SWIFT, inițial în calitate de operator, pentru a efectua transferul de date în timpul tranzacțiilor bancare. SWIFT a divulgat astfel de date privind tranzacțiile bancare, care erau stocate într-un centru de servicii de calcul din Statele Unite (SUA), Departamentului de Trezorerie al SUA, fără a i se solicita în mod explicit acest lucru de către instituțiile bancare europene care l-au angajat. Evaluând legalitatea acestei situații, Grupul de lucru „Articolul 29” a ajuns la concluzia că instituțiile bancare europene care au angajat SWIFT, precum și SWIFT în sine, trebuiau considerate operatori asociați răspunzători față de clienții europeni pentru divulgarea datelor lor către autoritățile din SUA[241].

Persoana împuternicită de operator

Persoana împuternicită de operator este definită **în dreptul UE** ca fiind persoana care prelucrează datele cu caracter personal în numele operatorului[242]. Activitățile încredințate unei persoane împuternicite de operator se pot limita la o sarcină sau la un context foarte specific sau pot fi relativ generale și cuprinzătoare.

În legislația CoE, înțelesul termenului este același ca în dreptul UE[243].

Pe lângă prelucrarea de date pentru alte entități, persoanele împuternicite de operator vor fi și operatori de date propriu-ziși în ceea ce privește prelucrarea pe care o efectuează în scopuri proprii, de exemplu gestionarea personalului, a vânzărilor și a clienților proprii.

240 *Ibidem*.

241 Avizul 10/2006 al Grupului de lucru „Articolul 29” privind prelucrarea datelor cu caracter personal de către Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT), WP 128, Bruxelles, 22 noiembrie 2006.

242 Regulamentul general privind protecția datelor, articolul 4 punctul 8.

243 Convenția 108 modernizată, articolul 2 litera (f).

Exemplu: Societatea Everready este specializată în prelucrarea de date în domeniul administrării datelor privind resursele umane pentru alte societăți. În această calitate, Everready este o persoană împuternicită de operator. Cu toate acestea, atunci când Everready prelucrează datele propriilor angajați, aceasta este operatorul care desfășoară operațiuni de prelucrare a datelor în scopul îndeplinirii obligațiilor sale ca angajator.

Relația dintre operator și persoana împuternicită de operator

După cum s-a precizat anterior, operatorul este definit ca fiind cel care stabilește scopurile și mijloacele de prelucrare. RGPD afirmă în mod clar că persoana împuternicită de operator nu prelucrează datele decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru[244]. Contractul dintre operator și persoana împuternicită de operator constituie un element esențial al relației dintre aceștia și are caracter juridic obligatoriu[245].

Exemplu: Directorul societății Sunshine decide că societatea Cloudy, specializată în stocarea de date bazată pe tehnologia cloud, va administra datele referitoare la clienții Sunshine. Societatea Sunshine rămâne operatorul de date, iar societatea Cloudy este doar o persoană împuternicită de operator, deoarece, potrivit contractului, Cloudy poate folosi datele referitoare la clienții societății Sunshine doar în scopurile stabilite de Sunshine.

În cazul în care autoritatea de stabilire a mijloacelor de prelucrare va fi delegată unei persoane împuternicite de operator, operatorul trebuie să poată exercita, totuși, un grad adecvat de control asupra deciziilor persoanei împuternicite de el referitoare la mijloacele de prelucrare. Responsabilitatea generală va reveni tot operatorului, care trebuie să supravegheze persoanele împuternicite de el pentru a se asigura că deciziile acestora respectă legislația privind protecția datelor și propriile sale instrucțiuni.

În plus, dacă o persoană împuternicită de operator nu respectă condițiile de prelucrare a datelor stabilite de operator înseamnă că persoana împuternicită de operator a devenit operator, cel puțin în măsura în care a încălcat instrucțiunile operatorului. Acest lucru va conduce, cel mai probabil, la transformarea persoanei împuternicite de operator într-un operator care acționează ilegal. În schimb,

244 Regulamentul general privind protecția datelor, articolul 29.

245 *Ibidem*, articolul 28 alineatul (3).

operatorul inițial va trebui să explice cum a fost posibil ca persoana împuternicită de el să își încalce mandatul[246]. Într-adevăr, Grupul de lucru „Articolul 29" tinde să admită controlul comun în astfel de cazuri, întrucât această soluție are ca rezultat cea mai bună protecție a intereselor persoanelor vizate[247].

De asemenea, pot exista probleme cu privire la împărțirea responsabilității în cazul în care operatorul este o întreprindere mai mică, iar persoana împuternicită de operator este o corporație mare, care are puterea de a dicta condițiile în care își oferă serviciile. Grupul de lucru „Articolul 29" afirmă că standardul de responsabilitate nu trebuie coborât totuși în astfel de situații din cauza dezechilibrului economic și că trebuie păstrat sensul conceptului de operator[248].

În vederea asigurării clarității și transparenței, detaliile relației dintre un operator și o persoană împuternicită de operator trebuie înregistrate într-un contract scris[249]. Contractul trebuie să precizeze în special obiectul, natura, scopul și durata prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate. De asemenea, trebuie să prevadă obligațiile și drepturile operatorului și ale persoanei împuternicite de operator, cum ar fi cerințele privind confidențialitatea și securitatea. Inexistența unui astfel de contract constituie o încălcare a obligației operatorului de a oferi o documentație scrisă privind responsabilitățile reciproce și poate atrage după sine sancțiuni. În cazul în care se produc prejudicii ca urmare a nerespectării instrucțiunilor legale ale operatorului sau a acționării în afara limitelor acestora, nu doar operatorul poate fi considerat răspunzător, ci și persoana împuternicită de operator[250]. Persoana împuternicită de operator trebuie să păstreze o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului[251]. Aceste evidențe trebuie să fie puse la dispoziția autorității de supraveghere, la cererea acesteia, deoarece atât operatorul, cât și persoana împuternicită de operator trebuie să coopereze în vederea îndeplinirii atribuțiilor de către autoritatea respectivă[252]. Operatorii

246 *Ibidem*, articolul 82 alineatul (2).

247 Avizul 1/2010 al Grupului de lucru „Articolul 29" privind conceptele „operator" și „persoană împuternicită de operator", WP 169, Bruxelles, 16 februarie 2010, p. 25; Avizul 10/2006 al Grupului de lucru „Articolul 29" privind prelucrarea datelor cu caracter personal de către Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT), WP 128, Bruxelles, 22 noiembrie 2006.

248 Avizul 1/2010 al Grupului de lucru „Articolul 29" privind conceptele „operator" și „persoană împuternicită de operator", WP 169, Bruxelles, 16 februarie 2010, p. 26.

249 Regulamentul general privind protecția datelor, articolul 28 alineatele (3) și (9).

250 *Ibidem*, articolul 82 alineatul (2).

251 *Ibidem*, articolul 30 alineatul (2).

252 *Ibidem*, articolul 30 alineatul (4) și articolul 31.

și persoanele împuternicite de operatori au, de asemenea, posibilitatea de a adera la un cod de conduită aprobat sau la un mecanism de certificare pentru a demonstra conformitatea cu cerințele RGPD[253].

Este posibil ca persoanele împuternicite de operatori să dorească să delege anumite sarcini altor subcontractanți. Legea permite acest lucru, cu condiția să se prevadă clauze contractuale adecvate între operator și persoana împuternicită de acesta, inclusiv să se prevadă dacă este necesară autorizarea operatorului în fiecare caz în parte sau dacă este suficientă o simplă informare. RGPD prevede că persoana împuternicită inițială rămâne pe deplin răspunzătoare față de operator în cazul în care a doua persoană împuternicită își încalcă obligațiile de protecție a datelor[254].

În legislația CoE se aplică pe deplin interpretarea conceptelor de operator și de persoană împuternicită de operator explicată mai sus[255].

2.3.2. Destinatari și părți terțe

Diferența dintre aceste două categorii de persoane sau entități introduse de Directiva privind protecția datelor constă în principal în relația acestora cu operatorul și, în consecință, în autorizarea lor pentru a accesa datele cu caracter personal deținute de operator.

„Partea terță" este o persoană diferită de operator și de persoana împuternicită de operator. Potrivit articolului 4 punctul 10 din RGPD, o parte terță este „o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal". Aceasta înseamnă că persoanele care lucrează pentru o organizație diferită de operator – chiar dacă aparține aceluiași grup sau societăți de tip holding – vor fi (sau vor aparține unei) „părți terțe". Pe de altă parte, sucursalele unei bănci care prelucrează conturile clienților sub autoritatea directă a sediului lor central nu pot fi considerate „părți terțe"[256].

253 *Ibidem*, articolul 28 alineatul (5) și articolul 42 alineatul (4).

254 *Ibidem*, articolul 28 alineatul (4).

255 Vezi, de exemplu, Convenția 108 modernizată, articolul 2 literele (b) și (f); Recomandarea privind crearea de profiluri, articolul 1.

256 Avizul 1/2010 al Grupului de lucru „Articolul 29" privind conceptele „operator" și „persoană împuternicită de operator", WP 169, Bruxelles, 16 februarie 2010, p. 31.

„Destinatar" este un termen cu semnificație mai largă decât „parte terță". În sensul articolului 4 punctul 9 din RGPD, destinatar înseamnă „persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță". Acest destinatar poate fi o persoană din afara operatorului sau a persoanei împuternicite de operator – în acest caz, o parte terță – sau cineva din cadrul operatorului sau al persoanei împuternicite de operator, cum ar fi un angajat sau un alt departament din cadrul aceleiași societăți sau autorități.

Diferența între destinatari și părți terțe este importantă numai din perspectiva condițiilor aplicabile divulgării legale a datelor. Angajații unui operator sau ai unei persoane împuternicite de operator pot fi, fără să se aplice nicio altă cerință legală, destinatari ai datelor cu caracter personal în cazul în care sunt implicați în operațiunile de prelucrare ale operatorului sau ale persoanei împuternicite de operator. În schimb, o parte terță, fiind separată de operator și de persoana împuternicită de operator, nu este autorizată să utilizeze datele cu caracter personal prelucrate de operator, cu excepția cazului în care există temeiuri juridice pentru aceasta într-o anumită situație.

Exemplu: Angajatul unui operator care utilizează datele cu caracter personal în limita atribuțiilor încredințate de angajatorul său este destinatarul datelor, însă nu parte terță, deoarece utilizează datele în numele operatorului și în conformitate cu instrucțiunile acestuia. De exemplu, dacă un angajator divulgă date cu caracter personal despre angajații săi către departamentul său de resurse umane în vederea unor evaluări viitoare ale performanței, echipa de resurse umane va fi destinatară a datelor cu caracter personal, deoarece datele i-au fost divulgate în cadrul prelucrării pentru operator.

Însă, dacă organizația furnizează date despre angajații săi unei societăți de formare profesională care va folosi aceste date pentru a adapta un program de pregătire a angajaților, societatea de formare profesională este o parte terță. Motivul este că societatea de formare profesională nu deține legitimare sau autorizare specifică pentru prelucrarea datelor cu caracter personal în cauză, legitimare sau autorizare care rezultă, în cazul „departamentului de resurse umane", din relația de muncă cu operatorul. Cu alte cuvinte, societatea de formare profesională nu a primit informațiile în cadrul unei relații de încadrare în muncă cu operatorul de date.

2.4. Consimțământ

Principalele elemente

- Consimțământul, ca temei juridic pentru prelucrarea datelor cu caracter personal, trebuie acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului pentru prelucrare.
- Prelucrarea categoriilor speciale de date cu caracter personal necesită un consimțământ explicit.

Astfel cum se va examina în detaliu în capitolul 4, consimțământul este unul dintre cele șase motive legitime pentru prelucrarea datelor cu caracter personal. Consimțământ înseamnă „orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate”[257].

Dreptul UE stabilește mai multe elemente necesare pentru ca un consimțimânt să fie valabil, care au ca scop garantarea intenției efective a persoanelor vizate de a accepta o anumită utilizare a datelor lor[258]:

- Consimțământul trebuie acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal. O astfel de manifestare poate fi o acțiune sau o declarație.

- Persoana vizată trebuie să aibă dreptul de a-și retrage în orice moment consimțământul.

- În contextul unei declarații scrise care include și alte aspecte, cum ar fi „condițiile de utilizare”, cererile de acordare a consimțământului trebuie să fie formulate într-un limbaj clar și simplu și într-o formă inteligibilă și ușor accesibilă, care să distingă în mod clar consimțământul de alte aspecte; dacă o parte din această declarație încalcă RGPD, aceasta nu are caracter obligatoriu.

Consimțământul va fi valabil numai în contextul legislației privind protecția datelor, cu condiția îndeplinirii tuturor acestor cerințe. Este responsabilitatea operatorului să

257 Regulamentul general privind protecția datelor, articolul 4 punctul 11. Vezi, de asemenea, Convenția 108 modernizată, articolul 5 alineatul (2).

258 Regulamentul general privind protecția datelor, articolul 7.

demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale[259]. Elementele consimțământului valabil vor fi discutate în continuare, în secțiunea 4.1.1 referitoare la motivele legale de prelucrare a datelor cu caracter personal.

Convenția 108 nu conține o definiție a consimțământului; interpretarea acestui concept este lăsată la aprecierea legislației interne. Totuși, **în legislația CoE**, elementele consimțământului valabil corespund celor explicate anterior[260].

Cerințele suplimentare pentru un consimțământ valabil prevăzute de dreptul civil, cum ar fi capacitatea juridică, se aplică, în mod evident, și în contextul protecției datelor, întrucât aceste cerințe reprezintă condiții juridice prealabile esențiale. Consimțământul lipsit de valabilitate al unor persoane lipsite de capacitate juridică va avea ca rezultat absența unui temei juridic pentru prelucrarea datelor acestor persoane. În ceea ce privește capacitatea juridică a minorilor de a încheia contracte, RGPD prevede că normele sale privind vârsta minimă necesară pentru a putea exprima un consimțământ valabil nu afectează dreptul general al contractelor aplicabil în statele membre[261].

Consimțământul trebuie să fie dat în mod clar, astfel încât să nu existe nicio îndoială cu privire la intenția persoanei vizate[262]. Consimțământul trebuie să fie explicit atunci când se referă la prelucrarea datelor sensibile și poate fi acordat verbal sau în scris[263]. Acesta din urmă poate fi acordat prin mijloace electronice[264]. În cadrul legislației **UE** și a **CoE** deopotrivă, acordul pentru prelucrarea datelor cu caracter personal ale unei persoane trebuie să fie exprimat printr-o declarație sau printr-o acțiune neechivocă[265]. Astfel, consimțământul nu poate fi dedus din absența unui răspuns, din căsuțe bifate în prealabil, din formulare completate în prealabil sau din absența unei acțiuni[266].

259 *Ibidem*, articolul 7 alineatul (1).

260 Convenția 108 modernizată, articolul 5 alineatul (2); Raportul explicativ privind Convenția 108 modernizată, punctele 42-45.

261 Regulamentul general privind protecția datelor, articolul 8 alineatul (3).

262 *Ibidem*, articolul 6 alineatul (1) litera (a) și articolul 9 alineatul (2) litera (a).

263 *Ibidem*, considerentul 32.

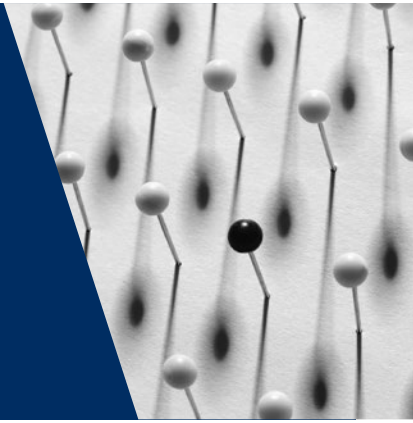
264 *Ibidem*.

265 *Ibidem*, articolul 4 punctul 11; Raportul explicativ privind Convenția 108 modernizată, punctul 42.

266 Regulamentul general privind protecția datelor, considerentul 32; Raportul explicativ privind Convenția 108 modernizată, punctul 42.

3

Principiile esențiale ale legislației europene privind protecția datelor



UE	Aspecte vizate	CoE
Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (a)	**Principiul legalității**	Convenția 108 modernizată, articolul 5 alineatul (3)
Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (a)	**Principiul echității**	Convenția 108 modernizată, articolul 5 alineatul (4) litera (a) Hotărârea CEDO în cauza *K.H. și alții/Slovacia*, nr. 32881/04, 2009
Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (a) Hotărârea CJUE în cauza C-201/14, *Smaranda Bara și alții/ Casa Națională de Asigurări de Sănătate și alții*, 2015	**Principiul transparenței**	Convenția 108 modernizată, articolul 5 alineatul (4) litera (a) și articolul 8 Hotărârea CEDO în cauza *Haralambie/România*, nr. 21737/03, 2009
Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (b)	**Principiul limitărilor legate de scop**	Convenția 108 modernizată, articolul 5 alineatul (4) litera (b)
Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (c) Hotărârea CJUE [MC] în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland* și *Kärntner Landesregierung și alții*, 2014	**Principiul reducerii la minimum a datelor**	Convenția 108 modernizată, articolul 5 alineatul (4) litera (c)

UE	Aspecte vizate	CoE
Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (d) Hotărârea CJUE în cauza C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, 2009	**Principiul exactității datelor**	Convenția 108 modernizată, articolul 5 alineatul (4) litera (d)
Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (e) Hotărârea CJUE [MC] în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland* și *Kärntner Landesregierung și alții*, 2014	**Principiul limitărilor legate de stocare**	Convenția 108 modernizată, articolul 5 alineatul (4) litera (e) Hotărârea CEDO [MC] în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04, 2008
Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (f) și articolul 32	**Principiul securității (integrității și confidențialității) datelor**	Convenția 108 modernizată, articolul 7
Regulamentul general privind protecția datelor, articolul 5 alineatul (2)	**Principiul responsabilității**	Convenția 108 modernizată, articolul 10

Articolul 5 din Regulamentul general privind protecția datelor stabilește principiile care reglementează prelucrarea datelor cu caracter personal. Aceste principii se referă la următoarele:

- legalitate, echitate și transparență;
- limitări legate de scop;
- reducerea la minimum a datelor;
- exactitatea datelor;
- limitări legate de stocare;
- integritate și confidențialitate.

Principiile servesc ca punct de plecare pentru dispoziții mai detaliate în articolele ulterioare ale regulamentului. Acestea apar, de asemenea, la articolele 5, 7, 8 și 10 din Convenția 108 modernizată. Orice legislație ulterioară privind protecția datelor

la nivelul CoE sau al UE trebuie să respecte aceste principii, iar acestea trebuie avute în vedere în momentul interpretării legislației. În cadrul legislației UE, restrângerea principiilor aplicabile prelucrării sunt permise numai în măsura în care corespund drepturilor și obligațiilor prevăzute la articolele 12-22 și trebuie să respecte esența drepturilor și libertăților fundamentale. La nivelul UE sau la nivel național se pot prevedea orice derogări și limitări ale acestor principii esențiale[267]; respectivele derogări și limitări trebuie să fie prevăzute de lege, să urmărească un scop legitim și să constituie măsuri necesare și proporționale într-o societate democratică[268].Toate cele trei condiții trebuie îndeplinite.

3.1. Principiile de legalitate, echitate și transparență a prelucrării

Principalele elemente

- Principiile de legalitate, echitate și transparență se aplică tuturor prelucrărilor de date cu caracter personal.
- În conformitate cu RGPD, legalitatea implică următoarele elemente:
  - consimțământul persoanei vizate;
  - necesitatea de a încheia un contract;
  - o obligație legală;
  - necesitatea protejării intereselor vitale ale persoanei vizate sau ale unei alte persoane;
  - necesitatea de a realiza o activitate în interes public;
  - necesitatea protejării intereselor legitime ale operatorului sau ale unei părți terțe, în măsura în care acestea nu prevalează în cazul respectiv interesele și drepturile persoanei vizate.
- Prelucrarea datelor cu caracter personal trebuie efectuată în mod echitabil.
  - Persoana vizată trebuie să fie informată cu privire la riscuri, pentru a se asigura faptul că prelucrarea nu are efecte negative neprevăzute.

267 Convenția 108 modernizată, articolul 11 alineatul (1); Regulamentul general privind protecția datelor, articolul 23 alineatul (1).

268 Regulamentul general privind protecția datelor, articolul 23 alineatul (1).

- Prelucrarea datelor cu caracter personal trebuie efectuată în mod transparent.
  - Înainte de a prelucra datele persoanelor vizate, operatorii trebuie să informeze aceste persoane, printre altele, cu privire la scopul prelucrării, precizând identitatea și adresa operatorului.
  - Informațiile privind operațiunile de prelucrare trebuie furnizate în limbaj clar și simplu, pentru a permite persoanelor vizate să înțeleagă cu ușurință normele, riscurile, garanțiile și drepturile implicate.
  - Persoanele vizate au dreptul de acces la datele lor, indiferent de locul unde sunt prelucrate acestea.

3.1.1. Legalitatea prelucrării

Legislația UE și a CoE în materie de protecție a datelor impune ca prelucrarea datelor cu caracter personal să respecte principiul legalității[269]. Prelucrarea legală implică consimțământul persoanei vizate sau un alt temei juridic prevăzut de legislația în materie de protecție a datelor[270]. Pe lângă consimțământ, articolul 6 alineatul (1) din RGPD menționează cinci temeiuri juridice pentru prelucrare, și anume atunci când prelucrarea datelor cu caracter personal este necesară: pentru executarea unui contract, pentru îndeplinirea unei sarcini care rezultă din exercitarea autorității publice, în vederea îndeplinirii unei obligații legale, în scopul intereselor legitime urmărite de operator sau de părți terțe sau pentru a proteja interesele vitale ale persoanei vizate. Acestea vor fi discutate mai detaliat în secțiunea 4.1.

3.1.2. Echitatea prelucrării

Pe lângă legalitatea prelucrării, legislația UE și a CoE în materie de protecție a datelor impun ca datele cu caracter personal să fie prelucrate în mod echitabil[271]. Principiul echității prelucrării reglementează în primul rând relația dintre operator și persoana vizată.

Operatorii ar trebui să înștiințeze persoanele vizate și publicul larg că vor prelucra datele într-un mod legal și transparent și trebuie să fie în măsură să demonstreze

269 Convenția 108 modernizată, articolul 5 alineatul (3); Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (a).

270 Carta drepturilor fundamentale a Uniunii Europene, articolul 8 alineatul (2); Regulamentul general privind protecția datelor, considerentul 40 și articolele 6-9; Convenția 108 modernizată, articolul 5 alineatul (2); Raportul explicativ privind Convenția 108 modernizată, punctul 41.

271 Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (a); Convenția 108 modernizată, articolul 5 alineatul (4) litera (a).

conformitatea operațiunilor de prelucrare cu RGPD. Operațiunile de prelucrare nu trebuie efectuate în secret, iar persoanele vizate ar trebui să fie conștiente de riscurile potențiale. În plus, operatorii, în măsura în care este posibil, trebuie să acționeze într-un mod care să respecte cu promptitudine voința persoanei vizate, în special atunci când consimțământul acesteia constituie temeiul juridic al prelucrării datelor.

Exemplu: În cauza *K.H. și alții/Slovacia*[272], reclamantele – mai multe femei de etnie romă – fuseseră tratate în două spitale din estul Slovaciei în timpul sarcinii și al nașterii. Ulterior, niciuna dintre ele nu a mai reușit să conceapă copii, în ciuda încercărilor repetate. Instanțele naționale au impus spitalelor să permită reclamantelor și reprezentanților acestora să consulte evidențele medicale și să extragă manual fragmente din acestea, dar au respins cererea de a realiza fotocopii după documente, invocând ca motiv prevenirea abuzurilor. Obligațiile pozitive ale statelor în temeiul articolului 8 din Convenția europeană a drepturilor omului includ în mod necesar o obligație de a pune la dispoziția persoanei vizate copii ale fișierelor sale de date. Statului îi revenea sarcina de a stabili modalitățile de copiere a fișierelor de date cu caracter personal sau, după caz, de a prezenta motivele imperioase ale refuzului de a face acest lucru. În cazul reclamantelor, instanțele naționale au justificat interzicerea realizării de copii după documentele medicale în principal prin necesitatea de a proteja informațiile în cauză împotriva abuzului. CEDO nu a reușit totuși să identifice în ce fel reclamantele, cărora li se acordase, oricum, accesul la întreaga documentație medicală care le privea, ar fi putut utiliza abuziv informații referitoare la ele însele. În plus, riscul unui astfel de abuz ar fi putut fi împiedicat prin alte mijloace decât refuzul de a acorda reclamantelor permisiunea realizării de fotocopii după documentele medicale, de exemplu prin limitarea categoriilor de persoane care aveau dreptul de acces la aceste documente. Statul nu a demonstrat existența unor motive suficient de convingătoare pentru a refuza reclamantelor accesul eficace la informațiile referitoare la sănătatea lor. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

În ceea ce privește serviciile internet, caracteristicile sistemelor de prelucrare a datelor trebuie să permită ca persoanele vizate să înțeleagă cu adevărat ce se întâmplă cu datele lor. În orice caz, principiul echității depășește obligațiile de

272 Hotărârea CEDO din 28 aprilie 2009 în cauza *K.H. și alții/Slovacia*, nr. 32881/04.

transparență, putând să se refere inclusiv la prelucrarea datelor cu caracter personal în mod etic.

Exemplu: Un departament de cercetare al unei universități efectuează un experiment prin care analizează schimbările de dispoziție a 50 de subiecți. Aceștia trebuie să își consemneze gândurile într-un fișier electronic, din oră în oră, la anumite momente stabilite. Cele 50 de persoane și-au dat consimțământul pentru acest proiect și pentru această utilizare specifică a datelor lor de către universitate. Departamentul de cercetare descoperă în curând că înregistrarea în format electronic a gândurilor persoanelor ar fi foarte utilă pentru un alt proiect, axat pe sănătatea mintală, sub coordonarea unei alte echipe. Chiar dacă universitatea, în calitate de operator, ar fi putut să folosească aceleași date pentru activitatea unei alte echipe fără a mai lua măsuri suplimentare pentru a asigura legalitatea prelucrării acestor date, având în vedere compatibilitatea scopurilor, universitatea a informat totuși subiecții și a cerut din nou consimțământul, urmând codul său de etică în domeniul cercetării și principiul echității prelucrării.

3.1.3. Transparența prelucrării

Legislația UE și a CoE în materie de protecție a datelor impune ca prelucrarea datelor cu caracter personal să se facă „în mod [...] transparent față de persoana vizată”[273].

Acest principiu stabilește obligația operatorului de a lua toate măsurile adecvate pentru a informa persoanele vizate – care pot fi utilizatori sau clienți – cu privire la modul în care sunt utilizate datele lor[274]. Transparența se poate referi la informațiile furnizate persoanei fizice înainte de începerea prelucrării[275], la informațiile care ar trebui să fie ușor accesibile persoanelor vizate în timpul prelucrării[276], precum și la informațiile furnizate persoanelor vizate în urma unei cereri de acces la propriile lor date[277].

273 Regulamentul general privind protecția datelor, articolul 5 alineatul (1); Convenția 108 modernizată, articolul 5 alineatul (4) litera (a) și articolul 8.

274 Regulamentul general privind protecția datelor, articolul 12.

275 *Ibidem*, articolele 13 și 14.

276 Avizul 2/2017 al Grupului de lucru „Articolul 29” privind prelucrarea datelor la locul de muncă, WP 249, Bruxelles, 8 iunie 2017, p. 23.

277 Regulamentul general privind protecția datelor, articolul 15.

Exemplu: În cauza *Haralambie/România*[278], reclamantului i s-a acordat accesul la informațiile deținute despre el de serviciul secret doar la cinci ani de la cererea sa. CEDO a reiterat faptul că persoanele care fac obiectul unor dosare cu caracter personal deținute de autoritățile publice au un interes vital să acceadă la aceste dosare. Autoritățile aveau obligația de a pune la dispoziție o procedură eficace de obținere a accesului la aceste informații. CEDO a considerat că nici cantitatea fișierelor transmise, nici deficiențele sistemului de arhivare nu justificau întârzierea de cinci ani în acordarea accesului reclamantului la dosarele care îl priveau. Autoritățile nu au furnizat reclamantului o procedură eficace și accesibilă pentru a-i permite să obțină accesul la dosarele care îl priveau într-un termen rezonabil. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Operațiunile de prelucrare trebuie să le fie explicate persoanelor vizate într-un mod ușor accesibil, care să garanteze că acestea înțeleg ce se va întâmpla cu datele lor. Aceasta înseamnă că persoana vizată ar trebui să cunoască scopul specific al prelucrării datelor cu caracter personal în momentul colectării acestora[279]. Transparența prelucrării necesită utilizarea unui limbaj clar și simplu[280]. Persoanele vizate ar trebui să înțeleagă riscurile, normele, garanțiile și drepturile aferente prelucrării datelor lor cu caracter personal[281].

Legislația CoE precizează, de asemenea, că este obligatoriu ca operatorul să furnizeze persoanei vizate, în mod proactiv, anumite informații esențiale. Informațiile privind numele și adresa operatorului (sau a operatorilor asociați), temeiul juridic și scopurile prelucrării datelor, categoriile de date prelucrate și destinatarii, precum și modalitățile de exercitare a drepturilor pot fi furnizate în orice format adecvat (printr-un site web, prin instrumente tehnologice instalate pe dispozitive personale etc.), atât timp cât informațiile sunt prezentate persoanei vizate în mod corect și eficace. Informațiile prezentate trebuie să fie ușor accesibile, lizibile, ușor de înțeles și adaptate persoanelor vizate în cauză (de exemplu, după caz, într-un limbaj accesibil copiilor). Trebuie furnizate, de asemenea, orice informații suplimentare necesare sau utile pentru a asigura o prelucrare echitabilă a datelor, cum ar fi perioada de păstrare a datelor, explicarea raționamentului care stă la baza prelucrării datelor sau informații despre transferurile de date către un destinatar dintr-o altă parte membră sau

278 Hotărârea CEDO din 27 octombrie 2009 în cauza *Haralambie/România*, nr. 21737/03.

279 Regulamentul general privind protecția datelor, considerentul 39.

280 *Ibidem*.

281 *Ibidem*.

nemembră (precizându-se inclusiv dacă o anumită parte nemembră oferă un nivel adecvat de protecție sau măsurile luate de operator pentru a garanta un astfel de nivel adecvat de protecție a datelor)[282].

În temeiul dreptului de acces[283], persoana vizată are dreptul de a i se comunica, la cerere, de către operator, dacă datele sale sunt prelucrate și, în caz afirmativ, care date fac obiectul respectivei prelucrări[284]. În plus, în temeiul dreptului la informare[285], persoanele ale căror date sunt prelucrate trebuie să fie informate în mod proactiv de operatori sau de persoanele împuternicite de aceștia, în principiu înainte de începerea activității de prelucrare, cu privire la scopurile, durata și mijloacele de prelucrare, printre alte detalii.

Exemplu: Cauza *Smaranda Bara și alții/Președintele Casei Naționale de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)*[286] viza transmiterea datelor fiscale referitoare la venitul persoanelor fizice care desfășoară activități independente de la Agenția Națională de Administrare Fiscală către Casa Națională de Asigurări de Sănătate din România, pe baza acestor date solicitându-se plata contribuțiilor datorate la asigurările de sănătate. CJUE i s-a solicitat să stabilească dacă persoanei vizate ar fi trebuit să i se furnizeze informații privind identitatea operatorului de date și scopul transmiterii datelor înainte de prelucrarea acestor date de către Casa Națională de Asigurări de Sănătate. CJUE a stabilit că, atunci când o autoritate a administrației publice dintr-un stat membru transmite date cu caracter personal unei alte autorități a administrației publice care prelucrează ulterior aceste date, persoanele vizate trebuie să fie informate cu privire la această transmitere sau prelucrare.

În anumite situații, sunt permise derogări de la obligația de a informa persoanele vizate cu privire la prelucrarea datelor; acestea vor fi discutate mai detaliat în secțiunea 6.1., care privește drepturile persoanei vizate.

282 Raportul explicativ privind Convenția 108 modernizată, punctul 68.

283 Regulamentul general privind protecția datelor, articolul 15.

284 Convenția 108 modernizată, articolul 8 și articolul 9 alineatul (1) litera (b).

285 Regulamentul general privind protecția datelor, articolele 13 și 14.

286 Hotărârea CJUE din 1 octombrie 2015 în cauza C-201/14, *Smaranda Bara și alții/Casa Națională de Asigurări de Sănătate și alții*, punctele 28-46.

3.2. Principiul limitărilor legate de scop

Principalele elemente

- Scopul prelucrării datelor trebuie să fie definit înainte de începerea prelucrării.
- Nu se poate face o prelucrare ulterioară a datelor într-un mod care să fie incompatibil cu scopul inițial, deși Regulamentul general privind protecția datelor prevede excepții de la această regulă în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică și în scopuri statistice.
- În esență, principiul limitărilor legate de scop înseamnă că orice prelucrare a datelor cu caracter personal trebuie realizată doar pentru un anumit scop inițial bine definit și pentru scopuri suplimentare determinate și compatibile cu cel inițial.

Principiul limitărilor legate de scop este unul dintre principiile fundamentale ale legislației europene în materie de protecție a datelor. Este strâns legat de transparență, de previzibilitate și de controlul de către utilizatori: dacă scopul prelucrării este suficient de bine determinat și de clar, persoanele vizate știu la ce să se aștepte, iar transparența și securitatea juridică sunt sporite. În același timp, este importantă o delimitare clară a scopului pentru a permite persoanelor vizate să își exercite în mod efectiv drepturile, cum ar fi dreptul de a se opune prelucrării[287].

Principiul impune ca orice prelucrare a datelor cu caracter personal să se facă în scopuri determinate, bine definite, și doar în acele scopuri suplimentare care sunt compatibile cu scopul inițial[288]. Prelucrarea datelor cu caracter personal în scopuri nedefinite și/sau nelimitate este, așadar, ilegală. Nu este legală nici prelucrarea datelor cu caracter personal fără un scop determinat, bazată exclusiv pe considerația că ar putea fi utilă la un moment dat în viitor. Legitimitatea prelucrării datelor cu caracter personal va depinde de scopul prelucrării, care trebuie să fie explicit, determinat și legitim.

Orice scop nou de prelucrare a datelor care nu este compatibil cu scopul inițial trebuie să aibă propriul temei juridic special și nu se poate baza pe faptul că datele au fost dobândite sau prelucrate inițial în alt scop legitim. Prelucrarea legitimă este limitată la scopul specificat inițial și orice scop nou de prelucrare va necesita un nou

287 Avizul 3/2013 al Grupului de lucru „Articolul 29" privind limitările legate de scop, WP 203, Bruxelles, 2 aprilie 2013.

288 Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (b).

temei juridic separat. De exemplu, divulgarea datelor cu caracter personal către părți terțe pentru un scop nou va trebui să fie luată în considerare cu atenție, deoarece o astfel de divulgare va necesita probabil un temei juridic suplimentar distinct de cel al colectării datelor.

Exemplu: O companie aeriană colectează date de la pasagerii săi pentru ca agențiile de rezervare de bilete să gestioneze zborurile în mod adecvat. Compania aeriană va avea nevoie de date privind: numerele de loc ale pasagerilor, limitări fizice speciale, cum ar fi necesitatea unui scaun cu rotile, și cerințe alimentare speciale, cum ar fi alimente de tip cușer sau halal. În cazul în care companiilor aeriene li se solicită să transmită aceste date, care sunt incluse în registrele cu numele pasagerilor, către autoritățile în domeniul imigrației de la aeroportul de debarcare, aceste date sunt astfel utilizate în scopuri de control al imigrației, care diferă de scopul inițial pentru care au fost colectate. Prin urmare, transmiterea acestor date către o autoritate din domeniul imigrației va necesita un temei juridic nou și separat.

Atunci când analizează întinderea și limitele unui anumit scop, Convenția 108 modernizată și Regulamentul general privind protecția datelor recurg la conceptul de compatibilitate: utilizarea datelor în scopuri compatibile este permisă în baza temeiului juridic inițial. În consecință, prelucrarea ulterioară a datelor nu poate fi efectuată într-un mod neașteptat, inadecvat sau inacceptabil pentru persoana vizată[289]. Pentru a evalua dacă prelucrarea ulterioară trebuie considerată compatibilă, operatorul trebuie să ia în considerare, printre altele, următoarele elemente:

- „orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate;
- contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește [așteptările rezonabile ale persoanelor vizate cu privire la utilizarea ulterioară a datelor, având în vedere] relația dintre persoanele vizate și operator;
- natura datelor cu caracter personal [...];
- posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;

289 Raportul explicativ privind Convenția 108 modernizată, punctul 49.

- existența unor garanții adecvate [atât în cadrul operațiunilor de prelucrare inițiale, cât și al celor ulterioare preconizate]"[290]. Acest lucru se poate face, de exemplu, prin criptare sau pseudonimizare.

Exemplu: Societatea Sunshine achiziționează date despre clienți în cadrul operațiunilor de gestionare a relațiilor cu clienții (GRC). Ulterior, transmite aceste date către o societate de marketing direct, societatea Moonlight, care dorește să utilizeze aceste date pentru a oferi asistență în cadrul campaniilor de marketing ale unor societăți terțe. Transmiterea datelor de către Sunshine în scopul utilizării în campanii de marketing ale altor societăți constituie o utilizare ulterioară a datelor într-un scop nou, care este incompatibil cu GRC, scopul inițial în care colectase societatea Sunshine datele despre clienți. Prin urmare, transmiterea datelor către societatea Moonlight necesită propriul temei juridic.

În schimb, utilizarea de către societatea Sunshine a datelor GRC pentru propriul scop de marketing, și anume transmiterea de mesaje de marketing către clienți în legătură cu produsele sale, este general acceptată drept scop compatibil.

Regulamentul general privind protecția datelor și Convenția 108 modernizată prevăd că „prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice" este considerată *a priori* compatibilă cu scopul inițial[291]. Cu toate acestea, trebuie aplicate măsuri de protecție adecvate, cum ar fi anonimizarea, criptarea sau pseudonimizarea datelor și restricționarea accesului la date în cazul unei prelucrări ulterioare a datelor cu caracter personal[292]. Regulamentul general privind protecția datelor adaugă că „[î]n cazul în care persoana vizată și-a dat consimțământul sau prelucrarea se bazează pe dreptul Uniunii sau pe dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja, în special, obiective importante de interes public general, operatorul ar trebui să aibă posibilitatea de a prelucra în continuare

290 Regulamentul general privind protecția datelor, considerentul 50 și articolul 6 alineatul (4); Raportul explicativ privind Convenția 108 modernizată, punctul 49.

291 Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (b); Convenția 108 modernizată, articolul 5 alineatul (4) litera (b). Un exemplu de astfel de dispoziție națională este Legea austriacă privind protecția datelor (Datenschutzgesetz), Monitorul Oficial Federal I nr. 165/1999, punctul 46.

292 Regulamentul general privind protecția datelor, articolul 6 alineatul (4); Convenția 108 modernizată, articolul 5 alineatul (4) litera (b); Raportul explicativ privind Convenția 108 modernizată, punctul 50.

datele cu caracter personal, indiferent de compatibilitatea scopurilor”[293]. Prin urmare, atunci când se întreprinde o prelucrare ulterioară, persoana vizată ar trebui să fie informată cu privire la scopurile prelucrării, precum și la drepturile sale, cum ar fi dreptul de a se opune prelucrării[294].

Exemplu: Societatea Sunshine a colectat și stocat date de gestionare a relațiilor cu clienții (GRC) cu privire la clienții săi. Utilizarea ulterioară a acestor date de către societatea Sunshine pentru o analiză statistică a comportamentului de cumpărare al clienților săi este permisă, deoarece statisticile reprezintă un scop compatibil. Nu este necesar un temei juridic suplimentar, cum ar fi consimțământul persoanelor vizate. Cu toate acestea, în vederea prelucrării ulterioare a datelor cu caracter personal în scopuri statistice, societatea Sunshine trebuie să instituie garanții adecvate pentru drepturile și libertățile persoanei vizate. Măsurile tehnice și organizatorice pe care trebuie să le pună în aplicare Sunshine pot include pseudonimizarea datelor.

3.3. Principiul reducerii la minimum a datelor

Principalele elemente

- Prelucrarea datelor trebuie să se limiteze la ceea ce este necesar pentru îndeplinirea unui scop legitim.
- Prelucrarea datelor cu caracter personal ar trebui să aibă loc numai atunci când scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace.
- Prelucrarea datelor nu poate interveni în mod disproporționat asupra intereselor, drepturilor și libertăților în cauză.

Vor fi prelucrate numai datele care sunt „adecvate, relevante și nu depășesc ceea ce este necesar în raport cu scopurile în care sunt colectate și/sau prelucrate ulterior”[295]. Categoriile de date alese pentru prelucrare trebuie să fie necesare pentru a atinge scopul general declarat al operațiunilor de prelucrare, iar un operator ar

293 Regulamentul general privind protecția datelor, considerentul 50.

294 *Ibidem*.

295 Convenția 108 modernizată, articolul 5 alineatul (4) litera (c); Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (c).

trebui să limiteze colectarea de date strict la acele informații direct relevante pentru scopul specific urmărit de prelucrare.

Exemplu: În cauza *Digital Rights Ireland*[296], CJUE a examinat valabilitatea Directivei privind păstrarea datelor, care urmărea armonizarea dispozițiilor naționale privind păstrarea datelor cu caracter personal generate sau prelucrate de către serviciile sau rețelele de comunicații electronice accesibile publicului pentru a fi transmise eventual autorităților competente în scopul combaterii infracțiunilor grave, cum ar fi criminalitatea organizată și terorismul. Deși s-a constatat că acest scop răspunde efectiv unui obiectiv de interes general, modul generalizat în care directiva viza „toate persoanele și toate mijloacele de comunicare electronică, precum și ansamblul datelor de trafic, fără a face vreo diferențiere, limitare sau excepție în funcție de obiectivul combaterii infracțiunilor grave" a fost considerat problematic[297].

În plus, prin utilizarea tehnologiilor speciale de îmbunătățire a confidențialității, uneori se poate evita complet utilizarea datelor cu caracter personal sau se pot aplica măsuri de reducere a posibilității de a asocia datele cu persoana vizată (de exemplu, prin pseudonimizare), ceea ce are ca rezultat o soluție care protejează viața privată. Acest lucru este potrivit în special pentru sistemele de prelucrare mai extinse.

Exemplu: Consiliul local al unui oraș oferă un card inteligent utilizatorilor frecvenți ai sistemului public de transport în schimbul unei taxe. Cardul poartă numele utilizatorului în formă scrisă pe suprafața sa și, de asemenea, în format electronic, în cip. Ori de câte ori persoana folosește autobuzul sau tramvaiul, cardul inteligent trebuie validat cu ajutorul dispozitivelor de citire instalate, de exemplu, în autobuze și tramvaie. Datele citite de dispozitiv sunt comparate electronic cu o bază de date care conține numele persoanelor care au cumpărat cardul de călătorie.

Acest sistem nu respectă în mod optim principiul reducerii la minimum a datelor, întrucât verificarea aspectului dacă o persoană are permisiunea de a utiliza mijloacele de transport se poate realiza fără compararea datelor

296 Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții* și *Kärntner Landesregierung și alții*.

297 *Ibidem*, punctele 44 și 57.

cu caracter personal de pe cipul cardului cu baza de date. Ar fi suficient, de exemplu, ca cipul cardului să conțină o imagine electronică specială, cum ar fi un cod de bare, care, la validarea cu ajutorul dispozitivului de citire, ar confirma valabilitatea cardului. Un astfel de sistem nu înregistrează cine, când și ce mijloc de transport a folosit. Aceasta ar fi soluția optimă în sensul principiului reducerii la minimum a datelor, întrucât acest principiu are ca rezultat obligația de a reduce la minimum colectarea de date.

Articolul 5 alineatul (1) din Convenția 108 modernizată conține o cerință de proporționalitate pentru prelucrarea datelor cu caracter personal în raport cu scopul legitim urmărit. Trebuie să existe un echilibru echitabil între toate interesele vizate în toate etapele prelucrării. Aceasta înseamnă că „[d]atele cu caracter personal care sunt adecvate și relevante, dar care ar implica o ingerință disproporționată în drepturile și libertățile fundamentale în cauză, ar trebui să fie considerate excesive”[298].

3.4. Principiul exactității datelor

Principalele elemente

- Operatorul trebuie să pună în aplicare principiul exactității datelor în cadrul tuturor operațiunilor de prelucrare.
- Datele inexacte trebuie să fie șterse sau rectificate fără întârziere.
- Este posibil să fie necesar ca datele să fie verificate periodic și actualizate pentru a se asigura exactitatea acestora.

Un operator care deține informații cu caracter personal nu utilizează aceste informații fără a lua măsuri pentru a se asigura cu suficientă certitudine că datele sunt exacte și actualizate[299].

Obligația de a asigura exactitatea datelor trebuie analizată în contextul scopului prelucrării datelor.

298 Raport explicativ privind Convenția 108 modernizată, punctul 52; Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (c).

299 Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (d); Convenția 108 modernizată, articolul 5 alineatul (4) litera (d).

Exemplu: În cauza *Rijkeboer*[300], CJUE a examinat solicitarea unui cetățean neerlandez de a primi de la administrația locală din orașul Amsterdam informații cu privire la identitatea persoanelor cărora le-au fost comunicate evidențele despre el deținute de autoritatea locală în cei doi ani anteriori, precum și cu privire la conținutul datelor divulgate. CJUE a stabilit că „[dreptul] la respectarea vieții private presupune ca persoana vizată să poată să se asigure că datele sale cu caracter personal sunt prelucrate în mod exact și legal, cu alte cuvinte, în special, că datele de bază care o privesc sunt exacte și sunt adresate unor destinatari autorizați". În continuare, CJUE a făcut trimitere la preambulul Directivei privind protecția datelor, care prevede că persoanele vizate trebuie să poată beneficia de dreptul de acces la datele lor cu caracter personal, pentru a se asigura de exactitatea datelor[301].

Pot exista și cazuri în care actualizarea datelor stocate este interzisă prin lege, întrucât scopul stocării datelor este, în principal, acela de a consemna evenimente sub forma unor „instantanee istorice".

Exemplu: Dosarul medical aferent unei intervenții chirurgicale nu trebuie modificat sau, cu alte cuvinte, „actualizat", chiar dacă ulterior se dovedește că unele observații menționate în dosar au fost greșite. În astfel de situații, pot fi făcute numai completări la observațiile din dosar, atât timp cât acestea sunt marcate în mod clar ca fiind contribuții adăugate ulterior.

Pe de altă parte, există situații în care verificarea periodică a exactității datelor, inclusiv actualizarea, constituie o necesitate absolută, date fiind daunele potențiale care pot fi cauzate persoanei vizate în cazul în care datele ar rămâne inexacte.

Exemplu: Dacă o persoană dorește să încheie un contract de creditare cu o instituție bancară, banca va verifica în mod normal bonitatea potențialului client. În acest sens există baze de date speciale, care conțin date privind istoricul creditării persoanelor fizice. Dacă o astfel de bază de date furnizează date incorecte sau perimate cu privire la o persoană, această persoană se

300 Hotărârea CJUE din 7 mai 2009 în cauza C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*.

301 Directiva 95/46/CE (abrogată), considerentul 41.

poate confrunta cu efecte negative. Prin urmare, operatorii unor astfel de baze de date trebuie să depună eforturi deosebite pentru a respecta principiul exactității datelor.

3.5. Principiul limitărilor legate de stocare

Principalele elemente

- Principiul limitărilor legate de stocare implică eliminarea sau anonimizarea datelor imediat ce acestea nu mai servesc scopurilor pentru care au fost colectate.

Articolul 5 alineatul (1) litera (e) din RGPD și, de asemenea, articolul 5 alineatul (4) litera (e) din Convenția 108 modernizată impune ca datele cu caracter personal să fie „păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele". Prin urmare, datele trebuie șterse sau anonimizate după atingerea acestor scopuri. În acest scop, „ar trebui să se stabilească de către operator termene pentru ștergere sau revizuirea periodică" pentru a asigura faptul că datele nu sunt păstrate mai mult decât este necesar[302].

În cauza *S. și Marper*, CEDO a concluzionat că principiile fundamentale ale instrumentelor relevante ale Consiliului Europei, precum și dreptul și practica celorlalte părți contractante impun ca durata de păstrare a datelor să fie proporțională cu scopul colectării și limitată, în special în sectorul polițienesc[303].

Exemplu: În cauza *S. și Marper*[304], CEDO a statuat că păstrarea pe durată nedeterminată a amprentelor digitale, a probelor celulare și a profilurilor ADN ale celor doi reclamanți a fost disproporționată și nenecesară într-o societate democratică, având în vedere că procedurile penale împotriva celor doi reclamanți se încheiaseră prin achitare, respectiv suspendare.

302 Regulamentul general privind protecția datelor, considerentul 39.

303 Hotărârea CEDO [MC] din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04; vezi, de asemenea, de exemplu, Hotărârea CEDO din 13 noiembrie 2012 în cauza *M. M./Regatul Unit*, nr. 24029/07.

304 Hotărârea CEDO [MC] din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04.

Limitarea duratei de stocare a datelor cu caracter personal se aplică numai datelor păstrate într-o formă care permite identificarea persoanelor vizate. Prin urmare, stocarea legală a datelor care nu mai sunt necesare se poate realiza prin anonimizarea acestora.

Datele arhivate în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice pot fi păstrate pe perioade mai lungi, cu condiția ca respectivele date să fie utilizate exclusiv în aceste scopuri[305]. Trebuie să se pună în aplicare măsuri de ordin tehnic și organizatoric adecvate pentru stocarea și utilizarea continuă a datelor cu caracter personal în vederea garantării drepturilor și libertăților persoanei vizate.

Convenția 108 modernizată permite, de asemenea, excepții de la principiul limitărilor legate de stocare, cu condiția ca aceste excepții să fie prevăzute de lege, să respecte substanța drepturilor și libertăților fundamentale și să fie necesare și proporționale din perspectiva atingerii unui număr limitat de obiective legitime[306]. Aceste obiective includ, printre altele, apărarea securității naționale, investigarea și urmărirea penală a infracțiunilor, executarea sancțiunilor penale, protejarea persoanei vizate și protejarea drepturilor și libertăților fundamentale ale celorlalți.

Exemplu: În cauza *Digital Rights Ireland*[307], CJUE a examinat valabilitatea Directivei privind păstrarea datelor, care urmărea armonizarea dispozițiilor naționale privind păstrarea datelor cu caracter personal generate sau prelucrate de către serviciile sau rețelele de comunicații electronice accesibile publicului în scopul combaterii infracțiunilor grave, cum ar fi criminalitatea organizată și terorismul. Directiva privind păstrarea datelor a impus o perioadă de păstrare a datelor de „cel puțin șase luni, fără a se face vreo distincție între categoriile de date prevăzute la articolul 5 din această directivă în funcție de utilitatea lor eventuală în scopul realizării obiectivului urmărit sau în funcție de persoanele vizate”[308]. CJUE a menționat, de asemenea, problema absenței criteriilor obiective în Directiva privind păstrarea datelor,

305 Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (e); Convenția 108 modernizată, articolul 5 alineatul (4) litera (b) și articolul 11 alineatul (2).

306 Convenția 108 modernizată, articolul 11 alineatul (1); Raportul explicativ privind Convenția 108 modernizată, punctele 91-98.

307 Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții* și *Kärntner Landesregierung și alții*.

308 *Ibidem*, punctul 63.

pe baza cărora ar trebui stabilită perioada exactă de păstrare a datelor – care poate varia de la minimum șase luni până la maximum 24 de luni – pentru a se asigura faptul că această perioadă este limitată la strictul necesar[309].

3.6. Principiul securității datelor

Principalele elemente

- Securitatea și confidențialitatea datelor cu caracter personal sunt esențiale pentru prevenirea efectelor negative asupra persoanei vizate.
- Măsurile de securitate pot fi de natură tehnică și/sau organizatorică.
- Pseudonimizarea este un proces care poate proteja datele cu caracter personal.
- Adecvarea măsurilor de securitate trebuie să fie stabilită de la caz la caz și revizuită periodic.

Principiul securității datelor implică punerea în aplicare, în cadrul prelucrării datelor cu caracter personal, a măsurilor tehnice sau organizatorice adecvate pentru a asigura protecția datelor împotriva accesului, utilizării, modificării, divulgării, pierderii, distrugerii sau deteriorării accidentale, neautorizate sau ilegale[310]. RGPD prevede că operatorul și persoana împuternicită de acesta ar trebui să țină seama, la punerea în aplicare a acestor măsuri, de „stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice”[311]. În funcție de circumstanțele specifice ale fiecărui caz, măsurile tehnice și organizatorice adecvate ar putea include, de exemplu, pseudonimizarea și criptarea datelor cu caracter personal și/sau testarea și evaluarea periodică a eficacității măsurilor, pentru a asigura faptul că prelucrarea datelor se face în condiții de siguranță[312].

309 *Ibidem*, punctul 64.

310 Regulamentul general privind protecția datelor, considerentul 39 și articolul 5 alineatul (1) litera (f); Convenția 108 modernizată, articolul 7.

311 Regulamentul general privind protecția datelor, articolul 32 alineatul (1).

312 *Ibidem*.

Astfel cum se explică în secțiunea 2.1.1, pseudonimizarea datelor înseamnă înlocuirea cu un pseudonim a acelor atribute conținute în datele cu caracter personal care permit identificarea persoanei vizate și păstrarea acestor atribute separat de date, prin intermediul unor măsuri tehnice sau organizatorice. Procesul de pseudonimizare nu trebuie confundat cu cel de anonimizare, prin care se distrug toate legăturile care ar permite identificarea persoanei vizate.

Exemplu: Propoziția „Charles Spencer, născut la 3 aprilie 1967, este tatăl a patru copii, doi băieți și două fete" poate fi, de exemplu, pseudonimizată după cum urmează:

„C. S. 1967 este tatăl a patru copii, doi băieți și două fete"; sau

„324 este tatăl a patru copii, doi băieți și două fete"; sau

„YESz3201 este tatăl a patru copii, doi băieți și două fete".

Utilizatorii care au acces la datele pseudonimizate nu vor putea, în mod normal, să îl identifice pe „Charles Spencer, născut la 3 aprilie 1967" din „324" sau „YESz3201". Prin urmare, aceste date sunt mai bine protejate împotriva utilizării incorecte.

Primul exemplu este însă mai puțin sigur. Dacă propoziția „C. S. 1967 este tatăl a patru copii, doi băieți și două fete" este utilizată în localitatea de domiciliu a lui Charles Spencer, un sat mic, domnul Spencer poate fi recunoscut cu ușurință. Metoda de pseudonimizare poate afecta eficacitatea protecției datelor.

Datele cu caracter personal care au atribute criptate sau păstrate separat sunt utilizate în multe situații ca mijloc de păstrare a secretului identității persoanelor. Acest lucru este foarte util atunci când operatorii de date trebuie să se asigure că lucrează cu aceleași persoane vizate, însă nu au nevoie, sau ar trebui să nu aibă nevoie, să cunoască identitatea reală a persoanelor vizate. Acest lucru este valabil, de exemplu, atunci când un cercetător studiază evoluția unei boli la pacienți a căror identitate este cunoscută numai de spitalul la care aceștia sunt tratați și de la care cercetătorul obține antecedentele pseudonimizate. Prin urmare, pseudonimizarea este o verigă puternică în cadrul arsenalului tehnologiei de îmbunătățire a confidențialității. Poate funcționa ca element important în aplicarea principiilor referitoare la protejarea vieții private din faza de proiectare. Aceasta înseamnă că protecția datelor este integrată în structura sistemelor de prelucrare a datelor.

Articolul 25 din RGPD, care abordează protecția datelor din faza de proiectare, menționează în mod explicit pseudonimizarea ca exemplu de măsură tehnică și organizatorică adecvată pe care trebuie să o aplice operatorii pentru a respecta principiile protecției datelor și pentru a integra garanțiile necesare. Datorită acestei măsuri, operatorii vor îndeplini cerințele regulamentului și vor proteja drepturile persoanelor vizate atunci când prelucrează datele cu caracter personal ale acestora.

Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate contribui la demonstrarea îndeplinirii cerinței de securitate a prelucrării[313]. În Avizul privind implicațiile prelucrării datelor din registrele cu numele pasagerilor asupra protecției datelor, Consiliul Europei oferă alte exemple de măsuri de securitate adecvate pentru protecția datelor cu caracter personal în sistemele de registre cu numele pasagerilor. Acestea includ stocarea datelor într-un mediu fizic securizat, controlul și limitarea accesului prin nivel stratificat de coduri de acces și protejarea comunicării datelor printr-o criptografie puternică[314].

Exemplu: Site-urile de socializare în rețea și furnizorii de servicii e-mail permit utilizatorilor să adauge un nivel suplimentar de securitate a datelor la serviciile furnizate, prin introducerea autentificării pe două niveluri. Pe lângă introducerea unei parole personale, utilizatorii trebuie să parcurgă o etapă suplimentară de conectare pentru a intra în contul personal. Aceasta ar putea consta, de exemplu, în introducerea unui cod de securitate trimis către numărul de telefon mobil asociat contului personal. Astfel, verificarea în două etape oferă o protecție superioară a informațiilor cu caracter personal împotriva accesului neautorizat la conturile personale prin spargerea de parole.

Raportul explicativ privind Convenția 108 modernizată oferă exemple suplimentare de măsuri de protecție adecvate, cum ar fi punerea în aplicare a obligației de păstrare a secretului profesional sau adoptarea unor măsuri tehnice de securitate calificate, cum ar fi criptarea datelor[315]. La punerea în aplicare a unor măsuri de securitate specifice, operatorul – sau, după caz, persoana împuternicită de acesta – trebuie să ia în considerare mai multe elemente, cum ar fi natura și volumul datelor cu caracter personal prelucrate, posibilele consecințe negative asupra persoanelor vizate

313 *Ibidem*, articolul 32 alineatul (3).

314 *Avizul din 19 august 2016 al Comitetului Convenției 108 a Consiliului Europei privind implicațiile prelucrării datelor din registrele cu numele pasagerilor asupra protecției datelor*, T-PD(2016)18rev, p. 9.

315 Raportul explicativ privind Convenția 108 modernizată, punctul 56.

și necesitatea restricționării accesului la date[316]. La punerea în aplicare a măsurilor de securitate adecvate, trebuie să se țină seama de stadiul actual al tehnologiei în materie de metode și tehnici de securitate a datelor utilizate în domeniul prelucrării datelor. Costul acestor măsuri trebuie să fie proporțional cu gravitatea și probabilitatea riscurilor potențiale. Este necesară o revizuire periodică a măsurilor de securitate, astfel încât acestea să poată fi actualizate atunci când este necesar[317].

În cazurile în care are loc o încălcare a securității datelor cu caracter personal, atât Convenția 108 modernizată, cât și RGPD impun operatorului să comunice autorității de supraveghere competente, fără întârzieri nejustificate, faptul că a avut loc o încălcare care generează riscuri pentru drepturile și libertățile persoanelor[318]. Se prevede o obligație similară de comunicare, către persoana vizată, în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile respectivei persoane[319]. Comunicarea acestor încălcări persoanelor vizate trebuie să folosească un limbaj clar și simplu[320]. Dacă persoana împuternicită de operator ia cunoștință de o încălcare a securității datelor cu caracter personal, trebuie să informeze imediat operatorul[321]. În anumite situații, se pot aplica excepții de la obligația de notificare. De exemplu, operatorul nu are obligația de a anunța autoritatea de supraveghere atunci când „[încălcarea securității datelor cu caracter personal nu] este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice”[322]. De asemenea, informarea persoanei vizate nu este necesară în cazul în care măsurile de securitate puse în aplicare asigură faptul că datele devin neinteligibile pentru persoanele neautorizate sau dacă măsurile ulterioare garantează că riscul ridicat nu mai este susceptibil să se materializeze[323]. În cazul în care informarea persoanelor vizate cu privire la o încălcare a securității datelor cu caracter personal ar implica eforturi disproporționate din partea operatorului, o informare publică sau o măsură similară poate asigura faptul că „persoanele vizate sunt informate într-un mod la fel de eficace[324]”.

316 *Ibidem*, punctul 62.

317 *Ibidem*, punctul 63.

318 Convenția 108 modernizată, articolul 7 alineatul (2); Regulamentul general privind protecția datelor, articolul 33 alineatul (1).

319 Convenția 108 modernizată, articolul 7 alineatul (2); Regulamentul general privind protecția datelor, articolul 34 alineatul (1).

320 Regulamentul general privind protecția datelor, articolul 34 alineatul (2).

321 *Ibidem*, articolul 33 alineatul (1).

322 *Ibidem*.

323 *Ibidem*, articolul 34 alineatul (3) literele (a) și (b).

324 *Ibidem*, articolul 34 alineatul (3) litera (c).

3.7. Principiul responsabilității

Principalele elemente

- Responsabilitatea impune operatorilor și persoanelor împuternicite de aceștia să pună în aplicare în mod activ și constant măsuri de promovare și de asigurare a protecției datelor în activitățile lor de prelucrare.
- Operatorii și persoanele împuternicite de aceștia sunt responsabili pentru conformitatea operațiunilor de prelucrare pe care le desfășoară cu legislația în materie de protecție a datelor și pentru respectarea obligațiilor aferente.
- Operatorii trebuie să fie în măsură să demonstreze în orice moment persoanelor vizate, publicului larg și autorităților de supraveghere că respectă dispozițiile privind protecția datelor. Persoanele împuternicite de operatori trebuie, de asemenea, să respecte anumite obligații legate strict de responsabilitate (cum ar fi păstrarea unei evidențe a operațiunilor de prelucrare și numirea unui responsabil cu protecția datelor).

RGPD și Convenția 108 modernizată prevăd că operatorul este responsabil pentru respectarea principiilor de prelucrare a datelor cu caracter personal descrise în prezentul capitol și trebuie să o poată demonstra[325]. În acest scop, operatorul trebuie să pună în aplicare măsuri tehnice și organizatorice adecvate[326]. Deși principiul responsabilității prevăzut la articolul 5 alineatul (2) din RGPD privește doar operatorii, se așteaptă proceduri responsabile și din partea persoanelor împuternicite de operatori, având în vedere diversele obligații ale acestora și faptul că au o legătură strânsă cu responsabilitatea.

Legislația UE și a CoE în materie de protecție a datelor stabilește, de asemenea, că operatorul este responsabil pentru respectarea principiilor de protecție a datelor discutate în secțiunile 3.1-3.6 și trebuie să o poată asigura[327]. Grupul de lucru „Articolul 29" subliniază că „tipul de proceduri și mecanisme variază în funcție de riscurile reprezentate de prelucrare și de natura datelor"[328].

325 *Ibidem*, articolul 5 alineatul (2); Convenția 108 modernizată, articolul 10 alineatul (1).

326 Regulamentul general privind protecția datelor, articolul 24.

327 *Ibidem*, articolul 5 alineatul (2); Convenția 108 modernizată, articolul 10 alineatul (1).

328 Avizul 3/2010 din 13 iulie 2010 al Grupului de lucru „Articolul 29" privind principiul responsabilității, WP 173, Bruxelles, punctul 12.

Operatorii pot asigura respectarea acestei cerințe în diverse moduri, printre care:

- păstrarea unor evidențe cu activitățile de prelucrare și punerea acestora la dispoziția autorității de supraveghere, la cererea acesteia[329];
- în anumite situații, desemnarea unui responsabil cu protecția datelor care să fie implicat în toate aspectele legate de protecția datelor cu caracter personal[330];
- efectuarea unor evaluări ale impactului asupra protecției datelor pentru tipurile de prelucrare care ar putea genera un risc ridicat pentru drepturile și libertățile persoanelor fizice[331];
- asigurarea protecției datelor din faza de proiectare și a protecției implicite a datelor[332];
- punerea în aplicare a unor metode și proceduri prin care persoanele vizate să își poată exercita drepturile[333];
- aderarea la coduri de conduită aprobate sau la mecanisme de certificare aprobate[334].

Deși principiul responsabilității prevăzut la articolul 5 alineatul (2) din RGPD nu se referă în mod specific la persoanele împuternicite de operatori, există dispoziții legate de responsabilitate care conțin, de asemenea, obligații pentru aceste persoane, cum ar fi păstrarea unor evidențe cu activitățile de prelucrare și numirea unui responsabil cu protecția datelor pentru orice activități de prelucrare care necesită un astfel de responsabil[335]. De asemenea, persoanele împuternicite cu prelucrarea trebuie să se asigure că s-au adoptat toate măsurile necesare pentru a asigura securitatea datelor[336]. Contractul obligatoriu din punct de vedere juridic între operator și persoana împuternicită de acesta trebuie să stabilească faptul că operatorul

329 Regulamentul general privind protecția datelor, articolul 30.

330 *Ibidem*, articolele 37-39.

331 *Ibidem*, articolul 35; Convenția 108 modernizată, articolul 10 alineatul (2).

332 Regulamentul general privind protecția datelor, articolul 25; Convenția 108 modernizată, articolul 10 alineatele (2) și (3).

333 *Ibidem*, articolul 12 și articolul 24.

334 *Ibidem*, articolul 40 și articolul 42.

335 *Ibidem*, articolul 5 alineatul (2), articolele 30 și 37.

336 *Ibidem*, articolul 28 alineatul (3) litera (c).

oferă asistență persoanei numite de el în ceea ce privește o parte dintre cerințele de conformitate, de exemplu efectuarea unei evaluări a impactului asupra protecției datelor sau informarea operatorului cu privire la orice încălcare a securității datelor cu caracter personal imediat ce persoana împuternicită ia cunoștință de aceasta[337].

Organizația pentru Cooperare și Dezvoltare Economică (OCDE) a adoptat în 2013 orientări privind respectarea vieții private, care au subliniat că operatorii joacă un rol important în aplicarea eficientă a protecției datelor în situațiile concrete. Orientările includ un principiu al responsabilității potrivit căruia „un operator de date ar trebui să fie responsabil pentru respectarea măsurilor care pun în aplicare principiile [materiale] menționate anterior"[338].

Exemplu: Un exemplu legislativ care pune în evidență principiul responsabilității este amendamentul din 2009[339] la Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice. Potrivit articolului 4 din versiunea modificată, directiva impune obligația de a „[asigura] punerea în aplicare a unei politici de securitate în ceea ce privește prelucrarea datelor cu caracter personal". Astfel, în ceea ce privește dispozițiile de securitate ale acestei directive, legiuitorul a decis că este necesară introducerea unei cerințe explicite pentru elaborarea și punerea în aplicare a unei politici de securitate.

Potrivit avizului Grupului de lucru „Articolul 29"[340], esența responsabilității constă în următoarele obligații ale operatorului:

- de a pune în aplicare măsuri care – în condiții normale – garantează respectarea normelor de protecție a datelor în contextul operațiunilor de prelucrare;

337 *Ibidem*, articolul 28 alineatul (3) litera (d).

338 Orientările OCDE din 2013 privind reglementarea protecției vieții private și a fluxurilor transfrontaliere de date cu caracter personal, articolul 14.

339 Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului, JO 2009 L 337.

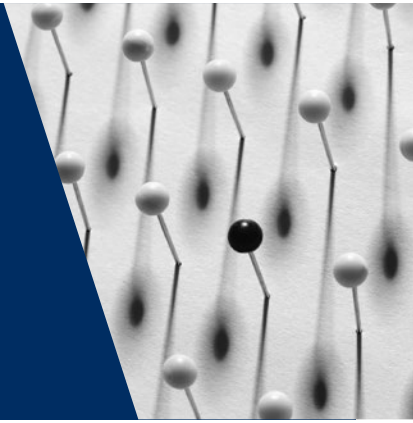
340 *Avizul 3/2010 din 13 iulie 2010 al Grupului de lucru „Articolul 29" privind principiul responsabilității*, WP 173, Bruxelles, 13 iulie 2010.

- de a pregăti documentația care demonstrează persoanelor vizate și autorităților de supraveghere măsurile luate în vederea respectării normelor de protecție a datelor.

Prin urmare, principul responsabilității impune operatorilor obligația de a demonstra în mod activ conformitatea, fără să aștepte ca persoanele vizate sau autoritățile de supraveghere să semnaleze deficiențele.

4

Normele legislației europene în materie de protecție a datelor



UE	Aspecte vizate	CoE
Norme privind prelucrarea legală a datelor		
Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (a) Hotărârea CJUE în cauza C-543/09, *Deutsche Telekom AG/ Bundesrepublik Deutschland*, 2011 Hotărârea CJUE în cauza C-536/15, *Tele2 (Netherlands) BV și alții/ Autoriteit Consument en Markt (ACM)*, 2017	**Consimțământul**	Recomandarea privind crearea de profiluri, articolul 3.4 litera (b) și articolul 3.6 Convenția 108 modernizată, articolul 5 alineatul (2)
Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (b)	**Relația (pre) contractuală**	Recomandarea privind crearea de profiluri, articolul 3.4 litera (b)
Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (c)	**Obligațiile legale ale operatorului**	Recomandarea privind crearea de profiluri, articolul 3.4 litera (a)
Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (d)	**Interesele vitale ale persoanei vizate**	Recomandarea privind crearea de profiluri, articolul 3.4 litera (b)
Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (e) Hotărârea CJUE [MC] în cauza C-524/06, *Huber/Bundesrepublik Deutschland*, 2008	**Interesul public și exercitarea autorității publice**	Recomandarea privind crearea de profiluri, articolul 3.4 litera (b)

UE	Aspecte vizate	CoE
Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (f) Hotărârea CJUE în cauza C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA „Rīgas satiksme”*, 2017 Hotărârea CJUE în cauzele conexate C-468/10 și C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) și Federación de Comercio Electrónico y Marketing Directo (FECEMD)/ Administración del Estado*, 2011	**Interesele legitime ale altora**	Recomandarea privind crearea de profiluri, articolul 3.4 litera (b) Hotărârea CEDO în cauza *Y/Turcia*, nr. 648/10, 2015
Regulamentul general privind protecția datelor, articolul 6 alineatul (4)	**Excepție de la limitările legate de scop: prelucrarea ulterioară în alte scopuri**	Convenția 108 modernizată, articolul 5 alineatul (4) litera (b)
Norme privind prelucrarea legală a datelor sensibile		
Regulamentul general privind protecția datelor, articolul 9 alineatul (1)	**Interdicție generală de prelucrare**	Convenția 108 modernizată, articolul 6
Regulamentul general privind protecția datelor, articolul 9 alineatul (2)	**Excepțări de la interdicția generală**	Convenția 108 modernizată, articolul 6
Norme privind prelucrarea securizată		
Regulamentul general privind protecția datelor, articolul 32	**Obligația de a asigura prelucrarea securizată**	Convenția 108 modernizată, articolul 7 alineatul (1) Hotărârea CEDO în cauza *I/Finlanda*, nr. 20511/03, 2008
Regulamentul general privind protecția datelor, articolul 28 și articolul 32 alineatul (1) litera (b)	**Obligația de confidențialitate**	Convenția 108 modernizată, articolul 7 alineatul (1)
Regulamentul general privind protecția datelor, articolul 34 Directiva asupra confidențialității și comunicațiilor electronice, articolul 4 alineatul (2)	**Notificările privind încălcarea securității datelor**	Convenția 108 modernizată, articolul 7 alineatul (2)
Norme privind responsabilitatea și promovarea conformității		
Regulamentul general privind protecția datelor, articolele 12, 13 și 14	**Generalități privind transparența**	Convenția 108 modernizată, articolul 8

UE	Aspecte vizate	CoE
Regulamentul general privind protecția datelor, articolele 37, 38 și 39	**Responsabilii cu protecția datelor**	Convenția 108 modernizată, articolul 10 alineatul (1)
Regulamentul general privind protecția datelor, articolul 30	**Evidențele activităților de prelucrare**	
Regulamentul general privind protecția datelor, articolele 35 și 36	**Evaluarea impactului asupra protecției datelor și consultarea prealabilă**	Convenția 108 modernizată, articolul 10 alineatul (2)
Regulamentul general privind protecția datelor, articolele 33 și 34	**Notificările privind încălcarea securității datelor**	Convenția 108 modernizată, articolul 7 alineatul (2)
Regulamentul general privind protecția datelor, articolele 40 și 41	**Coduri de conduită**	
Regulamentul general privind protecția datelor, articolele 42 și 43	**Certificarea**	
Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit		
Regulamentul general privind protecția datelor, articolul 25 alineatul (1)	**Protecția datelor începând cu momentul conceperii**	Convenția 108 modernizată, articolul 10 alineatul (2)
Regulamentul general privind protecția datelor, articolul 25 alineatul (2)	**Protecția implicită a datelor**	Convenția 108 modernizată, articolul 10 alineatul (3)

Principiile au, în mod necesar, caracter general. Aplicarea lor în situații concrete lasă o anumită marjă de interpretare și de alegere a mijloacelor. În cadrul **legislației CoE**, este la latitudinea părților la Convenția 108 modernizată să clarifice această marjă de interpretare în dreptul intern. Situația în **legislația UE** este diferită: pentru stabilirea protecției datelor în cadrul pieței interne, s-a considerat necesară instituirea unor norme mai detaliate la nivelul Uniunii pentru armonizarea nivelului de protecție a datelor din cadrul legislațiilor naționale ale statelor membre. Regulamentul general privind protecția datelor stabilește un nivel de norme detaliate, în conformitate cu principiile enunțate la articolul 5, care sunt direct aplicabile în ordinea juridică națională. Prin urmare, observațiile privind normele detaliate de protecție a datelor la nivel european prezentate în continuare privesc în principal dreptul UE.

4.1. Normele privind prelucrarea legală

Principalele elemente

- Datele cu caracter personal pot fi prelucrate în mod legal dacă îndeplinesc unul dintre următoarele criterii:
  - prelucrarea se bazează pe consimțământul persoanei vizate;
  - o relație contractuală necesită prelucrarea datelor cu caracter personal;
  - prelucrarea este necesară pentru respectarea unei obligații legale a operatorului;
  - interesele vitale ale persoanelor vizate sau ale altei persoane necesită prelucrarea datelor lor;
  - prelucrarea este necesară pentru îndeplinirea unei sarcini de interes public;
  - interesele legitime ale operatorilor sau ale unor părți terțe constituie motivul prelucrării, însă numai în măsura în care nu prevalează asupra lor interesele sau drepturile fundamentale ale persoanelor vizate.
- Prelucrarea legală a datelor cu caracter personal sensibile face obiectul unui regim special, mai strict.

4.1.1. Temeiuri juridice pentru prelucrarea datelor

Capitolul II din Regulamentul general privind protecția datelor, intitulat „Principii", prevede că orice prelucrare a unor date cu caracter personal trebuie să respecte, în primul rând, principiile referitoare la calitatea datelor prevăzute la articolul 5 din RGPD. Unul dintre principii este că datele cu caracter personal trebuie să fie „prelucrate în mod legal, echitabil și transparent". În al doilea rând, pentru ca datele să fie prelucrate în mod legal, prelucrarea trebuie să respecte unul dintre temeiurile juridice care asigură legitimitatea prelucrării datelor, enumerate la articolul 6[341] în ceea ce privește datele cu caracter personal nesensibile, respectiv la articolul 9 în ceea ce privește categoriile speciale de date (sau datele sensibile). În mod similar, capitolul II

341 Hotărârea CJUE din 20 mai 2003 în cauzele conexate C-465/00, C-138/01 și C-139/01, *Rechnungshof/Österreichischer Rundfunk și alții și Christa Neukomm și Joseph Lauermann/Österreichischer Rundfunk*, punctul 65; Hotărârea CJUE [MC] din 16 decembrie 2008 în cauza C-524/06, *Heinz Huber/Bundesrepublik Deutschland*, punctul 48; Hotărârea CJUE din 24 noiembrie 2011 în cauzele conexate C-468/10 și C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) și Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, punctul 26.

din Convenția 108 modernizată, care prevede „principiile de bază ale protecției datelor cu caracter personal", stabilește că, pentru a fi legală, prelucrarea datelor trebuie să fie „proporțională cu scopul legitim urmărit".

Indiferent de temeiul juridic al prelucrării pe care se bazează un operator pentru a iniția o operațiune de prelucrare a datelor cu caracter personal, operatorul va trebui, de asemenea, să aplice garanțiile prevăzute în regimul legislativ general de protecție a datelor.

Consimțământul

În cadrul legislației CoE, consimțământul este menționat la articolul 5 alineatul (2) din Convenția 108 modernizată. De asemenea, se face trimitere la el în jurisprudența CEDO și în mai multe recomandări ale CoE[342]. **În dreptul UE**, consimțământul ca bază a prelucrării legale a datelor este stabilit în mod ferm la articolul 6 din RGPD și este menționat, de asemenea, în mod explicit la articolul 8 din Cartă. Caracteristicile consimțământului valabil sunt explicate în definiția consimțământului de la articolul 4, condițiile pentru obținerea consimțământului valabil sunt detaliate la articolul 7, iar normele speciale privind consimțământul copiilor în legătură cu serviciile societății informaționale sunt stabilite la articolul 8 din RGPD.

Astfel cum se explică în secțiunea 2.4, consimțământul trebuie să fie acordat în cunoștință de cauză, în mod liber, specific și lipsit de ambiguitate. Consimțământul trebuie să constea într-o declarație sau o acțiune fără echivoc, prin care se dă acordul cu privire la prelucrare, iar persoana vizată are dreptul să își retragă consimțământul în orice moment. Operatorii au datoria de a păstra o evidență verificabilă a consimțământului.

Consimțământul liber exprimat

În cadrul **CoE** al Convenției 108 modernizate, consimțământul persoanei vizate trebuie să „reprezinte manifestarea liberă a unei alegeri voluntare"[343]. Existența consimțământului liber exprimat este valabilă numai „în cazul în care persoana vizată își poate exercita cu adevărat libertatea de alegere și nu există niciun risc de înșelăciune, intimidare, constrângere sau consecințe negative semnificative dacă nu

342 Vezi, de exemplu, Recomandarea CM/Rec(2010)13 din 23 noiembrie 2010 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal în contextul creării de profiluri, articolul 3.4 litera (b).

343 Raportul explicativ privind Convenția 108 modernizată, punctul 42.

își acordă consimțământul"[344]. În acest sens, **dreptul UE** prevede că consimțământul nu este considerat liber dacă „persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată"[345]. RGPD subliniază că „[a]tunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract"[346]. Raportul explicativ privind Convenția 108 modernizată prevede că „[p]ersoana vizată nu trebuie să fie supusă niciunei presiuni sau influențe nejustificate (care poate fi de natură economică sau de altă natură), directă sau indirectă, iar consimțământul nu trebuie considerat ca fiind acordat în mod liber în cazul în care persoana vizată nu are o libertate de alegere reală sau nu poate să refuze sau să își retragă consimțământul fără a fi prejudiciată"[347].

Exemplu: Unele municipalități din statul A au decis să emită carduri de rezidență cu un cip încorporat. Nu este obligatoriu ca locuitorii să achiziționeze aceste carduri electronice. Cu toate acestea, locuitorii care nu posedă cardul nu au acces la o serie de servicii administrative importante, cum ar fi posibilitatea de a plăti online taxele locale, de a depune plângeri în format electronic, la care autoritatea se angajează să răspundă în termen de trei zile, și chiar să evite cozile, să cumpere bilete la preț redus pentru evenimentele din sala de concerte a orașului și să folosească scanerele de la intrare.

Prelucrarea de către municipalitate a datelor cu caracter personal în acest exemplu nu se poate baza pe consimțământ. Întrucât există cel puțin o presiune indirectă asupra locuitorilor de a obține cardul electronic și de a-și da acordul cu privire la prelucrarea datelor, consimțământul nu este acordat în mod liber. Prin urmare, instituirea de către municipalitate a unui sistem de carduri electronice trebuie să se bazeze pe un alt temei juridic care să justifice prelucrarea. De exemplu, aceasta ar putea invoca faptul că prelucrarea

344 Vezi, de asemenea, Avizul 15/2011 din 13 iulie 2011 al Grupului de lucru „Articolul 29" privind conceptul de consimțământ, WP 187, Bruxelles, 13 iulie 2011, p. 12.

345 Regulamentul general privind protecția datelor, considerentul 42.

346 *Ibidem*, articolul 7 alineatul (4).

347 Raportul explicativ privind Convenția 108 modernizată, punctul 42.

este necesară pentru îndeplinirea unei sarcini care servește unui interes public, ceea ce constituie un temei legal pentru prelucrare în conformitate cu articolul 6 alineatul (1) litera (e) din RGPD[348].

Acordarea liberă a consimțământului poate fi, de asemenea, pusă la îndoială în situații de subordonare, dacă există un dezechilibru semnificativ, economic sau de altă natură, între operatorul care solicită consimțământul și persoana vizată care îl acordă[349]. Un exemplu tipic pentru astfel de dezechilibre și relații de subordonare este prelucrarea de către angajator a datelor cu caracter personal în contextul unui raport de muncă. Potrivit Grupului de lucru „Articolul 29", „[a]ngajații nu sunt aproape niciodată în situația de a acorda în mod liber, de a refuza sau de a-și retrage consimțământul, dată fiind dependența care rezultă din relația angajator/angajat. Având în vedere dezechilibrul de putere, angajații își pot acorda în mod liber consimțământul numai în circumstanțe excepționale, atunci când acceptarea sau respingerea unei oferte nu are nicio consecință"[350].

Exemplu: O întreprindere mare intenționează să creeze un repertoriu cu numele tuturor angajaților, funcția acestora în cadrul întreprinderii și adresele profesionale, exclusiv în scopul de a îmbunătăți comunicarea internă la nivelul întreprinderii. Șeful de personal propune adăugarea fotografiei fiecărui angajat în repertoriu, pentru a facilita recunoașterea colegilor la ședințe. Reprezentanții angajaților solicită ca adăugarea fotografiei să se facă doar cu consimțământul angajatului.

348 Avizul 15/2011 din 13 iulie 2011 al Grupului de lucru „Articolul 29" privind conceptul de consimțământ, WP 187, Bruxelles, 13 iulie 2011, p. 16. Alte exemple de cazuri în care prelucrarea datelor nu se poate baza pe consimțământ, ci necesită un alt temei juridic pentru legitimarea prelucrării, pot fi găsite la paginile 14 și 17 din aviz.

349 Vezi, de asemenea, Avizul 8/2001 din 13 septembrie 2001 al Grupului de lucru „Articolul 29" privind prelucrarea datelor cu caracter personal în contextul ocupării forței de muncă, WP 48, Bruxelles; Documentul de lucru din 25 noiembrie 2005 al Grupului de lucru „Articolul 29" privind interpretarea comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995, WP 114, Bruxelles; Avizul 2/2017 din 8 iunie 2017 al Grupului de lucru „Articolul 29" privind prelucrarea datelor la locul de muncă, WP 249, Bruxelles.

350 Avizul 2/2017 din 8 iunie 2017 al Grupului de lucru „Articolul 29" privind prelucrarea datelor la locul de muncă, WP 249, Bruxelles, 8 iunie 2017.

Într-o astfel de situație, consimțământul unui angajat trebuie să fie recunoscut drept temei juridic al prelucrării fotografiilor din repertoriu, deoarece este credibil că angajatul nu va avea de suferit nicio consecință, indiferent dacă decide să își dea acordul sau nu pentru publicarea fotografiei sale în repertoriu.

Exemplu: Întreprinderea A planifică o ședință cu trei dintre angajații săi și directorii întreprinderii B, pentru a discuta posibilitatea cooperării la un proiect. Întâlnirea va avea loc la sediul întreprinderii B, care solicită întreprinderii A să transmită prin e-mail numele, CV-urile și fotografiile participanților la întâlnire. Întreprinderea B susține că are nevoie de numele și fotografiile participanților pentru ca personalul de securitate de la intrarea în clădire să poată verifica identitatea persoanelor, iar CV-urile vor permite directorilor să se pregătească mai bine pentru întâlnire. În acest caz, transmiterea de către întreprinderea A a datelor cu caracter personal ale angajaților săi nu se poate baza pe consimțământ. Consimțământul nu poate fi considerat ca fiind „acordat în mod liber", deoarece angajații ar putea să se confrunte cu consecințe negative dacă resping oferta (de exemplu, aceștia ar putea fi înlocuiți cu un alt coleg nu doar la ședința respectivă, ci și în relația cu întreprinderea B și în ceea ce privește contribuția la proiect în general). Prin urmare, prelucrarea trebuie să se bazeze pe un alt temei juridic.

Nu înseamnă totuși că consimțământul nu poate fi valabil niciodată în situații în care neacordarea acestuia ar avea consecințe negative. De exemplu, dacă neacordarea consimțământului pentru emiterea unui card de client într-un supermarket are drept singură consecință faptul că nu se va primi o mică reducere de preț pentru anumite produse, consimțământul poate fi un temei juridic valabil pentru prelucrarea datelor cu caracter personal ale acelor clienți care și-au dat consimțământul pentru emiterea unui astfel de card. Nu există nicio subordonare între întreprindere și client, iar consecințele neacordării consimțământului nu sunt suficient de grave pentru a împiedica libertatea de alegere a persoanei vizate (cu condiția ca reducerea prețurilor să fie suficient de mică pentru a nu afecta această libertate de alegere).

În schimb, dacă produsele sau serviciile pot fi obținute numai în cazul în care se divulgă anumite date cu caracter personal operatorului sau, ulterior, unor părți terțe, atunci consimțământul persoanei vizate de a divulga date care nu sunt necesare pentru contract nu poate fi considerat o decizie liberă și, prin urmare, nu constituie

consimțământ valabil în temeiul legislației privind protecția datelor[351]. RGPD este destul de strict în acest sens, interzicând asocierea consimțământului cu furnizarea de produse și servicii[352].

Exemplu: Acordul pasagerilor unei companii aeriene pentru transmiterea așa-numitelor registre cu numele pasagerilor (mai exact, date privind identitatea, preferințele alimentare sau problemele de sănătate ale acestora) către autoritățile în domeniul imigrației dintr-o anumită țară străină nu poate fi considerat consimțământ valabil în temeiul legislației privind protecția datelor, întrucât pasagerii în cauză nu pot exercita altă opțiune dacă doresc să viziteze țara respectivă. Pentru ca aceste date să fie transmise în mod legal, este necesar un alt temei juridic decât consimțământul, cel mai probabil o lege specifică.

Consimțământul în cunoștință de cauză

Persoana vizată trebuie să dețină suficiente informații înainte de a-și exercita opțiunea. Consimțământul în cunoștință de cauză va cuprinde de obicei o descriere precisă și ușor de înțeles a subiectului care necesită acordarea consimțământului. Astfel cum explică Grupul de lucru „Articolul 29", consimțământul trebuie să se bazeze pe aprecierea și înțelegerea faptelor și implicațiilor acțiunii persoanei vizate de a accepta prelucrarea. Prin urmare, „[p]ersoana vizată trebuie să primească informații clare, inteligibile, exacte și complete cu privire la toate aspectele relevante [...], cum ar fi natura datelor prelucrate, scopurile prelucrării, destinatarii posibili ai datelor și drepturile persoanei vizate"[353]. Pentru ca consimțământul să fie în cunoștință de cauză, persoanele vizate trebuie, de asemenea, să fie conștiente de consecințele neacordării consimțământului pentru prelucrare.

Având în vedere importanța consimțământului în cunoștință de cauză, RGPD și Raportul explicativ privind Convenția 108 modernizată au încercat să clarifice această noțiune. În considerentele RGPD se precizează că, pentru ca acordarea consimțământului să fie în cunoștință de cauză, „persoana vizată ar trebui să fie la

351 Regulamentul general privind protecția datelor, articolul 7 alineatul (4).

352 *Ibidem*.

353 Documentul de lucru din 15 februarie 2007 al Grupului de lucru „Articolul 29" privind prelucrarea datelor cu caracter personal medicale din dosarul electronic de sănătate (DES), WP 131, Bruxelles.

curent cel puțin cu identitatea operatorului și cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal"[354].

În cazul excepțional al consimțământului folosit ca derogare pentru a asigura temeiul juridic al unui transfer internațional de date, pentru ca respectivul consimțământ să fie considerat valabil, operatorul trebuie să informeze persoana vizată asupra posibilelor riscuri pe care le poate implica un astfel de transfer ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate[355].

Raportul explicativ privind Convenția 108 modernizată precizează că trebuie să se furnizeze informații cu privire la implicațiile deciziei persoanei vizate, și anume „ce implică acordarea consimțământului și măsura până la care se acordă consimțământul"[356].

Calitatea informațiilor este importantă. Aceasta implică, printre altele, ca limba în care se furnizează informațiile să fie adaptată la beneficiarii previzibili. Informațiile trebuie furnizate fără a folosi jargon, într-un limbaj clar și simplu, pe care un utilizator obișnuit trebuie să fie în măsură să îl înțeleagă[357]. De asemenea, informațiile trebuie să fie ușor accesibile persoanei vizate și pot fi furnizate verbal sau în scris. Accesibilitatea și vizibilitatea informațiilor sunt elemente importante: informațiile trebuie să fie vizibile în mod clar și proeminente. O soluție adecvată pentru mediul online o reprezintă anunțurile stratificate, care permit persoanelor vizate să aleagă dacă doresc accesul la versiuni mai concise sau mai extinse ale informațiilor.

Consimțământul specific

Pentru ca consimțământul să fie valabil, acesta trebuie să fie, de asemenea, specific scopului prelucrării, care trebuie să fie descris în mod clar și neechivoc. Acest lucru este dublat de calitatea informațiilor furnizate cu privire la scopul pentru care se solicită consimțământul. În acest context, sunt relevante așteptările rezonabile ale unei persoane vizate obișnuite. Consimțământul unei persoane vizate trebuie solicitat din nou atunci când se adaugă operațiuni de prelucrare sau operațiunile urmează să fie modificate într-un mod care nu putea fi prevăzut în mod rezonabil

354 Regulamentul general privind protecția datelor, considerentul 42.

355 *Ibidem*, articolul 49 alineatul (1) litera (a).

356 Raportul explicativ privind Convenția 108 modernizată, punctul 42.

357 Avizul 15/2011 din 13 iulie 2011 al Grupului de lucru „Articolul 29" privind definiția consimțământului, WP 187, Bruxelles, p. 19.

în momentul acordării consimțământului inițial și care conduce, astfel, la modificarea scopului. Dacă prelucrarea datelor se face în mai multe scopuri, trebuie solicitat consimțământul pentru toate aceste scopuri[358].

Exemple: În cauza *Deutsche Telekom AG*[359], CJUE a analizat dacă un furnizor de servicii de telecomunicații care a trebuit să transmită datele cu caracter personal ale abonaților în vederea publicării în liste de abonați avea obligația de a reînnoi consimțământul persoanelor vizate[360], întrucât destinatarii datelor nu fuseseră numiți în momentul acordării consimțământului inițial.

CJUE a stabilit că, în temeiul articolului 12 din Directiva asupra confidențialității și comunicațiilor electronice, nu era necesară reînnoirea consimțământului înainte de transmiterea datelor. Dat fiind că persoanele vizate aveau doar opțiunea de a-și da acordul cu privire la scopul prelucrării – și anume publicarea datelor lor – nu puteau alege între diferite liste de abonați în care s-ar fi putut publica aceste date.

Astfel cum a subliniat CJUE, „dintr-o interpretare contextuală și sistematică a articolului 12 din Directiva asupra confidențialității și comunicațiilor electronice reiese că, în temeiul alineatului (2) al acestui articol, consimțământul privește finalitatea publicării datelor cu caracter personal într-o listă publică de abonați, iar nu identitatea furnizorului unei liste de abonați specifice”[361]. În plus, problema nu ar fi identitatea editorului listei, întrucât „însăși publicarea datelor cu caracter personal într-o listă de abonați cu o finalitate specifică se poate dovedi prejudiciabilă pentru un abonat”[362].

358 Regulamentul general privind protecția datelor, considerentul 32.

359 Hotărârea CJUE din 5 mai 2011 în cauza C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*. Vezi, în special, punctele 53 și 54.

360 Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), JO 2002 L 201.

361 Hotărârea CJUE din 5 mai 2011 în cauza C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, punctul 61.

362 *Ibidem*, punctul 62.

Cauza *Tele2 (Țările de Jos) BV, Ziggo BV, Vodafone Libertel BV/Autoriteit Consument en Markt (AMC)*[363] a vizat solicitarea întreprinderii belgiene ca serviciile de informații telefonice și listele de abonați administrate de societățile care alocă numere de telefon în Țările de Jos să îi permită accesul la datele referitoare la abonații acestora. Compania belgiană a invocat o obligație în temeiul Directivei privind serviciul universal[364]. Aceasta impune societăților care alocă numere de telefon să pună numerele la dispoziția serviciilor de informații telefonice care le solicită, în cazul în care abonații și-au dat consimțământul pentru publicarea numerelor lor. Societățile din Țările de Jos au refuzat să facă acest lucru, declarând că nu erau obligate să furnizeze datele în cauză unei întreprinderi stabilite într-un alt stat membru. Acestea au susținut că utilizatorii și-au dat consimțământul pentru publicarea numerelor lor, înțelegând faptul că aceste numere vor fi publicate într-o listă de abonați din Țările de Jos. CJUE a arătat că în domeniul de aplicare al Directivei privind serviciul universal intră toate solicitările societăților care furnizează liste de abonați telefonici, indiferent de statul membru în care sunt stabilite. De asemenea, CJUE a stabilit că transmiterea acelorași date unei alte întreprinderi care intenționează să publice o listă de abonați telefonici fără a obține consimțământul reînnoit al abonaților nu este de natură să afecteze substanțial dreptul la protecția datelor cu caracter personal[365]. În consecință, nu este necesar ca întreprinderea care alocă abonaților săi numere de telefon să includă, în cererea de consimțământ adresată abonatului, informații diferențiate în funcție de statul membru căruia i-ar putea fi trimise datele abonatului în cauză[366].

363 Hotărârea CJUE din 15 martie 2017 în cauza C-536/15, *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV/Autoriteit Consument en Markt (ACM)*.

364 Directiva 2002/22/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile electronice de comunicații (Directiva privind serviciul universal), JO 2002 L 108, p. 51, astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 (Directiva privind serviciul universal), JO 2009 L 337, p. 11.

365 Hotărârea CJUE din 15 martie 2017 în cauza C-536/15, *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV/Autoriteit Consument en Markt (ACM)*, punctul 36.

366 *Ibidem*, punctele 40-41.

Consimțământul lipsit de ambiguitate

Orice consimțământ trebuie acordat într-un mod lipsit de ambiguitate[367]. Aceasta înseamnă că nu trebuie să existe nicio îndoială rezonabilă cu privire la faptul că persoana vizată a dorit să își dea acordul pentru prelucrarea datelor sale. De exemplu, absența unei acțiuni din partea persoanei vizate nu indică un consimțământ lipsit de ambiguitate.

Acest lucru se aplică în cazul în care operatorul obține consimțământul prin intermediul unor declarații incluse în politicile sale de confidențialitate, cum ar fi „prin utilizarea serviciului nostru, sunteți de acord cu prelucrarea datelor dvs. cu caracter personal". În acest caz, operatorii ar trebui să se asigure că utilizatorii își exprimă manual și individual acordul cu privire la politicile în cauză.

În cazul în care consimțământul este acordat într-o formă scrisă care face parte dintr-un contract, consimțământul pentru prelucrarea datelor cu caracter personal trebuie să fie individualizat și, în orice caz, „garanțiile ar trebui să asigure că persoana vizată este conștientă de faptul că și-a dat consimțământul și în ce măsură a făcut acest lucru"[368].

Cerințe privind consimțământul pentru copii

RGPD prevede o protecție specifică pentru copii în contextul furnizării de servicii ale societății informaționale, întrucât aceștia „pot fi mai puțin conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal"[369]. Prin urmare, în conformitate cu **dreptul UE**, atunci când furnizorii de servicii ale societății informaționale prelucrează date cu caracter personal ale unor copii cu vârsta sub 16 ani pe baza consimțământului, această prelucrare va fi legală „numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului"[370]. Statele membre pot prevedea în dreptul intern o vârstă inferioară, dar nu mai mică de 13 ani[371]. Consimțământul titularului răspunderii părintești nu este necesar „în contextul serviciilor

367 Regulamentul general privind protecția datelor, articolul 4 punctul 11.

368 *Ibidem*, considerentul 42.

369 *Ibidem*, considerentul 38.

370 *Ibidem*, articolul 8 alineatul (1) primul paragraf. Noțiunea de servicii ale societății informaționale este definită la articolul 4 punctul 25 din Regulamentul general privind protecția datelor.

371 Regulamentul general privind protecția datelor, articolul 8 alineatul (1) al doilea paragraf.

de prevenire sau consiliere oferite direct copiilor"[372]. Informațiile și comunicările în cazul unei prelucrări adresate unui copil trebuie să utilizeze un limbaj clar și simplu, ușor de înțeles de către copil[373].

Dreptul de a retrage consimțământul în orice moment

RGPD prevede un drept general de retragere a consimțământului în orice moment[374]. Persoana vizată trebuie informată cu privire la acest drept înainte de a-și da consimțământul și poate exercita acest drept după cum consideră de cuviință. Nu ar trebui să existe nicio cerință de justificare a retragerii consimțământului și niciun risc de consecințe negative în afara încetării oricăror beneficii care au rezultat din utilizarea datelor pentru care s-a acordat anterior consimțământul. Retragerea consimțământului ar trebui să se facă la fel de simplu ca acordarea acestuia[375]. Nu se poate vorbi despre un consimțământ acordat în mod liber dacă persoana vizată nu este în măsură să își retragă consimțământul fără a fi prejudiciată sau dacă retragerea consimțământului nu se face la fel de simplu ca acordarea acestuia[376].

Exemplu: Un client este de acord să primească reclame prin poștă la o adresă pe care o oferă unui operator de date. În cazul în care clientul își retrage consimțământul, operatorul trebuie să sisteze imediat trimiterea reclamelor prin poștă. Nu ar trebui impuse niciun fel de consecințe represive, cum ar fi comisioane. Retragerea este exercitată totuși pentru viitor și nu are efect retroactiv. Perioada în care datele cu caracter personal ale clientului au fost prelucrate în mod legal – datorită consimțământului clientului – a fost legitimă. Retragerea consimțământului împiedică orice prelucrare ulterioară a datelor în cauză, cu excepția cazului în care o astfel de prelucrare este în conformitate cu dreptul la ștergerea datelor[377].

372 *Ibidem*, considerentul 38.

373 *Ibidem*, considerentul 58. Vezi, de asemenea, Convenția 108 modernizată, articolul 15 alineatul (2) litera (e). Raportul explicativ privind Convenția 108 modernizată, punctele 68 și 125.

374 Regulamentul general privind protecția datelor, articolul 7 alineatul (3). Raportul explicativ privind Convenția 108 modernizată, punctul 45.

375 Regulamentul general privind protecția datelor, articolul 7 alineatul (3).

376 Regulamentul general privind protecția datelor, considerentul 42; Raportul explicativ privind Convenția 108 modernizată, punctul 42.

377 Regulamentul general privind protecția datelor, articolul 17 alineatul (1) litera (b).

Necesitatea prelucrării pentru executarea unui contract

În cadrul dreptului UE, articolul 6 alineatul (1) litera (b) din RGPD prevede încă un temei juridic pentru prelucrarea legitimă a datelor, și anume dacă aceasta este „necesară pentru executarea unui contract la care persoana vizată este parte". Această dispoziție reglementează și relațiile precontractuale. De exemplu, în cazuri în care o parte intenționează să încheie un contract, dar încă nu l-a semnat, eventual pentru că mai trebuie efectuate anumite verificări. În cazul în care una dintre părți trebuie să prelucreze date în acest scop, această prelucrare este legitimă în măsura în care este „necesară [...] pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract"[378].

Noțiunea de prelucrare a datelor ca „temei legitim prevăzut de lege", menționată la articolul 5 alineatul 2 din Convenția 108 modernizată, include, de asemenea, „prelucrarea datelor pentru executarea unui contract (sau în cadrul unor măsuri precontractuale aplicate la cererea persoanei vizate) la care persoana vizată este parte"[379].

Obligațiile legale ale operatorului

Dreptul UE stabilește încă un criteriu care conferă legitimitate prelucrării datelor, și anume „[necesitatea prelucrării] în vederea îndeplinirii unei obligații legale care îi revine operatorului" [articolul 6 alineatul (1) litera (c) din RGPD]. Această dispoziție se referă atât la operatorii care își desfășoară activitatea în sectorul privat, cât și la cei din sectorul public; și obligațiile legale ale operatorilor de date din sectorul public pot intra sub incidența articolului 6 alineatul (1) litera (e) din RGPD. Există numeroase exemple de situații în care legea impune operatorilor din sectorul privat să prelucreze date despre persoane vizate concrete. De exemplu, angajatorii trebuie să prelucreze date despre angajații lor în scopuri fiscale și de asigurări sociale, iar întreprinderile trebuie să prelucreze date despre clienții lor în scopuri fiscale.

Obligația legală poate rezulta din dreptul Uniunii sau al statului membru, care ar putea constitui baza pentru una sau mai multe operațiuni de prelucrare. Ar trebui să se stabilească prin lege scopul prelucrării, specificațiile pentru stabilirea operatorului, tipul de date cu caracter personal care fac obiectul prelucrării, persoanele vizate

378 *Ibidem*, articolul 6 alineatul (1) litera (b).

379 Raportul explicativ privind Convenția 108 modernizată, punctul 46; Recomandarea CM/Rec(2010)13 din 23 noiembrie 2010 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal în contextul creării de profiluri, articolul 3.4 litera (b).

implicate, entitățile cărora le pot fi divulgate datele, limitările legate de scop, perioada de stocare și alte măsuri pentru a garanta o prelucrare legală și echitabilă[380]. Orice astfel de lege pe care se bazează prelucrarea datelor cu caracter personal trebuie să respecte atât articolele 7 și 8 din Cartă, cât și articolul 8 din Convenția europeană a drepturilor omului.

Obligațiile legale ale operatorului servesc drept temei juridic pentru prelucrarea legitimă a datelor și **în cadrul legislației CoE**[381]. Astfel cum s-a subliniat anterior, obligațiile legale ale unui operator din sectorul privat reprezintă doar un caz specific de interese legitime ale altor persoane, după cum se menționează la articolul 8 alineatul (2) din Convenția europeană a drepturilor omului. Exemplul cu angajatorii care prelucrează date despre angajații lor este, prin urmare, relevant și pentru legislația CoE.

Interesele vitale ale persoanei vizate sau ale altei persoane fizice

În dreptul UE, articolul 6 alineatul (1) litera (d) din RGPD prevede că prelucrarea datelor cu caracter personal este legală dacă este „necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice". Acest temei juridic poate fi invocat doar pentru prelucrarea datelor cu caracter personal pe baza intereselor vitale ale unei alte persoane fizice, în cazul în care o astfel de prelucrare „nu se poate baza în mod evident pe un alt temei juridic"[382]. Uneori, un tip de prelucrare se poate baza atât pe motive de interes public, cât și pe interesele vitale ale persoanei vizate sau ale altei persoane. Acesta este cazul, de exemplu, atunci când se monitorizează o epidemie și evoluția acesteia sau într-o situație de urgență umanitară.

În cadrul legislației CoE, articolul 8 din Convenția europeană a drepturilor omului nu menționează interesele vitale ale persoanei vizate. Cu toate acestea, se consideră că interesele vitale ale persoanei vizate sunt subînțelese în noțiunea de „temei legitim" de la articolul 5 alineatul (2) din Convenția 108 modernizată, care se referă la legitimitatea prelucrării datelor cu caracter personal[383].

380 Regulamentul general privind protecția datelor, considerentul 45.

381 Recomandarea CM/Rec(2010)13 din 23 noiembrie 2010 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal în contextul creării de profiluri, articolul 3.4 litera (a).

382 Regulamentul general privind protecția datelor, considerentul 46.

383 Raportul explicativ privind Convenția 108 modernizată, punctul 46.

Interesul public și exercitarea autorității publice

Având în vedere numeroasele modalități posibile de organizare a treburilor publice, articolul 6 alineatul (1) litera (e) din RGPD prevede că datele cu caracter personal pot fi prelucrate în mod legal dacă prelucrarea „este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul”[384].

Exemplu: În cauza *Huber/Bundesrepublik Deutschland*[385], domnul Huber, resortisant austriac cu reședința în Germania, a solicitat Oficiului Federal pentru Migrație și Refugiați să elimine datele sale din Registrul central al străinilor („AZR”). Registrul, care conține date cu caracter personal ale resortisanților UE care nu sunt cetățeni germani, dar au reședința în Germania de mai mult de trei luni, este utilizat în scopuri statistice și de autoritățile judiciare și de aplicare a legii atunci când cercetează și urmăresc penal infracțiuni sau activități care amenință siguranța publică. Instanța de trimitere a solicitat Curții să se pronunțe cu privire la compatibilitatea cu dreptul UE a prelucrării datelor cu caracter personal efectuată într-un registru precum Registrul central al străinilor, la care au acces și alte autorități publice, având în vedere că nu există un astfel de registru pentru resortisanții germani.

CJUE a precizat că, în temeiul articolului 7 litera (e) din Directiva 95/46/CE[386], datele cu caracter personal pot fi prelucrate în mod legal dacă acest lucru este necesar pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice.

Potrivit CJUE, „ținând seama de obiectivul care constă în asigurarea unui nivel de protecție echivalent în toate statele membre, noțiunea de necesitate, astfel cum rezultă aceasta din articolul 7 litera (e) din Directiva 95/46/CE[387] [...] nu poate avea un conținut care să varieze în funcție de statele membre. Este

384 Vezi Regulamentul general privind protecția datelor, considerentul 45.

385 Hotărârea CJUE [MC] din 16 decembrie 2008 în cauza C-524/06, *Heinz Huber/Bundesrepublik Deutschland*.

386 Directiva privind protecția datelor (abrogată), articolul 7 litera (e), acum Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (e).

387 *Ibidem*.

vorba, așadar, despre o noțiune autonomă de drept comunitar, care trebuie să primească o interpretare de natură să reflecte pe deplin obiectul acestei directive, astfel cum este definit la articolul 1 alineatul (1) din aceasta”[388].

CJUE a arătat că dreptul la libera circulație a unui cetățean al Uniunii pe teritoriul unui stat membru al căruia nu este resortisant nu este necondiționat, ci poate face obiectul unor limitări și condiții impuse prin Tratatul de instituire a Comunității Europene și prin măsurile adoptate pentru punerea în aplicare a acestuia. Astfel, dacă, în principiu, un stat membru poate utiliza în mod legitim un registru precum AZR pentru a susține autoritățile responsabile pentru aplicarea legislației referitoare la dreptul de ședere, acest registru nu trebuie să conțină alte informații decât cele necesare în acest scop specific. CJUE a concluzionat că acest sistem de prelucrare a datelor cu caracter personal este în conformitate cu dreptul UE în cazul în care conține numai datele necesare aplicării acestei legislații, iar structura sa centralizată contribuie la eficientizarea punerii în aplicare a acestei legislații. Instanța națională trebuie să verifice dacă aceste condiții sunt îndeplinite în speță. Dacă nu sunt îndeplinite, stocarea și prelucrarea datelor cu caracter personal în scopuri statistice într-un registru precum AZR nu poate fi considerată, în niciun caz, necesară în sensul articolului 7 litera (e)[389] din Directiva 95/46/CE[390].

În sfârșit, în ceea ce privește aspectul utilizării datelor incluse în registru în scopul combaterii criminalității, CJUE a stabilit că acest obiectiv „are în vedere în mod necesar anchetarea infracțiunilor comise, indiferent de cetățenia autorilor acestora”. Registrul în cauză nu include date cu caracter personal ale resortisanților statului membru în cauză, iar această diferență de tratament constituie discriminare, interzisă prin articolul 18 din TFUE. În consecință, CJUE a constatat că această dispoziție „se opune instituirii de către un stat membru, în vederea combaterii criminalității, a unui sistem specific de prelucrare a datelor cu caracter personal care privește cetățenii Uniunii care nu sunt resortisanți ai acestui stat membru”[391].

388 Hotărârea CJUE [MC] din 16 decembrie 2008 în cauza C-524/06, *Heinz Huber/Bundesrepublik Deutschland*, punctul 52.

389 Directiva privind protecția datelor (abrogată), articolul 7 litera (e), acum Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (e).

390 Hotărârea CJUE [MC] din 16 decembrie 2008 în cauza C-524/06, *Heinz Huber/Bundesrepublik Deutschland*, punctele 54, 58-59 și 66-68.

391 *Ibidem*, punctele 78 și 81.

Utilizarea datelor cu caracter personal de către autoritățile care acționează în domeniul public intră, de asemenea, sub incidența articolului 8 din **Convenția europeană a drepturilor omului** și trebuie să fie reglementată, după caz, de articolul 5 alineatul (2) din Convenția 108 modernizată[392].

Interesele legitime urmărite de operator sau de o parte terță

În conformitate cu **dreptul UE**, persoana vizată nu este singura cu interese legitime. Articolul 6 alineatul (1) litera (f) din RGPD prevede că datele cu caracter personal pot fi prelucrate în mod legal dacă prelucrarea „este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță [cu excepția prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor] [căreia îi sunt dezvăluite datele], cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită [protecție] [...]”[393].

Existența unui interes legitim trebuie evaluată cu atenție în fiecare caz specific[394]. În cazul în care se identifică interesele legitime ale operatorului, trebuie efectuat un exercițiu de echilibrare între aceste interese și interesele sau drepturile și libertățile fundamentale ale persoanei vizate[395]. Așteptările rezonabile ale persoanei vizate trebuie să fie luate în considerare în timpul unei astfel de evaluări, pentru a se stabili dacă interesele operatorului prevalează asupra intereselor sau a drepturilor fundamentale ale persoanei vizate[396]. Dacă drepturile persoanei vizate prevalează asupra intereselor legitime ale operatorului, atunci acesta din urmă trebuie să ia măsuri și să pună în aplicare garanții pentru a reduce la minimum impactul asupra drepturilor persoanelor vizate (de exemplu, prin pseudonimizarea datelor) și pentru a reface „echilibrul” înainte de a putea să recurgă în mod legitim la acest temei juridic pentru prelucrare. În Avizul privind noțiunea de interese legitime ale operatorului de date, Grupul de lucru „Articolul 29” a subliniat rolul crucial al responsabilității și al transparenței și importanța drepturilor persoanei vizate de a se opune prelucrării datelor sale sau accesului, modificării, eliminării sau transmiterii acestora în contextul

392 Raportul explicativ privind Convenția 108 modernizată, punctele 46 și 47.

393 În comparație cu Directiva 95/46/CE, Regulamentul general privind protecția datelor oferă mai multe exemple de cazuri care sunt considerate a constitui un interes legitim.

394 Regulamentul general privind protecția datelor, preambul, considerentul 47.

395 Avizul 6/2014 din 4 aprilie 2014 al Grupului de lucru „Articolul 29” privind noțiunea de interese legitime ale operatorului de date în temeiul articolului 7 din Directiva 95/46/CE, WP 217, Bruxelles, 4 aprilie 2014.

396 *Ibidem*.

stabilirii unui echilibru între interesele legitime ale operatorului și interesele și drepturile fundamentale ale persoanei vizate[397].

În considerentele RGPD se dau câteva exemple cu privire la ceea ce constituie un interes legitim al operatorului de date în cauză. De exemplu, prelucrarea datelor cu caracter personal este permisă fără consimțământul persoanei vizate atunci când este efectuată în scopuri de marketing direct sau atunci când o astfel de prelucrare este „strict necesară în scopul prevenirii fraudelor"[398].

În jurisprudența sa, CJUE a elaborat analiza menită să determine ce anume constituie interes legitim.

Exemplu: Cauza *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] a vizat avarierea unui troleibuz al societății de troleibuze din Riga, provocată de un pasager care a deschis brusc ușa unui taxi. Rīgas satiksme a intenționat să acționeze în justiție pasagerul în vederea obținerii de despăgubiri. Cu toate acestea, poliția a comunicat doar numele pasagerului și a refuzat să comunice numărul de identificare și adresa acestuia, susținând că divulgarea ar fi ilegală în temeiul legislației naționale în materie de protecție a datelor.

Instanța de trimitere din Letonia a solicitat CJUE să adopte o decizie preliminară pentru a stabili dacă legislația UE privind protecția datelor impune obligația de a divulga toate datele cu caracter personal necesare pentru introducerea unei acțiuni în fața unei instanțe civile împotriva persoanei presupuse a fi răspunzătoare pentru o contravenție[400].

CJUE a clarificat faptul că legislația UE în materie de protecție a datelor include posibilitatea, nu obligația, de a comunica date unei părți terțe în scopul realizării intereselor legitime urmărite de această parte[401]. CJUE a stabilit trei condiții cumulative care trebuie îndeplinite pentru ca prelucrarea datelor cu

397 *Ibidem*.

398 Regulamentul general privind protecția datelor, preambul, considerentul 47.

399 Hotărârea CJUE din 4 mai 2017 în cauza C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA „Rīgas satiksme"*.

400 *Ibidem*, punctul 23.

401 *Ibidem*, punctul 26.

caracter personal să fie legală pe baza „intereselor legitime”[402]. În primul rând, partea terță căreia i se divulgă datele trebuie să urmărească un interes legitim. În speță, aceasta înseamnă că solicitarea de informații cu caracter personal în scopul de a acționa în justiție o persoană pentru cauzarea de prejudicii materiale constituie un interes legitim al unei părți terțe. În al doilea rând, prelucrarea datelor cu caracter personal trebuie să fie necesară în scopul realizării intereselor legitime urmărite. În acest caz, obținerea de informații cu caracter personal, cum ar fi adresa și/sau numărul de identificare, este strict necesară pentru identificarea persoanei în cauză. În al treilea rând, drepturile și libertățile fundamentale ale persoanei vizate nu trebuie să prevaleze asupra intereselor legitime ale operatorului sau ale părților terțe. Echilibrul între interese trebuie stabilit de la caz la caz, ținând seama de elemente precum gravitatea încălcării drepturilor persoanelor vizate sau, în anumite circumstanțe, chiar vârsta persoanei vizate. Cu toate acestea, în speță, CJUE nu a considerat că refuzul de a divulga datele este justificat prin simplul fapt că persoana vizată era minoră.

În cauza *ASNEF și FECEMD*, CJUE s-a pronunțat în mod explicit cu privire la prelucrarea datelor pe baza temeiului juridic reprezentat de „interesele legitime”, care, la momentul respectiv, era consacrat la articolul 7 litera (f) din Directiva privind protecția datelor[403].

Exemplu: În cauza *ASNEF și FECEMD*[404], CJUE a clarificat faptul că nu este permis ca legislația națională să adauge condiții pentru prelucrarea legală a datelor în plus față de cele prevăzute la articolul 7 litera (f) din directivă[405]. Speța a vizat o situație în care legislația spaniolă privind protecția datelor includea o dispoziție prin care alte părți private puteau invoca un interes legitim în prelucrarea datelor cu caracter personal numai dacă informațiile în cauză se regăseau deja în surse publice.

402 *Ibidem*, punctele 28-34.

403 Directiva privind protecția datelor (abrogată), articolul 7 litera (f), acum Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (f).

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

405 Directiva privind protecția datelor (abrogată), articolul 7 litera (f), acum Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (f).

CJUE a remarcat, în primul rând, că Directiva 95/46/CE[406] urmărește ca nivelul protecției drepturilor și libertăților persoanei în ceea ce privește prelucrarea datelor cu caracter personal să fie echivalent în toate statele membre. Apropierea legislațiilor naționale aplicabile în acest domeniu nu trebuie să aibă ca rezultat scăderea protecției pe care o oferă. Dimpotrivă, trebuie să aibă drept obiectiv asigurarea unui nivel înalt de protecție în Uniune[407]. În consecință, CJUE a stabilit că „din obiectivul constând în asigurarea unui nivel de protecție echivalent în toate statele membre rezultă că articolul 7 din Directiva 95/46/CE[408] prevede o listă exhaustivă și limitativă de cazuri în care o prelucrare de date cu caracter personal poate fi considerată ca fiind legală". În plus, „statele membre nu pot nici să adauge principii noi privind legitimarea prelucrărilor de date cu caracter personal la articolul 7 din Directiva 95/46[409], nici să prevadă cerințe suplimentare care să modifice conținutul unuia dintre cele șase principii prevăzute" la articolul 7[410]. CJUE a admis că, în ceea ce privește ponderarea necesară în temeiul articolului 7 litera (f) din Directiva 95/46/CE, este posibil să se ia în considerare faptul că gravitatea atingerii aduse drepturilor fundamentale ale persoanei vizate care rezultă din prelucrarea în cauză poate varia în funcție de împrejurarea dacă datele în cauză sunt sau nu sunt deja conținute în surse aflate la dispoziția publicului.

Cu toate acestea, articolul 7 litera (f) din directivă „se opune ca un stat membru să excludă în mod categoric și generalizat posibilitatea ca anumite categorii de date cu caracter personal să fie prelucrate, fără a permite o ponderare a drepturilor și a intereselor opuse în cauză într-un anumit caz".

Având în vedere aceste considerații, CJUE a concluzionat că „articolul 7 litera (f) din Directiva 95/46/CE[411] trebuie interpretat în sensul că se opune unei reglementări naționale care, în lipsa consimțământului persoanei vizate

406 Directiva privind protecția datelor (abrogată), acum Regulamentul general privind protecția datelor.

407 Hotărârea CJUE din 24 noiembrie 2011 în cauzele conexate C-468/10 și C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) și Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, punctul 28. Vezi și Directiva privind protecția datelor, considerentele 8 și 10.

408 Directiva privind protecția datelor (abrogată), articolul 7, acum Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (f).

409 Directiva privind protecția datelor (abrogată), articolul 7, acum Regulamentul general privind protecția datelor, articolul 6.

410 *Ibidem*.

411 Directiva privind protecția datelor (abrogată), articolul 7 litera (f), acum Regulamentul general privind protecția datelor, articolul 6 alineatul (1) litera (f).

și pentru a permite prelucrarea datelor cu caracter personal ale acesteia, necesară pentru realizarea interesului legitim urmărit de operator sau de terțul ori de terții cărora le sunt comunicate aceste date, impune, pe lângă respectarea drepturilor și libertăților fundamentale ale persoanei vizate, ca datele în cauză să fie conținute în surse aflate la dispoziția publicului, excluzând astfel în mod categoric și generalizat orice prelucrare a unor date care nu se regăsesc în astfel de surse"[412].

Ori de câte ori se prelucrează date cu caracter personal în temeiul unor „interese legitime", persoana vizată are dreptul de a se opune în orice moment prelucrării invocând motive legate de situația sa specifică, în conformitate cu articolul 21 alineatul (1) din RGPD. Operatorul trebuie să pună capăt prelucrării, cu excepția cazului în care demonstrează temeiuri legitime convingătoare pentru a o continua.

În ceea ce privește **legislația CoE**, se pot găsi formulări similare în Convenția 108 modernizată[413] și în recomandările CoE. Recomandarea privind crearea de profiluri recunoaște ca fiind legitimă prelucrarea datelor cu caracter personal în scopul creării de profiluri, în măsura în care este necesară în scopul realizării intereselor legitime ale altor persoane, „cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanelor vizate"[414]. În plus, „protecția [...] drepturilor și a libertăților altora" este prevăzută la articolul 8 alineatul (2) din Convenția europeană a drepturilor omului ca motiv legitim pentru restrângerea dreptului la protecția datelor.

Exemplu: În cauza *Y/Turcia*[415], reclamantul era seropozitiv. Întrucât era inconștient când a fost dus la spital, echipajul ambulanței a informat personalul spitalului că pacientul este seropozitiv. Reclamantul a susținut în fața CEDO că divulgarea acestei informații i-a încălcat dreptul la respectarea vieții

412 Hotărârea CJUE din 24 noiembrie 2011 în cauzele conexate C-468/10 și C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) și Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, punctele 40, 44 și 48-49.

413 Raportul explicativ privind Convenția 108 modernizată, punctul 46.

414 Recomandarea CM/Rec(2010)13 din 23 noiembrie 2010 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal în contextul creării de profiluri (Recomandarea privind crearea de profiluri), articolul 3.4 litera (b).

415 Hotărârea CEDO din 17 februarie 2015 în cauza *Y/Turcia*, nr. 648/10.

private. Totuși, având în vedere necesitatea de a proteja siguranța personalului spitalicesc, împărtășirea acestei informații nu a fost considerată de Curte o încălcare a drepturilor reclamantului.

4.1.2. Prelucrarea categoriilor speciale de date (date sensibile)

Legislația CoE lasă la aprecierea legislației interne stabilirea protecției adecvate pentru utilizarea datelor sensibile, cu condiția îndeplinirii condițiilor de la articolul 6 din Convenția 108 modernizată, și anume ca garanțiile adecvate care completează celelalte dispoziții ale Convenției să fie consacrate prin lege. **Dreptul UE** prevede, la articolul 9 din RGPD, un regim detaliat de prelucrare a unor categorii speciale de date (denumite și „date sensibile"). Este vorba despre date care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filosofice și apartenența la sindicate, date genetice și biometrice prelucrate în scopul identificării unice a unei persoane fizice și date medicale, precum și date privind viața sexuală sau orientarea sexuală a unei persoane. Prelucrarea datelor sensibile este, în principiu, interzisă[416].

Cu toate acestea, la articolul 9 alineatul (2) din regulament se prevede o listă exhaustivă de excepțări de la această interdicție, care pot constitui motive legitime pentru prelucrarea datelor sensibile. Aceste excepțări includ situațiile în care:

- persoana vizată și-a dat consimțământul explicit pentru prelucrarea datelor;
- prelucrarea este efectuată în cadrul activităților legitime de către un organism fără scop lucrativ și cu specific politic, filosofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale;
- prelucrarea se referă la date făcute publice în mod explicit de persoana vizată;
- prelucrarea este necesară:

416 Directiva privind protecția datelor (abrogată), articolul 7 litera (f), acum Regulamentul general privind protecția datelor, articolul 9 alineatul (1).

- în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale;

- pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice (atunci când persoana vizată nu își poate da consimțământul);

- pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;

- în scopuri legate de medicina preventivă sau a muncii: „de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical";

- în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice;

- din motive de interes public în domeniul sănătății publice;

- din motive de interes public major.

Astfel, pentru a prelucra categorii speciale de date, relația contractuală cu persoana vizată nu este considerată temei juridic pentru prelucrarea legitimă a datelor sensibile, cu excepția contractelor încheiate cu cadre medicale, care fac obiectul obligației de păstrare a secretului profesional[417].

Consimțământul explicit al persoanei vizate

În conformitate cu **dreptul UE**, primul temei juridic posibil al prelucrării legale a oricăror date, indiferent dacă sunt date sensibile sau fără caracter sensibil, este consimțământul persoanei vizate. În cazul datelor sensibile, acest consimțământ trebuie să fie explicit. Dreptul Uniunii sau dreptul intern poate, totuși, să prevadă că interdicția de prelucrare a categoriilor speciale de date nu poate fi ridicată prin

417 Regulamentul general privind protecția datelor, articolul 9 alineatul (2) literele (h) și (i).

consimțământul persoanei vizate[418]. Acesta ar putea fi cazul, de exemplu, atunci când prelucrarea implică riscuri neobișnuite pentru persoana vizată.

Legislația muncii sau legislația în domeniul securității sociale și al protecției sociale

În conformitate cu **legislația UE**, interdicția de la articolul 9 alineatul (1) poate fi ridicată dacă prelucrarea este necesară pentru îndeplinirea obligațiilor sau a drepturilor operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă sau al securității sociale. Cu toate acestea, prelucrarea trebuie să fie autorizată de dreptul UE, de dreptul intern sau de un acord colectiv de muncă încheiat în temeiul dreptului intern, care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate[419]. Evidențele în materie de ocupare a forței de muncă deținute de o organizație pot include date cu caracter personal sensibile în anumite condiții specificate în RGPD și în dreptul intern relevant. Printre exemplele de date sensibile se numără apartenența sindicală și informațiile medicale.

Interesele vitale ale persoanei vizate sau ale unei alte persoane fizice

În conformitate cu **legislația UE**, la fel ca în cazul datelor fără caracter sensibil, datele sensibile pot fi prelucrate în temeiul intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice[420]. În cazul în care prelucrarea se bazează pe interesele vitale ale unei alte persoane, acest motiv legitim poate fi invocat numai dacă o astfel de prelucrare „nu se poate baza în mod evident pe un alt temei juridic"[421]. În unele cazuri, prelucrarea datelor cu caracter personal poate servi atât unor interese individuale, cât și interesului public, de exemplu în cazul în care prelucrarea este necesară în scopuri umanitare[422].

Pentru ca prelucrarea datelor sensibile să fie legitimă pe acest temei, ar trebui să fie imposibil să se ceară consimțământul persoanei vizate, deoarece, de exemplu, aceasta este în stare de inconștiență sau este absentă și nu poate fi contactată. Cu alte cuvinte, persoana este incapabilă din punct de vedere fizic sau juridic să își dea consimțământul.

418 *Ibidem*, articolul 9 alineatul (2) litera (a).

419 Regulamentul general privind protecția datelor, articolul 9 alineatul (2) litera (b).

420 *Ibidem*, articolul 9 alineatul (2) litera (c).

421 *Ibidem*, considerentul 46.

422 *Ibidem*.

Organizații caritabile sau organisme fără scop lucrativ

Prelucrarea datelor cu caracter personal este permisă și în cadrul activităților legitime ale fundațiilor, asociațiilor sau altor organisme fără scop lucrativ și cu specific politic, filosofic, religios sau sindical. Cu toate acestea, prelucrarea în cauză trebuie să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale[423]. Datele sensibile nu pot fi comunicate terților fără consimțământul persoanelor vizate.

Date făcute publice în mod manifest de către persoana vizată

Articolul 9 alineatul (2) litera (e) din RGPD prevede că prelucrarea nu este interzisă atunci când se referă la date care sunt făcute publice în mod manifest de către persoanele vizate. Chiar dacă în regulament nu este definit sensul formulării „făcute publice în mod manifest de către persoana vizată", având în vedere că este vorba despre o excepție de la interzicerea prelucrării datelor sensibile, aceasta trebuie interpretată în mod strict, în sensul că presupune în mod necesar ca persoana vizată să își facă publice datele cu caracter personal în mod deliberat. Astfel, dacă o televiziune difuzează o înregistrare video filmată de o cameră de supraveghere, care prezintă, printre altele, un pompier care se rănește încercând să evacueze o clădire, nu se poate considera că pompierul a făcut publice în mod manifest datele. Pe de altă parte, dacă pompierul decide să descrie incidentul și să publice înregistrarea video și fotografiile pe o pagină de internet publică, atunci se consideră că a făcut un gest deliberat și neechivoc pentru a face publice datele cu caracter personal. Este important de reținut că publicarea propriilor date de către o persoană nu constituie consimțământ, ci un alt tip de permisiune pentru prelucrarea unor categorii speciale de date.

Faptul că persoana vizată a făcut publice datele cu caracter personal prelucrate nu scutește operatorii de obligațiile care le revin în temeiul legislației privind protecția datelor. De exemplu, principiul limitării legate de scop continuă să se aplice datelor cu caracter personal chiar dacă acestea au fost făcute publice[424].

423 *Ibidem*, articolul 9 alineatul (2) litera (d).

424 Avizul 3/2013 al Grupului de lucru „Articolul 29" privind limitările legate de scop, WP 203, Bruxelles, 2 aprilie 2013, p. 14.

Apărarea unui drept în instanță

RGPD permite, de asemenea[425], prelucrarea unor categorii speciale de date care „este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță", fie în cadrul procedurilor judiciare, fie în cadrul unei proceduri administrative sau extrajudiciare[426]. În acest caz, prelucrarea trebuie să fie relevantă pentru apărarea în instanță a unui drept specific, respectiv pentru exercitarea sau pentru apărarea acestuia, și poate fi solicitată de oricare dintre părțile la litigiu.

Atunci când acționează în exercițiul funcției lor judiciare, instanțele pot prelucra categorii speciale de date în contextul soluționării unui litigiu[427]. Printre categoriile speciale de date prelucrate în acest context se pot număra, de exemplu, date genetice utilizate la stabilirea paternității sau date despre starea de sănătate utilizate atunci când o parte dintre probe se referă la detalii privind vătămările suferite de o victimă a unei infracțiuni.

Motive de interes public major

În temeiul articolului 9 alineatul (2) litera (g) din RGPD, statele membre pot prevedea circumstanțe suplimentare în care se pot prelucra datele sensibile, în măsura în care:

- prelucrarea este necesară din motive de interes public major;
- prelucrarea este prevăzută de dreptul UE sau de dreptul intern;
- dreptul UE sau dreptul intern este proporțional cu obiectivul urmărit, respectă dreptul la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor și a intereselor persoanei vizate[428].

Un exemplu important sunt dosarele electronice de sănătate. Aceste sisteme permit punerea la dispoziție a datelor privind starea de sănătate, colectate de către furnizorii de asistență medicală pe parcursul tratării unui pacient, pentru alți furnizori de asistență medicală ai aceluiași pacient, la scară largă, de regulă, la nivel național.

425 *Ibidem*, articolul 9 alineatul (2).

426 Regulamentul general privind protecția datelor, preambul, considerentul 52.

427 *Ibidem*.

428 *Ibidem*, articolul 9 alineatul (2) litera (g).

Grupul de lucru „Articolul 29" a concluzionat că aceste sisteme nu pot fi instituite în temeiul normelor juridice existente privind prelucrarea datelor pacienților[429]. Totuși, se pot crea dosare electronice de sănătate dacă acestea se bazează pe „motive de interes public major"[430]. Ar fi nevoie de un temei juridic explicit pentru crearea acestora, care să conțină, de asemenea, garanțiile necesare pentru a asigura funcționarea securizată a sistemului[431].

Alte temeiuri pentru prelucrarea datelor sensibile

RGPD prevede că datele sensibile pot fi prelucrate dacă prelucrarea este necesară pentru următoarele[432]:

- în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical;

- din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern. Legea trebuie să prevadă măsuri adecvate și specifice pentru protejarea drepturilor persoanei vizate;

- în scopuri de arhivare, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în baza dreptului Uniunii sau a dreptului intern. Legislația trebuie să fie proporțională cu obiectivul urmărit, să respecte substanța dreptului la protecția datelor și să prevadă măsuri adecvate și specifice pentru protejarea drepturilor și a intereselor persoanei vizate.

429 Documentul de lucru din 15 februarie 2007 al Grupului de lucru „Articolul 29" privind prelucrarea datelor medicale cu caracter personal din dosarul electronic de sănătate (DES), WP 131, Bruxelles. Vezi, de asemenea, Regulamentul general privind protecția datelor, articolul 9 alineatul (3).

430 Regulamentul general privind protecția datelor, articolul 9 alineatul (2) litera (g).

431 Documentul de lucru din 15 februarie 2007 al Grupului de lucru „Articolul 29" privind prelucrarea datelor medicale cu caracter personal din dosarul electronic de sănătate (DES), WP 131, Bruxelles.

432 Regulamentul general privind protecția datelor, articolul 9 alineatul (2) literele (h), (i) și (j).

Condiții suplimentare în temeiul dreptului intern

RGPD permite, de asemenea, statelor membre să introducă sau să mențină condiții suplimentare, inclusiv limitări ale prelucrării datelor genetice, biometrice și legate de starea de sănătate[433].

4.2. Norme privind securitatea prelucrării

Principalele elemente

- Normele privind securitatea prelucrării impun operatorului și persoanei împuternicite de operator să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a preveni orice intervenție neautorizată asupra operațiunilor de prelucrare a datelor.
- Nivelul necesar de securitate a datelor este determinat de:
  - elementele de securitate disponibile pe piață pentru orice tip specific de prelucrare;
  - costuri;
  - riscurile prezentate de prelucrarea datelor pentru drepturile fundamentale și libertățile persoanelor vizate.
- Asigurarea confidențialității datelor cu caracter personal face parte dintr-un principiu general recunoscut în Regulamentul general privind protecția datelor.

În conformitate atât cu **legislația UE, cât și cu cea a CoE**, operatorii au obligația generală de a acționa în mod transparent și responsabil atunci când prelucrează date cu caracter personal și, în special, în notificarea încălcărilor securității datelor. În cazul încălcării securității datelor cu caracter personal, operatorii trebuie să anunțe autoritățile de supraveghere, cu excepția cazului în care este puțin probabil ca încălcarea să genereze un risc pentru drepturile și libertățile persoanelor fizice. De asemenea, persoanele vizate trebuie să fie informate cu privire la încălcarea securității datelor cu caracter personal atunci când există posibilitatea ca aceasta să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice.

433 *Ibidem*, articolul 9 alineatul (2) litera (h) și articolul 9 alineatul (4).

4.2.1. Elementele securității datelor

Potrivit dispozițiilor relevante din **dreptul UE**:

> *„Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc [...].”*[434]

Aceste măsuri includ, printre altele:

- pseudonimizarea și criptarea datelor cu caracter personal[435];
- asigurarea confidențialității, integrității, disponibilității și rezistenței continue ale sistemelor și serviciilor de prelucrare[436];
- restabilirea disponibilității datelor cu caracter personal și a accesului la acestea în cazul în care are loc o pierdere de date[437];
- un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor pentru a garanta securitatea prelucrării[438].

Și **legislația CoE** conține o dispoziție similară:

> *„Fiecare parte prevede că operatorul și, după caz, persoana împuternicită de acesta iau măsurile de securitate adecvate împotriva riscurilor precum accesul, distrugerea, pierderea, utilizarea, modificarea sau divulgarea accidentale sau neautorizate ale datelor cu caracter personal.*[439]*”*

434 *Ibidem*, articolul 32 alineatul (1).

435 *Ibidem*, articolul 32 alineatul (1) litera (a).

436 *Ibidem*, articolul 32 alineatul (1) litera (b).

437 *Ibidem*, articolul 32 alineatul (1) litera (c).

438 *Ibidem*, articolul 32 alineatul (1) litera (d).

439 Convenția 108 modernizată, articolul 7 alineatul (1).

În conformitate cu **legislația UE și a CoE**, o încălcare a datelor care poate avea un impact asupra drepturilor și libertăților persoanelor fizice impune operatorului obligația de a notifica încălcarea autorității de supraveghere (vezi secțiunea 4.2.3).

Există, de asemenea, în multe cazuri, standarde industriale, naționale și internaționale care au fost elaborate pentru securizarea prelucrării datelor. Marca europeană de protecție a vieții private (EuroPriSe), de exemplu, este un proiect eTEN (Rețele transeuropene de telecomunicații) al UE, care explorează posibilitățile de certificare a produselor, în special a produselor software, ca facilitând conformitatea cu legislația europeană privind protecția datelor. Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) a fost înființată pentru consolidarea capacității UE, a statelor membre UE și a comunității de afaceri în vederea prevenirii, abordării și soluționării problemelor legate de securitatea rețelelor și a informațiilor[440]. ENISA publică periodic analize ale amenințărilor actuale la adresa securității și recomandări cu privire la modul în care trebuie abordate acestea[441].

Securitatea datelor nu se realizează numai prin utilizarea echipamentelor corespunzătoare hardware și software. Aceasta necesită și norme organizatorice interne adecvate. Ideal, acestea ar trebui să trateze următoarele aspecte:

- punerea la dispoziția tuturor angajaților, periodic, a informațiilor despre normele privind securitatea datelor și obligațiile lor în temeiul legislației privind protecția datelor, în special obligațiile lor de confidențialitate;

- distribuirea clară a responsabilităților și sublinierea clară a competențelor în materie de prelucrare a datelor, în special cu privire la deciziile de prelucrare a datelor cu caracter personal și de transmitere a datelor către terți sau către persoanele vizate;

- utilizarea datelor cu caracter personal numai în conformitate cu instrucțiunile persoanei competente sau în conformitate cu normele generale puse în aplicare;

440 Regulamentul (UE) nr. 526/2013 al Parlamentului European și al Consiliului din 21 mai 2013 privind Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) și de abrogare a Regulamentului (CE) nr. 460/2004, JO 2013 L 165.

441 De exemplu, ENISA (2016), *Cyber Security and Resilience of smart cars. Good practices and recommendations* (Securitatea și rezistența cibernetică a automobilelor inteligente. Bune practici și recomandări); ENISA (2016), *Security of Mobile Payments and Digital Wallets* (Securitatea plăților mobile și a portofelelor digitale).

- protejarea accesului în spațiile și la echipamentele hardware și software ale operatorului sau ale persoanei împuternicite de operator, inclusiv verificări ale autorizației de acces;

- asigurarea faptului că autorizațiile de acces la date cu caracter personal au fost acordate de persoana competentă și că sunt emise pe baza documentației adecvate;

- protocoale automatizate privind accesul electronic la datele cu caracter personal și verificarea periodică a acestor protocoale de către oficiul intern de supraveghere (prin urmare, necesitatea înregistrării tuturor activităților de prelucrare a datelor);

- documentarea atentă a altor forme de divulgare decât accesul automatizat la date, pentru a putea demonstra că nu s-a efectuat nicio transmitere ilegală de date.

Instruirea și formarea adecvată a membrilor personalului în domeniul securității datelor reprezintă, de asemenea, o măsură importantă de securitate eficace. Trebuie instituite, de asemenea, proceduri de verificare (cum ar fi audituri interne sau externe) pentru a garanta că măsurile adecvate există nu doar pe hârtie, ci sunt puse în practică și funcționează.

Măsurile de îmbunătățire a nivelului de securitate al unui operator sau al unei persoane împuternicite de operator includ instrumente precum desemnarea unor responsabili cu protecția datelor cu caracter personal, formarea angajaților în domeniul securității, audituri periodice, teste de penetrare și mărci de calitate.

Exemplu: În cauza *I/Finlanda*[442], reclamanta nu a putut dovedi că evidențele sale medicale au fost accesate ilegal de către alți angajați ai spitalului în care lucra. Prin urmare, cererea în care invoca încălcarea dreptului său la protecția datelor a fost respinsă de instanța internă. CEDO a concluzionat că a existat o încălcare a articolului 8 din Convenția europeană a drepturilor omului, întrucât registrul de evidențe medicale al spitalului „era de așa natură încât nu permitea clarificarea retroactivă a utilizării evidențelor pacienților, acesta prezentând numai cele mai recente cinci consultații și eliminând aceste

442 Hotărârea CEDO din 17 iulie 2008 în cauza *I/Finlanda*, nr. 20511/03.

informații odată ce dosarul era retrimis la arhivă". Pentru Curte, determinant a fost faptul că registrul de evidențe funcțional în spital nu era, în mod evident, conform cu dispozițiile legislației interne, fapt căruia instanțele interne nu i-au acordat importanța cuvenită.

UE a adoptat Directiva privind securitatea rețelelor și a informațiilor (Directiva NIS)[443], primul instrument juridic la nivelul UE privind securitatea cibernetică. Directiva urmărește, pe de o parte, îmbunătățirea securității cibernetice la nivel național și, pe de altă parte, creșterea nivelului de cooperare în cadrul UE. De asemenea, impune operatorilor de servicii esențiale (inclusiv operatorii din sectoarele energetic, al sănătății, bancar, al transporturilor, al infrastructurii digitale etc.) și furnizorilor de servicii digitale obligația de a gestiona riscurile, de a garanta securitatea rețelei și a sistemelor lor informatice, precum și de a raporta incidentele de securitate.

Perspective

În septembrie 2017, Comisia Europeană a propus un proiect de regulament care vizează reformarea mandatului ENISA, pentru a ține seama de noile competențe și responsabilități ale agenției în temeiul Directivei NIS. Obiectivul regulamentului propus este de a dezvolta sarcinile ENISA și de a consolida rolul acesteia de „punct de referință în ecosistemul de securitate cibernetică al UE"[444]. Regulamentul propus nu trebuie să aducă atingere principiilor RGPD și, prin clarificarea elementelor necesare care compun sistemele europene de certificare a securității cibernetice, ar trebui, de asemenea, să consolideze securitatea datelor cu caracter personal. În paralel, în septembrie 2017, Comisia Europeană a propus un proiect de regulament de punere în aplicare care să precizeze elementele pe care trebuie să le ia în considerare furnizorii de servicii digitale pentru a se asigura că rețeaua lor și sistemele lor informatice sunt sigure, conform articolului 16 alineatul (8) din Directiva NIS. La momentul redactării manualului, discuțiile privind aceste două propuneri erau în curs de desfășurare.

443 Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, JO 2016 L 194.

444 Propunere de regulament al Parlamentului European și al Consiliului privind ENISA, „Agenția UE pentru securitate cibernetică", de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică"), COM(2017) 477 final din 13 septembrie 2017, p. 6.

4.2.2. Confidențialitatea

În **cadrul dreptului UE**, RGPD recunoaște confidențialitatea datelor cu caracter personal ca parte a unui principiu general[445]. Furnizorii de servicii de comunicații electronice accesibile publicului trebuie să asigure confidențialitatea. Aceștia au, de asemenea, obligația de a proteja securitatea serviciilor lor[446].

Exemplu: Angajata unei societăți de asigurări primește un apel telefonic la locul de muncă de la o persoană care spune că este client și solicită informații cu privire la contractul său de asigurare.

Obligația de a păstra confidențialitatea datelor clienților impune ca angajata să aplice cel puțin măsurile de securitate minime înainte de a divulga date cu caracter personal. Acest lucru poate fi realizat, de exemplu, prin revenirea cu un apel telefonic la numărul înregistrat în dosarul clientului.

Potrivit articolului 5 alineatul (1) litera (f), datele cu caracter personal trebuie să fie prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate").

În conformitate cu articolul 32, operatorul și persoana împuternicită de operator trebuie să pună în aplicare măsuri tehnice și organizatorice pentru a asigura un nivel ridicat de securitate. Aceste măsuri includ, printre altele, pseudonimizarea și criptarea datelor cu caracter personal, capacitatea de a asigura permanent confidențialitatea, integritatea, disponibilitatea și rezistența prelucrării, evaluarea și testarea eficacității măsurilor și capacitatea de a restabili prelucrarea în eventualitatea unui incident fizic sau tehnic. În plus, aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate contribui la demonstrarea respectării principiului integrității și confidențialității. În plus, în conformitate cu articolul 28 din RGPD, contractul dintre operator și persoana împuternicită de acesta trebuie să prevadă că persoana împuternicită are obligația de a se asigura că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să păstreze confidențialitatea sau că au obligația legală de confidențialitate.

445 Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (f).

446 Directiva asupra confidențialității și comunicațiilor electronice, articolul 5 alineatul (1).

Obligația de confidențialitate nu se extinde asupra situațiilor în care datele sunt aduse la cunoștința unei persoane în calitatea acesteia de persoană fizică, nu de angajat al unui operator sau al unei persoane împuternicite de operator. În acest caz, articolele 32 și 28 din RGPD nu se aplică, întrucât utilizarea datelor cu caracter personal de către persoane fizice este exceptată integral de la aplicabilitatea regulamentului în cazul în care o astfel de utilizare se încadrează în limitele așa-numitei excepții privind activitățile domestice[447]. Excepția privind activitățile domestice se referă la utilizarea datelor cu caracter personal „de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice"[448]. De la hotărârea CJUE în cauza *Bodil Lindqvist*[449], această excepție trebuie totuși interpretată în mod restrictiv, în special în ceea ce privește divulgarea datelor. Mai exact, excepția privind activitățile domestice nu se aplică divulgării datelor cu caracter personal unui număr nelimitat de destinatari prin internet sau unei prelucrări a datelor care prezintă aspecte profesionale sau comerciale (pentru mai multe detalii cu privire la această speță, vezi secțiunile 2.1.2, 2.2.2 și 2.3.1).

„Confidențialitatea comunicațiilor" este un alt aspect al confidențialității, care face obiectul unei *lex specialis*. Normele speciale de asigurare a confidențialității comunicațiilor electronice în conformitate cu Directiva asupra confidențialității și comunicațiilor electronice impun statelor membre să interzică ascultarea, înregistrarea, stocarea sau alte tipuri de interceptare sau supraveghere a comunicațiilor și a datelor de transfer aferente de către persoane altele decât utilizatorul sau fără acordul utilizatorului în cauză[450]. Legislația națională poate să autorizeze excepții de la acest principiu numai din motive de securitate națională, apărare, prevenire sau detectare a infracțiunilor și numai dacă aceste măsuri sunt necesare și proporționale cu scopurile urmărite[451]. Aceleași reguli se vor aplica în temeiul viitorului regulament privind confidențialitatea comunicațiilor electronice, dar domeniul de aplicare al actului juridic privind confidențialitatea comunicațiilor electronice se va extinde de la serviciile de comunicații electronice accesibile publicului, astfel încât să acopere și comunicațiile realizate prin intermediul serviciilor OTT (cum ar fi aplicațiile mobile).

447 Regulamentul general privind protecția datelor, articolul 2 alineatul (2) litera (c).

448 *Ibidem*.

449 Hotărârea CJUE din 6 noiembrie 2003 în cauza C-101/01, *Proces penal/Bodil Lindqvist*.

450 Directiva asupra confidențialității și comunicațiilor electronice, articolul 5 alineatul (1).

451 *Ibidem*, articolul 15 alineatul (1).

În cadrul legislației CoE, obligația de confidențialitate este subsumată noțiunii de securitate a datelor prevăzută la articolul 7 alineatul (1) din Convenția 108 modernizată, care tratează securitatea datelor.

Pentru persoanele împuternicite de operatori, confidențialitatea înseamnă că nu pot divulga datele unor părți terțe sau altor destinatari fără autorizație. Pentru angajații unui operator sau ai unei persoane împuternicite de operator, confidențialitatea impune utilizarea datelor cu caracter personal exclusiv în conformitate cu instrucțiunile superiorilor competenți.

Obligația de confidențialitate trebuie inclusă în orice contract încheiat între operatori și persoanele împuternicite de aceștia. În plus, operatorii și persoanele împuternicite de operatori vor trebui să adopte măsuri specifice pentru a stabili o obligație juridică de confidențialitate pentru angajații lor, care se realizează în mod normal prin includerea unei clauze de confidențialitate în contractul de muncă al angajatului.

Încălcarea atribuțiilor profesionale în materie de confidențialitate se pedepsește conform dispozițiilor dreptului penal în multe state membre ale UE și părți la Convenția 108.

4.2.3. Notificări de încălcare a securității datelor cu caracter personal

Încălcarea securității datelor cu caracter personal înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal sau la accesul neautorizat la acestea[452]. Deși noile tehnologii, cum ar fi criptarea, oferă acum mai multe posibilități pentru a asigura securitatea prelucrării, încălcările securității datelor sunt încă un fenomen frecvent. Cauzele încălcărilor securității datelor pot varia de la greșeli accidentale comise de persoanele care lucrează în interiorul unei organizații până la amenințări externe, cum ar fi hackerii și organizațiile infracționale cibernetice.

Încălcarea securității datelor poate aduce prejudicii considerabile drepturilor la respectarea vieții private și la protecția datelor ale persoanelor care, ca urmare a încălcării, își pierd controlul asupra datelor lor cu caracter personal. Încălcările pot

452 Regulamentul general privind protecția datelor, articolul 4 punctul 12; vezi, de asemenea, Orientările din 3 octombrie 2017 ale Grupului de lucru „Articolul 29" privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679, WP 250, Bruxelles, 3 octombrie 2017, p. 8.

conduce la furt de identitate sau la fraudă, la pierderi financiare sau daune materiale, la pierderea confidențialității datelor cu caracter personal protejate prin secretul profesional și la prejudicierea reputației persoanei vizate. În Orientările privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679, Grupul de lucru „Articolul 29" explică faptul că încălcările pot avea trei tipuri de impact asupra datelor cu caracter personal: divulgarea, pierderea și/sau modificarea[453]. Pe lângă obligația de a lua măsuri pentru a asigura securitatea prelucrării, astfel cum se explică în secțiunea 4.2, este la fel de important să se asigure faptul că, atunci când se produc încălcări, operatorii le abordează prompt și adecvat.

Autoritățile de supraveghere și persoanele vizate nu sunt adesea conștiente de apariția unei încălcări a securității datelor și acest lucru împiedică persoanele vizate să ia măsuri pentru a se proteja de consecințele negative ale acesteia. Pentru a proteja drepturile persoanelor fizice și pentru a limita impactul încălcării securității datelor, **UE și CoE** impun operatorilor o cerință de notificare în anumite circumstanțe.

În conformitate cu Convenția 108 modernizată a **CoE**, părțile contractante trebuie să solicite operatorilor cel puțin să notifice autorității de supraveghere competente încălcările securității datelor care ar putea afecta grav drepturile persoanelor vizate. Această notificare trebuie să fie transmisă „fără întârziere"[454].

Dreptul UE stabilește un regim detaliat care reglementează termenul de transmitere și conținutul notificărilor[455]. Astfel, operatorii trebuie să notifice autorităților de supraveghere încălcarea securității datelor fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la momentul în care au luat cunoștință de încălcare. În cazul în care se depășește termenul de 72 de ore, notificarea trebuie să fie însoțită de o explicație privind întârzierea. Operatorii sunt scutiți de obligația de notificare numai în cazul în care pot demonstra că încălcarea securității datelor nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor în cauză.

Regulamentul precizează informațiile minime care trebuie incluse în notificare pentru a permite autorității de supraveghere să ia măsurile necesare[456]. Notificarea

453 Orientările din 3 octombrie 2017 ale Grupului de lucru „Articolul 29" privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679, WP 250, Bruxelles, 3 octombrie 2017, p. 6.

454 Convenția 108 modernizată, articolul 7 alineatul (2); Raportul explicativ privind Convenția 108 modernizată, punctele 64-66.

455 Regulamentul general privind protecția datelor, articolele 33 și 34.

456 *Ibidem*, articolul 33 alineatul (3).

trebuie să cuprindă cel puțin o descriere a caracterului încălcării securității datelor și a categoriilor și a numărului aproximativ al persoanelor vizate afectate, o descriere a posibilelor consecințe ale încălcării și a măsurilor luate de operator pentru a remedia problema și a atenua consecințele acesteia. În plus, trebuie furnizate numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact, pentru a permite autorității de supraveghere competente să obțină informații suplimentare, dacă este necesar.

În cazul în care încălcarea securității datelor este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorii trebuie să informeze aceste persoane (persoanele vizate), fără întârzieri nejustificate, cu privire la încălcare[457]. Notificarea transmisă persoanelor vizate, inclusiv descrierea încălcării securității datelor, trebuie să folosească un limbaj simplu și clar și să conțină informații similare celor necesare pentru notificările trimise autorităților de supraveghere. În anumite circumstanțe, operatorii pot fi scutiți de obligația de a notifica aceste încălcări persoanelor vizate. Exceptările se aplică în cazul în care operatorul a pus în aplicare măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea. Măsurile întreprinse de operator după producerea încălcării prin care se asigură că riscul pentru drepturile persoanelor vizate nu mai este susceptibil să se materializeze pot constitui, de asemenea, un temei pentru scutirea operatorului de obligația de a notifica încălcarea persoanelor vizate. În sfârșit, dacă notificarea ar necesita un efort disproporționat din partea operatorului, persoanele vizate pot fi informate despre încălcare prin alte mijloace, de exemplu printr-o informare publică sau prin măsuri similare[458].

Obligația de informare a autorităților de supraveghere și a persoanelor vizate cu privire la încălcările securității datelor le aparține operatorilor. Cu toate acestea, pot apărea încălcări ale securității datelor indiferent dacă prelucrarea este efectuată de un operator sau de o persoană împuternicită de operator. Din acest motiv, este esențial să se asigure faptul că și persoanele împuternicite de operatori au obligația de a raporta încălcările securității datelor. Într-un astfel de caz, persoanele împuternicite de operator trebuie să îi notifice acestuia fără întârzieri nejustificate încălcările

457 *Ibidem*, articolul 34.

458 *Ibidem*, articolul 34 alineatul (3) litera (c).

securității datelor[459]. În continuare, operatorul este responsabil pentru informarea autorităților de supraveghere și a persoanelor vizate în cauză, cu respectarea normelor și a termenelor menționate anterior.

4.3. Norme privind responsabilitatea și promovarea conformității

Principalele elemente

- Pentru a asigura responsabilitatea în operațiunile de prelucrare a datelor cu caracter personal, operatorii și persoanele împuternicite de operatori trebuie să păstreze evidențe cu activitățile de prelucrare desfășurate sub responsabilitatea lor și să le pună la dispoziția autorităților de supraveghere, la cererea acestora.
- Regulamentul general privind protecția datelor stabilește mai multe instrumente pentru promovarea conformității:
  - numirea unor responsabili cu protecția datelor în anumite situații;
  - efectuarea unei evaluări a impactului înainte de începerea activităților de prelucrare susceptibile să genereze riscuri ridicate pentru drepturile și libertățile persoanelor fizice;
  - consultarea prealabilă a autorității de supraveghere relevante în cazul în care evaluarea impactului indică faptul că prelucrarea prezintă riscuri care nu pot fi atenuate;
  - coduri de conduită pentru operatori și persoanele împuternicite de operatori care precizează modul în care se aplică regulamentul în diferite domenii de prelucrare;
  - mecanisme de certificare, sigilii și mărci.
- Legislația CoE propune instrumente similare pentru promovarea conformității în Convenția 108 modernizată.

Principiul responsabilității este deosebit de important pentru a garanta aplicarea normelor privind protecția datelor în Europa. Operatorul este responsabil pentru respectarea normelor privind protecția datelor și trebuie să demonstreze conformitatea. Nu ar trebui să se pună problema responsabilității doar după ce a avut loc o încălcare. Operatorii au mai degrabă o obligație proactivă de a adopta politici adecvate

459 *Ibidem*, articolul 33 alineatul (2).

de gestionare a datelor în toate etapele prelucrării acestora. Legislația europeană în materie de protecție a datelor impune operatorilor să pună în aplicare măsuri tehnice și organizatorice pentru a se asigura că prelucrarea respectă legea și pentru a putea demonstra conformitatea. Printre aceste măsuri se numără desemnarea responsabililor cu protecția datelor, păstrarea evidențelor și a documentelor legate de prelucrare și efectuarea evaluărilor impactului asupra vieții private.

4.3.1. Responsabilii cu protecția datelor

Responsabilii cu protecția datelor (RPD) sunt persoane care oferă consultanță privind respectarea normelor de protecție a datelor în cadrul organizațiilor care prelucrează date. Aceștia reprezintă „un punct de referință pentru responsabilitate", deoarece facilitează respectarea normelor, acționând în același timp ca intermediari între autoritățile de supraveghere, persoanele vizate și organizația care i-a desemnat.

În cadrul legislației CoE, articolul 10 alineatul (1) din Convenția 108 modernizată prevede obligația generală a operatorilor și a persoanelor împuternicite de operatori de a-și asuma responsabilitatea. Acest lucru impune operatorilor și persoanelor împuternicite de operatori să ia toate măsurile adecvate pentru a respecta normele de protecție a datelor prevăzute de convenție și pentru a demonstra că prelucrarea datelor desfășurată sub gestiunea lor respectă dispozițiile convenției. Deși convenția nu precizează măsurile concrete pe care trebuie să le adopte operatorii și persoanele împuternicite de operatori, Raportul explicativ privind Convenția 108 modernizată arată că desemnarea unui RPD ar fi o măsură posibilă prin care să se demonstreze conformitatea. RPD trebuie să dispună de toate mijloacele necesare pentru a-și îndeplini atribuțiile[460].

Spre deosebire de legislația CoE, **dreptul UE** nu lasă în toate cazurile desemnarea unui RPD la aprecierea operatorilor și a persoanelor împuternicite de operatori, ci prevede că aceasta este obligatorie în anumite circumstanțe. RGPD recunoaște că RPD joacă un rol-cheie în noul sistem de guvernanță și include dispoziții detaliate privind desemnarea, funcția, atribuțiile și sarcinile responsabilului[461].

RGPD prevede că desemnarea unui RPD este obligatorie în trei cazuri specifice: în cazul în care o autoritate sau un organism public efectuează prelucrarea; în cazul în care activitățile principale ale operatorului sau ale persoanei împuternicite de

460 Raportul explicativ privind Convenția 108 modernizată, punctul 87.

461 Regulamentul general privind protecția datelor, articolele 37-39.

operator constau în operațiuni de prelucrare care necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă; în cazul în care activitățile principale constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal referitoare la condamnări penale și infracțiuni[462]. Deși termenii „monitorizare sistematică pe scară largă" și „activități principale" nu sunt definiți în regulament, Grupul de lucru „Articolul 29" a emis orientări privind modul în care ar trebui interpretați[463].

Exemplu: Societățile care administrează platforme de comunicare socială și motoarele de căutare sunt susceptibile de a fi considerate operatori ale căror operațiuni de prelucrare necesită monitorizarea periodică și sistematică pe scară largă a persoanelor vizate. Modelul de afaceri al unor astfel de societăți se bazează pe prelucrarea unor cantități mari de date cu caracter personal și generează venituri semnificative prin oferirea de servicii de publicitate direcționată și permițând altor societăți să facă reclamă pe site-uri. Publicitatea direcționată este o modalitate de plasare a reclamelor pe baza datelor demografice și a istoricului sau a comportamentului anterior de cumpărare al consumatorilor. Prin urmare, este necesară monitorizarea sistematică a comportamentelor și a obiceiurilor în mediul online ale persoanelor vizate.

Exemplu: Un spital și o societate de asigurări de sănătate sunt exemple tipice de operatori ale căror activități constau în prelucrarea pe scară largă a categoriilor speciale de date cu caracter personal. Datele care dezvăluie informații privind starea de sănătate a unei persoane constituie o categorie specială de date cu caracter personal atât în temeiul legislației CoE, cât și al legislației UE, necesitând deci o protecție sporită. De asemenea, dreptul UE recunoaște datele genetice și biometrice ca fiind categorii speciale de date. În măsura în care unitățile medicale și societățile de asigurări prelucrează astfel de date pe scară largă, RGPD le impune obligația de a desemna un responsabil cu protecția datelor.

În plus, articolul 37 alineatul (4) din RGPD prevede că, în alte cazuri decât cele trei obligatorii prevăzute la articolul 37 alineatul (1), operatorii, persoanele împuternicite de operatori sau asociațiile și alte organisme care reprezintă categoriile de operatori

462 *Ibidem*, articolul 37 alineatul (1).

463 Orientările Grupului de lucru „Articolul 29" privind responsabilii cu protecția datelor (RPD), WP 243 rev.01, astfel cum au fost modificate ultima dată și adoptate la 5 aprilie 2017.

sau de persoane împuternicite de operatori pot desemna sau, dacă acest lucru este impus ca obligație de dreptul UE sau de dreptul intern, desemnează un responsabil cu protecția datelor.

Toate celelalte organizații nu sunt obligate din punct de vedere juridic să desemneze un RPD. Cu toate acestea, RGPD prevede că operatorii și persoanele împuternicite de operatori pot alege să desemneze în mod voluntar un RPD, permițând în același timp statelor membre să facă această desemnare obligatorie pentru mai multe tipuri de organizații decât cele prevăzute de regulament[464].

Odată ce un operator desemnează un RPD, trebuie să se asigure că acesta „este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal" în cadrul organizației[465]. De exemplu, RPD trebuie să fie implicați în furnizarea de consultanță cu privire la efectuarea evaluărilor impactului asupra protecției datelor și în crearea și păstrarea evidențelor cu activitățile de prelucrare dintr-o organizație. Pentru a permite RPD să își îndeplinească în mod eficient sarcinile, operatorii și persoanele împuternicite de operatori trebuie să le pună la dispoziție resursele necesare, inclusiv resursele financiare, infrastructura și echipamentele. Printre cerințele suplimentare se numără cele care impun ca RPD să li se acorde timp suficient pentru a-și îndeplini atribuțiile, precum și formare permanentă pentru a le permite să își dezvolte competența și să rămână la curent cu toate evoluțiile din legislația privind protecția datelor[466].

RGPD stabilește unele garanții de bază pentru a asigura faptul că RPD acționează independent. Operatorii și persoanele împuternicite de operatori trebuie să se asigure că, în exercitarea atribuțiilor legate de protecția datelor, RPD nu primesc nicio instrucțiune din partea întreprinderii, nici chiar din partea persoanelor de la cel mai înalt nivel de conducere. În plus, aceștia nu trebuie să fie demiși sau sancționați în niciun fel pentru îndeplinirea sarcinilor lor[467]. Să analizăm, de exemplu, cazul unui RPD care recomandă unui operator sau unei persoane împuternicite de operator să efectueze o evaluare a impactului asupra protecției datelor, deoarece consideră că prelucrarea este susceptibilă să genereze un risc ridicat pentru persoanele vizate. Societatea nu este de acord cu recomandarea RPD, considerând că nu este

464 Regulamentul general privind protecția datelor, articolul 37 alineatele (3) și (4).

465 *Ibidem*, articolul 38 alineatul (1).

466 Orientările Grupului de lucru „Articolul 29" privind responsabilii cu protecția datelor (RPD), WP 243 rev.01, astfel cum au fost modificate ultima dată și adoptate la 5 aprilie 2017, punctul 3.1.

467 Regulamentul general privind protecția datelor, articolul 38 alineatele (2) și (3).

întemeiată, și, prin urmare, decide să nu efectueze evaluarea impactului. Societatea poate ignora recomandarea, dar nu poate demite sau sancționa RPD pentru că a făcut această recomandare.

În sfârșit, sarcinile și atribuțiile RPD sunt detaliate la articolul 39 din RGPD. Acestea includ cerința de a informa și consilia societățile și angajații care efectuează prelucrarea cu privire la obligațiile care le revin în temeiul legislației și de a monitoriza respectarea normelor UE și naționale privind protecția datelor prin efectuarea de audituri și prin formarea personalului implicat în operațiunile de prelucrare. De asemenea, RPD trebuie să coopereze cu autoritatea de supraveghere și să acționeze ca punct de contact pentru aceasta privind aspectele legate de prelucrarea datelor, cum ar fi, de exemplu, o încălcare a securității datelor.

În ceea ce privește datele cu caracter personal gestionate de instituțiile și organele UE, Regulamentul (CE) nr. 45/2001 prevede că fiecare instituție și organism al Uniunii trebuie să desemneze un RPD. RPD are sarcina de a se asigura că dispozițiile regulamentului sunt aplicate corect în cadrul instituțiilor și organismelor UE și că atât persoanele vizate, cât și operatorii de date sunt informați cu privire la drepturile și obligațiile lor[468]. RPD are, de asemenea, sarcina de a răspunde solicitărilor AEPD și de a coopera cu aceasta atunci când este necesar. În mod similar cu RGPD, Regulamentul (CE) nr. 45/2001 conține dispoziții privind independența RPD în îndeplinirea atribuțiilor lor și necesitatea de a le asigura personalul și resursele necesare[469]. RPD trebuie să fie înștiințați înainte ca o instituție sau un organism al UE (ori departamente ale acestor organizații) să efectueze orice operațiune de prelucrare și trebuie să țină un registru al tuturor operațiunilor de prelucrare notificate[470].

4.3.2. Evidențele activităților de prelucrare

Pentru a putea demonstra conformitatea și a putea fi trase la răspundere, societățile sunt adesea obligate prin lege să își documenteze activitățile și să țină evidența acestora. Un exemplu important este legislația în materie fiscală și de audit, care impune tuturor societăților să păstreze o documentație și o evidență ample. Este important să se stabilească cerințe similare și în alte domenii de drept, în special în legislația privind protecția datelor, deoarece păstrarea de evidențe este o modalitate importantă de a facilita respectarea normelor privind protecția datelor. Astfel,

468 Vezi lista completă de sarcini ale RPD la articolul 24 alineatul (1) din Regulamentul (CE) nr. 45/2001.

469 Regulamentul (CE) nr. 45/2001, articolul 24 alineatele (6) și (7).

470 *Ibidem*, articolele 25 și 26.

dreptul UE prevede că operatorii sau reprezentanții acestora trebuie să păstreze o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor[471]. Această obligație are scopul de a asigura faptul că, dacă este necesar, autoritățile de supraveghere vor dispune de documentația necesară care să le permită să confirme legalitatea prelucrării.

Evidența trebuie să cuprindă următoarele informații:

- numele și datele de contact ale operatorului și ale operatorului asociat, ale reprezentantului operatorului și ale RPD, după caz;
- scopurile prelucrării;
- descrierea categoriilor de persoane vizate și a categoriilor de date cu caracter personal prelucrate;
- informații privind categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal;
- informații care să indice dacă s-au efectuat sau se vor efectua transferuri de date cu caracter personal către o țară terță sau o organizație internațională;
- acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date, precum și o descriere generală a măsurilor tehnice adoptate pentru a asigura securitatea prelucrării[472].

Obligația de a păstra evidența activităților de prelucrare prevăzută de RGPD se referă nu doar la operatori, ci și la persoanele împuternicite de operatori. Aceasta este o evoluție importantă, deoarece, înainte de adoptarea regulamentului, contractul încheiat între operator și persoana împuternicită de operator era, în principal, cel care stabilea obligațiile acesteia din urmă. Obligația persoanelor împuternicite de operatori de a păstra evidențe este prevăzută acum în mod direct de lege.

RGPD prevede o excepție de la această obligație. Cerința de a păstra evidențe nu se aplică unei întreprinderi sau unei organizații (operator sau persoană împuternicită de operator) cu mai puțin de 250 de angajați. Cu toate acestea, excepția face obiectul

471 Regulamentul general privind protecția datelor, articolul 30.

472 *Ibidem*, articolul 30 alineatul (1).

cerințelor ca organizația în cauză să nu efectueze o prelucrare care ar putea genera un risc pentru drepturile și libertățile persoanelor vizate, ca prelucrarea să fie doar ocazională și să nu includă categoriile speciale de date menționate la articolul 9 alineatul (1) sau date cu caracter personal referitoare la condamnări penale și infracțiuni, menționate la articolul 10.

Păstrarea evidențelor activităților de prelucrare ar trebui să permită operatorilor și persoanelor împuternicite de operatori să demonstreze conformitatea cu regulamentul. Ar trebui, de asemenea, să permită autorităților de supraveghere să monitorizeze legalitatea prelucrării. Atunci când o autoritate de supraveghere solicită accesul la aceste evidențe, operatorii și persoanele împuternicite de operatori au obligația de a coopera și de a le pune la dispoziție.

4.3.3. Evaluarea impactului asupra protecției datelor și consultarea prealabilă

Operațiunile de prelucrare prezintă anumite riscuri inerente pentru drepturile persoanelor fizice. Datele cu caracter personal pot fi pierdute, divulgate unor părți neautorizate sau prelucrate în mod ilegal. În mod evident, riscurile variază în funcție de natura și amploarea prelucrării. Operațiunile care implică prelucrarea datelor sensibile pe scară largă, de exemplu, prezintă un grad de risc mult mai ridicat pentru persoanele vizate în comparație cu riscurile potențiale generate în cazul unei întreprinderi mici care prelucrează adresele și numerele de telefon personale ale angajaților.

Odată cu apariția noilor tehnologii și a creșterii gradului de complexitate a prelucrării, operatorii trebuie să abordeze astfel de riscuri prin examinarea impactului probabil al prelucrării preconizate înainte de a începe operația de prelucrare. Acest lucru permite organizațiilor să identifice, să abordeze și să atenueze în mod corespunzător riscurile în avans, limitând în mod semnificativ probabilitatea unui impact negativ asupra persoanelor ca urmare a prelucrării.

Evaluările impactului asupra protecției datelor sunt prevăzute atât **în legislația CoE, cât și a UE**. În cadrul juridic al CoE, articolul 10 alineatul (2) din Convenția 108 modernizată impune părților contractante să se asigure că operatorii și persoanele împuternicite de operatori „examinează impactul probabil al prelucrării preconizate a datelor asupra drepturilor și libertăților fundamentale ale persoanelor vizate înainte de începerea prelucrării respective” și, ulterior evaluării, să proiecteze

prelucrarea astfel încât să prevină sau să reducă la minimum riscurile legate de prelucrare.

Legislația UE impune o obligație similară, mai detaliată, operatorilor care intră sub incidența RGPD. Articolul 35 prevede că trebuie efectuată o evaluare a impactului în cazul în care prelucrarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice. Regulamentul nu definește modalitatea de evaluare a probabilității de risc, ci mai degrabă indică în ce ar putea consta aceste riscuri[473]. Acesta conține o listă a operațiunilor de prelucrare considerate ca prezentând un risc ridicat și pentru care este necesară o evaluare prealabilă a impactului, și anume următoarele situații:

- datele cu caracter personal sunt prelucrate în vederea luării unor decizii cu privire la persoanele fizice, în urma unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice (crearea de profiluri);

- prelucrarea pe scară largă a datelor sensibile sau a datelor cu caracter personal referitoare la condamnări penale și infracțiuni;

- o prelucrare care implică monitorizarea sistematică pe scară largă a unei zone accesibile publicului.

Autoritățile de supraveghere trebuie să adopte și să publice o listă a tipurilor de operațiuni de prelucrare care trebuie să facă obiectul evaluărilor de impact. De asemenea, acestea pot stabili o listă a operațiunilor de prelucrare scutite de această obligație[474].

Atunci când este necesară o evaluare a impactului, operatorii trebuie să evalueze necesitatea și proporționalitatea prelucrării și posibilele riscuri pentru drepturile persoanelor fizice. Evaluarea impactului trebuie să conțină, de asemenea, măsurile de securitate planificate pentru abordarea riscurilor identificate. Pentru a stabili listele, autoritățile de supraveghere ale statelor membre trebuie să coopereze între ele și cu Comitetul European pentru Protecția Datelor. Acest lucru va asigura o abordare consecventă în întreaga Uniune a operațiunilor care necesită o evaluare a impactului, iar operatorii vor trebui să răspundă unor cerințe similare indiferent de localizarea lor.

473 Regulamentul general privind protecția datelor, preambul, considerentul 75.

474 *Ibidem*, articolul 35 alineatele (4) și (5).

Dacă, în urma unei evaluări a impactului, există indicii că prelucrarea va avea ca rezultat un risc ridicat pentru drepturile persoanelor fizice și nu au fost introduse măsuri de atenuare a riscului, operatorul trebuie să consulte autoritatea de supraveghere competentă înainte de a începe operațiunea de prelucrare[475].

Grupul de lucru „Articolul 29" a emis orientări privind evaluările impactului asupra protecției datelor și modalitățile prin care se poate stabili dacă prelucrarea este sau nu susceptibilă de a genera un risc ridicat[476]. Acesta a elaborat nouă criterii pentru a determina dacă este necesară o evaluare a impactului asupra protecției datelor într-un caz specific[477]: (1) evaluarea sau acordarea unui punctaj; (2) deciziile automatizate cu efect juridic sau similar semnificativ; (3) monitorizarea sistematică; (4) datele sensibile; (5) datele prelucrate pe scară largă; (6) seturile de date care au fost asociate sau combinate; (7) date privind persoanele vizate vulnerabile; (8) utilizarea inovatoare sau aplicarea de soluții tehnologice sau organizaționale; (9) cazurile în care prelucrarea în sine „împiedică persoanele vizate să își exercite un drept sau să utilizeze un serviciu sau un contract". Grupul de lucru „Articolul 29" a introdus o regulă de bază potrivit căreia operațiunile de prelucrare care îndeplinesc mai puțin de două criterii prezintă niveluri de risc mai scăzute și nu necesită o evaluare a protecției datelor, în timp ce acelea care îndeplinesc două sau mai multe criterii necesită o astfel de evaluare. În cazurile în care nu este clar dacă este necesară o evaluare a impactului asupra protecției datelor, Grupul de lucru „Articolul 29" recomandă efectuarea unei astfel de evaluări, deoarece este „un instrument util pentru a ajuta operatorii de date să respecte legislația privind protecția datelor"[478]. Atunci când se introduce o nouă tehnologie de prelucrare a datelor, este important să se efectueze o evaluare a impactului asupra protecției datelor[479].

4.3.4. Coduri de conduită

Codurile de conduită sunt menite să fie utilizate în mai multe sectoare de prelucrare, pentru a evidenția și preciza aplicarea RGPD în sectoarele specifice. Pentru operatorii

475 *Ibidem*, articolul 36 alineatul (1); Orientările din 4 octombrie 2017 ale Grupului de lucru „Articolul 29" privind evaluarea impactului asupra protecției datelor și determinarea aspectului dacă prelucrarea este „susceptibilă de a genera un risc ridicat" în sensul Regulamentului 2016/679, WP 248 rev.01, Bruxelles, 4 octombrie 2017..

476 Orientările din 4 octombrie 2017 ale Grupului de lucru „Articolul 29" privind evaluarea impactului asupra protecției datelor și determinarea aspectului dacă prelucrarea este „susceptibilă de a genera un risc ridicat" în sensul Regulamentului 2016/679, WP 248 rev.01, Bruxelles, 4 octombrie 2017..

477 *Ibidem*, pp. 9-11.

478 *Ibidem*, p. 9.

479 *Ibidem*.

și persoanele împuternicite de operatori care prelucrează date cu caracter personal, instituirea unor astfel de coduri poate îmbunătăți considerabil conformitatea și punerea în aplicare a normelor UE de protecție a datelor. Expertiza membrilor sectorului respectiv va facilita identificarea unor soluții practice, care să poată fi urmate. Recunoscând importanța acestor coduri pentru aplicarea eficace a legislației privind protecția datelor, RGPD invită statele membre, autoritățile de supraveghere, Comisia și Comitetul European pentru Protecția Datelor să încurajeze elaborarea de coduri de conduită menite să contribuie la buna aplicare a regulamentului în întreaga UE[480]. Codurile ar putea preciza modul în care se aplică regulamentul în sectoare specifice, inclusiv aspecte precum colectarea datelor cu caracter personal, informațiile care trebuie furnizate persoanelor vizate și publicului și exercitarea drepturilor persoanelor vizate.

Pentru a se asigura că codurile de conduită respectă normele stabilite în RGPD, codurile trebuie prezentate autorității competente de supraveghere înainte de a fi adoptate. Autoritatea de supraveghere emite apoi un aviz cu privire la conformitatea cu regulamentul a proiectului de cod prezentat și îl aprobă în cazul în care constată că acesta oferă garanții adecvate[481]. Autoritățile de supraveghere trebuie să publice codurile de conduită aprobate, precum și criteriile pe baza cărora au fost aprobate. În cazul în care un proiect de cod de conduită se referă la activități de prelucrare din mai multe state membre, înainte de a aproba proiectul de cod sau modificarea ori extinderea unui cod existent, autoritatea de supraveghere competentă transmite codul Comitetului European pentru Protecția Datelor, care emite un aviz privind conformitatea codului cu RGPD. Comisia poate decide, prin intermediul actelor de punere în aplicare, că codul de conduită aprobat care îi este prezentat are valabilitate generală în cadrul Uniunii.

Aderarea la un cod de conduită oferă avantaje importante atât persoanelor vizate, cât și operatorilor și persoanelor împuternicite de operatori. Aceste coduri oferă îndrumări detaliate care adaptează cerințele legale la sectoare specifice și sporesc transparența activităților de prelucrare. Operatorii și persoanele împuternicite de operatori pot, de asemenea, să adere la codurile de conduită pentru a demonstra conformitatea cu legislația UE și ca mijloc de promovare a unei imagini publice de organizație care se angajează să asigure protecția datelor și care acordă prioritate acestui aspect în operațiunile sale. Codurile de conduită aprobate, împreună cu angajamentele obligatorii și executorii, pot fi utilizate ca garanții adecvate pentru

480 Regulamentul general privind protecția datelor, articolul 40 alineatul (1).

481 *Ibidem*, articolul 40 alineatul (5).

transferul datelor către țări terțe. Pentru a se asigura faptul că organizațiile care aderă la coduri de conduită le respectă cu adevărat, se poate desemna un organism special (acreditat de autoritatea de supraveghere competentă) care să monitorizeze și să asigure conformitatea. Pentru a-și îndeplini sarcinile cu eficacitate, organismul trebuie să fie independent, să dispună de expertiză dovedită în privința aspectelor reglementate de codul de conduită și să aplice proceduri și structuri transparente care să îi permită să trateze plângerile referitoare la încălcările codului[482].

În cadrul **legislației CoE**, Convenția 108 modernizată prevede că nivelul de protecție a datelor garantat de legislația națională poate fi consolidat în mod util prin măsuri de reglementare voluntare, cum ar fi codurile de bune practici sau codurile de conduită profesională. Acestea constituie totuși doar măsuri voluntare în temeiul Convenției 108 modernizate: deși este recomandabilă, punerea lor în aplicare nu poate fi derivată ca obligație legală, iar măsurile singure nu sunt suficiente pentru a asigura respectarea deplină a convenției[483].

4.3.5. Certificarea

Pe lângă codurile de conduită, mecanismele de certificare și sigiliile și mărcile de protecție a datelor sunt alte mijloace prin care operatorii și persoanele împuternicite de operatori pot demonstra conformitatea cu RGPD. În acest sens, regulamentul prevede un sistem de certificare voluntară, prin care anumite organisme sau autorități de supraveghere pot emite certificări. Operatorii și persoanele împuternicite de operatori care aleg să adere la un mecanism de certificare pot obține o mai mare vizibilitate și credibilitate, deoarece certificările, sigiliile și mărcile permit persoanelor vizate să evalueze rapid nivelul de protecție a datelor aplicat de organizațiile respective. Este important de precizat că faptul că un operator sau o persoană împuternicită de operator deține o astfel de certificare nu îi reduce sarcinile și responsabilitățile de a respecta toate cerințele regulamentului.

482 *Ibidem*, articolul 41 alineatele (1) și (2).

483 Raportul explicativ privind Convenția 108 modernizată, punctul 33.

4.4. Protecția datelor din faza de proiectare și protecția implicită a datelor

Protecția datelor din faza de proiectare

Dreptul UE impune operatorilor să adopte măsuri pentru punerea în aplicare în mod eficient a principiilor de protecție a datelor și pentru integrarea garanțiilor necesare pentru a îndeplini cerințele regulamentului și a proteja drepturile persoanelor vizate[484]. Aceste măsuri ar trebui să fie puse în aplicare atât în momentul prelucrării, cât și la determinarea mijloacelor de prelucrare. La punerea în aplicare a acestor măsuri, operatorul trebuie să țină seama de stadiul actual al tehnologiei, de costurile implementării, de natura, domeniul de aplicare și scopurile prelucrării datelor cu caracter personal, precum și de riscurile cu grade diferite de gravitate pentru drepturile și libertățile persoanei vizate[485].

Legislația CoE impune ca operatorii și persoanele împuternicite de operatori să evalueze impactul potențial al prelucrării datelor cu caracter personal asupra drepturilor și libertăților persoanelor vizate înainte de a începe prelucrarea. În plus, operatorii și persoanele împuternicite de operatori sunt obligați să proiecteze prelucrarea datelor astfel încât să prevină sau să reducă la minimum riscul de ingerință în aceste drepturi și libertăți și să pună în aplicare măsuri tehnice și organizatorice care să țină seama de implicațiile dreptului la protecția datelor cu caracter personal în toate etapele prelucrării datelor[486].

Protecția implicită a datelor

Dreptul UE impune operatorului să pună în aplicare măsuri adecvate pentru a se asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru scopurile prelucrării respective. Această obligație se aplică volumului de date cu caracter personal colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor[487]. O astfel de măsură trebuie să garanteze,

484 Regulamentul general privind protecția datelor, articolul 25 alineatul (1).

485 Vezi Orientările din 4 octombrie 2017 ale Grupului de lucru „Articolul 29" privind evaluarea impactului asupra protecției datelor și determinarea aspectului dacă prelucrarea este „susceptibilă de a genera un risc ridicat" în sensul Regulamentului 2016/679, WP 248 rev.01, Bruxelles, 4 octombrie 2017. Vezi, de asemenea, ENISA (2015), Respectarea vieții private și protecția datelor din faza de proiectare – de la politică la inginerie, 12 ianuarie 2015.

486 Convenția 108 modernizată, articolul 10 alineatele (2) și (3), Raportul explicativ privind Convenția 108 modernizată, punctul 89.

487 Regulamentul general privind protecția datelor, articolul 25 alineatul (2).

de exemplu, că nu toți angajații operatorilor au acces la datele cu caracter personal ale persoanelor vizate. AEPD a elaborat orientări suplimentare în cadrul *Setului de instrumente privind necesitatea*[488].

Legislația CoE impune operatorilor și persoanelor împuternicite de operatori să pună în aplicare măsuri tehnice și organizatorice care să ia în considerare implicațiile dreptului la protecția datelor (cu caracter personal) în toate etapele prelucrării datelor[489].

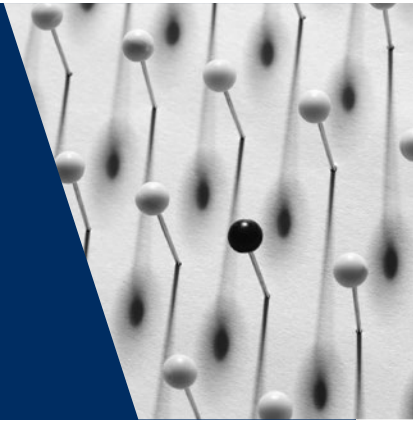
În 2016, ENISA a publicat un raport privind instrumentele și serviciile disponibile în materie de protecție a vieții private[490]. Printre alte considerente, această evaluare oferă un indice de criterii și parametri care reprezintă indicatori ai bunelor sau relelor practici în materie de asigurare a respectării vieții private. În timp ce unele criterii se referă direct la dispozițiile RGPD – cum ar fi utilizarea pseudonimizării și a mecanismelor de certificare aprobate –, altele propun inițiative inovatoare pentru a asigura respectarea vieții private din faza de proiectare și în mod implicit. De exemplu, criteriul ușurinței în utilizare, deși nu este direct legat de protecția vieții private, o poate îmbunătăți, deoarece poate permite adoptarea pe scară mai largă a instrumentului sau serviciului în cauză. Într-adevăr, instrumentele de protecție a vieții private care sunt dificil de pus în aplicare pot prezenta niveluri foarte reduse de adoptare de către publicul larg, chiar dacă oferă garanții foarte solide de respectare a vieții private. În plus, criteriul maturității și stabilității instrumentului de protecție a vieții private – adică modul în care un instrument evoluează în timp și răspunde provocărilor existente sau noi legate de respectarea vieții private – este de o importanță crucială. Alte tehnologii îmbunătățite de asigurare a respectării vieții private – de exemplu, în contextul comunicațiilor securizate – includ criptarea de la un capăt la altul (un tip de comunicare în care singurele persoane care pot citi mesajele sunt persoanele care comunică); criptarea client-server (criptarea canalului de comunicare stabilit între un client și un server); autentificarea (verificarea identității părților care comunică); și comunicarea anonimă (nicio parte terță nu poate identifica părțile care comunică).

488 Autoritatea Europeană pentru Protecția Datelor (AEPD) (2017), *Set de instrumente privind necesitatea*, Bruxelles, 11 aprilie 2017.

489 Convenția 108 modernizată, articolul 10 alineatul (3), Raportul explicativ privind Convenția 108 modernizată, punctul 89.

490 ENISA, Matricea de verificare a tehnologiilor de protecție a vieții private: o abordare sistematică a evaluării instrumentelor mobile și online de protecție a vieții private, 20 decembrie 2016.

5 Supraveghere independentă



UE	Aspecte vizate	CoE
Carta, articolul 8 alineatul (3) Tratatul privind funcționarea UE, articolul 16 alineatul (2) Regulamentul general privind protecția datelor, articolele 51-59 Hotărârea CJUE [MC] în cauza C-518/07, *Comisia Europeană/Republica Federală Germania*, 2010 Hotărârea CJUE [MC] din în cauza C-614/10, *Comisia Europeană/Republica Austria*, 2012 Hotărârea CJUE [MC] în cauza C-288/12, *Comisia Europeană/Ungaria*, 2014 Hotărârea CJUE [MC] în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*, 2015	**Autorități de supraveghere**	Convenția 108 modernizată, articolul 15
Regulamentul general privind protecția datelor, articolele 60-67	**Cooperarea dintre autoritățile de supraveghere**	Convenția 108 modernizată, articolele 16-21
Regulamentul general privind protecția datelor, articolele 68-76	**Comitetul European pentru Protecția Datelor**	

Principalele elemente

- Supravegherea independentă este o componentă esențială a legislației europene privind protecția datelor și este consacrată la articolul 8 alineatul (3) din Cartă.
- Pentru a asigura o protecție eficace a datelor, se impune înființarea de autorități de supraveghere independente în conformitate cu legislația națională.
- Autoritățile de supraveghere trebuie să acționeze cu independență deplină, garantată prin legea în temeiul căreia a fost instituită autoritatea respectivă și care se reflectă în structura organizatorică specifică a autorității de supraveghere.
- Autoritățile de supraveghere au competențe și sarcini specifice. Printre acestea se numără:
  - monitorizarea și promovarea protecției datelor la nivel național;
  - consilierea persoanelor vizate și a operatorilor, precum și a guvernului și publicului larg;
  - audierea plângerilor și furnizarea de asistență persoanei vizate în probleme legate de presupusele încălcări ale drepturilor la protecția datelor;
  - supravegherea operatorilor și a persoanelor împuternicite de operatori.
- Autoritățile de supraveghere au, de asemenea, competența de a interveni, dacă este necesar, prin:
  - avertizarea, mustrarea sau chiar amendarea operatorilor și a persoanelor împuternicite de aceștia;
  - solicitarea rectificării, blocării sau ștergerii datelor;
  - impunerea unei interdicții de prelucrare sau a unei amenzi administrative;
  - sesizarea unei instanțe de judecată.
- Dat fiind că prelucrarea datelor cu caracter personal implică deseori operatori, persoane împuternicite de operatori și persoane vizate din state diferite, autoritățile de supraveghere trebuie să coopereze între ele în privința aspectelor transfrontaliere pentru a asigura protecția eficace a persoanelor fizice în Europa.
- În UE, Regulamentul general privind protecția datelor instituie un mecanism al ghișeului unic pentru cazurile de prelucrare transfrontalieră. Unele societăți desfășoară activități de prelucrare transfrontaliere deoarece prelucrează date cu caracter personal în cadrul sediilor din mai multe state membre sau în cadrul unui singur sediu din Uniune, dar care afectează în mod semnificativ persoane vizate din mai multe state membre. În cadrul mecanismului, aceste societăți vor putea colabora cu o singură autoritate națională de supraveghere a protecției datelor.

- Un mecanism pentru asigurarea cooperării și a coerenței va permite o abordare coordonată între toate autoritățile de supraveghere implicate într-un caz. Autoritatea de supraveghere principală – corespunzătoare sediului principal sau unic al unei societăți – se consultă și transmite proiectul de decizie împreună cu celelalte autorități de supraveghere în cauză.
- În mod similar actualului Grup de lucru „Articolul 29", autoritatea de supraveghere a fiecărui stat membru și Autoritatea Europeană pentru Protecția Datelor (AEPD) vor face parte din Comitetul European pentru Protecția Datelor.
- Sarcinile Comitetului European pentru Protecția Datelor includ, printre altele, monitorizarea aplicării corecte a regulamentului, consilierea Comisiei cu privire la aspectele relevante și emiterea de avize, orientări sau bune practici privind o gamă largă de subiecte.
- Principala diferență constă în faptul că Comitetul European pentru Protecția Datelor nu va emite doar avize, așa cum prevedea Directiva 95/46/CE. Va emite, de asemenea, decizii cu caracter obligatoriu atunci când o autoritate de supraveghere a formulat o obiecție relevantă și motivată în cazuri privind ghișeele unice, atunci când există opinii divergente cu privire la care dintre autoritățile de supraveghere este cea principală și, în sfârșit, atunci când autoritatea de supraveghere competentă nu solicită sau nu ține seama de avizul CEPD. Obiectivul este de a asigura o aplicare consecventă a regulamentului în toate statele membre.

Supravegherea independentă este o componentă esențială a legislației europene privind protecția datelor. Atât legislația UE, cât și cea a CoE consideră existența unor autorități independente de supraveghere indispensabilă pentru protecția eficace a drepturilor și libertăților persoanelor în ceea ce privește prelucrarea datelor lor cu caracter personal. Întrucât prelucrarea datelor este acum omniprezentă și tot mai dificil de înțeles pentru publicul larg, aceste autorități sunt gardienii erei digitale. În UE, existența autorităților de supraveghere independente este considerată unul dintre elementele esențiale ale dreptului la protecția datelor cu caracter personal, consacrat în legislația primară a UE. Articolul 8 alineatul (3) din Carta drepturilor fundamentale a UE și articolul 16 alineatul (2) din TFUE recunosc protecția datelor cu caracter personal drept un drept fundamental și afirmă că respectarea normelor de protecție a datelor trebuie să facă obiectul controlului din partea unei autorități independente.

Importanța supravegherii independente a respectării legislației privind protecția datelor a fost, de asemenea, recunoscută în jurisprudență.

Exemplu: În cauza *Schrems*[491], CJUE a examinat dacă transmiterea datelor cu caracter personal către Statele Unite (SUA) în temeiul primului acord UE-SUA privind sfera de siguranță era conformă cu legislația UE privind protecția datelor, în contextul dezvăluirilor lui Edward Snowden cu privire la desfășurarea unor operațiuni de supraveghere în masă de către National Security Agency (Agenția Națională de Securitate) a SUA. Transferul de date cu caracter personal către SUA s-a bazat pe o decizie a Comisiei Europene adoptată în 2000, care permitea transferul de date cu caracter personal din UE către organizații din SUA care declarau pe propria răspundere că respectă regimul „sferei de siguranță", pe baza faptului că regimul asigura un nivel adecvat de protecție a datelor cu caracter personal. Când i s-a solicitat să examineze plângerea reclamantului cu privire la legalitatea transferurilor de date după dezvăluirile lui Snowden, autoritatea irlandeză de supraveghere a respins plângerea pentru motivul că existența deciziei Comisiei privind caracterul adecvat al regimului de protecție a datelor din SUA reflectat în principiile „sferei de siguranță" („Decizia privind sfera de siguranță") o împiedica să investigheze în continuare plângerea.

Cu toate acestea, CJUE a considerat că existența unei decizii a Comisiei care permite transferurile de date către țări terțe care asigură niveluri adecvate de protecție nu anulează, nici nu reduce competențele autorităților naționale de supraveghere. CJUE a arătat că competențele acestor autorități de a monitoriza și de a asigura respectarea normelor UE de protecție a datelor rezultă din dreptul primar al UE, în special articolul 8 alineatul (3) din Cartă și articolul 16 alineatul (2) din TFUE. „Instituirea [...] unor autorități de supraveghere independente constituie, așadar, [...] un element esențial al respectării protecției persoanelor în ceea ce privește prelucrarea datelor cu caracter personal"[492].

Prin urmare, CJUE a stabilit că, deși transferul datelor cu caracter personal făcea obiectul unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție, în cazul în care se depune o plângere la o autoritate națională de supraveghere, autoritatea trebuie să examineze plângerea cu diligență. Autoritatea de supraveghere poate respinge plângerea dacă constată că este neîntemeiată. CJUE a subliniat că, într-un astfel de caz, dreptul la o cale de atac eficientă implică necesitatea ca persoanele să poată contesta o astfel

491 Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*.

492 Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*, punctul 41.

de decizie în fața instanțelor naționale, care pot sesiza CJUE cu o cerere de decizie preliminară privind valabilitatea deciziei Comisiei. În cazul în care autoritatea de supraveghere consideră că plângerea este întemeiată, trebuie să fie în măsură să deschidă proceduri judiciare și să sesizeze instanțele naționale. Instanțele naționale pot trimite cauza la CJUE, aceasta fiind singurul organism care are competența de a decide asupra valabilității unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție[493].

În continuare, CJUE a examinat valabilitatea Deciziei privind sfera de siguranță pentru a stabili dacă sistemul de transferuri era sau nu conform cu normele UE de protecție a datelor. Curtea a constatat că articolul 3 din Decizia privind sfera de siguranță limita competențele autorităților naționale de supraveghere (acordate în temeiul Directivei privind protecția datelor) de a lua măsuri pentru a preveni transferurile de date în cazul unui nivel inadecvat de protecție a datelor cu caracter personal în SUA. Având în vedere importanța autorităților de supraveghere independente în asigurarea respectării legislației privind protecția datelor, CJUE a declarat că, în conformitate cu Directiva privind protecția datelor și în coroborare cu Carta, Comisia nu avea prerogativa de a limita competențele autorității de supraveghere independente în acest mod. Limitarea competențelor autorităților de supraveghere a fost unul dintre motivele pentru care CJUE a declarat nulă Decizia privind sfera de siguranță.

În concluzie, legislația europeană prevede supravegherea independentă ca mecanism important în asigurarea unei protecții eficiente a datelor. Autoritățile de supraveghere independente reprezintă primul punct de contact pentru persoanele vizate în cazurile de încălcare a vieții private[494]. Conform legislației UE și a CoE, instituirea autorităților de supraveghere este obligatorie. Ambele cadre juridice descriu sarcinile și competențele acestor autorități în mod similar cu cele incluse în RGPD. Astfel, autoritățile de supraveghere trebuie să funcționeze, în principiu, în același mod în temeiul legislației UE și a CoE[495].

493 *Ibidem*, punctele 53-66.

494 Regulamentul general privind protecția datelor, articolul 13 alineatul (2) litera (d).

495 *Ibidem*, articolul 51; Convenția 108 modernizată, articolul 15.

5.1. Independență

Legislația UE și a **CoE** impun fiecărei autorități de supraveghere să acționeze cu independență deplină în îndeplinirea sarcinilor sale și în exercitarea competențelor sale[496]. Independența autorității de supraveghere, a membrilor și a personalului acesteia față de influențe externe directe sau indirecte este esențială pentru garantarea obiectivității depline în luarea deciziilor cu privire la aspectele legate de protecția datelor. Independența trebuie garantată, în mod specific, nu numai prin prevederile legii în temeiul căreia se instituie organul de supraveghere, ci și prin structura organizațională specifică a autorității în cauză. CJUE a examinat în 2010, pentru prima dată, gradul de independență de care au nevoie autoritățile de supraveghere a protecției datelor[497]. Exemplele evidențiate ilustrează definiția CJUE a termenului „independență deplină".

Exemplu: În cauza *Comisia/Republica Federală Germania*[498], Comisia Europeană a solicitat CJUE să declare că Germania a transpus în mod eronat cerința de „independență deplină" cu care trebuie să acționeze autoritățile de supraveghere responsabile pentru garantarea protecției datelor, neîndeplinindu-și astfel obligațiile care îi revin conform articolului 28 alineatul (1) din Directiva privind protecția datelor. În opinia Comisiei, faptul că Germania a plasat autoritățile de supraveghere care monitorizează prelucrarea datelor cu caracter personal în diferite state federale (*Länder*) sub supravegherea statului pentru a asigura conformitatea cu legislația privind protecția datelor a încălcat cerința de independență.

CJUE a subliniat că termenul „independență deplină" trebuie interpretat pe baza formulării efective a dispoziției respective și a obiectivelor și structurii legislației privind protecția datelor[499]. CJUE a subliniat că autoritățile de supraveghere sunt „gardienii" drepturilor legate de prelucrarea datelor cu caracter personal. Astfel, instituirea lor în statele membre este considerată „un element esențial al protecției persoanelor în ceea ce privește prelucrarea

496 Regulamentul general privind protecția datelor, articolul 52 alineatul (1); Convenția 108 modernizată, articolul 15 alineatul (5).

497 FRA, *Fundamental rights: challenges and achievements in 2010* (Drepturile fundamentale: provocări și realizări în 2010), Raportul anual pe 2010, p. 59; FRA, *Data protection in the European Union: the role of National Data Protection Authorities* (Protecția datelor în Uniunea Europeană: rolul autorităților naționale pentru protecția datelor), mai 2010.

498 Hotărârea CJUE [MC] din 9 martie 2010 în cauza C-518/07, *Comisia Europeană/Republica Federală Germania*, punctul 27.

499 *Ibidem*, punctele 17 și 29.

datelor cu caracter personal”[500]. CJUE a concluzionat că „în exercitarea atribuțiilor, autoritățile de supraveghere trebuie să acționeze într-un mod obiectiv și imparțial. În acest sens, acestea trebuie să fie protejate de orice influență exterioară, inclusiv aceea directă sau indirectă a [autorităților publice]”[501].

CJUE a stabilit, de asemenea, că sensul termenului „independență deplină” trebuie interpretat având în vedere independența AEPD, astfel cum este definită în Regulamentul privind protecția datelor de către instituțiile europene. În acest regulament, conceptul de independență impune ca AEPD să nu solicite și să nu accepte instrucțiuni de la nicio parte externă.

În consecință, CJUE a stabilit că autoritățile de supraveghere din Germania – din cauza monitorizării de către autoritățile publice – nu erau pe deplin independente în sensul legislației UE privind protecția datelor.

Exemplu: În cauza *Comisia/Republica Austria*[502], CJUE a evidențiat probleme similare privind independența unor membri ai personalului Autorității pentru protecția datelor din Austria (Comisia pentru Protecția Datelor, DSK). CJUE a concluzionat că furnizarea de forță de muncă din partea cancelariei federale către autoritatea de supraveghere a subminat cerința de independență prevăzută de legislația UE privind protecția datelor. De asemenea, CJUE a stabilit că cerința ca autoritatea de supraveghere să informeze în permanență cancelaria cu privire la activitatea sa anula independența deplină a autorității de supraveghere.

Exemplu: În cauza *Comisia Europeană/Ungaria*[503] au fost interzise practici naționale similare care afectează independența forței de muncă. CJUE a subliniat că „cerința [...] potrivit căreia trebuie să se garanteze că fiecare autoritate de supraveghere exercită în condiții de independență deplină atribuțiile cu care este investită implică obligația statului membru în cauză de a respecta durata mandatului unei astfel de autorități până la termenul prevăzut inițial”. De asemenea, CJUE a declarat că, „prin faptul că a pus capăt în mod anticipat

500 *Ibidem*, punctul 23.

501 *Ibidem*, punctul 25.

502 Hotărârea CJUE [MC] din 16 octombrie 2012 în cauza C-614/10, *Comisia Europeană/Republica Austria*, punctele 59 și 63.

503 Hotărârea CJUE [MC] din 8 aprilie 2014 în cauza C-288/12, *Comisia Europeană/Ungaria*, punctele 50 și 67.

> mandatului autorității de supraveghere a protecției datelor cu caracter personal, Ungaria nu și-a îndeplinit obligațiile care îi revin în temeiul Directivei 95/46/CE [...]".

Noțiunea și criteriile „independenței depline" sunt prevăzute acum în mod explicit în RGPD, care încorporează principiile stabilite prin hotărârile CJUE descrise. În temeiul regulamentului, independența deplină în îndeplinirea sarcinilor și în exercitarea competențelor presupune următoarele[504]:

- membrii fiecărei autorități de supraveghere trebuie să rămână independenți de orice influență externă directă sau indirectă și nu trebuie să accepte instrucțiuni de la nicio parte externă;
- membrii fiecărei autorități de supraveghere trebuie să se abțină de la a întreprinde acțiuni incompatibile cu atribuțiile lor, pentru a evita conflictele de interese;
- statele membre trebuie să pună la dispoziția fiecărei autorități de supraveghere resursele umane, tehnice și financiare și infrastructura necesară pentru îndeplinirea eficientă a sarcinilor sale;
- statele membre trebuie să se asigure că fiecare autoritate de supraveghere își selectează personalul propriu;
- fiecare autoritate de supraveghere face obiectul unui control financiar în conformitate cu legislația națională, dar acest control nu trebuie să aducă atingere independenței autorității. Autoritățile de supraveghere trebuie să dispună de bugete anuale separate și publice, care să le permită funcționarea corectă.

Independența autorităților de supraveghere este considerată o cerință esențială și în cadrul legislației CoE. Convenția 108 modernizată impune autorităților de supraveghere „să acționeze cu independență și imparțialitate deplină în îndeplinirea sarcinilor și în exercitarea competențelor lor", fără să solicite sau să accepte instrucțiuni[505]. Astfel, convenția recunoaște că aceste autorități nu pot proteja în mod eficient drepturile și libertățile persoanelor fizice legate de prelucrarea datelor decât dacă își exercită funcțiile cu independență deplină. Raportul explicativ privind Convenția 108

504 Regulamentul general privind protecția datelor, articolul 52.

505 Convenția 108 modernizată, articolul 15 alineatul (5).

modernizată stabilește o serie de elemente care contribuie la protejarea acestei independențe. Printre aceste elemente se numără posibilitatea autorităților de supraveghere de a-și angaja personal propriu și de a adopta decizii fără a fi supuse ingerințelor externe, precum și factori legați de durata exercitării funcțiilor lor și de condițiile în care își pot înceta mandatul[506].

5.2. Competență și prerogative

În cadrul legislației UE, RGPD evidențiază competențele și structura organizatorică a autorităților de supraveghere și prevede că acestea trebuie să fie competente și să dețină prerogativa de a îndeplini sarcinile impuse de regulament.

Autoritatea de supraveghere este principalul organism care, în temeiul dreptului intern, asigură respectarea legislației UE privind protecția datelor. Autoritățile de supraveghere au un portofoliu cuprinzător de sarcini și competențe pe lângă monitorizare, care includ activități de supraveghere proactive și preventive. Pentru îndeplinirea acestor sarcini, autoritățile de supraveghere trebuie să dispună de competențe de investigare, corective și de consiliere adecvate, astfel cum sunt enumerate în articolul 57 și 58 din RGPD, pentru a asigura următoarele[507]:

- să ofere consiliere operatorilor și persoanelor vizate cu privire la toate aspectele legate de protecția datelor;
- să autorizeze clauze contractuale standard, reguli corporatiste obligatorii sau acorduri administrative;
- să investigheze operațiunile de prelucrare a datelor și să intervină în mod corespunzător;
- să solicite prezentarea oricărei informații relevante pentru supravegherea activităților operatorului;
- să emită avertizări sau mustrări adresate operatorilor și să solicite înștiințarea persoanelor vizate cu privire la încălcările securității datelor cu caracter personal;

506 Raportul explicativ privind Convenția 108 modernizată.

507 Regulamentul general privind protecția datelor, articolul 58. Vezi, de asemenea, articolul 2 alineatul (1) din Protocolul adițional la Convenția 108.

- să dispună blocarea accesului la date sau rectificarea, ștergerea sau distrugerea datelor;

- să interzică temporar sau definitiv prelucrarea sau să impună amenzi administrative;

- să sesizeze o instanță de judecată.

În vederea exercitării atribuțiilor cu care a fost învestită, o autoritate de supraveghere trebuie să aibă acces la toate datele cu caracter personal și la toate informațiile necesare pentru investigațiile desfășurate, precum și la orice sediu în care un operator păstrează informații relevante. Potrivit CJUE, competențele autorității de supraveghere trebuie interpretate în sens larg, pentru a se asigura eficacitatea deplină a protecției datelor pentru persoanele vizate în UE.

Exemplu: În cauza *Schrems*, CJUE a examinat dacă transferul datelor cu caracter personal către SUA în temeiul primului acord UE-SUA privind sfera de siguranță era conformă cu legislația UE privind protecția datelor, în contextul dezvăluirilor lui Edward Snowden. Raționamentul CJUE a stabilit că autoritățile naționale de supraveghere – care acționează în calitate de organisme independente de monitorizare a prelucrării datelor de către operatori – pot împiedica transferarea datelor cu caracter personal într-o țară terță, în pofida existenței unei decizii privind caracterul adecvat al nivelului de protecție, dacă există dovezi rezonabile că nivelul adecvat de protecție nu mai este garantat în țara terță[508].

Fiecare autoritate de supraveghere are competența de a exercita prerogative de investigare și de intervenție pe teritoriul său. Cu toate acestea, având în vedere că activitățile operatorilor și ale persoanelor împuternicite de operatori sunt deseori transfrontaliere, iar prelucrarea datelor afectează persoane vizate din mai multe state membre, se pune problema alocării competențelor între diferitele autorități de supraveghere. CJUE a avut ocazia să examineze acest aspect în cauza *Weltimmo*.

508 Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*, punctele 26-36 și 40-41.

Exemplu: În cauza *Weltimmo*[509], CJUE a examinat competența autorităților naționale de supraveghere de a aborda cazuri care implică organizații care nu sunt stabilite în jurisdicția lor. Weltimmo era o societate înmatriculată în Slovacia care administra o pagină de internet pe care publica anunțuri privind imobile situate în Ungaria. Autorii anunțurilor au formulat plângeri în fața autorității maghiare de supraveghere a protecției datelor pentru încălcarea legislației privind protecția datelor din Ungaria, iar autoritatea a amendat societatea Weltimmo. Societatea a contestat amenda în fața instanțelor naționale, iar cauza a fost trimisă CJUE pentru a se stabili dacă Directiva privind protecția datelor a UE permitea autorității de supraveghere a unui stat membru să aplice dreptul intern în materie de protecție a datelor unei societăți înmatriculate într-un alt stat membru.

CJUE a interpretat articolul 4 alineatul (1) litera (a) din Directiva privind protecția datelor în sensul că permite aplicarea legislației privind protecția datelor cu caracter personal a unui alt stat membru decât cel în care este înmatriculat operatorul acestor date, „în măsura în care acesta exercită, într-o formă de instalare stabilă pe teritoriul acestui stat membru, o activitate efectivă și reală, chiar minimă, în cadrul căreia este efectuată prelucrarea în discuție". CJUE a constatat că, pe baza informațiilor de care dispune, Weltimmo desfășura o activitate efectivă și reală în Ungaria, întrucât societatea dispunea de un reprezentant în Ungaria, care era menționat în registrul slovac al societăților cu o adresă situată în Ungaria, precum și de un cont bancar și de o căsuță poștală în Ungaria, și desfășura activități în Ungaria implicând anunțuri redactate în limba maghiară. Întrucât aceste informații indicau existența unui sediu, activitatea Weltimmo intra sub incidența legislației maghiare privind protecția datelor și sub jurisdicția autorității maghiare de supraveghere. Cu toate acestea, CJUE a stabilit că îi revine instanței naționale să verifice informațiile și să decidă dacă Weltimmo avea într-adevăr un sediu în Ungaria.

Dacă instanța de trimitere constata că Weltimmo are un sediu în Ungaria, autoritatea maghiară de supraveghere avea competența de a impune o amendă. În schimb, dacă instanța națională decidea contrariul, și anume că Weltimmo nu avea sediu în Ungaria, legislația aplicabilă ar fi fost, în consecință, aceea a statului membru (statelor membre) în care societatea era înmatriculată. În acest caz, deoarece competențele autorităților de

509 Hotărârea CJUE din 1 octombrie 2015 în cauza C-230/14, *Weltimmo s.r. o./Nemzeti Adatvédelmi és Információszabadság Hatóság*.

supraveghere trebuie să fie exercitate în conformitate cu suveranitatea teritorială a altor state membre, autoritatea maghiară nu ar fi avut competența de a impune sancțiuni. Întrucât Directiva privind protecția datelor a inclus o obligație de cooperare între autoritățile de supraveghere, autoritatea maghiară putea totuși să solicite omoloagei sale slovace să examineze chestiunea, să stabilească faptul că avusese loc o încălcare a legislației slovace și să impună sancțiunile prevăzute de legislația slovacă.

Odată cu adoptarea RGPD s-au introdus norme detaliate privind competența autorităților de supraveghere în cazurile transfrontaliere. Regulamentul stabilește un „mecanism al ghișeului unic" și include dispoziții care impun cooperarea între diferitele autorități de supraveghere. Pentru o cooperare eficientă în cazurile transfrontaliere, RGPD prevede că autoritatea de supraveghere a sediului principal sau a sediului unic al operatorului sau al persoanei împuternicite de operator este competentă să acționeze în calitate de autoritate de supraveghere principală[510]. Autoritatea de supraveghere principală este responsabilă pentru cazurile transfrontaliere, este singurul interlocutor al operatorului sau al persoanei împuternicite de operator și coordonează cooperarea cu alte autorități de supraveghere pentru a ajunge la un consens. Cooperarea include schimbul de informații și asistența reciprocă pentru monitorizare, investigare și adoptarea de decizii cu caracter obligatoriu[511].

În legislația CoE, competențele și prerogativele autorităților de supraveghere sunt prevăzute la articolul 15 din Convenția 108 modernizată. Aceste competențe corespund celor atribuite autorităților de supraveghere în temeiul legislației UE, inclusiv competențe de investigare și de intervenție, de adoptare a deciziilor și de impunere a unor sancțiuni administrative pentru încălcarea dispozițiilor convenției, precum și de a se constitui parte în proceduri judiciare. Autoritățile de supraveghere independente au, de asemenea, competența de a examina solicitări și plângeri depuse de persoanele vizate, de a sensibiliza publicul cu privire la legislația privind protecția datelor și de a oferi consiliere factorilor de decizie de la nivel național cu privire la orice măsuri legislative sau administrative care reglementează prelucrarea datelor cu caracter personal.

510 Regulamentul general privind protecția datelor, articolul 56 alineatul (1).

511 *Ibidem*, articolul 60.

5.3. Cooperare

RGPD stabilește un cadru general pentru cooperarea dintre autoritățile de supraveghere și prevede norme mai specifice privind cooperarea autorităților de supraveghere în cazul activităților transfrontaliere de prelucrare a datelor.

În temeiul RGPD, autoritățile de supraveghere își furnizează reciproc informații relevante și asistență pentru a pune în aplicare regulamentul în mod coerent[512]. Această prevedere include efectuarea de consultări, inspecții și investigații de către autoritatea de supraveghere căreia i se solicită cooperarea. Autoritățile de supraveghere pot desfășura operațiuni comune, inclusiv investigații comune și măsuri comune de aplicare a legii, în care sunt implicați membri ai personalului tuturor autorităților de supraveghere[513].

În UE, operatorii și persoanele împuternicite de operatori desfășoară tot mai multe acțiuni la nivel transnațional. Acest lucru necesită o cooperare strânsă între autoritățile de supraveghere competente din statele membre pentru a se asigura faptul că prelucrarea datelor cu caracter personal respectă cerințele RGPD. În conformitate cu mecanismul „ghișeului unic" instituit de regulament, dacă un operator sau o persoană împuternicită de operator deține sedii în mai multe state membre sau dacă are un singur sediu, dar operațiunile de prelucrare afectează în mod semnificativ persoane vizate din mai multe state membre, autoritatea de supraveghere a sediului principal (sau unic) acționează în calitate de autoritate principală pentru activitățile transfrontaliere ale operatorului sau ale persoanei împuternicite de operator. Autoritățile principale au competența de a lua măsuri de aplicare a legii împotriva operatorului sau a persoanei împuternicite de operator. Mecanismul ghișeului unic are scopul de a îmbunătăți armonizarea și aplicarea uniformă a legislației UE privind protecția datelor în diferitele state membre. De asemenea, este benefic pentru întreprinderi, deoarece acestea au posibilitatea de a colabora cu o singură autoritate, cea principală, în locul mai multor autorități de supraveghere. Acest lucru sporește securitatea juridică pentru întreprinderi și, la nivel concret, ar trebui, de asemenea, să permită adoptarea mai rapidă a deciziilor și să scutească întreprinderile de situația în care autorități de supraveghere diferite le-ar impune cerințe contradictorii.

Identificarea autorităților principale implică stabilirea localizării sediului principal al unei întreprinderi în UE. Termenul „sediu principal" este definit în RGPD. În plus, Grupul de lucru „Articolul 29" a emis orientări pentru identificarea autorității de

512 *Ibidem*, articolul 61 alineatele (1)-(3) și articolul 62 alineatul (1).

513 *Ibidem*, articolul 62 alineatul (1).

supraveghere principale a unui operator sau a unei persoane împuternicite de operator, care includ criteriile de identificare a sediului principal[514].

Pentru a asigura un nivel ridicat de protecție a datelor în întreaga UE, autoritatea de supraveghere principală nu acționează singură. Aceasta trebuie să coopereze cu celelalte autorități de supraveghere în cauză pentru a adopta decizii privind prelucrarea datelor cu caracter personal de către operatori și persoanele împuternicite de operatori, în încercarea de a ajunge la un consens și de a asigura coerența. Cooperarea dintre autoritățile de supraveghere competente include schimbul de informații, asistența reciprocă, desfășurarea de investigații comune și de activități comune de monitorizare[515]. În cadrul asistenței reciproce, autoritățile de supraveghere trebuie să răspundă cu exactitate cererilor de informații formulate de alte autorități de supraveghere și să exercite măsuri de supraveghere, cum ar fi, de exemplu, autorizări și consultări prealabile cu operatorul de date în ceea ce privește activitățile de prelucrare ale acestuia, precum și inspecții sau investigații. Asistența reciprocă acordată autorităților de supraveghere din alte state membre trebuie furnizată la cerere, fără întârzieri nejustificate și cel târziu în termen de o lună de la data primirii cererii[516].

În cazul în care operatorul are sedii în mai multe state membre, autoritățile de supraveghere pot desfășura operațiuni comune, inclusiv investigații comune și măsuri comune de aplicare a legii, în care sunt implicați membri ai personalului autorităților de supraveghere din alte state membre[517].

Cooperarea dintre diferitele autorități de supraveghere este o cerință importantă și în legislația CoE. Convenția 108 modernizată prevede că autoritățile de supraveghere trebuie să coopereze între ele în măsura necesară îndeplinirii sarcinilor care le revin[518]. Acest lucru ar trebui realizat, de exemplu, prin furnizarea reciprocă a oricăror informații relevante și utile și prin coordonarea investigațiilor și desfășurarea de acțiuni comune[519].

514 Orientările Grupului de lucru „Articolul 29" pentru identificarea autorității de supraveghere principale a unui operator sau a unei persoane împuternicite de operator, WP 244, Bruxelles, revizuite la 5 aprilie 2017.

515 Regulamentul general privind protecția datelor, articolul 60 alineatele (1)-(3).

516 *Ibidem*, articolul 61 alineatele (1) și (2).

517 *Ibidem*, articolul 62 alineatul (1).

518 Convenția 108 modernizată, articolele 16 și 17.

519 *Ibidem*, articolul 17.

5.4. Comitetul European pentru Protecția Datelor

Importanța autorităților de supraveghere independente și competențele principale atribuite acestora în temeiul legislației europene privind protecția datelor au fost descrise anterior în prezentul capitol. Comitetul European pentru Protecția Datelor (CEPD) este un alt actor important pentru asigurarea aplicării eficiente și consecvente a normelor de protecție a datelor în întreaga UE.

RGPD a instituit CEPD ca organ al UE cu personalitate juridică[520]. Acesta este succesorul Grupului de lucru „Articolul 29"[521], instituit de Directiva privind protecția datelor pentru a consilia Comisia cu privire la orice măsuri ale UE care afectează drepturile persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și respectarea vieții private, pentru a promova aplicarea uniformă a directivei și pentru a furniza expertiză Comisiei cu privire la aspectele legate de protecția datelor. Grupul de lucru „Articolul 29" a fost compus din reprezentanți ai autorităților de supraveghere ale statelor membre ale UE, precum și din reprezentanți ai Comisiei și ai AEPD.

Similar Grupului de lucru, CEPD este compus din șefii autorităților de supraveghere din fiecare stat membru și al AEPD sau din reprezentanții acestora[522]. AEPD deține drept de vot egal, cu excepția cazurilor legate de soluționarea litigiilor, în care poate vota numai deciziile care privesc principiile și normele aplicabile în ceea ce privește instituțiile Uniunii care corespund pe fond cu cele din RGPD. Comisia are dreptul de a participa la activitățile și reuniunile CEPD, însă nu are drept de vot[523]. Votând cu majoritate simplă, comitetul își alege un președinte (care este însărcinat cu reprezentarea acestuia) și doi vicepreședinți din rândul membrilor, pentru mandate de cinci ani. În plus, CEPD dispune de asemenea de un secretariat asigurat de AEPD, care furnizează comitetului sprijin analitic, administrativ și logistic[524].

520 Regulamentul general privind protecția datelor, articolul 68.

521 În temeiul Directivei 95/46/CE, Grupul de lucru „Articolul 29" avea sarcina de a consilia Comisia cu privire la orice măsuri ale UE care afectează drepturile persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și respectarea vieții private, de a promova aplicarea uniformă a directivei și de a furniza expertiză Comisiei cu privire la aspectele legate de protecția datelor. Grupul de lucru „Articolul 29" a fost compus din reprezentanți ai autorităților de supraveghere ale statelor membre ale UE, precum și din reprezentanți ai Comisiei și ai AEPD.

522 Regulamentul general privind protecția datelor, articolul 68 alineatul (3).

523 *Ibidem*, articolul 68 alineatele (4) și (5).

524 *Ibidem*, articolele 73 și 75.

Atribuțiile CEPD sunt detaliate la articolele 64, 65 și 70 din RGPD și includ sarcini cuprinzătoare, care pot fi defalcate în trei activități principale:

- **Coerență:** CEPD poate emite decizii cu caracter obligatoriu în trei cazuri: atunci când o autoritate de supraveghere a formulat o obiecție relevantă și motivată în cazuri privind ghișeele unice, atunci când există opinii divergente cu privire la care dintre autoritățile de supraveghere este cea „principală" și, în sfârșit, atunci când autoritatea de supraveghere competentă nu solicită sau nu ține seama de avizul CEPD[525]. Responsabilitatea principală a CEPD este de a se asigura că RGPD este aplicat în mod coerent în întreaga UE; comitetul joacă un rol esențial în mecanismul pentru asigurarea coerenței, astfel cum se descrie în secțiunea 5.5.

- **Consultare:** Sarcinile CEPD includ consilierea Comisiei cu privire la orice aspect legat de protecția datelor cu caracter personal în Uniune, cum ar fi modificările RGPD, revizuirile legislației UE care implică prelucrarea datelor și ar putea fi în conflict cu normele UE de protecție a datelor, precum și adoptarea deciziilor Comisiei privind caracterul adecvat al nivelului de protecție care permit transferul de date cu caracter personal către o țară terță sau o organizație internațională.

- **Orientări:** Comitetul emite, de asemenea, orientări, recomandări și bune practici pentru a încuraja aplicarea consecventă a regulamentului și promovează cooperarea și schimburile de cunoștințe între autoritățile de supraveghere. În plus, trebuie să încurajeze asociațiile operatorilor sau ale persoanelor împuternicite de operatori să elaboreze coduri de conduită, precum și să instituie mecanisme de certificare și mărci de protecție a datelor.

Deciziile CEPD pot fi contestate în fața CJUE.

5.5. Mecanismul pentru asigurarea coerenței instituit de RGPD

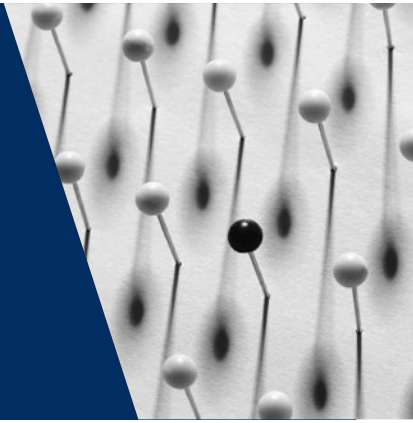
RGPD instituie un mecanism pentru asigurarea coerenței care să faciliteze aplicarea coerentă a regulamentului în toate statele membre, prin intermediul căruia autoritățile de supraveghere cooperează între ele și, după caz, cu Comisia. Mecanismul pentru asigurarea coerenței este utilizat în două tipuri de situații. Primul corespunde avizelor CEPD în cazurile în care o autoritate competentă de supraveghere

525 *Ibidem*, articolul 65.

intenționează să adopte măsuri, cum ar fi o listă a operațiunilor de prelucrare care necesită o evaluare a impactului asupra protecției datelor, sau să stabilească clauze contractuale standard. Al doilea privește deciziile CEPD cu caracter obligatoriu pentru autoritățile de supraveghere în cazurile de ghișee unice și în cazurile în care o autoritate de supraveghere nu solicită sau nu ține seama de avizul CEPD.

6

Drepturile persoanelor vizate și asigurarea respectării acestora



UE	Aspecte vizate	CoE
Dreptul de a fi informat		
Regulamentul general privind protecția datelor, articolul 12 Hotărârea CJUE în cauza C-473/12, *Institut professionnel des agents immobiliers (IPI)/Englebert*, 2013 Hotărârea CJUE în cauza C-201/14, *Smaranda Bara și alții/Casa Națională de Asigurări de Sănătate și alții*, 2015	**Transparența informațiilor**	Convenția 108 modernizată, articolul 8
Regulamentul general privind protecția datelor, articolul 13 alineatele (1) și (2) și articolul 14 alineatele (1) și (2)	**Conținutul informațiilor**	Convenția 108 modernizată, articolul 8 alineatul (1)
Regulamentul general privind protecția datelor, articolul 13 alineatul (1) și articolul 14 alineatul (3)	**Termenul de furnizare a informațiilor**	Convenția 108 modernizată, articolul 9 alineatul (1) litera (b)
Regulamentul general privind protecția datelor, articolul 12 alineatele (1), (5) și (7)	**Modalitatea de furnizare a informațiilor**	Convenția 108 modernizată, articolul 9 alineatul (1) litera (b)
Regulamentul general privind protecția datelor, articolul 13 alineatul (2) litera (d) și articolul 14 alineatul (2) litera (e), articolele 77, 78 și 79	**Dreptul de a depune o plângere**	Convenția 108 modernizată, articolul 9 alineatul (1) litera (f)

UE	Aspecte vizate	CoE
Dreptul de acces		
Regulamentul general privind protecția datelor, articolul 15 alineatul (1) Hotărârea CJUE în cauza C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, 2009 Hotărârea CJUE în cauzele conexate C-141/12 și C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel* și *Minister voor Immigratie, Integratie en Asiel/M și S*, 2014 Hotărârea CJUE în cauza C-434/16, *Peter Nowak/Data Protection Commissioner*, 2017	**Dreptul de acces la datele proprii**	Convenția 108 modernizată, articolul 9 alineatul (1) litera (b) Hotărârea CEDO în cauza *Leander/Suedia*, nr. 9248/81, 1987
Dreptul la rectificare		
Regulamentul general privind protecția datelor, articolul 16	**Rectificarea datelor cu caracter personal inexacte**	Convenția 108 modernizată, articolul 9 alineatul (1) litera (e) Hotărârea CEDO în cauza *Cemalettin Canli/Turcia*, nr. 22427/04, 2008 Hotărârea CEDO în cauza *Ciubotaru/Moldova*, nr. 27138/04, 2010
Dreptul la ștergerea datelor		
Regulamentul general privind protecția datelor, articolul 17 alineatul (1)	**Ștergerea datelor cu caracter personal**	Convenția 108 modernizată, articolul 9 alineatul (1) litera (e) Hotărârea CEDO în cauza *Segerstedt-Wiberg și alții/Suedia*, nr. 62332/00, 2006
Hotărârea CJUE [MC] în cauza C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 2014 Hotărârea CJUE în cauza C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 2017	**Dreptul de a fi uitat**	

UE	Aspecte vizate	CoE
Dreptul la restricționarea prelucrării		
Regulamentul general privind protecția datelor, articolul 18 alineatul (1)	**Dreptul de a obține restricționarea utilizării datelor cu caracter personal**	
Regulamentul general privind protecția datelor, articolul 19	**Obligația de notificare**	
Dreptul la portabilitatea datelor		
Regulamentul general privind protecția datelor, articolul 20	**Dreptul la portabilitatea datelor**	
Dreptul la opoziție		
Regulamentul general privind protecția datelor, articolul 21 alineatul (1) Hotărârea CJUE în cauza C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/ Salvatore Manni*, 2017	**Dreptul la opoziție ca urmare a situației particulare în care se află persoana vizată**	Recomandarea privind crearea de profiluri, articolul 5.3 Convenția 108 modernizată, articolul 9 alineatul (1) litera (d)
Regulamentul general privind protecția datelor, articolul 21 alineatul (2)	**Dreptul la opoziție față de utilizarea datelor în scopuri de marketing**	Recomandarea privind marketingul direct, articolul 4.1
Regulamentul general privind protecția datelor, articolul 21 alineatul (5)	**Dreptul de a se opune prin mijloace automate**	
Drepturi legate de procesul decizional automatizat și de crearea de profiluri		
Regulamentul general privind protecția datelor, articolul 22	**Drepturi legate de procesul decizional automatizat și de crearea de profiluri**	Convenția 108 modernizată, articolul 9 alineatul (1) litera (a)
Regulamentul general privind protecția datelor, articolul 21	**Dreptul de a se opune procesului decizional automatizat**	
Regulamentul general privind protecția datelor, articolul 13 alineatul (2) litera (f)	**Dreptul la o explicație pertinentă**	Convenția 108 modernizată, articolul 9 alineatul (1) litera (c)

UE	Aspecte vizate	CoE
Căi de atac, răspundere, sancțiuni și despăgubiri		
Carta, articolul 47 Hotărârea CJUE [MC] în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*, 2015 Regulamentul general privind protecția datelor, articolele 77-84	**Pentru încălcări ale legislației naționale privind protecția datelor**	Convenția europeană a drepturilor omului, articolul 13 (doar pentru statele membre ale CoE) Convenția 108 modernizată, articolul 9 alineatul (1) litera (f) și articolele 12, 15 și 16-21 Hotărârea CEDO în cauza *K.U./Finlanda*, nr. 2872/02 Hotărârea CEDO în cauza *Biriuk/Lituania*, nr. 23373/03, 2008
Regulamentul privind protecția datelor de către instituțiile europene, articolele 34 și 49 Hotărârea CJUE [MC] în cauza C-28/08 P, *Comisia Europeană/The Bavarian Lager Co. Ltd.*, 2010	**Pentru încălcări ale dreptului UE de către instituțiile și organismele UE**	

Eficacitatea normelor juridice, în general, și a drepturilor persoanelor vizate, în special, depinde într-o măsură considerabilă de existența unor mecanisme adecvate pentru punerea în aplicare a acestora. În era digitală, prelucrarea datelor a devenit omniprezentă și din ce în ce mai dificil de înțeles pentru publicul larg. Pentru a diminua dezechilibrele de putere dintre persoanele vizate și operatori, persoanelor fizice li se conferă anumite drepturi, pentru a exercita un control mai mare asupra prelucrării informațiilor lor cu caracter personal. Dreptul de acces la datele proprii și dreptul de a obține rectificarea acestora sunt consacrate la articolul 8 alineatul (2) din Carta drepturilor fundamentale a UE, document care face parte din legislația primară a UE și care are o valoare fundamentală în ordinea juridică a Uniunii. Legislația secundară a UE – în special Regulamentul general privind protecția datelor – a stabilit un cadru juridic coerent care capacitează persoanele vizate conferindu-le anumite drepturi în relația cu operatorii de date. Pe lângă drepturile de acces și de rectificare, RGPD recunoaște o serie de alte drepturi, cum ar fi dreptul la ștergerea datelor („dreptul de a fi uitat"), dreptul de opoziție sau de restricționare a prelucrării datelor, precum și drepturi legate de procesul decizional automatizat și de crearea de profiluri. În Convenția 108 modernizată sunt incluse măsuri similare de protecție pentru a permite persoanelor vizate să exercite un control eficace asupra datelor lor. Articolul 9 enumeră drepturile pe care ar trebui să le poată exercita persoanele fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Părțile contractante

trebuie să se asigure că aceste drepturi sunt disponibile tuturor persoanelor vizate din jurisdicția lor și că drepturile în cauză sunt însoțite de mijloace legale și practice eficiente care permit persoanelor vizate să le exercite.

Pe lângă consacrarea drepturilor persoanelor, este la fel de important să se stabilească mecanisme care să permită persoanelor vizate să conteste încălcarea drepturilor lor, să tragă la răspundere operatorii și să solicite despăgubiri. Dreptul la o cale de atac eficientă, astfel cum este garantat prin Convenția europeană a drepturilor omului și prin Cartă, prevede punerea la dispoziție a căilor de atac pentru fiecare persoană.

6.1. Drepturile persoanelor vizate

Principalele elemente

- Orice persoană vizată are dreptul de a primi informații privind orice prelucrare a datelor sale cu caracter personal de către un operator de date, sub rezerva unor excepții limitate.
- Persoanele vizate au următoarele drepturi:
  - să obțină accesul la propriile date și să primească anumite informații despre prelucrare;
  - să obțină rectificarea datelor lor de către operatorul care se ocupă de prelucrarea acestor date în cazul în care datele respective sunt incorecte;
  - să solicite, după caz, ștergerea datelor lor de către operator în cazul în care acesta prelucrează datele respective în mod ilegal;
  - să obțină restricționarea temporară a prelucrării;
  - să obțină portarea datelor lor la un alt operator în anumite condiții.
- De asemenea, persoanele vizate au dreptul de a se opune prelucrării în următoarele situații:
  - pentru motive legate de situația lor particulară;
  - în cazul utilizării datelor lor în scopuri de marketing direct.

- Persoanele vizate au dreptul de a nu face obiectul unor decizii bazate exclusiv pe prelucrarea automatizată, inclusiv crearea de profiluri, care au efecte juridice sau care afectează în mod semnificativ respectiva persoană. Persoanele vizate au, de asemenea, următoarele drepturi:
  - de a obține intervenție umană din partea operatorului;
  - de a-și exprima punctul de vedere și de a contesta o decizie bazată pe prelucrarea automatizată.

6.1.1. Dreptul de a fi informat

În conformitate cu **legislația CoE**, precum și cu **legislația UE**, operatorii au obligația de a informa persoana vizată, în momentul colectării datelor cu caracter personal, cu privire la intenția de prelucrare. Această obligație nu depinde de o solicitare din partea persoanei vizate, ci operatorul trebuie să o îndeplinească în mod proactiv, indiferent dacă persoana vizată se arată interesată sau nu de informații.

În conformitate cu legislația CoE, în temeiul articolului 8 din Convenția 108 modernizată, părțile contractante trebuie să prevadă obligația operatorilor de a informa persoanele vizate cu privire la identitatea și reședința lor obișnuită, temeiul juridic și scopul prelucrării, categoriile de date cu caracter personal prelucrate, destinatarii datelor cu caracter personal ale persoanei vizate (dacă există) și modul în care persoana vizată își poate exercita drepturile în temeiul articolului 9, inclusiv dreptul la acces, rectificare și căi de atac. Orice alte informații suplimentare considerate necesare pentru a asigura prelucrarea echitabilă și transparentă a datelor cu caracter personal trebuie, de asemenea, să fie comunicate persoanelor vizate. Raportul explicativ privind Convenția 108 modernizată clarifică faptul că informațiile prezentate persoanelor vizate „trebuie să fie ușor accesibile, lizibile, ușor de înțeles și adaptate persoanelor vizate în cauză”[526].

În conformitate cu legislația UE, principiul transparenței impune ca orice prelucrare a datelor cu caracter personal să fie, în general, transparentă pentru persoanele fizice. Persoanele fizice au dreptul de a fi informate despre categoriile de date cu caracter personal colectate, utilizate sau prelucrate în alt mod și despre modalitățile de colectare, utilizare și prelucrare, precum și despre riscurile, garanțiile și drepturile lor în ceea ce privește prelucrarea[527]. Astfel, articolul 12 din RGPD stabilește o obligație cuprinzătoare pentru operatori de a furniza informații transparente și/sau de

526 Raportul explicativ privind Convenția 108 modernizată, punctul 68.

527 Regulamentul general privind protecția datelor, considerentul 39.

a comunica modul în care persoanele vizate își pot exercita drepturile[528]. Informațiile trebuie să fie concise, transparente, inteligibile și ușor accesibile, formulate într-un limbaj clar și simplu. Trebuie furnizate în scris, inclusiv în format electronic, atunci când este oportun; la solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită fără echivoc prin alte mijloace. Informațiile sunt furnizate fără întârzieri sau cheltuieli excesive[529].

Articolele 13 și 14 din RGPD prevăd dreptul persoanelor vizate de a fi informate, fie în situațiile în care datele cu caracter personal au fost colectate direct de la persoana vizată, fie în situațiile în care datele nu au fost obținute de la persoana vizată.

Domeniul de aplicare al dreptului la informare și limitările acestuia în temeiul legislației UE au fost clarificate în jurisprudența CJUE.

Exemplu: În cauza *Institut professionnel des agents immobiliers (IPI)/Englebert*[530], CJUE i s-a solicitat să interpreteze articolul 13 alineatul (1) din Directiva 95/46/CE. Acest articol oferea statelor membre posibilitatea de a adopta măsuri legislative pentru a restrânge sfera de aplicare a dreptului la informare al persoanei vizate, în cazul în care acest lucru este necesar pentru a proteja, printre altele, drepturile și libertățile celorlalți și pentru a preveni și a investiga infracțiuni sau încălcări ale eticii în cazul profesiunilor reglementate. IPI este un organism profesional al agenților imobiliari din Belgia, responsabil pentru asigurarea exercitării corespunzătoare a profesiei de agent imobiliar. Acesta a solicitat unei instanțe naționale să constate că pârâții au încălcat normele profesionale și să le ordone să înceteze diverse activități imobiliare. Acțiunea s-a bazat pe probe furnizate de detectivii particulari ale căror servicii au fost utilizate de IPI.

Instanța națională a avut îndoieli cu privire la valoarea care trebuie atribuită probelor prezentate de detectivi, ținând seama de posibilitatea ca ele să fi fost obținute fără respectarea cerințelor în materie de protecție a datelor din legislația belgiană, în special a obligației de a informa persoanele vizate cu privire la prelucrarea datelor lor cu caracter personal înainte de colectarea

528 *Ibidem*, articolele 13 și 14; Convenția 108 modernizată, articolul 8 alineatul (1) litera (b).

529 Regulamentul general privind protecția datelor, articolul 12 alineatul (5); Convenția 108 modernizată, articolul 9 alineatul (1) litera (b).

530 Hotărârea CJUE din 7 noiembrie 2013 în cauza C-473/12, *Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert și alții*.

datelor în cauză. CJUE a arătat că articolul 13 alineatul (1) prevede că statele membre „pot" – fără a fi obligate – să prevadă în dreptul lor național excepții de la obligația de a informa persoanele vizate cu privire la prelucrarea datelor lor. Întrucât articolul 13 alineatul (1) include prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor sau a încălcărilor eticii ca motive pentru care statele membre pot limita drepturile persoanelor fizice, activitatea unui organism precum IPI și a detectivilor particulari care au acționat în numele acestuia se poate baza pe această dispoziție. Cu toate acestea, dacă statul membru nu a prevăzut o astfel de excepție, persoanele vizate trebuie informate.

Exemplu: În cauza *Smaranda Bara și alții/Casa Națională de Asigurări de Sănătate și alții*[531], CJUE a clarificat dacă legislația UE împiedică o autoritate a administrației publice naționale să transmită date cu caracter personal unei alte autorități a administrației publice în scopul prelucrării ulterioare fără ca persoanele vizate să fie informate despre această transmitere și despre prelucrarea ulterioară. În această speță, Agenția Națională de Administrare Fiscală nu informase reclamanții că transmisese datele lor Casei Naționale de Asigurări de Sănătate înainte de a efectua această transmitere.

CJUE a considerat că cerința legislației UE de informare a persoanei vizate cu privire la prelucrarea datelor cu caracter personal ale acesteia este „cu atât mai importantă cu cât este o condiție necesară exercitării de către aceste persoane a dreptului lor de acces și de rectificare a datelor prelucrate [...] și a dreptului de opoziție al acestora față de prelucrarea datelor respective". Principiul prelucrării echitabile impune informarea persoanelor vizate cu privire la transmiterea datelor lor către o altă autoritate a administrației publice în vederea prelucrării ulterioare de către aceasta din urmă. În conformitate cu articolul 13 alineatul (1) din Directiva 95/46/CE, statele membre pot restrânge dreptul de a fi informat dacă acest lucru este considerat necesar pentru protejarea unui interes economic major al statului, inclusiv în ceea ce privește aspecte legate de impozitare. Cu toate acestea, astfel de restricții trebuie impuse prin măsuri legislative. Întrucât nici definiția datelor transmisibile, nici modalitățile de efectuare a transmiterii nu au fost elaborate prin intermediul unei măsuri legislative, ci printr-un protocol între cele două autorități ale administrației publice, condițiile de derogare prevăzute de legislația UE nu au

531 Hotărârea CJUE din 1 octombrie 2015 în cauza C-201/14, *Smaranda Bara și alții/Casa Națională de Asigurări de Sănătate și alții*.

fost îndeplinite. Reclamanții ar fi trebuit să fie informați în prealabil cu privire la transmiterea datelor lor către Casa Națională de Asigurări de Sănătate și cu privire la prelucrarea ulterioară a acestor date de către organismul respectiv.

Conținutul informațiilor

În conformitate cu articolul 8 alineatul (1) din Convenția 108 modernizată, operatorul este obligat să furnizeze persoanei vizate orice informații necesare pentru a asigura prelucrarea echitabilă și transparentă a datelor cu caracter personal, inclusiv:

- identitatea și reședința sau sediul obișnuit al operatorului;
- temeiul juridic și scopul prelucrării preconizate;
- categoriile de date cu caracter personal prelucrate;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;
- modalitățile în care persoanele vizate își pot exercita drepturile.

În conformitate cu RGPD, atunci când se colectează date cu caracter personal de la persoana vizată, operatorul, în momentul obținerii acestor date cu caracter personal, are obligația de a furniza persoanei vizate următoarele informații[532]:

- identitatea și datele de contact ale operatorului, inclusiv datele de contact ale RPD, dacă există;
- scopul și temeiul juridic al prelucrării, și anume obligația legală sau contractuală;
- interesul legitim urmărit de operatorul de date, în cazul în care acesta constituie temeiul juridic al prelucrării;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

532 Regulamentul general privind protecția datelor, articolul 13 alineatul (1).

- dacă datele vor fi transferate către o țară terță sau o organizație internațională și dacă acest transfer se bazează pe o decizie privind caracterul adecvat al nivelului de protecție a datelor sau pe garanții adecvate;

- perioada pentru care vor fi stocate datele cu caracter personal și, dacă stabilirea acestei perioade nu este posibilă, criteriile utilizate pentru a stabili perioada de stocare;

- drepturile persoanelor vizate în ceea ce privește prelucrarea, cum ar fi dreptul de a obține acces la date, rectificarea sau ștergerea acestora ori restricționarea prelucrării sau dreptul de a se opune prelucrării;

- dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală, dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;

- existența unui proces decizional automatizat incluzând crearea de profiluri;

- dreptul de a depune o plângere în fața unei autorități de supraveghere;

- existența dreptului de a retrage consimțământul.

În cazul unui proces decizional automatizat incluzând crearea de profiluri, persoanele vizate trebuie să primească informații pertinente privind logica utilizată în crearea profilurilor, precum și importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

În cazurile în care datele cu caracter personal nu sunt obținute direct de la persoana vizată, operatorul de date trebuie să înștiințeze persoana vizată cu privire la originea datelor cu caracter personal. În orice caz, operatorul trebuie, printre altele, să informeze persoanele vizate cu privire la existența unui proces decizional automatizat incluzând crearea de profiluri[533]. În sfârșit, dacă un operator intenționează să prelucreze date cu caracter personal într-un alt scop decât cel comunicat inițial persoanei vizate, principiul limitărilor legate de scop și principiul transparenței impun ca operatorul să furnizeze persoanei vizate informații cu privire la acest nou scop al

533 Regulamentul general privind protecția datelor, articolul 13 alineatul (2) și articolul 14 alineatul (2) litera (f).

prelucrării. Operatorii trebuie să furnizeze informații înainte de orice prelucrare ulterioară. Cu alte cuvinte, dacă persoana vizată și-a dat consimțământul pentru prelucrarea datelor cu caracter personal, operatorul trebuie să primească consimțământul reînnoit al persoanei vizate în cazul în care scopul prelucrării datelor se modifică sau dacă se adaugă alte scopuri.

Termenul de furnizare a informațiilor

RGPD distinge între două scenarii și două termene la care operatorul de date trebuie să furnizeze informații persoanei vizate:

- În cazul în care datele cu caracter personal sunt obținute direct de la persoana vizată, operatorul trebuie să înștiințeze persoana vizată cu privire la toate informațiile și drepturile sale conexe prevăzute de RGPD în momentul obținerii datelor[534].

- În cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop, operatorul furnizează toate informațiile relevante înainte de această prelucrare ulterioară.

- În cazul în care datele cu caracter personal nu au fost obținute direct de la persoana vizată, operatorul are obligația de a furniza persoanei vizate informații privind prelucrarea „într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună", sau înainte ca datele să fie divulgate unei părți terțe[535].

Raportul explicativ privind Convenția 108 modernizată prevede că, dacă nu este posibilă informarea persoanelor vizate la începerea prelucrării, aceasta se poate efectua într-o etapă ulterioară, de exemplu atunci când operatorul intră în contact cu persoana vizată, indiferent de motiv[536].

534 *Ibidem*, articolul 13 alineatele (1) și (2), fraza introductivă, în care Regulamentul general privind protecția datelor se referă la informațiile care fac obiectul obligației de transmitere „în momentul obținerii acestor date cu caracter personal".

535 *Ibidem*, articolul 13 alineatul (3) și articolul 14 alineatul (3); vezi, de asemenea, menționarea termenelor rezonabile și a transmiterii fără întârziere excesivă din Convenția 108 modernizată, articolul 8 alineatul (1) litera (b).

536 Raportul explicativ privind Convenția 108 modernizată, punctul 70.

Diferite modalități de furnizare a informațiilor

Atât în conformitate cu legislația CoE, cât și cu cea a UE, informațiile pe care operatorul trebuie să le furnizeze persoanelor vizate trebuie să fie concise, transparente, inteligibile și ușor accesibile. Trebuie să fie furnizate în scris sau prin alte mijloace, inclusiv în format electronic, folosind un limbaj clar, simplu și ușor de înțeles. Atunci când furnizează informații, operatorul poate folosi pictograme standardizate pentru a furniza informațiile într-o manieră ușor vizibilă și inteligibilă[537]. De exemplu, o pictogramă care reprezintă un lacăt poate fi utilizată pentru a semnala faptul că datele sunt colectate în mod securizat și/sau criptate. Persoanele vizate pot solicita ca informațiile să le fie furnizate verbal. Informațiile trebuie să fie furnizate gratuit, cu excepția cazurilor în care cererile persoanei vizate sunt în mod vădit nefondate sau excesive (în special din cauza caracterului lor repetitiv)[538]. Accesul facil la informațiile furnizate este esențial pentru capacitatea persoanei vizate de a-și exercita drepturile prevăzute de legislația UE în materie de protecție a datelor.

Principiul prelucrării echitabile impune ca informațiile să poată fi ușor de înțeles de către persoanele vizate. Trebuie să se utilizeze un limbaj adecvat destinatarilor. Nivelul și tipul de limbaj trebuie adaptat în funcție de publicul vizat, de exemplu adulți sau copii, publicul larg sau un expert din mediul academic. Problema modului de echilibrare a acestui aspect al informațiilor ușor de înțeles este analizată în Avizul Grupului de lucru „Articolul 29” privind dispoziții de informare mai armonizate. Acesta promovează ideea așa-numitelor notificări stratificate[539], care permit persoanei vizate să decidă ce nivel de detaliere preferă. Totuși, această modalitate de prezentare a informațiilor nu scutește operatorul de obligațiile care îi revin în temeiul articolelor 13 și 14 din RGPD. Operatorul trebuie, în orice caz, să furnizeze persoanei vizate toate informațiile necesare.

Una dintre cele mai eficiente modalități de furnizare a informațiilor este publicarea unor clauze adecvate de informare pe pagina principală a operatorului, cum ar fi o politică de confidențialitate a site-ului. Cu toate acestea, există un procent

537 Comisia va elabora în continuare, prin intermediul actelor delegate, informațiile care urmează să fie prezentate de pictograme și procedurile pentru furnizarea de pictograme standardizate; vezi Regulamentul general privind protecția datelor, articolul 12 alineatul (8).

538 Regulamentul general privind protecția datelor, articolul 12 alineatele (1), (5) și (7) și Convenția 108 modernizată, articolul 9 alineatul (1) litera (b).

539 Avizul 10/2004 din 25 noiembrie 2004 al Grupului de lucru „Articolul 29” privind dispoziții de informare mai armonizate, WP 100, Bruxelles, 25 noiembre 2004.

semnificativ de populație care nu utilizează internetul, iar politica de informare a unei societăți sau a unei autorități publice ar trebui să țină seama de acest aspect.

O notificare privind respectarea vieții private în contextul prelucrării datelor cu caracter personal pe o pagină web ar putea arăta după cum urmează.

Cine suntem?

Operatorul de prelucrare a datelor este Bed and Breakfast C&U, cu sediul în [adresa: xxx], tel.: xxx, fax: xxx; e-mail info@c&u.com; datele de contact ale responsabilului cu protecția datelor: [xxx].

Notificarea cu privire la informațiile cu caracter personal face parte din termenele și condițiile care reglementează utilizarea serviciilor noastre hoteliere.

Ce date colectăm de la dumneavoastră?

Colectăm următoarele date cu caracter personal: numele și prenumele dumneavoastră, adresa poștală, numărul de telefon, adresa de e-mail, informații despre sejur, numărul cardului de credit și de debit și adresele IP sau numele de domeniu ale computerelor pe care le-ați utilizat pentru a vă conecta la site-ul nostru.

De ce colectăm datele dumneavoastră?

Prelucrăm datele dumneavoastră pe baza consimțământului pe care îl exprimați și în scopul efectuării rezervărilor, încheierii și executării contractelor referitoare la serviciile pe care vi le oferim și pentru a respecta cerințele impuse de lege, de exemplu Legea privind taxele locale, care ne impune să colectăm date cu caracter personal în vederea achitării taxei municipale aferente cazării.

Cum prelucrăm datele dumneavoastră?

Datele dumneavoastră cu caracter personal vor fi păstrate pentru o perioadă de trei luni. Datele dumneavoastră nu fac obiectul unor procese decizionale automatizate.

Pensiunea noastră Bed and Breakfast C&U aplică proceduri stricte de securitate pentru a asigura faptul că informațiile dumneavoastră cu caracter personal nu sunt deteriorate, distruse sau divulgate unei terțe părți fără permisiunea dumneavoastră și pentru a împiedica accesul neautorizat la acestea. Computerele pe care se stochează informațiile sunt păstrate într-un mediu securizat, cu acces fizic restricționat. Utilizăm firewall-uri sigure și alte măsuri de restricționare a accesului electronic. Dacă este necesar să transmitem datele dumneavoastră unei părți terțe, îi solicităm să adopte măsuri similare de protejare a datelor cu caracter personal.

Toate informațiile pe care le colectăm sau le înregistrăm sunt prelucrate exclusiv în birourile noastre. Numai persoanele care au nevoie de aceste informații pentru a-și îndeplini atribuțiile în temeiul prezentului contract beneficiază de acces la datele cu caracter personal. Atunci când avem nevoie de informații pentru a vă identifica, vă vom solicita aceste informații în mod explicit. Este posibil să vă cerem să cooperați la verificările noastre de securitate înainte de a vă divulga informații. Puteți actualiza în orice moment informațiile cu caracter personal pe care ni le oferiți, contactându-ne direct.

Ce drepturi aveți?

Aveți dreptul să accesați datele, să obțineți o copie a datelor dumneavoastră, să solicitați ștergerea sau rectificarea acestora sau să solicitați portarea datelor la un alt operator.

Ne puteți transmite cererile dumneavoastră la adresa info@c&u.com. Avem obligația de a răspunde solicitării dumneavoastră în termen de o lună, dar dacă solicitarea dumneavoastră este prea complexă sau primim prea multe alte solicitări, vă vom informa că această perioadă poate fi prelungită cu încă două luni.

Accesul la datele dumneavoastră cu caracter personal

Aveți dreptul să accesați datele dumneavoastră, să primiți, la cerere, explicații privind raționamentul pe care se bazează prelucrarea datelor, să solicitați ștergerea sau rectificarea acestora; de asemenea, aveți dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automatizată fără a se ține seama de opiniile dumneavoastră. Ne puteți transmite cererile dumneavoastră la adresa info@c&u.com. De asemenea, aveți dreptul să vă opuneți

prelucrării, să vă retrageți consimțământul și să depuneți o plângere la autoritatea națională de supraveghere în cazul în care considerați că această prelucrare a datelor încalcă legea și aveți dreptul de a solicita despăgubiri pentru prejudiciile suferite ca urmare a prelucrării ilegale.

Dreptul de a depune o plângere

RGPD impune operatorului să informeze persoanele vizate cu privire la mecanismele de punere în aplicare a legii prevăzute de dreptul intern și de dreptul UE pentru cazurile de încălcare a securității datelor cu caracter personal. Operatorul trebuie să informeze persoanele vizate cu privire la dreptul lor de a depune o plângere privind încălcarea securității datelor cu caracter personal în fața unei autorități de supraveghere și, dacă este necesar, în fața unei instanțe naționale[540]. Legislația CoE prevede, de asemenea, dreptul persoanelor vizate de a fi informate cu privire la mijloacele prin care își pot exercita drepturile, inclusiv dreptul la o cale de atac prevăzut la articolul 9 alineatul (1) litera (f) din Convenția 108 modernizată.

Excepții de la obligația de informare

RGPD prevede excepții de la obligația de informare. În temeiul articolului 13 alineatul (4) și al articolului 14 alineatul (5) din RGPD, obligația de informare a persoanelor vizate nu se aplică în cazul în care persoana vizată deține deja toate informațiile relevante[541]. În plus, în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, obligația de informare nu se aplică în cazul în care furnizarea informațiilor este imposibilă sau disproporționată, în special atunci când datele cu caracter personal sunt prelucrate în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice[542].

În plus, statele membre se bucură de o marjă de apreciere în temeiul RGPD, având posibilitatea de a restrânge obligațiile și drepturile conferite persoanelor în temeiul regulamentului dacă aceasta este o măsură necesară și proporțională într-o societate democratică, de exemplu pentru a asigura securitatea națională și publică și apărarea, pentru a proteja desfășurarea anchetelor și a procedurilor judiciare sau

540 Regulamentul general privind protecția datelor, articolul 13 alineatul (2) litera (d); Convenția 108 modernizată, articolul 8 alineatul (1) litera (f).

541 *Ibidem*, articolul 13 alineatul (4) și articolul 14 alineatul (5) litera (a).

542 *Ibidem*, articolul 14 alineatul (5) literele (b)-(e).

interese economice și financiare publice, precum și interese private care prevalează asupra intereselor în materie de protecție a datelor[543].

Excepțiile sau restricțiile trebuie să fie necesare într-o societate democratică și proporționale cu scopul urmărit. În cazuri cu totul excepționale, de exemplu în temeiul unor recomandări medicale, însăși protecția persoanei vizate poate necesita o restrângere a transparenței; aceasta implică, în special, limitarea dreptului de acces al fiecărei persoane vizate[544]. Cu toate acestea, ca nivel minim de protecție, dreptul intern trebuie să respecte substanța drepturilor și libertăților fundamentale protejate de dreptul UE[545]. Aceasta impune ca dreptul intern să conțină dispoziții specifice care clarifică scopul prelucrării, categoriile de date cu caracter personal incluse, garanțiile și alte cerințe procedurale[546].

În cazul în care datele sunt colectate în scopuri de cercetare științifică sau istorică, în scopuri statistice sau pentru arhivare în scopuri de interes public, dreptul Uniunii sau dreptul intern poate să prevadă derogări de la obligația de informare, în măsura în care drepturile respective sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice[547].

Există limitări similare în cadrul legislației CoE, care prevede că drepturile acordate persoanelor vizate în temeiul articolului 9 din Convenția 108 modernizată pot face obiectul unor eventuale restricții în temeiul articolului 11 din Convenția 108 modernizată, în anumite condiții stricte. În plus, în conformitate cu articolul 8 alineatul (2) din Convenția 108 modernizată, obligația de transparență a prelucrării impusă operatorilor nu se aplică în cazul în care persoana vizată deține deja informațiile.

Dreptul de acces al unei persoane la datele proprii

În cadrul legislației CoE, dreptul de acces al unei persoane la datele proprii este recunoscut în mod explicit la articolul 9 din Convenția 108 modernizată. Acesta prevede că fiecare persoană are dreptul de a obține, la cerere, informații privind prelucrarea datelor sale cu caracter personal, care să îi fie comunicate într-o manieră inteligibilă. Dreptul de acces a fost recunoscut nu doar de dispozițiile Convenției 108

543 Regulamentul general privind protecția datelor, articolul 23 alineatul (1).

544 Regulamentul general privind protecția datelor, articolul 15.

545 Regulamentul general privind protecția datelor, articolul 23 alineatul (1).

546 *Ibidem*, articolul 23 alineatul (2).

547 *Ibidem*, articolul 89 alineatele (2) și (3).

modernizate, ci și în jurisprudența CEDO. CEDO a constatat în repetate rânduri că persoanele fizice au dreptul de acces la informații despre datele lor cu caracter personal și că acest drept rezultă din necesitatea de a respecta viața privată[548]. Cu toate acestea, dreptul de acces la datele cu caracter personal stocate de organizațiile publice sau private poate fi restrâns în anumite circumstanțe[549].

În cadrul legislației UE, dreptul de acces la propriile date este recunoscut în mod explicit la articolul 15 din RGPD și este, de asemenea, stabilit ca element al dreptului fundamental la protecția datelor cu caracter personal la articolul 8 alineatul (2) din Carta drepturilor fundamentale a UE[550]. Dreptul unei persoane de a obține acces la propriile sale date cu caracter personal este un element esențial al legislației europene în materie de protecție a datelor[551].

RGPD prevede că fiecare persoană vizată are dreptul de a obține din partea operatorului acces la datele sale cu caracter personal și anumite informații despre prelucrare[552]. În special, fiecare persoană vizată are dreptul de a obține (din partea operatorului) confirmarea că se prelucrează sau nu date care o privesc și informații referitoare cel puțin la următoarele:

- scopurile prelucrării;
- categoriile de date vizate;
- destinatarii sau categoriile de destinatari cărora li se divulgă datele;
- perioada pentru care se preconizează că vor fi stocate datele sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

548 Hotărârea CEDO din 7 iulie 1989 în cauza *Gaskin/Regatul Unit*, nr. 10454/83; Hotărârea CEDO [MC] din 13 februarie 2003 în cauza *Odièvre/Franța*, nr. 42326/98; Hotărârea CEDO din 28 aprilie 2009 în cauza *K.H. și alții/Slovacia*, nr. 32881/04; Hotărârea CEDO din 25 septembrie 2012 în cauza *Godelli/Italia*, nr. 33783/09.

549 Hotărârea CEDO din 26 martie 1987 în cauza *Leander/Suedia*, nr. 9248/81.

550 Vezi, de asemenea, Hotărârea CJUE din 17 iulie 2014 în cauzele conexate C-141/12 și C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel și Minister voor Immigratie, Integratie en Asiel/M și S*; Hotărârea CJUE din 16 iulie 2015 în cauza C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/Autoritatea Europeană pentru Siguranța Alimentară (EFSA), Comisia Europeană*.

551 Hotărârea CJUE din 17 iulie 2014 în cauzele conexate C-141/12 și C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel și Minister voor Immigratie, Integratie en Asiel/M și S*.

552 Regulamentul general privind protecția datelor, articolul 15 alineatul (1).

- existența dreptului de a obține rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal;
- dreptul de a depune o plângere în fața unei autorități de supraveghere;
- orice informații disponibile privind sursa datelor care fac obiectul unei prelucrări, în cazul în care datele nu sunt colectate de la persoana vizată;
- în cazul deciziilor automatizate, logica utilizată de orice prelucrare automatizată a datelor.

Operatorul de date trebuie să furnizeze persoanei vizate o copie a datelor cu caracter personal prelucrate. Orice informație comunicată persoanei vizate trebuie furnizată într-o formă inteligibilă, ceea ce înseamnă că operatorul trebuie să se asigure că persoana vizată poate înțelege informațiile furnizate. De exemplu, includerea unor abrevieri tehnice, a termenilor codificați sau a acronimelor în răspunsul la o solicitare de acces la date nu va fi suficientă, în general, cu excepția cazului în care sensul acestor termeni este explicat. În cazul unui proces decizional automatizat, inclusiv a creării de profiluri, trebuie explicată logica generală a procesului decizional automatizat, inclusiv criteriile care au fost luate în considerare la evaluarea persoanei vizate. În **legislația CoE** există cerințe similare[553].

> Exemplu: Accesul la datele sale cu caracter personal va ajuta persoana vizată să determine dacă datele sunt sau nu exacte. Prin urmare, este esențial ca persoana vizată să fie informată, într-o formă inteligibilă, nu numai în legătură cu datele cu caracter personal efective care sunt prelucrate, ci și în legătură cu categoriile în care sunt prelucrate aceste date cu caracter personal, cum ar fi nume, adresă IP, coordonate de geolocalizare, numărul cardului de credit etc.

Trebuie furnizate informații privind sursa datelor – în cazul în care acestea nu sunt colectate de la persoana vizată – drept răspuns la o cerere de acces, în măsura în care aceste informații sunt disponibile. Această dispoziție trebuie înțeleasă în contextul principiilor echității, transparenței și responsabilității. Un operator nu poate distruge informațiile despre sursa datelor pentru a fi scutit de divulgarea acestora – cu excepția cazului în care eliminarea ar fi avut loc indiferent de faptul că s-a primit

553 Convenția 108 modernizată, articolul 8 alineatul (1) litera (c).

cererea de acces – și trebuie să respecte în continuare cerințele generale de „responsabilitate" care i se aplică.

Astfel cum se subliniază în jurisprudența CJUE, dreptul de acces la datele proprii nu poate fi restricționat în mod nejustificat prin termene limită. Persoanelor vizate trebuie să li se acorde, de asemenea, o posibilitate rezonabilă de a obține informații cu privire la operațiunile de prelucrare a datelor efectuate anterior.

Exemplu: În cauza *Rijkeboer*[554], CJUE i s-a solicitat să stabilească dacă dreptul unei persoane de a avea acces la informații privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal și la conținutul datelor poate fi limitat la o perioadă de un an anterioară datei de prezentare a cererii de acces.

Pentru a stabili dacă legislația UE permite un astfel de termen limită, CJUE a hotărât să interpreteze articolul 12 în lumina scopului directivei. CJUE a constatat în primul rând că dreptul de acces este necesar pentru a-i permite persoanei vizate să își exercite dreptul de a obține de la operator rectificarea, ștergerea sau blocarea datelor sale ori înștiințarea părților terțe cărora le-au fost divulgate datele în legătură cu rectificarea, ștergerea sau blocarea în cauză. Dreptul eficace de acces este necesar, de asemenea, pentru a permite persoanei vizate să își exercite dreptul de a se opune prelucrării datelor cu caracter personal sau dreptul de a depune o plângere și de a solicita despăgubiri[555].

Pentru a se asigura efectul practic al drepturilor acordate persoanelor vizate, CJUE a constatat că „acest drept trebuie să se refere în mod obligatoriu la trecut. Într-adevăr, în caz contrar, persoana [vizată] nu ar fi în măsură să își exercite în mod eficient dreptul său de a obține rectificarea, ștergerea sau blocarea datelor prezumate nelegale sau incorecte și nici de a introduce o acțiune în justiție și de a obține repararea prejudiciului suferit".

554 Hotărârea CJUE din 7 mai 2009 în cauza C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*.

555 Regulamentul general privind protecția datelor, articolul 15 alineatul (1) literele (c) și (f), articolul 16, articolul 17 alineatul (2) și articolul 21, precum și capitolul VIII.

6.1.2. Dreptul la rectificarea datelor

În temeiul legislației UE și **a legislației CoE**, persoanele vizate au dreptul de a obține rectificarea datelor lor cu caracter personal. Exactitatea datelor cu caracter personal este esențială pentru a asigura un nivel ridicat de protecție a datelor pentru persoanele vizate[556].

> Exemplu: În cauza *Ciubotaru/Moldova*[557], reclamantul nu a avut posibilitatea de a modifica înregistrarea privind originea sa etnică, inclusă în documentele oficiale, din „moldovenească" în „română", solicitarea depusă de el fiind respinsă pentru motivul că ar fi nefondată. CEDO a considerat că este acceptabil ca statele să solicite probe obiective în vederea înregistrării identității etnice a unei persoane. Atunci când o astfel de cerere se bazează pe motive pur subiective și nefondate, autoritățile pot respinge cererea respectivă. Cu toate acestea, cererea reclamantului nu a fost întemeiată doar pe percepția subiectivă privind propria etnie; acesta a fost în măsură să facă dovada unor legături, verificabile în mod obiectiv, cu grupul etnic român, precum limba, numele, empatia și alte aspecte. Cu toate acestea, în conformitate cu dreptul intern, reclamantului i s-a solicitat să prezinte probe privind apartenența părinților acestora la grupul etnic român. Având în vedere realitatea istorică din Republica Moldova, această cerință a creat o barieră insurmontabilă privind înregistrarea unei alte identități decât cea înregistrată în cazul părinților acestuia de către autoritățile sovietice. Nepermițând examinarea cererii reclamantului pe baza unor probe verificabile în mod obiectiv, statul nu și-a respectat obligația pozitivă de a asigura reclamantului respectarea efectivă a vieții private. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

În anumite cazuri, este suficient ca persoana vizată să solicite pur și simplu rectificarea, de exemplu, a ortografiei numelui sau modificarea adresei sau a numărului de telefon. Atât în temeiul **legislației UE**, cât și al **legislației CoE**, datele cu caracter personal inexacte trebuie să poată fi rectificate fără întârzieri nejustificate sau excesive[558]. Totuși, în cazul în care astfel de cereri vizează aspecte semnificative din punct de vedere juridic, precum identitatea juridică a persoanei vizate sau locul de

556 *Ibidem*, articolul 16 și considerentul 65; Convenția 108 modernizată, articolul 9 alineatul (1) litera (e).

557 Hotărârea CEDO din 27 aprilie 2010 în cauza *Ciubotaru/Moldova*, nr. 27138/04, punctele 51 și 59.

558 Regulamentul general privind protecția datelor, articolul 16; Convenția 108 modernizată, articolul 9 alineatul (1).

reședință corect pentru transmiterea documentelor juridice, este posibil ca cererile de rectificare să nu fie suficiente, operatorul având dreptul de a solicita dovezi privind presupusa inexactitate. Aceste cereri nu trebuie să impună persoanei vizate o sarcină a probei nejustificată, împiedicând astfel persoanele vizate să obțină rectificarea datelor lor. CEDO a constatat încălcări ale articolului 8 din Convenția europeană a drepturilor omului în numeroase cazuri în care reclamantul nu a putut să conteste exactitatea informațiilor păstrate în registre secrete[559].

Exemplu: În cauza *Cemalettin Canli/Turcia*[560], CEDO a constatat încălcarea articolului 8 din Convenția europeană a drepturilor omului într-un caz de raportare incorectă de către organele de poliție în cadrul procedurilor penale.

Reclamantul a fost implicat de două ori în proceduri penale din cauza presupusei apartenențe la organizații ilegale, fără a fi vreodată condamnat. Atunci când reclamantul a fost arestat din nou și acuzat de o nouă infracțiune, organele de poliție au prezentat instanței penale un raport intitulat „formular de informare privind alte infracțiuni", în care reclamantul apărea ca membru a două organizații ilegale. Cererea reclamantului privind rectificarea raportului și înregistrărilor deținute de organele de poliție a fost respinsă. CEDO a stabilit că informațiile din raportul de poliție se încadrează în domeniul de aplicare al articolului 8 din Convenția europeană a drepturilor omului, deoarece informațiile colectate sistematic despre public și păstrate în dosare de către autorități pot, de asemenea, să se încadreze în sfera de aplicare a termenului „viață privată". În plus, raportul organelor de poliție a fost elaborat într-un mod inexact, iar prezentarea acestuia în fața instanței penale nu a respectat dreptul intern. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

În cadrul unei acțiuni sau proceduri civile desfășurate în fața unei autorități publice pentru a se stabili dacă datele sunt exacte sau nu, persoana vizată poate solicita menționarea sau atașarea unei adnotări sau a unei note la dosar, în care să se specifice faptul că se contestă exactitatea datelor și că este în curs de adoptare o decizie oficială[561]. În această perioadă, operatorul de date nu trebuie să prezinte datele, în special părților terțe, ca fiind exacte sau definitive.

559 Hotărârea CEDO [MC] din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95.

560 Hotărârea CEDO din 18 noiembrie 2008 în cauza *Cemalettin Canli/Turcia*, nr. 22427/04, punctele 33 și 42-43. Hotărârea CEDO din 2 februarie 2010 în cauza *Dalea/Franța*, nr. 964/07, 2 februarie 2010.

561 Regulamentul general privind protecția datelor, articolul 18 și considerentul 67.

6.1.3. Dreptul la ștergerea datelor („dreptul de a fi uitat”)

Prevederea dreptului persoanelor fizice de a obține ștergerea propriilor date este deosebit de importantă pentru aplicarea eficientă a principiilor protecției datelor și, în special, a principiului reducerii la minimum a datelor (datele cu caracter personal trebuie să se limiteze la ceea ce este necesar pentru scopurile în care sunt prelucrate aceste date). Prin urmare, dreptul la ștergerea datelor se regăsește atât în instrumentele juridice ale CoE, cât și ale UE[562].

Exemplu: În cauza *Segerstedt-Wiberg și alții/Suedia*[563], reclamanții erau afiliați unor partide politice liberale și comuniste. Aceștia au bănuit că anumite informații despre ei au fost înregistrate în evidențele forțelor de securitate și au solicitat ștergerea respectivelor informații. CEDO a constatat că stocarea datelor în cauză a avut un temei juridic și a urmărit un scop legitim. Totuși, în cazul unora dintre reclamanți, CEDO a constatat că păstrarea în continuare a datelor constituia o ingerință disproporționată în viața privată a acestora. De exemplu, în cazul unui reclamant, autoritățile au păstrat informații potrivit cărora, în 1969, acesta ar fi susținut opunerea de rezistență violentă la controlul organelor de poliție în timpul demonstrațiilor. CEDO a constatat că această informație nu putea urmări niciun interes relevant privind securitatea națională, având în vedere, în special, caracterul istoric al acesteia. Curtea a constatat încălcarea articolului 8 din Convenția europeană a drepturilor omului în cazurile a patru dintre cei cinci reclamanți, întrucât, dată fiind perioada lungă de timp de la presupusele acțiuni ale reclamanților, păstrarea în continuare a datelor lor era lipsită de relevanță.

Exemplu: În cazul *Brunet/Franța*[564], reclamantul a denunțat păstrarea informațiilor sale cu caracter personal într-o bază de date a poliției care conținea informații despre persoane condamnate, persoane inculpate și victime. Deși acțiunea penală împotriva reclamantului fusese suspendată, datele despre el apăreau în baza de date. CEDO a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului. Pentru a ajunge la

562 *Ibidem*, articolul 17.

563 Hotărârea CEDO din 6 iunie 2006 în cauza *Segerstedt-Wiberg și alții/Suedia*, nr. 62332/00, punctele 89 și 90; vezi, de asemenea, de exemplu, Hotărârea CEDO din 18 aprilie 2013 în cauza *M.K./Franța*, nr. 19522/09.

564 Hotărârea CEDO din 18 septembrie 2014 în cauza *Brunet/Franța*, nr. 21010/10.

această concluzie, Curtea a considerat că, în practică, reclamantul nu avea posibilitatea de a obține ștergerea datelor sale cu caracter personal din baza de date. De asemenea, CEDO a examinat natura informațiilor incluse în baza de date și a considerat că era invazivă pentru viața privată a reclamantului, deoarece conținea detalii despre identitatea și personalitatea sa. În plus, Curtea a constatat că perioada de păstrare a înregistrărilor cu caracter personal în baza de date, care era de 20 de ani, era excesiv de lungă, în special având în vedere că reclamantul nu fusese condamnat de nicio instanță.

Convenția 108 modernizată recunoaște în mod explicit că fiecare persoană are dreptul la ștergerea datelor inexacte, false sau prelucrate ilegal[565].

În cadrul legislației UE, articolul 17 din RGPD prevede posibilitatea persoanelor vizate de a solicita ștergerea sau eliminarea datelor. Dreptul la ștergerea datelor cu caracter personal fără întârzieri nejustificate se aplică în următoarele cazuri:

- datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea și nu există niciun alt temei juridic pentru prelucrare;
- persoana vizată se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea;
- datele cu caracter personal au fost prelucrate ilegal;
- datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul;
- datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la articolul 8 din RGPD[566].

Sarcina probei care să confirme că prelucrarea datelor este legitimă le revine operatorilor de date, deoarece aceștia sunt responsabili pentru legalitatea

565 Convenția 108 modernizată, articolul 9 alineatul (1) litera (e).

566 Regulamentul general privind protecția datelor, articolul 17 alineatul (1).

prelucrării[567]. În conformitate cu principiul responsabilității, operatorul trebuie, în orice moment, să poată demonstra că există un temei juridic solid pentru prelucrarea datelor, în caz contrar prelucrarea trebuind oprită[568]. RGPD definește excepțiile de la dreptul de a fi uitat, inclusiv cazurile în care prelucrarea datelor cu caracter personal este necesară pentru următoarele:

- pentru exercitarea dreptului la liberă exprimare și la informare;
- pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul;
- din motive de interes public în domeniul sănătății publice;
- în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice;
- pentru constatarea, exercitarea sau apărarea unui drept în instanță[569].

CJUE a confirmat importanța dreptului la ștergerea datelor pentru asigurarea unui nivel ridicat de protecție a datelor.

Exemplu: În cauza *Google Spain*[570], CJUE a analizat dacă Google avea obligația de a elimina din rezultatele căutării informații perimate despre dificultățile financiare ale reclamantului. Printre altele, Google a contestat că ar fi responsabilă, argumentând că oferă doar un hyperlink la pagina web a editorului care găzduiește informațiile, în acest caz un ziar care publicase informații cu

567 *Ibidem*.

568 *Ibidem*, articolul 5 alineatul (2).

569 *Ibidem*, articolul 17 alineatul (3).

570 Hotărârea CJUE [MC] 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 55-58.

privire la falimentul societății reclamantului[571]. Google a susținut că solicitarea de a șterge informațiile perimate de pe o pagină web ar trebui adresată publicației care găzduiește pagina web, iar nu societății Google, care oferă pur și simplu un link către pagina originală. CJUE a concluzionat că Google, atunci când caută pe web informații și pagini web și indexează conținutul pentru a furniza rezultate ale căutării, devine un operator de date căruia i se aplică responsabilitățile și obligațiile prevăzute de legislația UE.

CJUE a clarificat că motoarele de căutare pe internet și rezultatele căutării care furnizează date cu caracter personal pot stabili un profil detaliat al unei persoane[572]. Prin intermediul motoarelor de căutare, informațiile conținute într-o astfel de listă de rezultate ajung să fie omniprezente. Având în vedere gravitatea potențială a acestui fapt, ingerința nu poate fi justificată prin simplul interes economic pe care operatorul unui astfel de motor îl are în prelucrarea respectivă. Trebuie să se găsească un echilibru just, în special între interesul legitim al utilizatorilor de internet în ceea ce privește accesul la informații și drepturile fundamentale ale persoanei vizate în temeiul articolelor 7 și 8 din Carta drepturilor fundamentale a UE. Într-o societate din ce în ce mai digitizată, cerința ca datele cu caracter personal să fie corecte și să nu depășească ceea ce este necesar (și anume informarea publicului) este esențială pentru asigurarea unui nivel ridicat de protecție a datelor cu caracter personal. „[Operatorul] prelucrării respective trebuie să asigure, în cadrul responsabilităților, al competențelor și al posibilităților sale, că aceasta îndeplinește cerințele" legislației UE, pentru ca garanțiile juridice stabilite să își producă efectul deplin[573]. Aceasta înseamnă că dreptul de a obține

571 Google a contestat, de asemenea, aplicabilitatea normelor UE de protecție a datelor, întrucât Google Inc. are sediul în SUA, iar prelucrarea datelor cu caracter personal în cauză se efectua, de asemenea, în SUA. Un al doilea argument pentru inaplicabilitatea legislației UE privind protecția datelor a fost legat de susținerea că motoarele de căutare nu pot fi considerate „operatori" în ceea ce privește datele afișate în rezultatele lor, deoarece nu au cunoștință despre aceste date și nu exercită control asupra lor. CJUE a respins ambele argumente, considerând că Directiva 95/46/CE era aplicabilă în acest caz, și a continuat examinarea domeniului de aplicare al drepturilor garantate de aceasta, în special dreptul la ștergerea datelor cu caracter personal.

572 *Ibidem*, punctele 36, 38, 80-81 și 97.

573 *Ibidem*, punctele 81-83.

ștergerea datelor cu caracter personal proprii atunci când prelucrarea este permisă sau nu mai este necesară este opozabil și operatorilor de date care reproduc informațiile[574].

Examinând dacă Google avea sau nu obligația de a elimina linkurile legate de reclamant, CJUE a declarat că, în anumite condiții, persoanele au dreptul să solicite ștergerea datelor cu caracter personal. Acest drept poate fi invocat atunci când informațiile referitoare la o persoană sunt inexacte, inadecvate, irelevante sau excesive în raport cu scopurile prelucrării datelor. CJUE a recunoscut că acest drept nu este absolut; trebuie stabilit un echilibru între acesta și alte drepturi și interese, în special interesul publicului larg de a avea acces la anumite informații. Fiecare solicitare de ștergere a datelor necesită o evaluare de la caz la caz pentru a se găsi un echilibru între drepturile fundamentale la protecția datelor cu caracter personal și la respectarea vieții private ale persoanei vizate, pe de o parte, și interesele legitime ale tuturor utilizatorilor de internet, pe de altă parte. CJUE a oferit orientări 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 se referă la viața privată a persoanei vizate și nu există un interes public de a pune la dispoziție informațiile în cauză, protecția datelor și respectarea vieții private prevalează asupra dreptului publicului larg de a avea acces la informații. Dimpotrivă, dacă persoana vizată pare să fie o personalitate publică sau dacă informațiile sunt de natură să justifice punerea acestora la dispoziția publicului larg, atunci interesul preponderent al publicului larg de a avea acces la informații poate justifica intervenția asupra drepturilor fundamentale ale persoanei vizate la protecția datelor și la respectarea vieții private.

Ca urmare a pronunțării acestei hotărâri, Grupul de lucru „Articolul 29” a adoptat orientări privind punerea în aplicare a hotărârii CJUE[575]. Orientările cuprind o listă

574 Hotărârea CJUE [MC] din 13 mai 2014 în cauza C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, punctul 88. Vezi, de asemenea, Orientările din 26 noiembrie 2014 ale Grupului de lucru „Articolul 29” privind punerea în aplicare a hotărârii CJUE în cauza Google Spain și Google Inc/Agencia Española de Protección de Datos (AEPD) și Mario Costeja González, C-131/12, WP 225, Bruxelles, și Recomandarea CM/Rec 2012 (3) din 4 aprilie 2012 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția drepturilor omului în ceea ce privește motoarele de căutare.

575 Orientările din 26 noiembrie 2014 ale Grupului de lucru „Articolul 29” privind punerea în aplicare a hotărârii CJUE în cauza Google Spain și Google Inc/Agencia Española de Protección de Datos (AEPD) și Mario Costeja González, C-131/12, WP 225, Bruxelles.

de criterii comune care să fie utilizate de autoritățile de supraveghere atunci când analizează plângeri legate de cereri ale persoanelor fizice de ștergere a datelor, care explică ce presupune acest drept la ștergerea datelor și ghidează autoritățile în cadrul exercițiului de echilibrare a drepturilor. Orientările reiterează faptul că evaluările trebuie efectuate de la caz la caz. Deoarece dreptul de a fi uitat nu este absolut, rezultatul unei solicitări în acest sens poate să difere în funcție de circumstanțele cazului. Acest lucru este ilustrat și în jurisprudența CJUE ulterioară cauzei *Google*.

Exemplu: În cauza *Camera di Commercio di Lecce/Manni*[576], CJUE a analizat dacă o persoană avea dreptul de a obține ștergerea datelor sale cu caracter personal publicate într-un registru al societăților comerciale în condițiile în care societatea sa fusese închisă. Domnul Manni a solicitat Camerei de Comerț din Lecce să îi elimine datele cu caracter personal din registrul respectiv după ce a descoperit că potențialii clienți care ar consulta registrul ar vedea că a fost anterior administratorul unei societăți care a fost declarată în stare de faliment cu mai mult de zece ani în urmă. Reclamantul considera că această informație ar descuraja clienții potențiali.

Prin echilibrarea dreptului domnului Manni la protecția datelor sale cu caracter personal cu interesul publicului larg de a avea acces la informații, CJUE a examinat mai întâi scopul registrului public. Curtea a subliniat că divulgarea este prevăzută de lege și, în special, de o directivă a UE care urmărește să faciliteze accesul terților la informații despre societățile comerciale. Astfel, terții trebuie să aibă acces la documentele esențiale ale unei societăți comerciale și la alte informații referitoare la aceasta și să le poată examina, „în special identitatea persoanelor care au competența să angajeze societatea". Scopul divulgării era, de asemenea, garantarea securității juridice în perspectiva intensificării schimburilor comerciale dintre statele membre, prin asigurarea faptului că terții au acces la toate informațiile relevante despre societățile comerciale din întreaga UE.

CJUE a mai arătat că, chiar și după trecerea timpului și chiar după dizolvarea unei societăți, drepturile și obligațiile legale legate de societate continuă să existe. Litigiile legate de dizolvare pot dura mult, iar întrebările referitoare la societatea comercială, la administratorii și la lichidatorii acesteia pot apărea la mulți ani după ce o societate a încetat să existe. CJUE a constatat că,

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

având în vedere gama de posibile scenarii și diferențele dintre termenele de prescripție prevăzute în fiecare stat membru, „pare imposibil, în stadiul actual, să se identifice un termen unic, începând de la dizolvarea unei societăți, la expirarea căruia nu ar mai fi necesare înscrierea datelor menționate în registru și publicitatea lor". Având în vedere scopul legitim al divulgării și dificultățile de stabilire a unei perioade la sfârșitul căreia datele cu caracter personal ar putea fi șterse din registru fără a aduce atingere intereselor părților terțe, CJUE a constatat că normele UE de protecție a datelor nu garantează un drept la ștergerea datelor cu caracter personal pentru persoanele aflate în situația domnului Manni.

În cazul în care operatorul a făcut publice datele cu caracter personal și este obligat să șteargă informațiile, are obligația de a lua măsuri „rezonabile" pentru a informa alți operatori care prelucrează aceleași date cu privire la cererea persoanei vizate de ștergere a datelor. Activitățile operatorului trebuie să țină seama de tehnologiile disponibile și de costul implementării[577].

6.1.4. Dreptul la restricționarea prelucrării

Articolul 18 din RGPD prevede posibilitatea persoanelor vizate de a restricționa temporar prelucrarea datelor lor cu caracter personal de către un operator. Persoanele vizate pot solicita operatorului să restricționeze prelucrarea în următoarele cazuri:

- exactitatea datelor cu caracter personal este contestată;
- prelucrarea este ilegală, iar persoana vizată preferă să solicite restricționarea utilizării datelor cu caracter personal în locul ștergerii acestora;
- datele trebuie păstrate pentru exercitarea sau apărarea unor drepturi în instanță;
- se așteaptă pronunțarea deciziei dacă interesele legitime ale operatorului prevalează asupra intereselor persoanei vizate[578].

Metodele prin care operatorul poate restricționa prelucrarea datelor cu caracter personal ar putea include, printre altele, mutarea temporară a datelor selectate

577 Regulamentul general privind protecția datelor, articolul 17 alineatul (2) și considerentul 66.

578 *Ibidem*, articolul 18 alineatul (1).

într-un alt sistem de prelucrare, datele nemaifiind astfel disponibile utilizatorilor, sau înlăturarea temporară a datelor cu caracter personal[579]. Operatorul trebuie să informeze persoana vizată înainte de ridicarea restricției de prelucrare[580].

Obligația de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării

Operatorul trebuie să comunice fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării, cu excepția cazului în care acest lucru este imposibil sau disproporționat[581]. Dacă persoana vizată solicită informații despre respectivii destinatari, operatorul trebuie să îi furnizeze aceste informații[582].

6.1.5. Dreptul la portabilitatea datelor

În conformitate cu RGPD, persoanele vizate beneficiază de dreptul la portabilitatea datelor în situațiile în care datele cu caracter personal pe care le-au furnizat unui operator sunt prelucrate prin mijloace automate pe baza consimțământului sau în cazul în care prelucrarea datelor cu caracter personal este necesară pentru executarea unui contract și se efectuează prin mijloace automate. Aceasta înseamnă că dreptul la portabilitatea datelor nu se aplică în situațiile în care prelucrarea datelor cu caracter personal se bazează pe un alt temei juridic decât consimțământul sau un contract[583].

În cazul în care dreptul la portabilitatea datelor este aplicabil, persoanele vizate au dreptul ca datele lor cu caracter personal să fie transmise direct de la un operator la altul dacă acest lucru este fezabil din punct de vedere tehnic[584]. Pentru a facilita acest lucru, operatorul ar trebui să dezvolte formate interoperabile care să permită portabilitatea datelor pentru persoanele vizate[585]. RGPD specifică faptul că aceste formate trebuie să fie structurate, utilizate în mod curent și prelucrabile automat

579 *Ibidem*, considerentul 67.

580 *Ibidem*, articolul 18 alineatul (3).

581 *Ibidem*, articolul 19.

582 *Ibidem*.

583 *Ibidem*, considerentul 68 și articolul 20 alineatul (1).

584 *Ibidem*, articolul 20 alineatul (2).

585 *Ibidem*, considerentul 68 și articolul 20 alineatul (1).

pentru a facilita interoperabilitatea[586]. Interoperabilitatea poate fi definită în sens larg ca fiind capacitatea sistemelor de informații de a face schimb de date și de a permite schimbul de informații[587]. Deși scopul formatelor utilizate este de a realiza interoperabilitatea, RGPD nu impune recomandări specifice privind formatul specific care trebuie furnizat: formatele pot diferi de la un sector la altul[588].

Potrivit orientărilor Grupului de lucru „Articolul 29", dreptul la portabilitatea datelor „sprijină libertatea de alegere, controlul și capacitarea utilizatorilor", scopul său fiind ca persoanele vizate să aibă control asupra propriilor date cu caracter personal[589]. Orientările clarifică principalele elemente ale portabilității datelor, care includ:

- dreptul persoanelor vizate de a primi propriile date cu caracter personal prelucrate de către operator într-un format structurat, utilizat în mod curent, prelucrabil automat și interoperabil;

- dreptul ca datele cu caracter personal să fie transmise de la un operator de date către alt operator de date fără obstacole, dacă acest lucru este fezabil din punct de vedere tehnic;

- controlul asupra procesului – atunci când un operator răspunde la o cerere de portabilitate a datelor, acesta acționează pe baza instrucțiunilor persoanei vizate, ceea ce înseamnă că nu este responsabil pentru respectarea de către destinatar a legislației privind protecția datelor, întrucât persoana vizată decide spre cine se portează datele;

- exercițiul dreptului la portabilitatea datelor nu aduce atingere niciunui alt drept, de exemplu oricăror alte drepturi prevăzute de RGPD.

586 *Ibidem*, considerentul 68.

587 Comunicarea Comisiei Europene din 2 aprilie 2016 intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate", COM(2016) 205 final.

588 Orientările Grupului de lucru „Articolul 29" privind dreptul la portabilitatea datelor, WP 242, Bruxelles, adoptate la 13 decembrie 2016 și revizuite la 5 aprilie 2017, p. 13.

589 *Ibidem*.

6.1.6. Dreptul la opoziție

Persoanele vizate își pot invoca dreptul de a se opune prelucrării datelor cu caracter personal pentru motive legate de situația lor particulară și dreptul de a se opune prelucrării în scopuri de marketing direct. Dreptul la opoziție poate fi exercitat prin mijloace automate.

Dreptul la opoziție legat de situația particulară a persoanei vizate

Persoanele vizate nu dețin un drept general de a se opune prelucrării datelor lor[590]. Articolul 21 alineatul (1) din RGPD împuternicește persoana vizată să formuleze obiecții pentru motive legate de situația sa particulară atunci când temeiul juridic al prelucrării este îndeplinirea de către operator a unei sarcini care servește unui interes public sau dacă prelucrarea se bazează pe interesele legitime ale operatorului[591]; Dreptul la opoziție se aplică activităților de creare de profiluri. În Convenția 108 modernizată se recunoaște un drept similar[592].

Dreptul de a formula obiecții pentru motive legate de situația particulară a persoanei vizate urmărește găsirea unui echilibru just între drepturile la protecția datelor ale persoanei vizate și drepturile legitime ale altora ca datele lor să fie prelucrate. CJUE a clarificat totuși că drepturile persoanelor vizate prevalează, „ca regulă generală", asupra intereselor economice ale operatorului de date, dar că acest lucru depinde de „natura informației în discuție și de caracterul sensibil al acesteia în ceea ce privește viața privată a persoanei vizate, precum și de interesul publicului de a dispune de informația respectivă"[593]. În conformitate cu RGPD, sarcina probei le revine operatorilor, care trebuie să prezinte motive convingătoare pentru continuarea prelucrării[594]. În mod similar, Raportul explicativ privind Convenția 108 modernizată clarifică faptul

590 Vezi, de asemenea, Hotărârea CEDO din 27 august 1997 în cauza *M.S./Suedia*, nr. 20837/92 (în care datele medicale au fost comunicate fără consimțământ sau posibilitatea de opoziție); Hotărârea CEDO din 26 martie 1987 în cauza *Leander/Suedia*, nr. 9248/81; Hotărârea CEDO din 10 mai 2011 în cauza *Mosley/Regatul Unit*, nr. 48009/08.

591 Regulamentul general privind protecția datelor, considerentul 69 și articolul 6 alineatul (1) literele (e) și (f).

592 Convenția 108 modernizată, articolul 9 alineatul (1) litera (d); Recomandare privind crearea de profiluri, articolul 5 punctul 3.

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

594 Vezi, de asemenea, Convenția 108 modernizată, articolul 98 alineatul (1) litera (d), care precizează că persoana vizată se poate opune prelucrării datelor sale „cu excepția cazului în care operatorul demonstrează existența unor motive legitime pentru prelucrare care prevalează asupra intereselor sau drepturilor și libertăților fundamentale ale persoanei vizate".

că motivele legitime pentru prelucrarea datelor (care pot prevala asupra dreptului la opoziție al persoanelor vizate) trebuie să fie demonstrate de la caz la caz[595].

Exemplu: În cauza *Manni*[596], CJUE a declarat că, dat fiind scopul legitim al publicării datelor cu caracter personal în registrul societăților comerciale, în special necesitatea de a proteja interesele terților și de a asigura securitatea juridică, în principiu, domnul Manni nu avea dreptul să obțină ștergerea datelor sale cu caracter personal din registrul societăților comerciale. CJUE a recunoscut totuși existența unui drept de a obiecta față de prelucrarea datelor, arătând următoarele: „nu este exclusă [...] posibilitatea existenței unor situații speciale în care motive preponderente și legitime care țin de situația concretă a persoanei interesate să justifice în mod excepțional ca accesul la datele cu caracter personal care o privesc înscrise în registru să fie limitat, la expirarea unui termen suficient de lung [...], la terții care justifică un interes specific pentru consultare".

CJUE a considerat că ține de responsabilitatea instanțelor naționale să evalueze fiecare caz, luând în considerare toate circumstanțele relevante ale persoanei și eventuala existență a motivelor legitime și preponderente care ar putea justifica, în mod excepțional, accesul restricționat al părților terțe la datele cu caracter personal conținute în registrele de societăți comerciale. Cu toate acestea, Curtea a precizat că, în cazul domnului Manni, simplul fapt că publicarea datelor sale cu caracter personal în registru ar fi putut să-i afecteze clientela nu putea fi considerat un astfel de motiv legitim și preponderent. Clienții potențiali ai domnului Manni au un interes legitim de a avea acces la informațiile referitoare la falimentul vechii sale societăți.

Rezultatul unei opoziții reușite este că operatorul nu mai poate prelucra datele în cauză. Cu toate acestea, operațiunile de prelucrare a datelor persoanei vizate efectuate înainte de exprimarea opoziției își păstrează caracterul legitim.

595 Raportul explicativ privind Convenția 108 modernizată, punctul 78.

596 Hotărârea CJUE din 9 martie 2017 în cauza C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, punctele 47 și 60.

Dreptul la opoziție față de prelucrarea datelor în scopuri de marketing direct

Articolul 21 alineatul (2) din RGPD prevede un drept specific de opoziție față de prelucrarea datelor cu caracter personal în scopuri de marketing direct, clarificând mai mult articolul 13 din Directiva asupra confidențialității și comunicațiilor electronice. Acest drept este prevăzut, de asemenea, în Convenția 108 modernizată, precum și în Recomandarea CoE privind marketingul direct[597]. Raportul explicativ privind Convenția 108 modernizată clarifică faptul că obiecțiile față de prelucrarea datelor în scopuri de marketing direct ar trebui să aibă ca rezultat ștergerea sau eliminarea necondiționată a datelor cu caracter personal în cauză[598].

Persoana vizată are dreptul, în orice moment și gratuit, să se opună utilizării datelor sale cu caracter personal în scopuri de marketing direct. Persoanele vizate trebuie să fie informate cu privire la acest drept într-o manieră clară, separat de orice alte informații.

Dreptul la opoziție prin mijloace automate

În cazul în care informațiile cu caracter personal sunt utilizate și prelucrate pentru serviciile societății informaționale, persoana vizată își poate exercita dreptul de a se opune prelucrării datelor sale cu caracter personal prin mijloace automate.

Serviciile societății informaționale sunt definite ca fiind orice serviciu prestat în mod normal în scopul obținerii unei remunerații, la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciului[599].

Operatorii de date care furnizează servicii ale societății informaționale trebuie să adopte măsuri tehnice și proceduri adecvate pentru a se asigura că dreptul la opoziție prin mijloace automate poate fi exercitat în mod eficient[600]. De exemplu, acest lucru poate implica blocarea modulelor cookie pe paginile web sau oprirea urmăririi navigării pe internet.

---

597 Recomandarea Rec(85)20 din 25 octombrie 1985 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția datelor cu caracter personal utilizate în scopuri de marketing direct, articolul 4 alineatul (1).

598 Raportul explicativ privind Convenția 108 modernizată, punctul 79.

599 Directiva 98/48/CE de modificare a Directivei 98/34/CE de stabilire a unei proceduri pentru furnizarea de informații în domeniul standardelor și reglementărilor tehnice, articolul 1 punctul 2.

600 Regulamentul general privind protecția datelor, articolul 21 alineatul (5).

Dreptul la opoziție față de prelucrarea datelor în scopuri de cercetare științifică sau istorică ori în scopuri statistice

În temeiul legislației UE, prelucrarea datelor cu caracter personal în scopuri de cercetare științifică ar trebui să fie interpretată în sens larg, incluzând de exemplu dezvoltarea tehnologică și activitățile demonstrative, cercetarea fundamentală, cercetarea aplicată și cercetarea finanțată din surse private[601]. Cercetarea istorică include cercetarea în scopuri genealogice, ținând seama de faptul că regulamentul nu ar trebui să se aplice persoanelor decedate[602]. Scopuri statistice înseamnă orice operațiune de colectare și prelucrare de date cu caracter personal necesară pentru anchetele statistice sau pentru producerea de rezultate statistice[603]. Din nou, situația particulară a persoanei vizate reprezintă temeiul juridic al dreptului la opoziție față de prelucrarea datelor cu caracter personal în scopuri de cercetare[604]. Singura excepție este necesitatea prelucrării în scopul îndeplinirii unei sarcini care servește unui interes public. Cu toate acestea, dreptul la ștergerea datelor nu se aplică atunci când prelucrarea este necesară (cu sau fără motive de interes public) în scopuri de cercetare științifică sau istorică ori în scopuri statistice[605].

RGPD echilibrează cerințele cercetării științifice, statistice sau istorice și drepturile persoanelor vizate cu garanțiile specifice și derogările prevăzute la articolul 89. Astfel, legislația Uniunii sau legislația națională poate să prevadă derogări de la dreptul la opoziție, în măsura în care acest drept este de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor cercetării, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

În cadrul **legislației CoE**, articolul 9 alineatul (2) din Convenția 108 modernizată stabilește că restrângerea drepturilor persoanelor vizate, inclusiv a dreptului la opoziție, poate fi prevăzută de lege în ceea ce privește prelucrarea datelor în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice atunci când nu există niciun risc previzibil de încălcare a drepturilor și a libertăților fundamentale ale persoanelor vizate.

Cu toate acestea, Raportul explicativ (la punctul 41) recunoaște, de asemenea, că persoanele vizate ar trebui să aibă posibilitatea de a-și da consimțământul numai

601 *Ibidem*, considerentul 159.

602 *Ibidem*, considerentul 160.

603 *Ibidem*, considerentul 162.

604 *Ibidem*, articolul 21 alineatul (6).

605 *Ibidem*, articolul 17 alineatul (3) litera (d).

pentru anumite domenii de cercetare sau părți ale proiectelor de cercetare, în măsura în care scopul preconizat permite acest lucru, și de a se opune prelucrării în cazul în care consideră că aceasta aduce atingere în mod excesiv drepturilor și libertăților lor fără un motiv legitim.

Cu alte cuvinte, o astfel de prelucrare ar fi considerată a priori compatibilă, cu condiția să existe alte garanții și ca operațiunile să excludă, în principiu, orice utilizare a informațiilor obținute pentru decizii sau măsuri referitoare la o anumită persoană.

6.1.7. Procesul decizional individual automatizat, inclusiv crearea de profiluri

Deciziile automatizate sunt decizii adoptate pe baza datelor cu caracter personal prelucrate exclusiv prin mijloace automatizate, fără intervenție umană. **În cadrul legislației UE**, persoanele vizate nu trebuie să facă obiectul unor decizii automatizate care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă. Dacă există posibilitatea ca astfel de decizii să afecteze în mod semnificativ viețile persoanelor în cauză, întrucât fac referire, de exemplu, la bonitatea, angajarea online, randamentul profesional, analiza conduitei sau a încrederii pe care o prezintă persoana, se impune asigurarea unei protecții speciale pentru a se evita consecințele negative. Procesul decizional automat include crearea de profiluri, care constă în orice formă de evaluare automată a „aspectelor personale referitoare la o persoană fizică, în special în vederea analizării sau preconizării anumitor aspecte privind randamentul la locul de muncă al persoanei vizate, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările”[606].

Exemplu: Pentru a evalua rapid bonitatea unui viitor client, agențiile de informații privind creditele colectează anumite date, cum ar fi modul în care clientul și-a administrat conturile de credit și de servicii/utilități, detaliile adreselor anterioare ale clientului, precum și informații din surse publice, cum ar fi registrul electoral, evidențele publice (inclusiv hotărârile judecătorești) sau datele privind falimentul și insolvența. Aceste date cu caracter personal sunt introduse ulterior într-un algoritm de evaluare, care calculează o valoare totală reprezentând bonitatea potențialului client.

606 *Ibidem*, considerentul 71, articolul 4 punctul 4 și articolul 22.

Potrivit Grupului de lucru „Articolul 29”, dreptul de a nu face obiectul unor decizii bazate exclusiv pe prelucrarea automatizată care poate avea efecte juridice asupra persoanei vizate sau care o afectează în mod semnificativ este echivalent cu o interdicție generală, prin urmare nu presupune că persoanele vizate ar trebui să se opună în mod proactiv unei astfel de decizii[607].

Cu toate acestea, conform RGPD, procesul decizional automatizat care produce efecte juridice sau afectează într-o măsură semnificativă persoanele poate fi acceptabil dacă este necesară pentru încheierea sau executarea unui contract între operatorul de date și persoana vizată sau dacă persoana vizată și-a dat consimțământul în mod explicit. De asemenea, procesul decizional automatizat este acceptabil dacă este autorizată prin lege și dacă drepturile, libertățile și interesele legitime ale persoanei vizate sunt protejate în mod corespunzător[608].

De asemenea, RGPD prevede că printre obligațiile operatorului în ceea ce privește informațiile care trebuie furnizate în cazul colectării de date cu caracter personal se numără informarea persoanelor vizate cu privire la existența unui proces decizional automatizat incluzând crearea de profiluri[609]. Dreptul de acces la datele cu caracter personal prelucrate de operator rămâne neafectat[610]. Informațiile ar trebui nu doar să semnaleze faptul că va avea loc crearea de profiluri, ci și să conțină informații pertinente cu privire la logica utilizată pentru crearea acestor profiluri și la consecințele preconizate ale prelucrării pentru persoanele vizate[611]. De exemplu, o societate de asigurări de sănătate care utilizează procese decizionale automatizate la tratarea cererilor ar trebui să furnizeze persoanelor vizate informații generale despre modul în care funcționează algoritmul, precizând ce criterii utilizează acesta pentru a calcula primele de asigurare. În mod similar, atunci când își exercită „dreptul de acces”, persoanele vizate pot solicita operatorului informații cu privire la existența unui proces decizional automatizat și informații pertinente cu privire la logica utilizată[612].

Informațiile furnizate persoanelor vizate sunt menite să asigure transparența și să permită persoanelor vizate să își dea consimțământul, dacă este cazul, în cunoștință de cauză, sau să obțină intervenție umană. Operatorul de date trebuie să ia măsuri

607 Orientările din 3 octombrie 2017 ale Grupului de lucru „Articolul 29” privind procesul decizional automatizat și crearea de profiluri în sensul Regulamentului 2016/679, WP 251, Bruxelles, p. 15.

608 Regulamentul general privind protecția datelor, articolul 22 alineatul (2).

609 *Ibidem*, articolul 12.

610 *Ibidem*, articolul 15.

611 *Ibidem*, articolul 13 alineatul (2) litera (f).

612 *Ibidem*, articolul 15 alineatul (1) litera (h).

adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate. Aceasta include cel puțin dreptul de a obține intervenție umană din partea operatorului și posibilitatea persoanei vizate de a-și exprima punctul de vedere și de a contesta o decizie bazată pe prelucrarea automatizată a datelor sale cu caracter personal[613].

Grupul de lucru „Articolul 29" a oferit orientări suplimentare cu privire la modul în care este abordat procesul decizional automatizat în cadrul RGPD[614].

În cadrul legislației CoE, persoanele fizice au dreptul de a nu face obiectul unei decizii care le va afecta în mod semnificativ și care se bazează exclusiv pe prelucrarea automată fără a le fi luate în considerare opiniile[615]. Cerința de a lua în considerare opiniile persoanei vizate atunci când deciziile se bazează exclusiv pe prelucrarea automată înseamnă că aceste persoane au dreptul de a contesta astfel de decizii și ar trebui să aibă posibilitatea de a contesta orice inexactitate a datelor cu caracter personal pe care le utilizează operatorul, precum și relevanța oricărui profil care le-a fost aplicat[616]. Cu toate acestea, o persoană nu își poate exercita acest drept dacă decizia automatizată este autorizată printr-o lege sub a cărei incidență intră operatorul și care prevede, de asemenea, măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate. În plus, persoanele vizate au dreptul să obțină, la cerere, informații privind raționamentul care stă la baza prelucrării datelor[617]. Raportul explicativ privind Convenția 108 modernizată oferă exemplul de evaluare a solvabilității. Persoanele fizice ar trebui să aibă dreptul de a fi informate nu doar cu privire la rezultatul pozitiv sau negativ al evaluării, ci și cu privire la *logica* pe care se bazează prelucrarea datelor lor cu caracter personal și care a condus la rezultatul respectiv. „Înțelegerea acestor elemente contribuie la exercitarea eficace a altor garanții esențiale, cum ar fi dreptul la opoziție și dreptul de a depune o plângere în fața unei autorități competente"[618].

Recomandarea privind crearea de profiluri, deși nu are caracter obligatoriu din punct de vedere juridic, precizează condițiile pentru colectarea și prelucrarea datelor cu

613 *Ibidem*, articolul 22 alineatul (3).

614 Orientările din 3 octombrie 2017 ale Grupului de lucru „Articolul 29" privind procesul decizional automatizat și crearea de profiluri în sensul Regulamentului 2016/679, WP 251, Bruxelles.

615 Convenția 108 modernizată, articolul 9 alineatul (1) litera (a).

616 Raportul explicativ privind Convenția 108 modernizată, punctul 75.

617 Convenția 108 modernizată, articolul 9 alineatul (1) litera (c).

618 Raportul explicativ privind Convenția 108 modernizată, punctul 77.

caracter personal în contextul creării de profiluri[619]. Aceasta include dispoziții privind necesitatea de a se asigura faptul că prelucrarea în contextul creării de profiluri trebuie să fie echitabilă, legală, proporțională și în scopuri precise și legitime. De asemenea, include dispoziții privind informațiile pe care operatorii ar trebui să le furnizeze persoanelor vizate. Recomandarea menționează și principiul calității datelor, care impune operatorilor să ia măsuri pentru a corecta factorii de inexactitate a datelor, pentru a limita riscurile sau erorile pe care le implică crearea de profiluri și pentru a evalua periodic calitatea datelor și a algoritmilor utilizați.

6.2. Căi de atac, răspundere, sancțiuni și despăgubiri

Principalele elemente

- În conformitate cu Convenția 108 modernizată și cu Directiva privind protecția datelor, dreptul intern al părților contractante trebuie să stabilească căi de atac și sancțiuni corespunzătoare pentru încălcarea dreptului la protecția datelor.
- În UE, RGPD prevede căi de atac pentru persoanele vizate în cazul în care le sunt încălcate drepturile, precum și sancțiuni împotriva operatorilor și persoanelor împuternicite de operatori care nu respectă dispozițiile regulamentului. Acesta prevede, de asemenea, dreptul la despăgubiri și răspunderea.
    - Persoanele vizate au dreptul să depună o plângere în fața unei autorități de supraveghere pentru presupuse încălcări ale regulamentului, precum și dreptul la o cale de atac eficientă și la acordarea de despăgubiri.
    - În exercițiul dreptului la o cale de atac eficientă, persoanele pot fi reprezentate de organizații fără scop lucrativ care activează în domeniul protecției datelor.
    - Operatorul sau persoana împuternicită de operator răspunde pentru orice prejudicii materiale și morale produse ca urmare a încălcării.
    - Autoritățile de supraveghere au competența de a impune, pentru încălcări ale regulamentului, amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală, luându-se în calcul cea mai mare valoare.

619 Recomandarea CM/Rec(2010)13 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal în contextul creării de profiluri, articolul 5 alineatul (5).

- În ultimă instanță și în anumite condiții, persoanele vizate pot să aducă în atenția CEDO cazurile de încălcare a legislației privind protecția datelor.
- Orice persoană fizică sau juridică are dreptul de a depune o plângere împotriva oricărei decizii a Comitetului European pentru Protecția Datelor în fața CJUE, în condițiile prevăzute de tratate.

Adoptarea instrumentelor juridice nu este suficientă pentru a asigura protecția datelor cu caracter personal în Europa. Pentru ca normele europene de protecție a datelor să fie eficiente, este necesar să se stabilească mecanisme care să permită persoanelor să contracareze încălcările drepturilor lor și să solicite despăgubiri pentru orice prejudiciu suferit. De asemenea, este important ca autoritățile de supraveghere să aibă competența de a impune sancțiuni eficiente, disuasive și proporționale cu încălcarea în cauză.

Drepturile acordate în temeiul legislației privind protecția datelor pot fi exercitate numai de către persoana ale cărei drepturi sunt amenințate, și anume persoana vizată. Cu toate acestea, alte persoane – care îndeplinesc cerințele necesare în temeiul legislației naționale – pot, de asemenea, să reprezinte persoanele vizate în exercițiul drepturilor lor. În conformitate cu o serie de legislații naționale, copiii și persoanele cu dizabilități intelectuale trebuie să fie reprezentate de tutorii lor legali[620]. Conform legislației UE privind protecția datelor, o asociație al cărei scop legitim este de a promova drepturile la protecția datelor poate reprezenta persoanele vizate în fața unei autorități de supraveghere sau a unei instanțe[621].

6.2.1. Dreptul de a depune o plângere în fața unei autorități de supraveghere

Atât în cadrul **legislației CoE**, cât și a **UE**, persoanele fizice au dreptul de a depune cereri și plângeri în fața autorității de supraveghere competente dacă consideră că prelucrarea datelor lor cu caracter personal nu este efectuată în conformitate cu legea.

620 FRA (2015), *Manual de legislație europeană privind drepturile copilului*, Luxemburg, Oficiul pentru Publicații; FRA (2013), *Legal capacity of persons with intellectual disabilities and persons with mental health problems* (Capacitatea juridică a persoanelor cu dizabilități intelectuale și a persoanelor cu probleme de sănătate mintală), Luxemburg, Oficiul pentru Publicații.

621 Regulamentul general privind protecția datelor, articolul 80.

Convenția 108 modernizată recunoaște dreptul persoanelor vizate de a beneficia de asistența unei autorități de supraveghere în exercițiul drepturilor lor în temeiul convenției, indiferent de cetățenie sau de reședință[622]. O cerere de asistență poate fi respinsă numai în circumstanțe excepționale, iar persoanele vizate nu ar trebui să acopere costurile și taxele aferente asistenței[623].

În sistemul juridic al UE se regăsesc dispoziții similare. RGPD impune autorităților de supraveghere să adopte măsuri pentru a facilita depunerea plângerilor, cum ar fi elaborarea unui formular electronic de depunere a plângerilor[624]. Persoana vizată poate depune plângerea la autoritatea de supraveghere din statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare[625]. Plângerile trebuie să fie investigate, iar autoritatea de supraveghere trebuie să informeze persoana în cauză cu privire la rezultatul procedurii care tratează plângerea[626].

Eventualele încălcări ale protecției datelor de către instituțiile sau organismele UE pot fi aduse la cunoștința Autorității Europene pentru Protecția Datelor[627]. Dacă AEPD nu furnizează un răspuns în termen de șase luni, plângerea se consideră a fi respinsă. Deciziile AEPD pot fi contestate prin introducerea unei acțiuni în fața CJUE în temeiul Regulamentului (CE) nr. 45/2001, care prevede obligația instituțiilor și a organismelor UE de a respecta normele de protecție a datelor.

Trebuie să existe posibilitatea de a contesta în instanță deciziile luate de o autoritate națională de supraveghere. Această regulă se aplică atât persoanei vizate, cât și operatorilor și persoanelor împuternicite de operatori care au participat la procedura desfășurată în fața unei autorități de supraveghere.

Exemplu: În septembrie 2017, autoritatea pentru protecția datelor din Spania a amendat Facebook pentru încălcarea mai multor reglementări privind protecția datelor. Autoritatea de supraveghere a impus rețelei sociale această

622 Convenția 108 modernizată, articolul 18.

623 *Ibidem*, articolele 16-17.

624 Regulamentul general privind protecția datelor, articolul 57 alineatul (2).

625 *Ibidem*, articolul 77 alineatul (1).

626 *Ibidem*, articolul 77 alineatul (2).

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

sancțiune pentru colectarea, stocarea și prelucrarea datelor cu caracter personal, inclusiv a unor categorii speciale de date cu caracter personal, în scopuri publicitare și fără a obține consimțământul persoanei vizate. Decizia s-a bazat pe o anchetă efectuată de autoritatea de supraveghere din proprie inițiativă.

6.2.2. Dreptul la o cale de atac eficientă

Pe lângă dreptul de a depune plângeri în fața autorității de supraveghere, persoanele fizice trebuie să aibă dreptul la o cale de atac eficientă și la apărarea propriilor interese în fața unei instanțe. Dreptul la o cale de atac este consacrat în mod ferm în tradiția juridică europeană și este recunoscut ca drept fundamental, atât în temeiul articolului 47 din Carta drepturilor fundamentale a UE, cât și al articolului 13 din Convenția europeană a drepturilor omului[628].

În cadrul legislației UE, importanța punerii la dispoziția persoanelor vizate a unor căi de atac eficiente în caz de încălcare a drepturilor lor reiese cu claritate atât din dispozițiile RGPD – care instituie un drept la o cale de atac eficientă împotriva autorităților de supraveghere, a operatorilor și a persoanelor împuternicite de operatori –, cât și din jurisprudența CJUE.

Exemplu: În cauza *Schrems*[629], CJUE a declarat nulă decizia privind caracterul adecvat al nivelului de protecție cunoscută drept „Decizia privind sfera de siguranță". Această decizie permitea transferurile internaționale de date din UE către organizații din SUA care declarau pe propria răspundere că respectă regimul „sferei de siguranță". CJUE a considerat că regimul sferei de siguranță prezintă mai multe deficiențe, ceea ce a compromis drepturile fundamentale ale cetățenilor UE la respectarea vieții private și la protecția datelor cu caracter personal, precum și dreptul la o cale de atac eficientă.

În ceea ce privește încălcarea drepturilor la respectarea vieții private și la protecția datelor, CJUE a subliniat că legislația SUA permite anumitor autorități publice să acceadă la datele cu caracter personal transferate din statele membre în SUA și să le prelucreze, într-un mod incompatibil cu scopul inițial al transferului și depășind ceea ce este strict necesar și proporțional cu apărarea

628 Vezi, de exemplu, Hotărârea CEDO din 7 iunie 2016 în cauza *Karabeyoğlu/Turcia*, nr. 30083/10; Hotărârea CEDO din 18 iulie 2017 în cauza *Mustafa Sezgin Tanrıkulu/Turcia*, nr. 27473/06.

629 Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*.

securității naționale. În ceea ce privește dreptul la o cale de atac eficientă, Curtea a constatat că persoanele vizate nu aveau nicio cale de atac administrativă sau juridică prin care să li se permită accesul la datele care le priveau și obținerea rectificării sau a ștergerii acestora, după caz. CJUE a concluzionat că o reglementare care nu prevede nicio posibilitate a persoanelor vizate de a recurge la căi de atac pentru a obține accesul la datele cu caracter personal sau rectificarea ori ștergerea acestora „nu respectă nici substanța dreptului fundamental la o protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din [C]artă". Curtea a subliniat că existența unei căi de atac care garantează respectarea normelor juridice este inerentă statului de drept.

Persoanele fizice, operatorii sau persoanele împuternicite de operatori care intenționează să conteste decizia cu caracter obligatoriu din punct de vedere juridic a unei autorități de supraveghere pot introduce o acțiune în instanță[630]. Termenul „decizie" trebuie interpretat în sens larg, cuprinzând exercitarea de către autoritățile de supraveghere a competențelor de investigare, de sancționare și de autorizare, precum și deciziile de refuz sau respingere a unei plângeri. În schimb, măsurile autorităților de supraveghere care nu sunt obligatorii din punct de vedere juridic, cum ar fi avizele emise de autoritatea de supraveghere sau consilierea furnizată de aceasta, nu pot face obiectul unei acțiuni în instanță[631]. Acțiunile trebuie introduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere în cauză[632].

În cazurile în care un operator sau o persoană împuternicită de operator încalcă drepturile unei persoane vizate, persoana în cauză are dreptul să depună o plângere în fața unei instanțe[633]. În ceea ce privește procedurile introduse împotriva unui operator sau a unei persoane împuternicite de operator, este deosebit de important ca persoanele fizice să aibă posibilitatea de a alege unde să introducă acțiunea. Acestea pot alege să introducă acțiunea fie în statul membru în care operatorul sau persoana împuternicită de acesta își are sediul, fie în statul membru în care persoanele vizate în cauză își au reședința obișnuită[634]. A doua posibilitate facilitează considerabil exercițiul drepturilor persoanelor fizice, deoarece le permite să introducă acțiunile judiciare în statul în care își au reședința, într-o jurisdicție familiară lor. Limitarea locului de

630 Regulamentul general privind protecția datelor, articolul 78.

631 *Ibidem*, considerentul 143.

632 *Ibidem*, articolul 78 alineatul (3).

633 *Ibidem*, articolul 79.

634 *Ibidem*, articolul 79 alineatul (2).

desfășurare a procedurilor împotriva operatorilor și a persoanelor împuternicite de operatori la statul membru în care aceștia au un sediu ar putea descuraja persoanele vizate care locuiesc în alte state membre să introducă o acțiune în justiție, deoarece aceasta ar presupune costuri de călătorie și alte costuri suplimentare, iar procedura s-ar putea desfășura într-o limbă și într-o jurisdicție străine. Singura excepție se referă la cazurile în care operatorul sau persoana împuternicită de operator este autoritate publică, iar prelucrarea este efectuată în exercitarea competențelor publice ale acestei autorități. Într-un astfel de caz, numai instanțele din statul autorității publice în cauză sunt competente să se pronunțe cu privire la o plângere în acest sens[635].

Deși, în majoritatea cazurilor, cauzele având ca obiect normele de protecție a datelor sunt soluționate de instanțele din statele membre, unele cauze pot fi trimise în fața CJUE. Prima posibilitate este aceea în care o persoană vizată, un operator, o persoană împuternicită de operator sau o autoritate de supraveghere introduce o acțiune în anularea unei decizii a CEPD. Acțiunea face totuși obiectul condițiilor prevăzute la articolul 263 din TFUE, ceea ce înseamnă că, pentru a fi admisibilă, persoanele și entitățile în cauză trebuie să demonstreze că decizia comitetului le afectează în mod direct și individual.

Cel de al doilea scenariu se referă la cazurile în care instituțiile sau organele UE prelucrează în mod ilegal date cu caracter personal. În cazurile în care instituțiile UE încalcă legislația privind protecția datelor, persoanele vizate pot adresa o plângere direct în fața Tribunalului UE (Tribunalul face parte din CJUE). Tribunalul este responsabil în primă instanță pentru soluționarea plângerilor având ca obiect încălcarea dreptului UE de către instituțiile UE. Astfel, plângerile împotriva AEPD, în calitatea acesteia de instituție UE, pot fi depuse și în fața Tribunalului[636].

> Exemplu: În cauza *Bavarian Lager*[637], această societate a solicitat Comisiei Europene să îi acorde accesul la conținutul complet al procesului-verbal al unei reuniuni organizate de Comisie și despre care societatea susținea că a vizat aspecte juridice care o privesc. Comisia a respins cererea de acces

635 *Ibidem*.

636 Regulamentul (CE) nr. 45/2001, articolul 32 alineatul (3).

637 Hotărârea CJUE [MC] din 29 iunie 2010 în cauza C-28/08 P, *Comisia Europeană/The Bavarian Lager Co. Ltd.*.

a societății pentru motivul că primează interesele privind protecția datelor[638]. În temeiul articolului 32 din Regulamentul privind protecția datelor de către instituțiile europene, Bavarian Lager a introdus o plângere în fața Tribunalului de Primă Instanță (predecesorul Tribunalului) împotriva acestei decizii. Prin hotărârea pronunțată în cauza T-194/04, *The Bavarian Lager Co. Ltd/Comisia Comunităților Europene*, Tribunalul de Primă Instanță a anulat decizia Comisiei de respingere a cererii de acces. Comisia Europeană a atacat această decizie la CJUE.

CJUE a pronunțat (în Marea Cameră) hotărârea de anulare a hotărârii Tribunalului de Primă Instanță și de confirmare a respingerii de către Comisia Europeană a cererii de acces la procesul-verbal complet al reuniunii pentru motivul protejării datelor cu caracter personal ale persoanelor prezente la reuniune. CJUE a considerat că Comisia a refuzat în mod justificat să divulge aceste informații, întrucât participanții nu își dăduseră consimțământul pentru divulgarea datelor lor cu caracter personal. În plus, Bavarian Lager nu a demonstrat necesitatea obținerii accesului la informațiile respective.

În sfârșit, persoanele vizate, autoritățile de supraveghere, operatorii sau persoanele împuternicite de operatori pot, în cursul procedurilor interne, să solicite instanței naționale să ceară clarificări din partea CJUE cu privire la interpretarea și valabilitatea actelor instituțiilor, organelor, oficiilor sau agențiilor UE. Aceste clarificări sunt cunoscute sub numele de decizii preliminare. Această procedură nu reprezintă o cale de atac directă disponibilă reclamantului, însă permite instanțelor naționale să se asigure că aplică interpretarea corectă a dreptului UE. Tocmai prin intermediul acestui mecanism al deciziilor preliminare au ajuns la CJUE cauze de referință – precum *Digital Rights Ireland*, *Kärntner Landesregierung și alții*[639] sau *Schrems*[640] – care au afectat semnificativ dezvoltarea legislației UE privind protecția datelor.

638 Pentru analiza argumentului, vezi AEPD (2011), *Public access to documents containing personal data after the Bavarian Lager ruling* (Accesul public la documente care conțin date cu caracter personal în urma hotărârii din cauza Bavarian Lager), Bruxelles.

639 Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții* și *Kärntner Landesregierung și alții*.

640 Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*.

Exemplu: *Digital Rights Ireland* și *Kärntner Landesregierung și alții*[641] au fost două cauze conexate trimise CJUE de Înalta Curte irlandeză și de Curtea Constituțională austriacă și având ca obiect conformitatea Directivei 2006/24/CE (Directiva privind păstrarea datelor) cu legislația UE privind protecția datelor. Curtea Constituțională austriacă a adresat CJUE întrebări cu privire la valabilitatea articolelor 3-9 din Directiva 2006/24/CE în lumina articolelor 7, 9 și 11 din Carta drepturilor fundamentale a UE. Printre acestea se număra întrebarea dacă anumite dispoziții ale Legii federale a telecomunicațiilor din Austria, care transpunea Directiva privind păstrarea datelor, erau incompatibile cu anumite aspecte din Directiva abrogată privind protecția datelor și cu Regulamentul privind protecția datelor de către instituțiile europene.

În cauza *Kärntner Landesregierung și alții*, domnul Seitlinger, unul dintre reclamanții în procedura desfășurată în fața Curții Constituționale, a afirmat că utilizează serviciile de telefonie, internet și e-mail atât în interes de serviciu, cât și în interes personal. Astfel, informațiile pe care le trimitea și pe care le primea erau transmise utilizând rețelele publice de telecomunicații. În conformitate cu Legea austriacă privind telecomunicațiile din 2003, furnizorul acestuia de servicii de telecomunicații era obligat prin lege să colecteze și să stocheze date privind modul în care clientul utilizează rețeaua. Domnul Seitlinger a considerat că această colectare și stocare a datelor sale cu caracter personal nu este necesară în scopurile tehnice de trimitere și primire de informații prin intermediul rețelei. Colectarea și stocarea datelor respective nu erau necesare nici în vederea facturării. Domnul Seitlinger a declarat că nu și-a dat consimțământul cu privire la această utilizare a datelor sale cu caracter personal, care erau colectate și stocate exclusiv în temeiul Legii austriece privind telecomunicațiile din 2003.

În consecință, domnul Seitlinger a introdus o acțiune în fața Curții Constituționale a Austriei, susținând că obligațiile legale impuse furnizorului de servicii de telecomunicații îi încălcau lui drepturile fundamentale consacrate la articolul 8 din Carta UE. Având în vedere că legea austriacă în cauză punea în aplicare legislația UE (Directiva privind păstrarea datelor), Curtea Constituțională austriacă a sesizat CJUE solicitând să se stabilească compatibilitatea directivei cu dreptul la respectarea vieții private și cu dreptul la protecția datelor consacrate în Carta drepturilor fundamentale a UE.

641 Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții* și *Kärntner Landesregierung și alții*.

Marea Cameră a CJUE a judecat cauza, hotărând anularea Directivei privind păstrarea datelor a UE. CJUE a constatat că directiva presupunea o ingerință deosebit de gravă în drepturile fundamentale la respectarea vieții private și la protecția datelor, fără ca această ingerință să se limiteze la ceea ce este strict necesar. Directiva urmărea un obiectiv legitim, deoarece oferea autorităților naționale posibilități suplimentare de a investiga și de a urmări penal infracțiuni grave și, prin urmare, constituia un instrument valoros pentru anchetele penale. CJUE a precizat totuși că limitările drepturilor fundamentale ar trebui să se aplice numai dacă sunt strict necesare și ar trebui să fie însoțite de norme clare și precise privind domeniul lor de aplicare, precum și de garanții pentru persoanele fizice.

Potrivit CJUE, directiva nu a trecut acest test al necesității. În primul rând, nu stabilea norme clare și precise care să limiteze întinderea ingerinței. În loc să prevadă necesitatea unei legături între datele păstrate și infracțiunile grave, directiva se aplica tuturor metadatelor tuturor utilizatorilor tuturor mijloacelor de comunicații electronice. Astfel, directiva constituia o ingerință în dreptul la respectarea vieții private și în dreptul la protecția datelor, practic, ale întregii populații a UE, ceea ce poate fi considerat disproporționat. Directiva nu prevedea condiții de limitare a persoanelor autorizate să acceseze datele cu caracter personal, iar accesul nu făcea nici obiectul unor condiții procedurale, cum ar fi cerința de a obține aprobare din partea unei autorități administrative sau a unei instanțe înainte de accesarea datelor. În sfârșit, directiva nu stabilea garanții clare pentru protecția datelor păstrate. În consecință, directiva nu asigura o protecție eficientă a datelor împotriva riscurilor de abuz, precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date[642].

În principiu, CJUE trebuie să răspundă întrebărilor primite și nu poate refuza pronunțarea unei decizii preliminare pentru motivul că răspunsul nu ar fi relevant sau nu ar fi furnizat în timp util în ceea ce privește cauza inițială. În schimb, CJUE poate refuza furnizarea unui răspuns dacă întrebarea nu se încadrează în sfera sa de competență[643]. CJUE pronunță o hotărâre numai cu privire la elementele constitutive ale

642 Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții* și *Kärntner Landesregierung și alții*, punctul 69.

643 Hotărârea CJUE din 16 decembrie 1981 în cauza C-244/80, *Pasquale Foglia/Mariella Novello* (nr. 2); Hotărârea CJUE din 28 septembrie 2006 în cauza C-467/04, *Proces penal/Gasparini și alții*.

cererii de pronunțare a unei decizii preliminare, iar instanța națională își păstrează competența de a se pronunța în cauza inițială[644].

În conformitate cu legislația CoE, părțile contractante trebuie să instituie căi de atac judiciare și extrajudiciare adecvate pentru încălcarea dispozițiilor Convenției 108 modernizate[645]. Plângerile având ca obiect încălcarea drepturilor la protecția datelor cu încălcarea articolului 8 din Convenția europeană a drepturilor omului introduse împotriva unei părți contractante la această convenție pot fi introduse, de asemenea, în fața CEDO atunci când toate căile de atac interne disponibile au fost epuizate. Invocarea unei încălcări a articolului 8 din Convenția europeană a drepturilor omului în fața CEDO trebuie să îndeplinească și alte criterii de admisibilitate (articolele 34-35 din Convenția europeană a drepturilor omului)[646].

Deși cererile adresate CEDO pot fi formulate exclusiv împotriva părților contractante, acestea pot viza, de asemenea, în mod indirect, acțiuni sau omisiuni ale unor părți private, în măsura în care o parte contractantă nu și-a îndeplinit obligațiile pozitive care îi revin în conformitate cu Convenția europeană a drepturilor omului și nu a prevăzut în legislația națională un nivel corespunzător de protecție împotriva încălcării drepturilor la protecția datelor.

Exemplu: În cauza *K.U./Finlanda*[647], reclamantul minor a depus o plângere privind postarea unui anunț de natură sexuală referitor la el pe un site web de întâlniri. Furnizorul de servicii nu a dezvăluit identitatea persoanei care postase informațiile, invocând ca motiv obligațiile de confidențialitate prevăzute de legislația finlandeză. Reclamantul a susținut că legislația finlandeză nu asigura un nivel suficient de protecție împotriva unor astfel de acțiuni desfășurate de o persoană particulară care posta pe internet informații incriminatoare privind reclamantul. CEDO a stabilit că statele nu numai că au obligația de a se abține de la a interveni în mod arbitrar în viața privată a persoanelor fizice, ci trebuie să îndeplinească, de asemenea, o serie de obligații pozitive care implică „adoptarea unor măsuri care să asigure respectarea vieții private chiar și în ceea ce privește relațiile dintre persoane". În cazul reclamantului, pentru a se asigura protecția practică și eficientă a acestuia, era necesar să

644 Hotărârea CJUE [MC] din 11 decembrie 2007 în cauza C-438/05, *International Transport Workers' Federation, Finnish Seamen's Union/Viking Line ABP, OÜ Viking Line Eesti*, punctul 85.

645 Convenția 108 modernizată, articolul 12.

646 Convenția europeană a drepturilor omului, articolele 34-37.

647 Hotărârea CEDO din 2 decembrie 2008 în cauza *K.U./Finlanda*, nr. 2872/02.

se ia măsuri eficiente pentru identificarea și urmărirea penală a făptuitorului. Întrucât statul nu acordase această protecție, Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Exemplu: În cauza *Köpke/Germania*[648], reclamanta a fost suspectată de furt la locul de muncă și, astfel, a fost supravegheată prin mijloace video în secret. CEDO a concluzionat că „niciun aspect nu a indicat că autoritățile naționale nu ar fi stabilit un echilibru corect, în cadrul marjei lor de apreciere, între dreptul reclamantei la respectarea vieții private prevăzut la articolul 8, pe de o parte, și interesul angajatorului de a-și proteja drepturile de proprietate, precum și interesul public de bună administrare a justiției, pe de altă parte". În consecință, cererea a fost declarată inadmisibilă.

Dacă CEDO constată că o parte contractantă a încălcat oricare dintre drepturile protejate de Convenția europeană a drepturilor omului, partea contractantă în cauză are obligația de a executa hotărârea pronunțată de CEDO (articolul 46 din Convenția europeană a drepturilor omului). Măsurile de executare trebuie, în primul rând, să pună capăt încălcării și să remedieze, pe cât posibil, consecințele negative ale acesteia asupra reclamantului. Este, de asemenea, posibil ca pentru executarea hotărârilor judecătorești să fie necesară adoptarea de măsuri generale pentru a preveni încălcări similare celor constatate de Curte, fie prin modificarea legislației sau a jurisprudenței, fie prin aplicarea altor măsuri.

Pentru cazurile în care CEDO constată o încălcare a Convenției europene a drepturilor omului, la articolul 41 din aceasta se prevede posibilitatea CEDO de a acorda o „satisfacție echitabilă" reclamantului, pe spezele părții contractante.

Dreptul de a mandata un organism, o organizație sau o asociație fără scop lucrativ

RGPD permite persoanelor care depun o plângere în fața unei autorități de supraveghere sau care introduc o acțiune în instanță să mandateze un organism, o organizație sau o asociație fără scop lucrativ să le reprezinte[649]. Aceste entități fără scop lucrativ trebuie să aibă obiective statutare în sfera interesului public și să își desfășoare activitatea în domeniul protecției datelor. Acestea pot depune plângerea sau pot exercita dreptul la o cale de atac în numele persoanei (persoanelor) vizate.

648 Hotărârea CEDO din 5 octombrie 2010 în cauza *Köpke/Germania* (dec.), nr. 420/07.

649 Regulamentul general privind protecția datelor, articolul 80.

Regulamentul oferă statelor membre posibilitatea de a decide – în conformitate cu legislația națională – dacă un organism poate depune plângeri în numele persoanelor vizate fără a fi mandatat de acestea.

Acest drept de reprezentare le permite persoanelor fizice să beneficieze de expertiza și de capacitatea organizatorică și financiară a acestor entități fără scop lucrativ, oferind astfel o asistență semnificativă persoanelor fizice în exercițiul drepturilor lor. RGPD permite acestor entități să depună plângeri colective în numele mai multor persoane vizate. Acest lucru aduce, de asemenea, beneficii funcționării și eficienței sistemului judiciar, întrucât plângerile similare sunt grupate și examinate împreună.

6.2.3. Răspunderea și dreptul la despăgubiri

Dreptul la o cale de atac eficientă trebuie să permită persoanelor fizice să solicite despăgubiri pentru orice prejudiciu suferit ca urmare a prelucrării datelor lor cu caracter personal într-un mod care încalcă legislația aplicabilă. Răspunderea operatorilor și a persoanelor împuternicite de operatori pentru prelucrarea ilegală este recunoscută în mod explicit în RGPD[650]. Regulamentul acordă persoanelor dreptul de a primi despăgubiri de la operator sau de la persoana împuternicită de operator atât pentru prejudiciile materiale, cât și pentru cele morale, prevăzând la preambul că „[c]onceptul de prejudiciu ar trebui interpretat în sens larg, din perspectiva jurisprudenței Curții de Justiție, într-un mod care să reflecte pe deplin obiectivele prezentului regulament”[651]. Operatorii sunt răspunzători și pot face obiectul unor cereri de despăgubire dacă nu își respectă obligațiile care le revin în temeiul regulamentului. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligațiile din RGPD care revin în mod specific persoanelor împuternicite de operator sau a acționat în afara sau în contradicție cu instrucțiunile legale ale operatorului. În cazul în care un operator sau o persoană împuternicită de operator a plătit în totalitate despăgubirile, RGPD prevede că respectivul operator sau respectiva persoană împuternicită de operator are dreptul să solicite – de la ceilalți operatori sau celelalte persoane împuternicite de operator implicate în aceeași operațiune de prelucrare – recuperarea acelei părți din despăgubiri care corespunde părții lor de răspundere pentru prejudiciu[652]. În același timp, exceptările de la răspundere sunt foarte stricte și sunt condiționate de

650 *Ibidem*, articolul 82.

651 *Ibidem*, considerentul 146.

652 *Ibidem*, articolul 82 alineatele (2) și (5).

prezentarea dovezii că operatorul sau persoana împuternicită de operator nu poartă în niciun caz răspunderea pentru incidentul care a cauzat prejudiciul.

Despăgubirea trebuie să fie „integrală și eficace" în raport cu prejudiciul suferit. În cazul în care prejudiciul este cauzat de o operațiune de prelucrare desfășurată de mai mulți operatori și persoane împuternicite de operatori, fiecare operator sau persoană împuternicită de operator trebuie să fie tras(ă) la răspundere pentru întregul prejudiciu. Această normă urmărește să asigure despăgubirea eficace a persoanelor vizate și o abordare coordonată a conformității de către operatorii și persoanele împuternicite de operatori implicați în operațiunile de prelucrare.

Exemplu: Persoanele vizate nu sunt obligate să introducă acțiuni și să solicite despăgubiri de la toate entitățile răspunzătoare pentru prejudiciu, deoarece aceasta ar putea conduce la proceduri costisitoare și îndelungate. Este suficientă introducerea unei acțiuni împotriva unuia dintre operatorii asociați, care pot fi considerați răspunzători în mod solidar pentru întregul prejudiciu. În astfel de cazuri, un operator sau o persoană împuternicită de operator care plătește prejudiciul este ulterior îndreptățit să recupereze suma plătită de la celelalte entități implicate în prelucrare și răspunzătoare pentru încălcare, în cuantumul corespunzător răspunderii lor pentru prejudiciu. Aceste proceduri între diferiți operatori și persoane împuternicite de operatori asociați au loc după ce persoana vizată a primit despăgubirile, aceasta din urmă neparticipând la ele.

În cadrul juridic al CoE, articolul 12 din Convenția 108 modernizată impune părților contractante să instituie căi de atac adecvate pentru încălcările dreptului intern de punere în aplicare a cerințelor convenției. Raportul explicativ privind Convenția 108 modernizată arată că orice cale de atac trebuie să includă posibilitatea contestării în instanță a unei decizii sau a unei practici și că trebuie să fie puse la dispoziție, în același timp, și căi de atac extrajudiciare[653]. Diferitele modalități și norme privind accesul la aceste căi de atac, împreună cu procedura care trebuie urmată, sunt lăsate la aprecierea fiecărei părți contractante. Părțile contractante și instanțele naționale ar trebui, de asemenea, să ia în considerare dispozițiile privind compensațiile financiare pentru prejudiciile materiale și morale cauzate de prelucrare, precum și posibilitatea de a permite introducerea unor acțiuni colective[654].

653 Raportul explicativ privind Convenția 108 modernizată, punctul 100.

654 *Ibidem*.

6.2.4. Sancțiuni

În cadrul legislației CoE, articolul 12 din Convenția 108 modernizată prevede că fiecare parte contractantă trebuie să stabilească sancțiuni și căi de atac adecvate pentru încălcarea dispozițiilor dreptului intern care pun în aplicare principiile de bază ale protecției datelor prevăzute de Convenția 108. Convenția nu stabilește și nu impune un set specific de sancțiuni. Dimpotrivă, aceasta arată în mod clar că fiecare parte contractantă are libertatea de a stabili natura sancțiunilor judiciare sau extrajudiciare, care pot fi penale, administrative sau civile. Raportul explicativ privind Convenția 108 modernizată prevede că sancțiunile trebuie să fie eficiente, proporționale și disuasive[655]. Părțile contractante trebuie să respecte acest principiu atunci când determină natura și severitatea sancțiunilor disponibile în ordinea lor juridică internă.

În cadrul legislației UE, articolul 83 din RGPD împuternicește autoritățile de supraveghere ale statelor membre să impună amenzi administrative pentru încălcarea regulamentului. Valoarea amenzilor și aspectele pe care autoritățile naționale le iau în considerare atunci când decid să impună o amendă, precum și plafoanele maxime totale ale acestei amenzi sunt prevăzute, de asemenea, la articolul 83. Astfel, regimul de sancționare este armonizat la nivelul UE.

RGPD adoptă o abordare graduală a amenzilor. Autoritățile de supraveghere au competența de a impune, pentru încălcări ale regulamentului, amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală, luându-se în calcul cea mai mare valoare. Printre încălcările care pot determina această valoare a amenzii se numără încălcări ale principiilor de bază pentru prelucrare, inclusiv condițiile privind consimțământul, încălcările drepturilor persoanelor vizate și ale dispozițiilor regulamentului care reglementează transferul datelor cu caracter personal către destinatari din țări terțe. Pentru alte încălcări, autoritățile de supraveghere pot impune amenzi de până la 10 000 000 EUR sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală, luându-se în calcul cea mai mare valoare.

La determinarea tipului și a valorii amenzii de aplicat, autoritățile de supraveghere trebuie să ia în considerare o serie de aspecte[656]. De exemplu, trebuie să ia în considerare în mod corespunzător natura, gravitatea și durata încălcării, categoriile de date cu caracter personal afectate și dacă încălcarea a fost comisă intenționat sau din neglijență. În cazul în care un operator sau o persoană împuternicită de operator

655 *Ibidem*.

656 Regulamentul general privind protecția datelor, articolul 83 alineatul (2).

a luat măsuri pentru a diminua prejudiciul suferit de persoanele vizate, acest lucru ar trebui, de asemenea, să fie luat în considerare. În mod similar, gradul de cooperare cu autoritatea de supraveghere după producerea încălcării și modul în care autoritatea de supraveghere a aflat despre încălcare (de exemplu, dacă aceasta a fost raportată de entitatea responsabilă pentru prelucrare sau de o persoană vizată ale cărei drepturi fuseseră încălcate) reprezintă alți factori importanți după care se ghidează autoritățile de supraveghere în adoptarea deciziei lor[657].

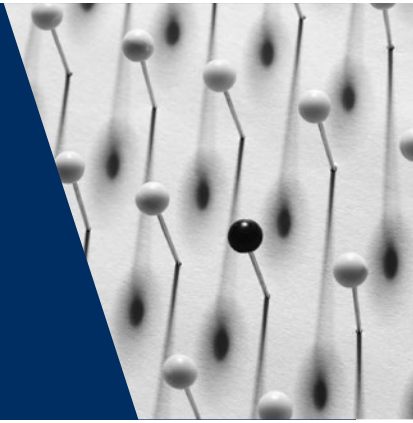
Pe lângă capacitatea de a impune amenzi administrative, autoritățile de supraveghere dispun de o gamă largă de alte competențe corective. Așa-numitele competențe „corective" ale autorităților de supraveghere sunt prevăzute la articolul 58 din RGPD. Acestea variază de la emiterea de dispoziții, avertizări și mustrări la adresa operatorilor și a persoanelor împuternicite de operatori până la impunerea unor interdicții temporare sau chiar permanente asupra activităților de prelucrare.

În ceea ce privește sancțiunile împotriva încălcărilor dreptului UE de către instituții sau organisme europene, având în vedere caracterul special al Regulamentului privind protecția datelor de către instituțiile europene, sancțiunile pot fi prevăzute sub formă de acțiuni disciplinare. În conformitate cu articolul 49 din regulamentul respectiv, „[o]rice neîndeplinire a obligațiilor prevăzute de prezentul regulament, fie aceasta intenționată sau din culpă, atrage după sine sancțiuni disciplinare asupra funcționarului sau agentului Comunităților Europene [...]".

657 Orientările din 3 octombrie 2017 ale Grupului de lucru „Articolul 29" privind aplicarea amenzilor administrative și stabilirea valorii acestora în sensul Regulamentului 2016/679, WP 253, Bruxelles, 3 octombrie 2017.

7

Transferurile și fluxurile internaționale de date cu caracter personal



UE	Aspecte vizate	CoE
Transferurile de date cu caracter personal		
Regulamentul general privind protecția datelor, articolul 44	**Concept**	Convenția 108 modernizată, articolul 14 alineatele (1) și (2)
Fluxul liber al datelor cu caracter personal		
Regulamentul general privind protecția datelor, articolul 1 alineatul (3) și considerentul 170	**Între statele membre ale UE**	
	Între părțile contractante la Convenția 108	Convenția 108 modernizată, articolul 14 alineatul (1)
Transferurile de date cu caracter personal către țări terțe sau organizații internaționale		
Regulamentul general privind protecția datelor, articolul 45 Hotărârea CJUE [MC] în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*, 2015	**Decizie privind caracterul adecvat al nivelului de protecție/țări terțe sau organizații internaționale cu niveluri adecvate de protecție**	Convenția 108 modernizată, articolul 14 alineatul (2)

UE	Aspecte vizate	CoE
Regulamentul general privind protecția datelor, articolul 46 alineatele (1) și (2)	**Garanții adecvate, inclusiv drepturi opozabile și căi de atac judiciare pentru persoanele vizate, prevăzute prin clauze contractuale standard, reguli corporatiste obligatorii, coduri de conduită și mecanisme de certificare**	Convenția 108 modernizată, articolul 14 alineatele (2), (3), (5) și (6)
Regulamentul general privind protecția datelor, articolul 46 alineatul (3)	**Sub rezerva autorizării din partea autorității de supraveghere competente: clauze contractuale și dispoziții incluse în acordurile administrative dintre autoritățile publice**	
Regulamentul general privind protecția datelor, articolul 46 alineatul (5)	**Autorizații existente, acordate în temeiul Directivei 95/46/CE**	
Regulamentul general privind protecția datelor, articolul 47	**Reguli corporatiste obligatorii**	
Regulamentul general privind protecția datelor, articolul 49	**Derogări pentru situații specifice**	Convenția 108 modernizată, articolul 14 alineatul (4)
Exemple: Acordul PNR între UE și SUA Acordul SWIFT între UE și SUA	**Acorduri internaționale**	Convenția 108 modernizată, articolul 14 alineatul (3) litera (a)

În cadrul legislației UE, Regulamentul general privind protecția datelor prevede fluxul liber al datelor în cadrul Uniunii Europene. Cu toate acestea, regulamentul conține cerințe specifice referitoare la transferurile de date cu caracter personal către țări terțe din afara UE și către organizații internaționale. Regulamentul recunoaște importanța acestor transferuri, în special în perspectiva comerțului și a cooperării internaționale, dar recunoaște, de asemenea, riscul crescut pentru datele cu caracter personal. Prin urmare, regulamentul urmărește să asigure, pentru datele cu caracter personal transferate în țări terțe, același nivel de protecție de care se bucură în cadrul UE[658]. Legislația CoE recunoaște, de asemenea, importanța punerii în aplicare a normelor privind fluxurile de date transfrontaliere, bazate pe un flux liber între părțile membre și pe cerințe specifice privind transferurile către părți nemembre.

658 Regulamentul general privind protecția datelor, considerentele 101 și 116.

7.1. Natura transferurilor de date cu caracter personal

Principalele elemente

- Legislația UE și a CoE cuprinde norme privind transferurile de date cu caracter personal către destinatari din țări terțe sau către organizații internaționale.
- Asigurarea protecției drepturilor persoanelor vizate atunci când datele sunt transferate în afara UE permite ca protecția acordată de legislația UE să însoțească datele cu caracter personal originare din UE.

În cadrul **legislației CoE**, fluxurile transfrontaliere de date sunt descrise drept transferuri de date cu caracter personal către destinatari care aparțin unei jurisdicții străine[659]. Fluxurile transfrontaliere de date către un destinatar care nu face parte din jurisdicția unei părți contractante sunt permise numai dacă există un nivel adecvat de protecție[660].

Legislația UE reglementează transferurile de „date cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate după ce sunt transferate într-o țară terță sau către o organizație internațională [...]"[661]. Aceste fluxuri de date sunt permise numai dacă respectă normele stabilite în capitolul V din RGPD.

Fluxurile transfrontaliere de date cu caracter personal sunt permise în cazul în care destinatarul aparține jurisdicției unei părți contractante sau a unui stat membru, în conformitate cu legislația CoE sau, respectiv, a UE. Ambele sisteme juridice permit, de asemenea, transferarea datelor către o țară care nu este parte contractantă sau stat membru, cu condiția îndeplinirii anumitor condiții.

659 Raportul explicativ privind Convenția 108 modernizată, punctul 102.

660 Convenția 108 modernizată, articolul 14 alineatul (2).

661 Regulamentul general privind protecția datelor, articolul 44.

7.2. Libera circulație/fluxul liber de date cu caracter personal între statele membre sau părțile contractante

Principalele elemente

- Fluxul de date cu caracter personal în întreaga UE, precum și transferurile de date cu caracter personal între părțile contractante la Convenția 108 modernizată trebuie să fie libere de restricții. Cu toate acestea, întrucât nu toate părțile contractante la Convenția 108 modernizată sunt state membre ale UE, transferurile dintr-un stat membru al UE într-o țară terță care este, totuși, parte contractantă la Convenția 108 nu sunt posibile decât dacă îndeplinesc condițiile stabilite de RGPD.

În temeiul legislației CoE, trebuie să existe un flux liber de date cu caracter personal între părțile contractante la Convenția 108 modernizată. Cu toate acestea, transferul poate fi interzis dacă există un „risc real și grav ca transferul către o altă parte să conducă la eludarea dispozițiilor convenției" sau dacă o parte are obligația să procedeze astfel în temeiul unor „norme armonizate de protecție comune statelor membre ale unei organizații internaționale regionale"[662].

În temeiul legislației UE, restricțiile sau interdicțiile privind libera circulație a datelor cu caracter personal între statele membre ale UE pentru motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal sunt interzise[663]. Zona fluxului gratuit de date a fost extinsă prin Acordul privind Spațiul Economic European (SEE)[664], în temeiul căruia Islanda, Liechtenstein și Norvegia au fost incluse în piața internă.

662 Convenția 108 modernizată, articolul 14 alineatul (1).

663 Regulamentul general privind protecția datelor, articolul 1 alineatul (3).

664 Decizia 94/1/CECO, CE a Consiliului și a Comisiei din 13 decembrie 1993 privind încheierea Acordului privind Spațiul Economic European între Comunitățile Europene, statele membre ale acestora și Republica Austria, Republica Finlanda, Republica Islanda, Principatul Liechtenstein, Regatul Norvegiei, Regatul Suediei și Confederația Elvețiană, JO 1994 L 1.

Exemplu: Dacă o societate afiliată unui grup internațional de societăți, având sedii în mai multe state membre, printre care Slovenia și Franța, transferă date cu caracter personal din Slovenia în Franța, fluxul de date respectiv nu trebuie să fie restricționat sau interzis de dreptul intern al Sloveniei pentru motive legate de protecția datelor cu caracter personal.

În schimb, dacă aceeași societate afiliată slovenă intenționează să transfere aceleași date cu caracter personal societății-mamă din Malaysia, atunci exportatorul de date sloven trebuie să țină seama de normele prevăzute la capitolul V din RGPD. Aceste dispoziții sunt menite să protejeze datele cu caracter personal ale persoanelor vizate care aparțin jurisdicției UE.

În conformitate cu legislația UE, fluxurile de date cu caracter personal către statele membre ale SEE în scopuri legate de prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale sunt reglementate de Directiva (UE) 2016/680[665]. Acest lucru garantează, de asemenea, că schimbul de date cu caracter personal de către autoritățile competente din cadrul Uniunii nu este restricționat sau interzis pentru motive legate de protecția datelor. În conformitate cu legislația CoE, prelucrarea tuturor datelor cu caracter personal (inclusiv fluxul transfrontalier al acestora către alte părți membre ale Convenției 108), fără excepții bazate pe scopurile sau sectoarele prelucrării, este inclusă în domeniul de aplicare al Convenției 108, deși părțile contractante pot să prevadă derogări. Toate statele membre ale SEE sunt, de asemenea, părți la Convenția 108.

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

7.3. Transferuri de date cu caracter personal către țări terțe/părți nemembre sau către organizații internaționale

Principalele elemente

- Atât **CoE**, cât și **EU** permit transferul datelor cu caracter personal către țări terțe sau organizații internaționale, sub rezerva îndeplinirii anumitor condiții de protecție a datelor cu caracter personal.
  - **În conformitate cu legislația CoE**, se poate asigura un nivel adecvat de protecție prin intermediul dispozițiilor juridice prevăzute de statul sau de organizația internațională în cauză sau prin aplicarea unor standarde adecvate.
  - **În conformitate cu legislația UE**, transferurile pot avea loc în cazul în care țara terță asigură un nivel adecvat de protecție sau dacă operatorul de date sau persoana împuternicită de acesta oferă garanții adecvate, inclusiv drepturi opozabile și căi de atac pentru persoanele vizate, prin intermediul unor clauze standard de protecție a datelor sau a unor reguli corporatiste obligatorii.
- **Atât legislația CoE, cât și a UE** prevăd clauze de derogare care permit transferul datelor cu caracter personal în anumite circumstanțe chiar dacă nu există nici un nivel adecvat de protecție, nici garanții adecvate.

Deși atât legislația CoE, cât și legislația UE permit fluxurile de date către țări terțe sau către organizații internaționale, cele două ordini juridice prevăd condiții diferite. Fiecare set de condiții ia în considerare structura și scopurile organizației în cauză.

În conformitate cu **legislația UE**, există, în principiu, două modalități de a permite transferul datelor cu caracter personal către țări terțe sau către organizații internaționale. Transferurile de date cu caracter personal pot avea loc pe baza unei decizii privind caracterul adecvat al nivelului de protecție adoptată de Comisia Europeană[666] sau, în lipsa unei astfel de decizii, în cazul în care operatorul sau persoana împuternicită de acesta oferă garanții adecvate, inclusiv drepturi opozabile și căi de atac eficiente pentru persoanele vizate[667]. În lipsa atât a unei decizii privind caracterul adecvat al nivelului de protecție, cât și a unor garanții adecvate, sunt disponibile o serie de derogări.

666 Regulamentul general privind protecția datelor, articolul 45.

667 *Ibidem*, articolul 46.

În conformitate cu legislația **CoE**, transferurile libere de date către părți nemembre ale convenției sunt permise numai pe baza:

- unei legi a statului sau a organizației internaționale în cauză, inclusiv tratate sau acorduri internaționale aplicabile, care asigură garanții adecvate;

- unor garanții standardizate sau ad hoc aprobate, furnizate prin instrumente juridice obligatorii și executorii, adoptate și puse în aplicare de persoanele implicate în transferul și prelucrarea ulterioară a datelor[668].

În mod similar cu legislația UE, în lipsa unui nivel adecvat de protecție a datelor, sunt disponibile o serie de derogări.

7.3.1. Transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecție

În temeiul dreptului UE, fluxul liber de date cu caracter personal către țări terțe cu un nivel adecvat de protecție a datelor este prevăzut la articolul 45 din RGPD. CJUE clarifică faptul că termenul „nivel adecvat de protecție" impune țării terțe să asigure un nivel de protecție a drepturilor și libertăților fundamentale „în esență echivalent"[669] cu garanțiile oferite prin lege în UE. În același timp, mijloacele la care o țară terță a recurs pentru a asigura un astfel de nivel de protecție pot fi diferite de cele puse în aplicare în cadrul UE; cu alte cuvinte, standardul privind nivelul adecvat de protecție nu impune o replică fidelă a normelor UE[670].

Comisia Europeană evaluează nivelul protecției datelor în țările străine analizând legislația națională și obligațiile internaționale aplicabile. Trebuie luată în considerare participarea unei țări la sisteme multilaterale sau regionale, în special în ceea ce privește protecția datelor cu caracter personal. În cazul în care Comisia Europeană constată că țara terță sau organizația internațională asigură un nivel adecvat de protecție, poate emite o decizie privind caracterul adecvat al nivelului de protecție,

668 Convenția 108 modernizată, articolul 14 alineatul (3) literele (a) și (b).

669 Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*, punctul 96.

670 *Ibidem*, punctul 74. Vezi, de asemenea, Comunicarea Comisiei către Parlamentul European și Consiliu intitulată „Schimbul de date cu caracter personal și protecția acestora într-o lume globalizată", COM(2017) 7 final din 10 ianuarie 2017, p. 6.

această decizie având caracter obligatoriu[671]. Cu toate acestea, CJUE a stabilit că autoritățile de supraveghere naționale au totuși competența de a examina cererea unei persoane referitoare la protecția datelor sale cu caracter personal care au fost transferate către o țară terță despre care Comisia a considerat că asigură un nivel adecvat de protecție, atunci când această persoană invocă faptul că dreptul și practicile în vigoare în țara terță menționată nu asigură un nivel de protecție adecvat[672].

Comisia Europeană poate, de asemenea, să evalueze caracterul adecvat al nivelului de protecție dintr-un teritoriu al unei țări terțe sau să limiteze decizia la sectoare specifice, cum a fost cazul legislației comerciale pentru sectorul privat din Canada, de exemplu[673]. Există, de asemenea, constatări privind caracterul adecvat al nivelului de protecție în cazul transferurilor efectuate în temeiul acordurilor dintre UE și țări terțe. Aceste decizii se referă exclusiv la un singur tip de transfer de date, precum transmiterea registrelor cu numele pasagerilor (PNR) deținute de companiile aeriene către autoritățile de control la frontierele străine, atunci când o companie aeriană efectuează zboruri din UE către anumite destinații transoceanice (vezi secțiunea 7.3.4).

Deciziile privind caracterul adecvat al nivelului de protecție fac obiectul unei monitorizări continue. Comisia Europeană revizuiește periodic aceste decizii pentru a urmări evoluțiile care le-ar putea afecta statutul. Astfel, dacă Comisia Europeană constată că țara terță sau organizația internațională nu mai îndeplinește condițiile care justifică decizia privind caracterul adecvat al nivelului de protecție, Comisia poate să modifice, să suspende sau să abroge decizia. Comisia poate, de asemenea, să inițieze negocieri cu țara terță sau cu organizația internațională în cauză pentru a remedia problema care stă la baza deciziei sale.

Deciziile privind caracterul adecvat al nivelului de protecție adoptate de Comisia Europeană în temeiul Directivei 95/46/CE rămân în vigoare până la modificarea, înlocuirea sau abrogarea lor printr-o decizie a Comisiei adoptată în conformitate cu normele prevăzute la articolul 45 din RGPD.

671 Pentru a vedea lista actualizată în mod constant a țărilor care au primit o constatare privind caracterul adecvat al nivelului de protecție, vezi pagina de start a Direcției Generale Justiție a Comisiei Europene.

672 Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*, punctele 63 și 65-66.

673 Decizia 2002/2/CE a Comisiei din 20 decembrie 2001 în conformitate cu Directiva 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției datelor cu caracter personal asigurat prin legea canadiană referitoare la protecția informațiilor cu caracter personal și documentele electronice (Personal Information Protection and Electronic Documents Act), JO 2002 L 2.

Până în prezent, Comisia Europeană a recunoscut Andorra, Argentina, Canada [organizațiile comerciale care intră sub incidența Legii referitoare la protecția informațiilor cu caracter personal și documentele electronice (*Personal Information and Electronic Documents Act*, PIPEDA)], Elveția, Insulele Feroe, Insula Guernsey, Insula Man, Israel, Jersey, Noua Zeelandă și Uruguay ca oferind un nivel adecvat de protecție. În ceea ce privește transferurile de date către SUA, Comisia Europeană a adoptat o decizie privind caracterul adecvat al nivelului de protecție în 2000, permițând transferuri către societăți din SUA care declaraseră pe propria răspundere că vor proteja datele cu caracter personal transferate din UE și vor respecta așa-numitele principii ale „sferei de siguranță"[674]. CJUE a anulat această decizie în 2015 și a adoptat o nouă decizie privind caracterul adecvat al nivelului de protecție în iulie 2016, permițând societăților să adere la acest regim începând cu 1 august 2016.

Exemplu: În cauza *Schrems*[675], Maximillian Schrems, cetățean austriac, era utilizator al platformei Facebook de câțiva ani. Unele dintre datele furnizate de domnul Schrems către Facebook – sau toate aceste date – au fost transferate de filiala irlandeză a Facebook către serverele din SUA, unde au fost prelucrate. Domnul Schrems a depus o plângere la autoritatea irlandeză pentru protecția datelor, susținând că, având în vedere dezvăluirile făcute de avertizorul Edward Snowden din SUA cu privire la activitățile de supraveghere ale serviciilor de informații din SUA, legislația și practica Statelor Unite nu oferă o protecție suficientă a datelor transferate în țara respectivă. Autoritatea irlandeză a respins plângerea, motivând că, în decizia din 26 iulie 2000, Comisia a considerat că, în cadrul regimului „sferei de siguranță", SUA asigură un nivel adecvat de protecție a datelor cu caracter personal transferate. Acțiunea a fost introdusă la Înalta Curte din Irlanda, care a trimis-o CJUE pentru o decizie preliminară.

CJUE a hotărât că decizia Comisiei privind caracterul adecvat al nivelului de protecție asigurat de regimul sferei de siguranță era nulă. În primul rând, CJUE a remarcat că decizia permitea limitarea aplicabilității principiilor de protecție a datelor în temeiul „sferei de siguranță" pe baza cerințelor privind

674 Decizia 2000/520/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță" privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al S.U.A., JO 2000 L 215. Decizia a fost anulată de CJUE [MC] prin Hotărârea pronunțată în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*.

675 Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*.

securitatea națională, interesul public sau respectarea legilor interne ale SUA. Prin urmare, decizia a permis ingerința în drepturile fundamentale ale persoanelor ale căror date fuseseră sau puteau fi transferate către SUA[676]. De asemenea, Curtea a constatat că decizia nu cuprinde nicio constatare în privința existenței în Statele Unite a unor norme destinate să limiteze astfel de ingerințe sau a unei protecții juridice eficiente împotriva unor astfel de ingerințe[677]. CJUE a subliniat că nivelul de protecție a drepturilor și libertăților fundamentale garantat în cadrul UE impune obligația ca o reglementare care implică o ingerință în drepturile fundamentale garantate la articolele 7 și 8 din Cartă să prevadă norme clare și precise care să reglementeze conținutul și aplicarea unei măsuri și care să impună o serie de cerințe minime, de derogări și de limitări privind protecția datelor cu caracter personal[678]. Având în vedere că decizia Comisiei nu a afirmat că Statele Unite asigură efectiv un astfel de nivel de protecție în temeiul legislației interne sau al angajamentelor lor internaționale, CJUE a concluzionat că decizia în cauză nu respectă cerințele dispoziției relevante privind transferul din Directiva privind protecția datelor și, prin urmare, este nulă[679].

Prin urmare, nivelul de protecție din SUA nu era „în esență echivalent" cu drepturile și libertățile fundamentale garantate de UE[680]. CJUE a susținut că au fost încălcate mai multe articole din Carta drepturilor fundamentale a UE. În primul rând, s-a adus atingere substanței articolului 7, deoarece reglementarea SUA în cauză „permite autorităților publice să acceadă în mod generalizat la conținutul comunicărilor electronice". În al doilea rând, s-a adus atingere, de asemenea, substanței articolului 47, întrucât reglementarea în cauză nu prevedea nicio posibilitate a justițiabililor de a exercita căi legale pentru a avea acces la datele cu caracter personal sau pentru a obține rectificarea sau ștergerea unor astfel de date. În sfârșit, întrucât regimul sferei de siguranță încălcase articolele menționate mai sus, datele cu caracter personal nu mai erau prelucrate în mod legal, ceea ce a condus la încălcarea articolului 8.

După ce CJUE a anulat regimul „sferei de siguranță", Comisia și SUA au convenit asupra unui nou cadru, „Scutul de confidențialitate UE-SUA". La 12 iulie 2016, Comisia

676 *Ibidem*, punctul 84.

677 *Ibidem*, punctele 88-89.

678 *Ibidem*, punctele 91-92.

679 *Ibidem*, punctele 96-97.

680 *Ibidem*, punctele 73-74 și 96.

a adoptat o decizie prin care a declarat că SUA asigură un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune către organizații din SUA în temeiul Scutului de confidențialitate UE-SUA[681].

În mod similar regimului sferei de siguranță, cadrul scutului de confidențialitate UE-SUA vizează protejarea datelor cu caracter personal transferate din UE în SUA în scopuri comerciale[682]. Societățile comerciale din SUA pot declara pe propria răspundere, în mod voluntar, că aderă la lista prevăzută de scutul de confidențialitate, angajându-se să respecte standardele de protecție a datelor din acest cadru. Autoritățile competente din SUA monitorizează și verifică respectarea acestor standarde de către societățile certificate.

În special, regimul scutului de confidențialitate prevede următoarele:

- obligații de protecție a datelor pentru societățile care primesc date cu caracter personal din UE;

- protecția și căile de atac disponibile persoanelor fizice, în special instituirea unui mecanism al Avocatului Poporului, care este independent de serviciile de informații din SUA și care examinează plângerile depuse de persoanele care consideră că datele lor cu caracter personal au fost folosite în mod ilegal de către autoritățile SUA din domeniul securității naționale;

- o evaluare anuală comună pentru a monitoriza punerea în aplicare a cadrului[683]; prima evaluare a avut loc în septembrie 2017[684].

---

681 Decizia de punere în aplicare (UE) 2016/1250 a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA, JO 2016 L 207. Grupul de lucru „Articolul 29" a salutat îmbunătățirile aduse de mecanismul „scutului de confidențialitate" în comparație cu decizia privind „sfera de siguranță" și a felicitat Comisia și autoritățile SUA pentru luarea în considerare în versiunea finală a documentelor aferente „scutului de confidențialitate" preocupările exprimate în avizul său WP 238 referitor la proiectul de decizie privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA. Grupul de lucru „Articolul 29" a subliniat totuși o serie de preocupări nesoluționate. Pentru mai multe detalii, vezi Avizul 1/2016 al Grupului de lucru „Articolul 29" referitor la proiectul de decizie privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA, adoptat la 13 aprilie 2016, 16/EN WP 238.

682 Pentru mai multe informații, vezi Fișa informativă privind Scutul de confidențialitate UE-SUA.

683 Pentru mai multe informații, vezi pagina web a Comisiei Europene dedicată Scutului de confidențialitate UE-SUA.

684 Comisia Europeană, Raport al Comisiei către Parlamentul European și Consiliu privind prima evaluare anuală privind funcționarea Scutului de confidențialitate UESUA, COM(2017) 611 final din 18 octombrie 2017. Vezi, de asemenea, Grupul de lucru „Articolul 29", *Scutul de confidențialitate UE-SUA – Prima evaluare anuală comună*, document adoptat la 28 noiembrie 2017, 17/EN WP 255.

Guvernul SUA a adoptat angajamente și asigurări scrise, care însoțesc decizia privind caracterul adecvat al protecției oferite de scutul de confidențialitate. Acestea prevăd limitări și garanții privind accesul guvernului SUA la datele cu caracter personal în scopuri legate de aplicarea legii și de securitatea națională.

7.3.2. Transferuri în temeiul unor garanții adecvate

Atât **legislația UE**, cât și **legislația CoE** recunosc garanțiile adecvate prevăzute între operatorul care exportă date și destinatarul din țara terță sau organizația internațională ca fiind un mijloc posibil de asigurare a unui nivel suficient de protecție a datelor la destinatar.

În conformitate cu **legislația UE**, transferurile de date cu caracter personal către o țară terță sau către o organizație internațională sunt permise dacă operatorul sau persoana împuternicită de operator oferă garanții adecvate și drepturi opozabile și dacă persoanelor vizate li se pun la dispoziție căi de atac eficiente[685]. Lista „garanțiilor adecvate" acceptabile este prevăzută exclusiv în legislația UE privind protecția datelor. Garanțiile adecvate pot fi stabilite prin următoarele:

- un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;
- reguli corporatiste obligatorii;
- clauze standard de protecție a datelor adoptate fie de Comisia Europeană, fie de o autoritate de supraveghere;
- coduri de conduită;
- mecanisme de certificare[686].

Clauzele contractuale personalizate între operator sau persoana împuternicită de operator din UE și destinatarul datelor din țara terță constituie un alt mijloc de asigurare a garanțiilor adecvate. Aceste clauze contractuale trebuie totuși să fie autorizate de autoritatea de supraveghere competentă înainte să poată fi invocate ca

685 Regulamentul general privind protecția datelor, articolul 46.

686 Regulamentul general privind protecția datelor, articolul 46 alineatul (1) literele (c) și (d) și alineatul (2) literele (a), (b), (e) și (f) și articolul 47.

instrument pentru transferul de date cu caracter personal. În mod similar, autoritățile publice pot utiliza dispozițiile privind protecția datelor incluse în acordurile administrative pe care le-au încheiat, cu condiția ca acestea să fi fost autorizate de autoritatea de supraveghere[687].

În conformitate cu legislația CoE, sunt permise fluxurile de date către un stat sau o organizație internațională care nu este parte la Convenția 108 modernizată, cu condiția să se asigure un nivel de protecție adecvat. Acest lucru se poate realiza:

- prin intermediul dispozițiilor juridice prevăzute de statul sau de organizația internațională în cauză; sau
- prin garanții ad hoc sau standardizate integrate într-un document obligatoriu din punct de vedere juridic[688].

Transferuri în temeiul unor clauze contractuale

Atât **legislația CoE**, cât și **legislația UE** recunosc clauzele contractuale prevăzute între operatorul care exportă date și destinatarul din țara terță ca fiind un mijloc posibil de asigurare a unui nivel suficient de protecție a datelor la destinatar[689].

La **nivelul UE**, Comisia Europeană, cu sprijinul Grupului de lucru „Articolul 29", a elaborat clauze contractuale standard privind protecția datelor, care au fost certificate oficial printr-o decizie a Comisiei ca dovadă a faptului că asigură un nivel adecvat de protecție a datelor[690]. Întrucât deciziile Comisiei sunt obligatorii în toate elementele lor pentru statele membre, autoritățile naționale care supraveghează transferurile de date trebuie să confirme aceste clauze contractuale standard în procedurile lor[691]. Astfel, dacă operatorul care exportă date și destinatarul din țara terță sunt de acord cu aceste clauze și le semnează, acest lucru trebuie să constituie, pentru autoritatea de supraveghere, o dovadă suficientă a faptului că se oferă garanții adecvate. Cu toate acestea, în cauza *Schrems*, CJUE a stabilit că Comisia Europeană nu are competența de a limita competențele autorităților naționale de supraveghere de a monitoriza transferul datelor cu caracter personal către o țară terță care face

687 *Ibidem*, articolul 46 alineatul (3).

688 Convenția 108 modernizată, articolul 14 alineatul (3) litera (b).

689 Regulamentul general privind protecția datelor, articolul 46 alineatul (3); Convenția 108 modernizată, articolul 14 alineatul (3) litera (b).

690 *Ibidem*, articolul 46 alineatul (2) litera (b) și articolul 46 alineatul (5).

691 *Ibidem*, articolul 46 alineatul (2) litera (c); Tratatul privind funcționarea Uniunii Europene, articolul 288.

obiectul unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție[692]. Astfel, autoritățile naționale de supraveghere nu sunt împiedicate să își exercite competențele, inclusiv competența de a suspenda sau interzice un transfer de date cu caracter personal atunci când transferul este efectuat cu încălcarea legislației UE sau a legislației naționale privind protecția datelor, cum ar fi, de exemplu, cazul în care importatorul datelor nu respectă clauzele contractuale standard[693].

Existența unor clauze standard de protecție a datelor în cadrul juridic al UE nu împiedică operatorii să formuleze alte clauze contractuale ad hoc, cu condiția ca acestea să fie aprobate de autoritatea de supraveghere[694]. Cu toate acestea, operatorii trebuie să asigure același nivel de protecție prevăzut de clauzele standard de protecție a datelor. Atunci când aprobă clauze ad hoc, autoritățile de supraveghere trebuie să aplice mecanismul pentru asigurarea coerenței, astfel încât să asigure o abordare consecventă a reglementării în întreaga UE[695]. Aceasta înseamnă că autoritatea de supraveghere competentă trebuie să comunice CEPD proiectul de decizie privind clauzele. CEPD emite un aviz cu privire la această chestiune, iar autoritatea de supraveghere trebuie să țină seama în cea mai mare măsură posibilă de acest aviz atunci când adoptă decizia. Dacă autoritatea intenționează să nu se conformeze avizului CEPD, se declanșează mecanismul de soluționare a litigiilor de către Comitet, acesta din urmă trebuind să adopte o decizie cu caracter obligatoriu[696].

Cele mai importante caracteristici ale unei clauze contractuale standard sunt:

- o clauză privind un beneficiar terț, care permite persoanelor vizate să își exercite drepturile contractuale, chiar dacă acestea nu sunt o parte contractantă;

- destinatarul sau importatorul datelor care, în caz de litigiu, este de acord să se supună procedurii desfășurate de autoritatea națională de supraveghere și/sau de instanțele în a căror jurisdicție se află operatorul care exportă datele.

692 Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*, punctele 96-98 și 102-105.

693 Pentru a ține seama de poziția CJUE în cauza *Schrems*, Comisia și-a modificat decizia privind clauzele contractuale standard. Decizia de punere în aplicare (UE) 2016/2297 a Comisiei din 16 decembrie 2016 de modificare a Deciziilor 2001/497/CE și 2010/87/UE privind clauzele contractuale standard pentru transferul de date cu caracter personal către țările terțe și către persoanele împuternicite de către operator stabilite în țări terțe, în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului, JO 2016 L 344.

694 Regulamentul general privind protecția datelor, articolul 46 alineatul (3) litera (a).

695 *Ibidem*, articolul 63 și articolul 64 alineatul (1) litera (e).

696 *Ibidem*, articolele 64 și 65.

În prezent, operatorul care exportă date are posibilitatea de a alege între două seturi de clauze standard pentru transferurile de la operator la operator[697]. Pentru transferurile de la operator la persoana împuternicită de operator există un singur set de clauze contractuale standard[698]. Cu toate acestea, clauzele contractuale standard menționate fac în prezent obiectul unor proceduri judiciare.

Exemplu: După ce CJUE a anulat Decizia privind sfera de siguranță[699], transferurile de date cu caracter personal către SUA nu s-au mai putut întemeia pe acea decizie privind caracterul adecvat al nivelului de protecție. În timp ce negocierile cu autoritățile SUA erau în curs de desfășurare și în așteptarea adoptării unei noi decizii privind caracterul adecvat al nivelului de protecție (adoptată în cele din urmă la 12 iulie 2016)[700], transferurile nu s-au putut efectua decât pe alte temeiuri juridice, cum ar fi clauzele contractuale standard sau regulile corporatiste obligatorii. Mai multe societăți, inclusiv Facebook Ireland (împotriva căreia a fost introdusă acțiunea care a condus la anularea Deciziei privind sfera de siguranță), au trecut la utilizarea clauzelor contractuale standard pentru a continua transferurile de date între UE și SUA.

Domnul Schrems a depus o plângere la autoritatea irlandeză de supraveghere, solicitându-i să suspende transferurile de date către SUA efectuate în temeiul clauzelor contractuale standard. În esență, el a susținut că, atunci când datele sale cu caracter personal sunt transferate de la filiala irlandeză a Facebook către Facebook Inc. și către serverele din SUA, nu există nicio garanție că datele vor fi protejate. Facebook Inc. intră sub incidența legilor SUA care o pot obliga să divulge date cu caracter personal autorităților de aplicare

697 Setul I este inclus în anexa la Decizia 2001/497/CE a Comisiei din 15 iunie 2001 privind clauzele contractuale standard pentru transferul de date cu caracter personal către țările terțe în temeiul Directivei 95/46/CE, JO 2001 L 181; setul II este inclus în anexa la Decizia 2004/915/CE a Comisiei din 27 decembrie 2004 de modificare a Deciziei 2001/497/CE privind introducerea unui set alternativ de clauze contractuale standard pentru transferul de date cu caracter personal către țări terțe, JO 2004 L 385.

698 Decizia 2010/87/UE a Comisiei din 5 februarie 2010 privind clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele împuternicite de către operatori stabilite în țări terțe în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului, JO 2010 L 39. La momentul redactării manualului, utilizarea clauzelor contractuale standard ca temei al transferurilor de date cu caracter personal către SUA făcea obiectul unei proceduri judiciare în fața Înaltei Curți a Irlandei.

699 Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*.

700 Decizia de punere în aplicare (UE) 2016/1250 a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA, JO 2016 L 207.

a legii din această țară, iar persoanele vizate din Europa nu dispun de nicio cale de atac prin care să conteste această practică[701]. Pentru aceste motive, CJUE a concluzionat că Decizia privind sfera de siguranță este nulă și, deși hotărârea Curții se limita la examinarea acestei decizii, reclamantul a considerat că problemele ridicate sunt la fel de pertinente atunci când transferul se întemeiază pe clauze contractuale. La momentul redactării prezentului manual, cauza era examinată în fața Înaltei Curți a Irlandei. Se pare că reclamantul intenționează să sesizeze CJUE, în fața căreia urmărește să conteste valabilitatea deciziei Comisiei Europene întemeiate pe clauze contractuale standard. Astfel cum s-a descris la capitolul 5, numai CJUE are competența de a declara nul un instrument al UE.

Transferuri în temeiul unor reguli corporatiste obligatorii

Dreptul UE permite, de asemenea, efectuarea transferurilor de date cu caracter personal în temeiul unor reguli corporatiste obligatorii în cazul transferurilor internaționale desfășurate în cadrul unui grup de întreprinderi sau între întreprinderi implicate într-o activitate economică comună[702]. Înainte ca un set de reguli corporatiste obligatorii să poată fi utilizat ca instrument de transfer al datelor cu caracter personal, aceste reguli trebuie să fie aprobate de autoritatea competentă de supraveghere în conformitate cu mecanismul pentru asigurarea coerenței.

Pentru a fi aprobate, regulile corporatiste obligatorii trebuie să fie obligatorii din punct de vedere juridic, să includă toate principiile esențiale în materie de protecție a datelor și să se aplice fiecărui membru vizat al grupului, precum și să fie puse în aplicare de membrii în cauză. Acestea trebuie să confere, în mod expres, drepturi opozabile persoanelor vizate, să includă toate principiile esențiale în materie de protecție a datelor și să îndeplinească anumite cerințe formale, de exemplu să descrie structura întreprinderii, transferurile și modul în care vor fi aplicate principiile în materie de protecție a datelor. Aici se include furnizarea acestor informații persoanelor vizate. Regulile corporatiste obligatorii trebuie să precizeze, printre altele, drepturile persoanelor vizate și dispozițiile privind răspunderea pentru orice încălcare a acestor reguli[703]. Atunci când se aprobă reguli corporatiste obligatorii

701 Pentru mai multe informații, vezi plângerea revizuită împotriva Facebook Ireland Ltd depusă la 1 decembrie 2015 de către Maximillian Schrems în fața comisarului însărcinat cu protecția datelor din Irlanda.

702 Regulamentul general privind protecția datelor, articolul 47.

703 Pentru o descriere mai detaliată, vezi Regulamentul general privind protecția datelor, articolul 47.

se declanșează mecanismul pentru asigurarea coerenței în cadrul cooperării dintre autoritățile de supraveghere (descris la capitolul 5).

În cadrul mecanismului pentru asigurarea coerenței, autoritatea principală de supraveghere revizuiește regulile corporatiste obligatorii propuse, adoptă un proiect de decizie și îl comunică CEPD. Comitetul emite un aviz cu privire la această chestiune, iar autoritatea principală de supraveghere poate aproba în mod oficial regulile corporatiste obligatorii, ținând seama „în cea mai mare măsură posibilă" de avizul comitetului. Avizul nu este obligatoriu din punct de vedere juridic; dacă autoritatea de supraveghere intenționează să nu i se conformeze, se declanșează mecanismul de soluționare a litigiilor și comitetul va trebui să adopte o decizie cu caracter obligatoriu din punct de vedere juridic cu o majoritate de două treimi dintre membrii săi[704].

În conformitate cu **legislația CoE**, regulile corporatiste obligatorii fac parte din categoria garanțiilor ad hoc sau standardizate care sunt integrate într-un document obligatoriu din punct de vedere juridic[705].

7.3.3. Derogări pentru situații specifice

În conformitate cu legislația UE, transferurile de date cu caracter personal către o țară terță pot fi justificate, chiar dacă nu există o decizie privind caracterul adecvat al nivelului de protecție sau garanții adecvate cum ar fi clauzele contractuale standard sau regulile corporatiste obligatorii, în oricare dintre următoarele situații:

- persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul de date;
- persoana vizată încheie sau se pregătește să încheie un contract pentru a cărui executare este necesar transferul datelor în străinătate;
- pentru încheierea unui contract între un operator de date și o parte terță, în interesul persoanei vizate;
- din considerente importante de interes public;

704 *Ibidem*, articolul 57 alineatul (1) litera (s), articolul 58 alineatul (1) litera (j), articolul 64 alineatul (1) litera (f), articolul 65 alineatele (1) și (2).

705 Convenția 108 modernizată, articolul 14 alineatul (3) litera (b).

- pentru stabilirea, exercitarea sau apărarea unui drept în instanță;
- pentru protejarea intereselor vitale ale persoanei vizate;
- în vederea transferului de date din registre publice (acesta este un exemplu în care prevalează interesele publicului larg de a avea acces la informațiile stocate în registrele publice)[706].

În cazul în care nu se aplică niciuna dintre aceste condiții și transferurile nu se pot întemeia pe o decizie privind caracterul adecvat al nivelului de protecție sau pe garanții adecvate, transferul poate avea loc numai dacă nu este repetitiv, se referă la un număr limitat de persoane vizate și este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează drepturile persoanei vizate[707]. În aceste cazuri, operatorul trebuie să evalueze circumstanțele aferente transferului și să prezinte garanții. De asemenea, operatorul trebuie să informeze autoritatea de supraveghere și persoanele vizate cu privire la transfer și la interesul legitim care îl justifică.

Faptul că derogările reprezintă o soluție de ultimă instanță pentru efectuarea unor transferuri legale[708] (care trebuie să fie utilizate numai în absența unei decizii privind caracterul adecvat al nivelului de protecție și dacă nu există alte garanții adecvate) subliniază caracterul lor excepțional, care este evidențiat și în considerentele RGPD[709]. Astfel, derogările sunt acceptate ca o posibilitate pentru efectuarea de „transferuri în anumite circumstanțe", pe bază de consimțământ, și în cazul în care „transferul este ocazional și necesar" în legătură cu un contract sau cu o acțiune în justiție[710].

În plus, potrivit orientărilor Grupului de lucru „Articolul 29", utilizarea unor derogări pentru situații specifice trebuie să fie excepțională, bazată pe cazuri individuale, și nu poate fi utilizată pentru transferuri masive sau repetitive[711]. Autoritatea Europeană

706 Regulamentul general privind protecția datelor, articolul 49.

707 *Ibidem*.

708 *Ibidem*, articolul 49 alineatul (1).

709 Vezi Regulamentul general privind protecția datelor, articolul 49 alineatul (1) literele (a), (b) și (e) și considerentul 113.

710 *Ibidem*, articolul 49 alineatul (1).

711 Documentul de lucru din 25 noiembrie 2005 al Grupului de lucru „Articolul 29" privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995, WP 114, Bruxelles, 25 noiembrie 2005.

pentru Protecția Datelor a subliniat, de asemenea, caracterul excepțional al derogărilor utilizate ca temei juridic pentru transferuri de date în temeiul Regulamentului (CE) nr. 45/2001, menționând că această soluție ar trebui utilizată „în cazuri limitate" și „pentru transferuri ocazionale"[712].

Exemplu: O societate care furnizează servicii în domeniul sistemelor de distribuție globală (GDS), cu sediul în SUA, furnizează un sistem de rezervări online pentru mai multe companii aeriene, hoteluri și nave de croazieră din întreaga lume, prelucrând datele a zeci de milioane de persoane din UE. Pentru transferul inițial al datelor către serverele din SUA, GDS utilizează ca temei juridic al transferurilor o derogare bazată pe necesitatea de a încheia un contract. Astfel, GDS nu oferă alte garanții pentru protecția datelor cu caracter personal originare din Europa, transferate în SUA și apoi redistribuite către hoteluri din întreaga lume (ceea ce înseamnă că nu există garanții nici pentru transferurile subsecvente). GDS nu respectă cerințele RGPD privind legalitatea transferurilor internaționale de date, deoarece utilizează o derogare ca temei juridic pentru transferuri masive.

Cu excepția cazului în care există o decizie privind caracterul adecvat al nivelului de protecție, UE sau statele sale membre sunt împuternicite să stabilească limite asupra transferului unor categorii specifice de date cu caracter personal către o țară terță din considerente importante de interes public, chiar dacă se îndeplinesc alte condiții care reglementează aceste transferuri. Aceste limite ar trebui să fie percepute ca fiind excepționale, iar statele membre trebuie să comunice Comisiei dispozițiile în cauză adoptate[713].

Legislația CoE permite transferurile de date către teritorii care nu garantează o protecție adecvată a datelor în cazurile în care:

- persoana vizată își dă consimțământul în acest sens;
- interesele persoanei vizate impun un astfel de transfer;

712 Documentul de poziție din 14 iulie 2014 al Autorității Europene pentru Protecția Datelor intitulat *The transfer of personal data to third countries and international organisations by EU institutions and bodies* (Transferul de date cu caracter personal către țări terțe și organizații internaționale de către instituțiile și organismele UE), Bruxelles, p. 15.

713 Regulamentul general privind protecția datelor, articolul 49 alineatul (5).

- există interese legitime predominante, în special interese publice majore, prevăzute de lege;

- transferul constituie o măsură necesară și proporțională într-o societate democratică[714].

7.3.4. Transferuri în temeiul acordurilor internaționale

UE poate încheia cu țări terțe acorduri internaționale care să reglementeze transferul datelor cu caracter personal în scopuri specifice. Aceste acorduri trebuie să includă garanții adecvate pentru a asigura protecția datelor cu caracter personal ale persoanelor vizate. RGPD nu aduce atingere acestor acorduri internaționale[715].

De asemenea, statele membre pot să încheie, cu țări terțe sau cu organizații internaționale, acorduri internaționale care asigură un nivel adecvat de protecție a drepturilor și libertăților fundamentale ale persoanelor, în măsura în care aceste acorduri nu afectează aplicarea RGPD.

Articolul 12 alineatul (3) litera (a) din Convenția 108 modernizată include o dispoziție similară.

Un exemplu de acorduri internaționale care implică transferul de date cu caracter personal îl reprezintă acordurile privind registrele cu numele pasagerilor (PNR).

Registre cu numele pasagerilor

Datele PNR sunt colectate de transportatorii aerieni pe parcursul procesului de rezervare și includ, printre altele, nume, adrese, detalii privind cărțile de credit și numerele locurilor pasagerilor transportului aerian. Transportatorii aerieni colectează, de asemenea, aceste informații pentru propriile scopuri comerciale. UE a încheiat acorduri cu anumite țări terțe (Australia, Canada și SUA) în ceea ce privește transferul datelor PNR pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor transnaționale grave. În plus, Uniunea a adoptat în 2016 Directiva (UE) 2016/861[716], cunoscută sub numele de

714 Convenția 108 modernizată, articolul 14 alineatul (4).

715 Regulamentul general privind protecția datelor, considerentul 102.

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

„Directiva UE privind PNR". Această directivă instituie un cadru juridic pe baza căruia statele membre ale UE pot transfera datele PNR către autoritățile competente din țări terțe în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor de terorism și a altor infracțiuni grave. Transferurile de date PNR către autoritățile din țări terțe se autorizează de la caz la caz, fac obiectul unei evaluări individuale a necesității transferului din perspectiva scopurilor specificate în directivă și sunt condiționate de respectarea drepturilor fundamentale.

În ceea ce privește acordurile PNR dintre UE și țările terțe, compatibilitatea acestora cu drepturile fundamentale la respectarea vieții private și la protecția datelor, consacrate de Carta drepturilor fundamentale a UE, a fost contestată. Atunci când, în urma negocierilor cu Canada, UE a semnat un acord privind transferul și prelucrarea datelor PNR în 2014, Parlamentul European a decis să sesizeze CJUE, solicitându-i să evalueze legalitatea acestui acord din perspectiva dreptului UE și în special a articolelor 7 și 8 din Cartă.

Exemplu: În avizul său privind legalitatea acordului PNR dintre UE și Canada[717], CJUE a stabilit că, în forma sa curentă, acordul preconizat era incompatibil cu drepturile fundamentale recunoscute de Cartă și, prin urmare, nu putea fi încheiat. Întrucât implica prelucrarea datelor cu caracter personal, acordul în cauză constituia o ingerință în dreptul la protecția datelor cu caracter personal protejat în temeiul articolului 8 din Cartă. În același timp, acordul reprezenta, de asemenea, o limitare a dreptului la respectarea vieții private, consacrat la articolul 7, întrucât datele PNR considerate în ansamblu pot fi agregate și analizate într-un mod care să dezvăluie obiceiuri de călătorie, relații între diferite persoane, informații despre situația lor financiară, obiceiuri alimentare și starea de sănătate, aducând astfel atingere vieții lor private.

Ingerința în drepturile fundamentale pe care o constituia acordul preconizat urmărea un obiectiv de interes general, și anume securitatea publică și combaterea terorismului și a altor infracțiuni transnaționale grave. CJUE a reamintit totuși că, pentru a fi justificată, ingerința trebuie să se limiteze la ceea ce este strict necesar pentru atingerea scopului urmărit. După analizarea dispozițiilor acordului preconizat, CJUE a concluzionat că acesta nu respecta criteriul „necesității stricte". Printre factorii luați în considerare de CJUE în analiza care a condus la această concluzie s-au numărat următorii:

717 CJUE, *Avizul 1/15 din 26 iulie 2017 al Curții* [MC].

- Faptul că acordul preconizat presupunea transferul de date sensibile. Datele PNR colectate în temeiul acordului preconizat puteau include date sensibile, cum ar fi informații care dezvăluie originea rasială sau etnică, convingerile religioase sau starea de sănătate a unui pasager. Transferul și prelucrarea datelor sensibile de către autoritățile canadiene puteau prezenta un risc pentru principiul nediscriminării și, prin urmare, necesitau o justificare precisă și solidă, întemeiată pe alte motive decât securitatea publică și combaterea infracțiunilor grave. Acordul preconizat nu oferea o astfel de justificare[718].

- S-a considerat, de asemenea, că stocarea datelor PNR ale tuturor pasagerilor pe o perioadă de cinci după ce aceștia părăseau Canada depășea limitele necesității stricte. CJUE a considerat că se poate admite ca autoritățile canadiene să păstreze datele pasagerilor despre care există dovezi obiective că ar putea prezenta o amenințare la adresa securității publice chiar și după ce aceștia părăsesc Canada. În schimb, stocarea datelor cu caracter personal ale *tuturor* pasagerilor, despre care nu există nici măcar probe indirecte că ar prezenta un risc pentru securitatea publică, nu este justificată[719].

Comitetul consultativ al Convenției 108 a emis un aviz cu privire la implicațiile acordurilor PNR asupra protecției datelor în temeiul legislației CoE[720].

Date de mesagerie

Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT) cu sediul în Belgia, care este persoana împuternicită de operator pentru majoritatea transferurilor financiare de la băncile europene la nivel mondial, colabora cu

718 *Ibidem*, punctul 165.

719 *Ibidem*, punctele 204-207.

720 Consiliul Europei, *Avizul din 19 august 2016 privind implicațiile prelucrării datelor din registrele cu numele pasagerilor asupra protecției datelor*, T-PD(2016)18rev.

un centru „în oglindă" în SUA și i s-a solicitat să divulge date Departamentului de Trezorerie al acestei țări în cadrul Programului de urmărire a finanțărilor în scopuri teroriste[721].

Din perspectiva UE, nu exista un temei juridic suficient pentru a divulga aceste date – în special date privind cetățeni ai UE – autorităților SUA pentru simplul motiv că unul dintre centrele SWIFT de prelucrare a datelor era localizat în această țară.

Un acord specific între UE și SUA, cunoscut sub numele de Acordul SWIFT, a fost încheiat în 2010, pentru a furniza temeiul juridic necesar și pentru a asigura standarde adecvate de protecție a datelor[722].

În conformitate cu acest acord, datele financiare stocate de SWIFT continuă să fie furnizate Departamentului de Trezorerie al SUA în scopul prevenirii, investigării, identificării sau urmăririi penale a actelor de terorism sau a finanțării acestora. Departamentul de Trezorerie al SUA poate solicita date financiare de la SWIFT, cu condiția ca cererea:

- să identifice datele financiare în modul cel mai clar posibil;
- să conțină justificarea clară a necesității datelor respective;
- să fie formulată cât mai precis pentru a reduce la minimum cantitatea de date solicitate;
- să nu solicite nicio dată privind Zona unică de plăți în euro (SEPA)[723].

721 Vezi, în acest context, Avizul 14/2011 din 13 iunie 2011 al Grupului de lucru „Articolul 29" privind aspecte de protecție a datelor legate de prevenirea spălării banilor și a finanțării terorismului, WP 186, Bruxelles; Avizul 10/2006 din 22 noiembrie 2006 al Grupului de lucru „Articolul 29" privind prelucrarea datelor cu caracter personal de către Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT), WP 128, Bruxelles; Decizia din 9 decembrie 2008 a Comisiei pentru protecția vieții private din Belgia (*Commission de la protection de la vie privée*), intitulată „Procedură de control și recomandare inițiată în legătură cu societatea SWIFT scrl".

722 Decizia 2010/412/UE a Consiliului din 13 iulie 2010 privind încheierea Acordului dintre Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțărilor în scopuri teroriste, JO 2010 L 195, pp. 3 și 4. Textul acordului este anexat la această decizie, JO 2010 L 195, pp. 5-14.

723 *Ibidem*, articolul 4 alineatul (2).

Europol trebuie să primească o copie a fiecărei cereri formulate de Departamentul de Trezorerie al SUA și să verifice conformitatea acesteia cu principiile Acordului SWIFT[724]. În cazul în care se confirmă conformitatea cu aceste principii, SWIFT trebuie să furnizeze datele financiare direct Departamentului de Trezorerie al SUA. Departamentul trebuie să stocheze datele financiare într-un mediu fizic sigur, din care acestea pot fi accesate exclusiv de analiștii care investighează actele de terorism sau finanțarea terorismului; datele financiare nu trebuie să fie interconectate cu nicio altă bază de date. În general, datele financiare primite de la SWIFT sunt șterse în termen de maximum cinci ani de la primirea acestora. Datele financiare relevante pentru anumite investigații sau urmăriri penale pot fi păstrate atât timp cât sunt necesare pentru operațiunile respective.

Departamentul de Trezorerie al SUA poate transfera informații extrase din datele primite de SWIFT către autorități specifice responsabile cu aplicarea legii, siguranța publică sau combaterea terorismului din interiorul sau din afara SUA exclusiv în scopul investigării, identificării, prevenirii sau urmăririi penale a actelor de terorism sau a finanțării acestora. În cazul în care transferul ulterior de date financiare se referă la un cetățean sau la un rezident al unui stat membru UE, orice comunicare de date către autoritățile unei țări terțe se face doar cu acordul prealabil al autorităților competente din statul membru în cauză. Se pot face excepții în cazul în care comunicarea datelor este esențială pentru prevenirea unei amenințări imediate și grave la adresa securității publice.

Supraveghetori independenți, inclusiv o persoană desemnată de Comisia Europeană, monitorizează respectarea principiilor Acordului SWIFT. Acești supraveghetori au posibilitatea de a revizui în timp real și retroactiv toate căutările efectuate cu privire la datele furnizate și de a solicita informații suplimentare pentru a justifica legătura acestor căutări cu terorismul, precum și autoritatea de a bloca orice căutare care pare să încalce garanțiile prevăzute de acord.

Persoanele vizate au dreptul de a obține confirmarea autorității competente pentru protecția datelor din UE că drepturile lor la protecția datelor cu caracter personal au fost respectate. De asemenea, persoanele vizate au dreptul la rectificarea, ștergerea sau blocarea accesului la datele lor colectate și stocate de Departamentul de Trezorerie al SUA în temeiul Acordului SWIFT. Cu toate acestea, dreptul de acces la date al persoanelor vizate poate fi supus unor restricții legale. Atunci când se refuză accesul,

724 Organismul comun de supraveghere al Europol a efectuat audituri asupra activităților Europol din acest domeniu.

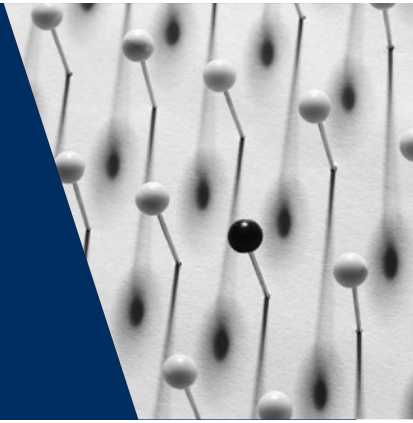
persoana vizată trebuie informată în scris cu privire la refuz și la dreptul său de a utiliza căile de atac administrative și juridice din SUA.

Acordul SWIFT rămâne in vigoare pentru o perioadă de cinci ani; prima perioadă de valabilitate a acestuia a durat până în luna august 2015. Acordul se prelungește automat cu perioade ulterioare de câte un an – cu un preaviz de cel puțin șase luni – cu excepția cazului în care una dintre părți notifică celeilalte intenția sa de a nu prelungi acordul. Prelungirea automată a fost aplicată în august 2015, 2016 și 2017, valabilitatea Acordului SWIFT fiind asigurată cel puțin până în august 2018[725].

725 *Ibidem*, articolul 23 alineatul (2).

8

Protecția datelor în sectorul polițienesc și al justiției penale



UE	Aspecte vizate	CoE
Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale	**Generalități**	Convenția 108 modernizată
	Autorități polițienești	Recomandarea privind sectorul polițienesc Ghid practic privind utilizarea datelor cu caracter personal în sectorul polițienesc
	Supraveghere	Hotărârea CEDO în cauza *B.B./Franța*, nr. 5335/06, 2009 Hotărârea CEDO [MC] în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04, 2008 Hotărârea CEDO în cauza *Allan/Regatul Unit*, nr. 48539/99, 2002 Hotărârea CEDO în cauza *Malone/Regatul Unit*, nr. 8691/79, 1984 Hotărârea CEDO în cauza *Klass și alții/Germania*, nr. 5029/71, 1978 Hotărârea CEDO în cauza *Szabó și Vissy/Ungaria*, nr. 37138/14, 2016 Hotărârea CEDO în cauza *Vetter/Franța*, nr. 59842/00, 2005

UE	Aspecte vizate	CoE
	Criminalitatea informatică	Convenția privind criminalitatea informatică
Alte instrumente juridice specifice		
Decizia Prüm	**Pentru date speciale: amprente digitale, ADN, huliganism, informații despre pasagerii transportului aerian, date despre telecomunicații etc.**	Convenția 108 modernizată, articolul 6 Recomandarea privind sectorul polițienesc, Ghid practic privind utilizarea datelor cu caracter personal în sectorul polițienesc
Inițiativa suedeză (Decizia-cadru 2006/960/JAI a Consiliului)	**Simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii**	Hotărârea CEDO [MC] în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04, 2008
Directiva (UE) 2016/681 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave Hotărârea CJUE [MC] în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland și Kärntner Landesregierung și alții*, 2014 Hotărârea CJUE [MC] în cauzele conexate C-203/15 și C-698/15, *Tele2 Sverige* și *Home Department/Tom Watson și alții*, 2016	**Păstrarea datelor cu caracter personal**	Hotărârea CEDO în cauza *B.B./Franța*, nr. 5335/06, 2009
Regulamentul Europol Decizia Eurojust	**De către agenții speciale**	Recomandarea privind sectorul polițienesc
Decizia Schengen II Regulamentul VIS Regulamentul privind Eurodac Decizia CIS	**Prin sisteme de informații comune speciale**	Recomandarea privind sectorul polițienesc Hotărârea CEDO în cauza *Dalea/Franța*, nr. 964/07, 2010

CoE și UE au adoptat instrumente juridice specifice pentru a stabili un echilibru între interesele persoanelor fizice în ceea ce privește protecția datelor și interesele societății în ceea ce privește colectarea de date pentru combaterea criminalității și asigurarea siguranței publice și naționale. Prezenta secțiune oferă o imagine de ansamblu asupra legislației CoE (secțiunea 8.1) și a legislației UE (secțiunea 8.2) în ceea ce privește protecția datelor în sectorul polițienesc și al justiției penale.

8.1. Legislația CoE privind protecția datelor în contextul securității naționale, al sectorului polițienesc și al justiției penale

Principalele elemente

- Convenția 108 modernizată și Recomandarea CoE privind sectorul polițienesc tratează protecția datelor în toate domeniile de activitate ale poliției.
- Convenția privind criminalitatea informatică (Convenția de la Budapesta) este un instrument juridic internațional cu caracter obligatoriu care tratează infracțiunile comise împotriva și prin intermediul rețelelor electronice. Este, de asemenea, relevantă pentru investigarea infracțiunilor fără caracter informatic care implică dovezi electronice.

O diferență importantă între legislația CoE și a UE este faptul că **legislația CoE**, spre deosebire de legislația UE, se aplică și în domeniul securității naționale. Aceasta înseamnă că părțile contractante trebuie să rămână în sfera de aplicare a articolului 8 din Convenția europeană a drepturilor omului chiar și în ceea ce privește activitățile legate de securitatea națională. Mai multe hotărâri ale CEDO au ca obiect activitățile statului în domeniile sensibile ale legislației și practicii în materie de securitate națională[726].

În ceea ce privește sectorul polițienesc și al justiției penale, Convenția 108 modernizată se aplică, la nivel european, tuturor domeniilor implicate în protecția datelor, iar dispozițiile acesteia vizează reglementarea prelucrării datelor cu caracter personal în general. În consecință, Convenția 108 modernizată se aplică protecției

726 Vezi, de exemplu, Hotărârea CEDO din 6 septembrie 1978 în cauza *Klass și alții/Germania*, nr. 5029/71; Hotărârea CEDO [MC] din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95; și Hotărârea CEDO din 12 ianuarie 2016 în cauza *Szabó și Vissy/Ungaria*, nr. 37138/14.

datelor în domeniul polițienesc și al justiției penale. Prelucrarea datelor genetice, a datelor cu caracter personal referitoare la infracțiuni, proceduri și condamnări penale și orice măsuri de securitate conexe, a datelor biometrice care identifică în mod unic o persoană, precum și a oricăror date cu caracter personal sensibile este permisă numai atunci când există garanții adecvate împotriva riscurilor pe care le poate prezenta prelucrarea acestor date pentru interesele, drepturile și libertățile fundamentale ale persoanei vizate, în special împotriva riscului de discriminare[727].

Sarcinile juridice ale autorităților polițienești și ale autorităților judiciare penale necesită adesea prelucrarea datelor cu caracter personal, care poate avea consecințe grave asupra persoanelor în cauză. Recomandarea privind sectorul polițienesc adoptată de CoE în 1987 oferă orientări statelor membre ale CoE cu privire la modul în care ar trebui să pună în aplicare principiile Convenției 108 în contextul prelucrării datelor cu caracter personal de către autoritățile polițienești[728]. Recomandarea a fost completată de un ghid practic privind utilizarea datelor cu caracter personal în sectorul polițienesc, adoptat de Comitetul consultativ al Convenției 108[729].

Exemplu: În cauza *D.L./Bulgaria*[730], direcția de servicii sociale l-a plasat pe reclamant într-o instituție de învățământ de corecție în temeiul unei hotărâri judecătorești. Întreaga corespondență scrisă și convorbirile telefonice ale acestuia au făcut obiectul unei supravegheri generalizate și nediferențiate de către instituția respectivă. CEDO a considerat că s-a încălcat articolul 8, deoarece măsura în cauză nu era necesară într-o societate democratică. Curtea a subliniat că trebuie depuse toate eforturile pentru a permite minorilor plasați într-o instituție să aibă suficient contact cu lumea exterioară, întrucât acest lucru face parte integrantă din dreptul lor de a fi tratați cu demnitate și este absolut esențial pentru pregătirea reintegrării lor în societate. Acest lucru este valabil atât în cazul vizitelor, cât și al corespondenței scrise sau al conversațiilor telefonice. Mai mult, supravegherea nu a făcut nicio distincție între comunicarea cu membrii familiei, respectiv cu ONG-urile care reprezintă drepturile copiilor sau cu avocații. În plus, decizia de a intercepta comunicările nu s-a bazat pe o analiză individualizată a riscurilor în fiecare caz în parte.

727 Convenția 108 modernizată, articolul 6.

728 *Recomandarea Rec(87)15 din 17 septembrie 1987 a Comitetului de Miniștri al Consiliului Europei către statele membre privind reglementarea utilizării datelor cu caracter personal în sectorul polițienesc.*

729 Consiliul Europei, Comitetul consultativ al Convenției 108, Ghid practic privind utilizarea datelor cu caracter personal în sectorul polițienesc, T-PD(2018)1.

730 Hotărârea CEDO din 19 mai 2016 în cauza *D.L./Bulgaria*, nr. 7472/14.

Exemplu: În cauza *Dragojević/Croația*[731], reclamantul a fost suspectat că era implicat în traficul de droguri. A fost găsit vinovat de această faptă după ce un judecător de instrucție a autorizat utilizarea măsurilor de supraveghere în secret pentru a intercepta apelurile telefonice ale reclamantului. CEDO a considerat că această măsură, împotriva căreia s-a formulat o plângere, constituia o ingerință în dreptul la respectarea vieții private și a corespondenței. Autorizația acordată de judecătorul de instrucție se baza doar pe declarația autorității de urmărire penală potrivit căreia „ancheta nu se putea desfășura prin alte mijloace". CEDO a constatat, de asemenea, că instanțele penale își limitaseră evaluarea în ceea ce privește utilizarea măsurilor de supraveghere și că guvernul nu a prezentat căile de atac disponibile. Prin urmare, s-a încălcat articolul 8.

8.1.1. Recomandarea privind sectorul polițienesc

CEDO a susținut în permanență că stocarea și păstrarea datelor cu caracter personal de către autoritățile din sectorul polițienesc sau al securității naționale aduc atingere articolului 8 alineatul (1) din Convenția europeană a drepturilor omului. Multe hotărâri ale CEDO tratează motivarea unor astfel de intervenții asupra drepturilor[732].

Exemplu: În cauza *B.B./Franța*[733], reclamantul a fost condamnat pentru că a comis infracțiuni sexuale împotriva unor minori în vârstă de 15 ani în calitate de persoană aflată într-o poziție de încredere. Reclamantul și-a ispășit pedeapsa cu închisoarea în anul 2000. Un an mai târziu, a solicitat ca menționarea acestei sentințe să fie eliminată din cazierul său judiciar, dar cererea i-a fost respinsă. În 2004, o lege franceză a instituit o bază națională de date judiciare cu infractorii sexuali, iar reclamantul a fost informat despre includerea sa în aceasta. CEDO a stabilit că introducerea unui infractor sexual condamnat într-o bază națională de date judiciare intră sub incidența articolului 8 din Convenția europeană a drepturilor omului. Cu toate acestea, având în vedere că au fost aplicate suficiente garanții de protecție a datelor, cum ar fi dreptul persoanei vizate de a solicita ștergerea datelor, durata limitată de păstrare a datelor și accesul restricționat la datele respective, s-a stabilit

731 Hotărârea CEDO din 15 ianuarie 2015 în cauza *Dragojević/Croația*, nr. 68955/11.

732 Vezi, de exemplu, Hotărârea CEDO din 26 martie 1987 în cauza *Leander/Suedia*, nr. 9248/81; Hotărârea CEDO din 13 noiembrie 2012 în cauza *M.M./Regatul Unit*, nr. 24029/07; Hotărârea CEDO din 22 iunie 2017 în cauza *Aycaguer/Franța*, nr. 8806/12.

733 Hotărârea CEDO din 17 decembrie 2009 în cauza *B.B./Franța*, nr. 5335/06.

un echilibru corect între interesele private și publice concurente implicate. Curtea a concluzionat că nu a existat nicio încălcare a articolului 8 din Convenția europeană a drepturilor omului.

Exemplu: În cauza *S. și Marper/Regatul Unit*[734], cei doi reclamanți au fost acuzați de comiterea unor infracțiuni, dar nu au fost condamnați. Cu toate acestea, amprentele, probele celulare și profilurile ADN ale acestora au fost păstrate și stocate de către poliție. Păstrarea pe termen nelimitat a datelor biometrice menționate era permisă prin lege în cazul în care o persoană era suspectată de comiterea unei infracțiuni, chiar dacă ulterior suspectul era achitat sau exonerat. CEDO a constatat că păstrarea generală și nediferențiată a datelor cu caracter personal care nu a fost limitată în timp și în cazul căreia persoanele achitate aveau doar posibilități limitate de a solicita ștergerea datelor a constituit o ingerință disproporționată în dreptul reclamanților de respectare a vieții private. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Un aspect crucial al comunicațiilor electronice este ingerința autorităților publice în drepturile la respectarea vieții private și la protecția datelor. Mijloacele de supraveghere sau de interceptare a comunicațiilor, cum ar fi dispozitivele de ascultare sau de înregistrare, sunt permise numai dacă acest lucru este prevăzut de lege și dacă constituie o măsură necesară într-o societate democratică în interesul următoarelor:

- apărarea securității statului;
- sănătatea publică;
- interesele financiare ale statului;
- combaterea infracțiunilor;
- protecția persoanei vizate sau a drepturilor și libertăților altor persoane.

Multe hotărâri ulterioare ale CEDO tratează motivarea ingerinței în dreptul la respectarea vieții private reprezentate de operațiunile de supraveghere.

734 Hotărârea CEDO din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04, punctele 119 și 125.

Exemplu: În cauza *Allan/Regatul Unit*[735], conversațiile private ale unui deținut cu un prieten în zona de vizită a penitenciarului și conversațiile cu un alt deținut într-o celulă au fost înregistrate în secret de către autorități. CEDO a constatat că utilizarea de dispozitive de înregistrare audio și video în celula reclamantului, în zona de vizită a penitenciarului și în apropierea unui alt deținut a adus atingere dreptului reclamantului la respectarea vieții private. Întrucât, la momentul respectiv, nu exista niciun sistem legal de reglementare a utilizării de către poliție a dispozitivelor de înregistrare secrete, ingerința respectivă nu a fost în conformitate cu legea. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Exemplu: În cauza *Roman Zakharov/Rusia*[736], reclamantul a introdus o acțiune judiciară împotriva a trei operatori de rețele mobile. Acesta a susținut că dreptul său la confidențialitatea comunicațiilor telefonice a fost încălcat, deoarece operatorii instalaseră echipamente care permiteau serviciului federal de securitate să îi intercepteze comunicațiile telefonice fără autorizare judiciară prealabilă. CEDO a constatat că dispozițiile legale interne care reglementează interceptarea comunicațiilor nu oferă garanții adecvate și eficiente împotriva caracterului arbitrar și a riscului de abuzuri. În special, legislația internă nu impune ștergerea datelor stocate odată ce s-a realizat obiectivul stocării. În plus, deși era necesară autorizarea judiciară, controlul judiciar a fost limitat.

Exemplu: În cauza *Szabó și Vissy/Ungaria*[737], reclamanții au susținut că legislația maghiară încălca articolul 8 din Convenția europeană a drepturilor omului, întrucât nu era suficient de detaliată sau de precisă. Mai mult, s-a susținut că legislația în cauză nu oferă suficiente garanții împotriva abuzurilor și a caracterului arbitrar. CEDO a constatat că legislația maghiară nu impune ca supravegherea să facă obiectul autorizării de către o instanță. Cu toate acestea, Curtea a constatat că, deși făcea obiectul aprobării de către ministrul justiției, această supraveghere a fost eminamente politică, neputând trece testul obligatoriu al „necesității stricte". În plus, legislația națională nu prevedea o cale de atac judiciară, întrucât subiecții supravegherii nu primeau nicio notificare. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

735 Hotărârea CEDO din 5 noiembrie 2002 în cauza *Allan/Regatul Unit*, nr. 48539/99.

736 Hotărârea CEDO [MC] din 4 decembrie 2015 în cauza *Roman Zakharov/Rusia*, nr. 47143/06.

737 Hotărârea CEDO din 12 ianuarie 2016 în cauza *Szabó și Vissy/Ungaria*, nr. 37138/14.

Având în vedere că prelucrarea datelor de către autoritățile polițienești poate avea un impact semnificativ asupra persoanelor în cauză, sunt deosebit de necesare norme detaliate de protecție a datelor în ceea ce privește prelucrarea datelor cu caracter personal în acest domeniu. Recomandarea CoE privind sectorul polițienesc a vizat abordarea problemei, oferind orientări cu privire la modul de colectare a datelor cu caracter personal în cadrul activității polițienești, modul de păstrare a fișierelor de date din domeniu, persoanele cărora trebuie să li se permită accesul la aceste fișiere, inclusiv condițiile pentru transferul de date cu caracter personal către autoritățile polițienești străine, modul în care persoanele vizate ar trebui să își poată exercita drepturile la protecția datelor, precum și modul în care autoritățile independente ar trebui să își exercite controlul. De asemenea, a fost luată în considerare obligația de a asigura o securitate adecvată a datelor.

Recomandarea nu prevede colectarea nediferențiată, pe termen nedeterminat a datelor de către autoritățile polițienești. Aceasta limitează colectarea datelor cu caracter personal de către autoritățile polițienești la minimul necesar pentru prevenirea unui pericol real sau pentru urmărirea penală unei infracțiuni specifice. Orice colectare suplimentară de date trebuie să se întemeieze pe legislația națională specifică. Prelucrarea datelor sensibile trebuie să se limiteze la ceea ce este absolut necesar în cadrul unei anumite anchete.

În cazul în care datele cu caracter personal sunt colectate fără știința persoanei vizate, aceasta trebuie să fie informată cu privire la colectarea datelor imediat ce divulgarea acestui fapt nu mai periclitează ancheta. Colectarea de date prin supraveghere tehnică sau prin alte mijloace automatizate ar trebui, de asemenea, să aibă un temei juridic specific.

Exemplu: În cauza *Versini-Campinchi și Crasnianski/Franța*[738], reclamanta, de profesie avocat, a avut o convorbire telefonică cu un client a cărui linie telefonică era interceptată la cererea unui judecător de instrucție. Transcrierea conversației a arătat că reclamanta a dezvăluit informații care fac obiectul secretului profesional al avocatului. Procurorul a transmis aceste informații Consiliului Baroului, care a impus reclamantei o sancțiune. CEDO a recunoscut existența unei ingerințe în dreptul la respectarea vieții private și a corespondenței, nu numai al persoanei al cărui telefon a fost ascultat, ci și al reclamantei, a cărei comunicare fusese interceptată și transcrisă. Ingerința s-a produs

738 Hotărârea CEDO din 16 iunie 2016 în cauza *Versini-Campinchi și Crasnianski/Franța*, nr. 49176/11.

în conformitate cu legea și a urmărit scopul legitim al prevenirii dezordinii. Reclamanta a obținut reexaminarea legalității transmiterii transcrierii înregistrărilor telefonice în cadrul procedurii disciplinare introduse împotriva ei. Deși reclamanta nu a avut posibilitatea de a solicita anularea transcrierii conversației telefonice, CEDO a considerat că existase un control eficient capabil să limiteze ingerința contestată la ceea ce era necesar într-o societate democratică. CEDO a considerat că argumentul potrivit căruia posibilitatea de a introduce o procedură penală împotriva unui avocat pe baza transcrierii ar putea avea un efect de descurajare asupra libertății de comunicare între un avocat și clientul său și, prin urmare, ar aduce atingere dreptului la apărare al acestuia din urmă nu era credibil în cazul în care divulgarea făcută de avocatul însuși putea să constituie un comportament ilegal din partea sa. În consecință, nu a fost constatată nicio încălcare a articolului 8.

Recomandarea CoE privind sectorul polițienesc prevede că, atunci când se stochează date cu caracter personal, trebuie să se facă o distincție clară între: datele administrative și datele deținute de poliție; datele cu caracter personal ale diferitelor categorii de persoane vizate, cum ar fi suspecți, persoane condamnate, victime și martori; și datele considerate a fi elemente concrete și datele bazate pe suspiciuni sau speculații.

Scopul pentru care pot fi utilizate datele deținute de poliție trebuie să fie limitat cu strictețe. Acest lucru are consecințe asupra divulgării datelor deținute de poliție către terți: transferul sau divulgarea acestor date în cadrul sectorului polițienesc ar trebui reglementate în funcție de existența sau lipsa unui interes legitim de comunicare a informațiilor. Transferul sau divulgarea acestor date în afara sectorului polițienesc ar trebui permise doar în cazul în care există o obligație sau o autorizație legală clară în acest sens.

Exemplu: În cauza *Karabeyoğlu/Turcia*[739], reclamantului, de profesie judecător, i-au fost monitorizate liniile telefonice în contextul unei anchete penale privind o organizație ilegală din care era suspectat că ar face parte sau căreia se suspecta că i-ar oferi asistență și sprijin. Ca urmare a deciziei de neîncepere a urmăririi penale, procurorul însărcinat cu ancheta penală a distrus înregistrările în cauză. Cu toate acestea, o copie a rămas în posesia anchetatorilor judiciari, care au folosit materialele în cauză în cadrul unei anchete

739 Hotărârea CEDO din 7 iunie 2016 în cauza *Karabeyoğlu/Turcia*, nr. 30083/10.

disciplinare împotriva reclamantului. CEDO a constatat că s-a încălcat legislația relevantă, deoarece informațiile au fost utilizate în alte scopuri decât cele pentru care fuseseră colectate și nu au fost distruse într-un termen legal. Ingerința în dreptul reclamantului la respectarea vieții private nu se produsese în conformitate cu legea în ceea ce privește procedura disciplinară inițiată împotriva sa.

Transferul sau divulgarea la nivel internațional ar trebui să se limiteze la autoritățile polițienești străine și să se întemeieze pe dispoziții legale speciale, inclusiv pe acorduri internaționale, cu excepția cazului în care sunt necesare pentru prevenirea unui pericol grav și iminent.

Prelucrarea datelor de către autoritățile polițienești trebuie să facă obiectul unei supravegheri independente în vederea asigurării conformității cu legislația națională privind protecția datelor. Persoanele vizate trebuie să aibă toate drepturile de acces prevăzute de Convenția 108 modernizată. În cazul în care drepturile de acces ale persoanelor vizate au fost restrânse în conformitate cu articolul 9 din Convenția 108 în interesul unor investigații polițienești eficiente și în vederea executării sancțiunilor penale, persoana vizată trebuie să aibă dreptul, în temeiul legislației naționale, să se adreseze autorității naționale de supraveghere a protecției datelor sau altui organism independent.

8.1.2. Convenția de la Budapesta privind criminalitatea informatică

Întrucât activitățile infracționale utilizează și afectează din ce în ce mai mult sistemele electronice de prelucrare a datelor, sunt necesare noi prevederi penale pentru a face față acestei provocări. Prin urmare, CoE a adoptat un instrument juridic internațional, Convenția privind criminalitatea informatică – cunoscută, de asemenea, drept Convenția de la Budapesta – pentru a aborda problema infracțiunilor comise împotriva și prin intermediul rețelelor electronice[740]. Această convenție este, de asemenea, deschisă pentru aderarea unor părți care nu sunt membre ale CoE. La

740 Comitetul de Miniștri al Consiliului Europei (2001), Convenția privind criminalitatea informatică, CETS nr. 185, Budapesta, 23 noiembrie 2001, intrat în vigoare la 1 iulie 2004.

începutul anului 2018, 14 state din afara CoE erau părți la convenție[741] și alte șapte părți nemembre fuseseră invitate să adere la aceasta.

Convenția privind criminalitatea informatică rămâne tratatul internațional cel mai influent care tratează încălcarea legii prin utilizarea internetului sau a altor rețele de informații. Aceasta impune părților actualizarea și armonizarea legislației lor penale împotriva pirateriei informatice și altor încălcări ale securității, inclusiv încălcarea drepturilor de autor, frauda facilitată prin computer, pornografia infantilă și alte activități informatice ilicite. Convenția prevede, de asemenea, competențe procedurale care vizează căutarea în rețelele informatice și interceptarea comunicațiilor în contextul combaterii criminalității informatice. În sfârșit, aceasta permite o cooperare internațională eficientă. Protocolul adițional la convenție are ca obiect incriminarea propagandei de natură rasistă și xenofobă desfășurate prin intermediul sistemelor informatice.

Deși convenția nu este un instrument care să vizeze promovarea protecției datelor, aceasta incriminează activitățile susceptibile de a încălca dreptul unei persoane vizate la protecția datelor care o privesc. Mai mult, aceasta solicită părților contractante să adopte măsuri legislative care să le permită autorităților naționale să intercepteze metadatele și datele privind conținutul[742]. De asemenea, prin punerea în aplicare a convenției, părțile contractante sunt obligate să prevadă un nivel adecvat de protecție a drepturilor și libertăților omului, inclusiv a drepturilor garantate prin Convenția europeană a drepturilor omului, cum ar fi dreptul la protecția datelor[743]. Părțile contractante nu sunt obligate să adere la Convenția 108 pentru a adera la Convenția de la Budapesta privind criminalitatea informatică.

741 Australia, Canada, Chile, Columbia, Republica Dominicană, Israel, Japonia, Mauritius, Panama, Senegal, Sri Lanka, Tonga, Tunisia și Statele Unite. Vezi Situația semnăturilor și a ratificărilor Tratatului 185, în iulie 2017.

742 Comitetul de Miniștri al Consiliului Europei, Convenția privind criminalitatea informatică, CETS nr. 185, Budapesta, 23 noiembrie 2001, articolele 20 și 21.

743 *Ibidem*, articolul 15 alineatul (1).

8.2. Legislația UE privind protecția datelor în sectorul polițienesc și al justiției penale

Principalele elemente

- În cadrul UE, protecția datelor în sectorul polițienesc și al justiției penale este reglementată atât în contextul prelucrării naționale, cât și în cel al prelucrării transfrontaliere de către autoritățile polițienești și autoritățile de justiție penală ale statelor membre și ale actorilor UE.
- La nivelul statelor membre, Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale trebuie să fie integrată în legislația națională.
- Instrumentele juridice specifice reglementează protecția datelor în cadrul cooperării transfrontaliere în domeniul aplicării legii, în special în combaterea terorismului și a criminalității transfrontaliere.
- Există norme speciale de protecție a datelor pentru Oficiul European de Poliție (Europol) și Unitatea Europeană de Cooperare Judiciară (Eurojust), precum și pentru nou-înființatul Parchet European, organisme ale UE care sprijină și promovează aplicarea legii la nivel transfrontalier.
- Există, de asemenea, norme speciale de protecție a datelor pentru sistemele comune de informații instituite la nivelul UE pentru schimburile transfrontaliere de informații între autoritățile polițienești și judiciare competente. Exemple importante sunt Sistemul de informații Schengen de a doua generație (SIS II), Sistemul de informații privind vizele (VIS) și Eurodac, un sistem centralizat care conține datele dactiloscopice ale resortisanților țărilor terțe și ale apatrizilor care solicită azil într-unul dintre statele membre ale UE.
- UE se află în proces de actualizare a dispozițiilor privind protecția datelor prezentate mai sus, astfel încât acestea să fie în conformitate cu dispozițiile Directivei privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale.

8.2.1. Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale

Directiva (UE) 2016/680 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării

pedepselor și privind libera circulație a acestor date[744] (Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale) vizează protejarea datelor cu caracter personal colectate și prelucrate în următoarele scopuri legate de justiția penală:

- prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;

- executarea unei sancțiuni penale;

- în cazurile în care poliția sau alte autorități de aplicare a legii acționează pentru a respecta legea, pentru a proteja împotriva amenințărilor la adresa siguranței publice și a drepturilor fundamentale ale societății și pentru a preveni aceste amenințări, care ar putea constitui infracțiuni.

Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale protejează datele cu caracter personal ale diferitelor categorii de persoane implicate în procedurile penale, cum ar fi martorii, informatorii, victimele, suspecții și complicii. Autoritățile polițienești și autoritățile judiciare penale au obligația de a respecta dispozițiile directivei ori de câte ori prelucrează astfel de date cu caracter personal în scopul aplicării legii, atât în cadrul domeniului de aplicare personal, cât și al celui material al directivei[745].

Cu toate acestea, utilizarea datelor în alte scopuri este permisă în anumite condiții. Prelucrarea datelor pentru un scop de aplicare a legii diferit de cel pentru care au fost colectate este permisă numai dacă este legală, necesară și proporțională, în conformitate cu dreptul Uniunii sau cu dreptul intern[746]. Pentru alte scopuri, se aplică normele din Regulamentul general privind protecția datelor. Înregistrarea și documentarea transferurilor de date reprezintă o obligație specifică a autorităților competente, menită să contribuie la clarificarea răspunderii în cazul depunerii unor plângeri.

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

745 Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale, articolul 2 alineatul (1).

746 *Ibidem*, articolul 4 alineatul (2).

Autoritățile competente care activează în sectorul polițienesc și al justiției penale sunt autorități publice sau autorități împuternicite prin dreptul intern și de către autoritățile publice să îndeplinească funcțiile unei autorități publice[747], de exemplu penitenciarele private[748]. Aplicabilitatea directivei se extinde atât la prelucrarea datelor la nivel național, cât și la prelucrarea transfrontalieră între autoritățile polițienești și judiciare ale statelor membre, precum și la transferurile internaționale, de la autoritățile competente către țări terțe și organizații internaționale[749]. Directiva nu se aplică în domeniul securității naționale, nici prelucrării datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile UE[750].

Directiva se bazează, în mare măsură, pe principiile și definițiile cuprinse în Regulamentul general privind protecția datelor, dar ține seama de natura specifică a sectorului polițienesc și al justiției penale. Supravegherea poate fi efectuată de aceleași autorități ale statului membru care o exercită și în temeiul Regulamentului general privind protecția datelor. Numirea responsabililor cu protecția datelor și efectuarea evaluărilor impactului asupra protecției datelor au fost introduse în directivă ca noi obligații ale autorităților polițienești și ale autorităților judiciare penale[751]. Deși aceste concepte sunt inspirate de Regulamentul general privind protecția datelor, directiva abordează caracterul specific al autorităților polițienești și al autorităților juridice penale. În comparație cu prelucrarea datelor în scopuri comerciale, care este reglementată de regulament, prelucrarea legată de securitate poate necesita un anumit nivel de flexibilitate. De exemplu, dacă persoanelor vizate li s-ar asigura – în ceea ce privește dreptul la informare, la obținerea accesului la datele lor cu caracter personal sau la obținerea ștergerii acestora – același nivel de protecție prevăzut de Regulamentul general privind protecția datelor, aceasta ar putea însemna că orice operațiune de supraveghere efectuată în scopul aplicării legii ar deveni ineficientă în acest context. Prin urmare, directiva nu include principiul transparenței. În mod similar, principiul reducerii la minimum a datelor și principiul limitărilor legate de scop

747 *Ibidem*, articolul 3 alineatul (7).

748 Comunicare a Comisiei către Parlamentul European în conformitate cu articolul 294 alineatul (6) din Tratatul privind funcționarea Uniunii Europene privind poziția Consiliului în ceea ce privește adoptarea unei directive a Parlamentului European și a Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și la libera circulație a acestor date, și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, COM(2016) 213 final din 11 aprilie 2016, Bruxelles.

749 Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale, capitolul V.

750 *Ibidem*, articolul 2 alineatul (3).

751 *Ibidem*, la articolul 32, respectiv la articolul 27.

– potrivit cărora prelucrarea datelor cu caracter personal trebuie să se limiteze la ceea ce este necesar în raport cu scopurile sale, respectiv prelucrarea datelor trebuie să se facă în scopuri specificate și explicite – trebuie, de asemenea, să fie aplicate în mod flexibil în cadrul prelucrării legate de securitate. Informațiile colectate și stocate de autoritățile competente pentru un anumit caz pot fi extrem de utile pentru soluționarea cazurilor viitoare.

Principii privind prelucrarea

Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale stabilește unele garanții esențiale privind utilizarea datelor cu caracter personal. De asemenea, descrie principiile care guvernează prelucrarea acestor date. Statele membre trebuie să se asigure că datele cu caracter personal:

- sunt prelucrate în mod legal și echitabil;
- sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate într-un mod incompatibil cu aceste scopuri;
- sunt adecvate, relevante și neexcesive în ceea ce privește scopurile în care sunt prelucrate;
- sunt exacte și, dacă este necesar, sunt actualizate; trebuie să se ia toate măsurile rezonabile pentru a asigura faptul că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;
- sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru care sunt prelucrate datele respective;
- sunt prelucrate într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare[752].

752 *Ibidem*, articolul 4 alineatul (1).

În conformitate cu directiva, prelucrarea este legală numai atunci când are loc în măsura necesară îndeplinirii sarcinilor relevante. În plus, aceasta ar trebui să fie realizată de către o autoritate competentă în vederea atingerii obiectivelor specificate în directivă și să se întemeieze pe dreptul Uniunii sau pe dreptul intern[753]. Datele nu trebuie păstrate mai mult decât este necesar și trebuie șterse sau revizuite periodic în anumite termene. Datele se utilizează numai de către o autoritate competentă și exclusiv în scopul pentru care au fost colectate, transmise sau puse la dispoziție.

Drepturile persoanei vizate

Directiva stabilește, de asemenea, drepturile persoanei vizate. Printre ele se numără:

- Dreptul de a primi informații. Statele membre trebuie să impună operatorului de date să pună la dispoziția persoanei vizate următoarele: 1) identitatea și datele de contact ale operatorului; 2) datele de contact ale responsabilului cu protecția datelor; 3) scopurile prelucrării preconizate; 4) dreptul de a depune o plângere în fața autorității de supraveghere și datele de contact ale acesteia; și 5) dreptul de acces la datele cu caracter personal, de a obține rectificarea sau ștergerea acestor date sau de a restricționa prelucrarea lor[754]. În plus față de aceste cerințe generale de informare, directiva prevede că, în anumite cazuri și pentru a permite exercitarea drepturilor persoanelor vizate, operatorii trebuie să le comunice acestora informații cu privire la temeiul juridic al prelucrării și la perioada pentru care vor fi stocate datele. În cazul în care datele cu caracter personal urmează să fie transmise altor destinatari, inclusiv din țări terțe sau organizații internaționale, persoanele vizate trebuie să fie informate cu privire la categoriile de destinatari. În sfârșit, operatorii trebuie să furnizeze orice informații suplimentare necesare, luând în considerare circumstanțele specifice în care sunt prelucrate datele – de exemplu, atunci când se colectează date cu caracter personal în timpul supravegherii sub acoperire, adică fără știrea persoanei vizate. Acest lucru garantează o prelucrare echitabilă în raport cu persoana vizată[755].

- Dreptul de acces la datele cu caracter personal. Statele membre trebuie să se asigure că persoana vizată beneficiază de dreptul de a ști dacă datele sale cu caracter personal sunt prelucrate sau nu. Dacă sunt, persoana vizată ar trebui să

753 *Ibidem*, articolul 8.

754 *Ibidem*, articolul 13 alineatul (1).

755 *Ibidem*, articolul 13 alineatul (2).

aibă acces la anumite informații, cum ar fi categoriile de date prelucrate[756]. Acest drept poate fi totuși limitat – de exemplu, pentru a evita obstrucționarea anchetei, pentru a nu prejudicia urmărirea penală a unei infracțiuni sau pentru a proteja securitatea publică și drepturile și libertățile celorlalți[757].

- Dreptul la rectificarea datelor cu caracter personal. Statele membre au obligația de a se asigura că persoana vizată poate obține, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte. În plus, persoana vizată are, de asemenea, dreptul de a obține completarea datelor cu caracter personal care sunt incomplete[758].

- Dreptul la ștergerea datelor cu caracter personal și la restricționarea prelucrării. În anumite cazuri, operatorul trebuie să șteargă datele cu caracter personal. În plus, persoana vizată poate obține ștergerea datelor cu caracter personal, însă numai atunci când acestea sunt prelucrate în mod ilegal[759]. În anumite situații, în loc să se șteargă datele cu caracter personal, se poate restricționa prelucrarea lor. Acest lucru se poate întâmpla în cazurile în care: 1) exactitatea datelor cu caracter personal este contestată, dar nu poate fi stabilită cu certitudine; sau 2) datele cu caracter personal trebuie să fie păstrate ca mijloace de probă[760].

Ori de câte ori operatorul refuză să rectifice sau să șteargă date cu caracter personal sau să restricționeze prelucrarea datelor, persoana vizată trebuie informată în scris cu privire la aceasta. Statele membre pot restricționa acest drept la informare, printre altele, pentru a proteja securitatea publică sau drepturile și libertățile celorlalți, din aceleași motive ca și restricționarea dreptului de acces[761].

În mod normal, persoana vizată are dreptul să fie informată cu privire la prelucrarea datelor sale cu caracter personal și are dreptul de acces la date, precum și dreptul de a obține rectificarea sau ștergerea acestora ori restricționarea prelucrării lor; persoana vizată își poate exercita aceste drepturi în mod direct, în relație cu operatorul. Ca opțiune de rezervă, este posibilă, de asemenea, exercitarea indirectă a drepturilor persoanelor vizate, prin intermediul autorității de supraveghere a protecției datelor,

756 *Ibidem*, articolul 14.
757 *Ibidem*, articolul 15.
758 *Ibidem*, articolul 16 alineatul (1).
759 *Ibidem*, articolul 16 alineatul (2).
760 *Ibidem*, articolul 16 alineatul (3).
761 *Ibidem*, articolul 16 alineatul (4).

în temeiul Directivei privind protecția datelor cu caracter personal destinată autorităților polițienești și autorităților judiciare penale; această posibilitate devine aplicabilă atunci când operatorul restrânge dreptul persoanei vizate[762]. Articolul 17 din directivă impune statelor membre să adopte măsuri care să garanteze că drepturile persoanelor vizate pot fi, de asemenea, exercitate prin intermediul autorității de supraveghere relevante. Acesta este motivul pentru care operatorul de date trebuie să informeze persoana vizată cu privire la posibilitatea accesului indirect.

Obligațiile operatorilor și ale persoanelor împuternicite de operatori

În contextul Directivei privind protecția datelor destinată autoritățile polițienești și autorităților judiciare penale, operatorii de date sunt autorități publice competente sau alte organisme competente cu atribuții publice și autoritate publică care stabilesc scopurile și mijloacele de prelucrare a datelor cu caracter personal. Directiva stabilește mai multe obligații pentru operatorii de date pentru a asigura un nivel înalt de protecție a datelor cu caracter personal prelucrate în scopurile aplicării legii.

Autoritățile competente trebuie să înregistreze operațiunile de prelucrare pe care le efectuează în cadrul sistemelor de prelucrare automată. Trebuie efectuate înregistrări cel puțin pentru colectarea, modificarea, consultarea, divulgarea inclusiv transferurile, combinarea și ștergerea datelor cu caracter personal[763]. Directiva prevede că înregistrările consultărilor și ale divulgărilor trebuie să facă posibilă determinarea datei și a momentului operațiunilor, a motivelor acestora și, în măsura în care este posibil, identificarea persoanei care a consultat sistemul sau a divulgat datele cu caracter personal și identitatea destinatarilor acestor date cu caracter personal. Înregistrările trebuie să fie utilizate numai pentru verificarea legalității prelucrării, monitorizare proprie, asigurarea integrității și a securității datelor cu caracter personal și în cadrul unor proceduri penale[764]. Operatorul și persoana împuternicită de operator pun înregistrările la dispoziția autorității de supraveghere, la cererea acesteia.

În special, se prevede o obligație generală a operatorilor de a pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta că prelucrarea se efectuează în conformitate cu directiva și pentru a fi în măsură să demonstreze legalitatea acestei prelucrări[765]. Atunci când elaborează aceste măsuri, operatorii trebuie să ia în

762 *Ibidem*, articolul 17.

763 *Ibidem*, articolul 25 alineatul (1).

764 *Ibidem*, articolul 25 alineatul (2).

765 *Ibidem*, articolul 19.

considerare natura, domeniul de aplicare, contextul prelucrării și, foarte important, orice riscuri potențiale la adresa drepturilor și libertăților persoanelor fizice. Operatorii ar trebui să adopte politici interne și să pună în aplicare măsuri care să faciliteze respectarea principiilor protecției datelor, în special protecția datelor din faza de proiectare și protecția implicită a datelor[766]. În cazul în care prelucrarea este susceptibilă să genereze un risc ridicat la adresa drepturilor persoanelor fizice – de exemplu, din cauza utilizării de noi tehnologii – operatorii trebuie să efectueze, înainte de prelucrare, o evaluare a impactului asupra protecției datelor[767]. Directiva enumeră, de asemenea, măsurile care trebuie puse în aplicare de operatori pentru a asigura securitatea prelucrării. Acestea includ măsuri de prevenire a accesului neautorizat la datele cu caracter personal prelucrate de aceștia, pentru a se asigura că persoanele autorizate au acces numai la datele cu caracter personal pentru care au autorizare, că sistemul de prelucrare funcționează corespunzător și că datele cu caracter personal stocate nu pot fi corupte de o funcționare defectuoasă a sistemului[768]. În cazul în care se produce o încălcare a securității datelor cu caracter personal, operatorii trebuie să notifice acest lucru autorității de supraveghere în cel mult trei zile, descriind caracterul încălcării, consecințele probabile ale acesteia, categoriile de date cu caracter personal în cauză și numărul aproximativ de persoane vizate afectate. Încălcarea securității datelor cu caracter personal trebuie să fie comunicată, de asemenea, persoanei vizate, „fără întârzieri nejustificate", în cazul în care încălcarea este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților respectivei persoane[769].

Directiva include principiul responsabilității, impunând operatorilor sarcina de a pune în aplicare măsuri care să asigure respectarea acestui principiu. Operatorii trebuie să păstreze înregistrări cu toate categoriile de operațiuni de prelucrare aflate sub responsabilitatea lor: conținutul detaliat al acestor înregistrări este precizat la articolul 24 din directivă. Înregistrările trebuie puse la dispoziția autorității de supraveghere, la cererea acesteia, astfel încât autoritatea să poată monitoriza operațiunile de prelucrare ale operatorului. O altă măsură importantă de sporire a responsabilității este desemnarea unui responsabil cu protecția datelor (RPD). Operatorii trebuie să desemneze un RPD, deși directiva permite statelor membre să scutească de această obligație instanțele și alte autorități judiciare independente[770]. Obligațiile RPD sunt

766 *Ibidem*, articolul 20.

767 *Ibidem*, articolul 27.

768 *Ibidem*, articolul 29.

769 *Ibidem*, articolele 30 și 31.

770 *Ibidem*, articolul 32.

similare cu cele prevăzute de Regulamentul general privind protecția datelor. RPD monitorizează respectarea directivei, informează și consiliază angajații care efectuează prelucrarea datelor cu privire la obligațiile care le revin în temeiul legislației privind protecția datelor. De asemenea, RPD furnizează consiliere cu privire la necesitatea efectuării unei evaluări a impactului asupra protecției datelor și acționează ca punct de contact pentru autoritatea de supraveghere.

Transferuri către țări terțe sau organizații internaționale

În mod similar cu Regulamentul general privind protecția datelor, directiva stabilește condițiile pentru transferul de date cu caracter personal către țări terțe sau organizații internaționale. Dacă datele cu caracter personal ar fi transmise în mod liber în afara jurisdicției UE, garanțiile și protecția solidă prevăzute de legislația UE ar putea fi subminate. Cu toate acestea, condițiile referitoare la transfer sunt foarte diferite de cele prevăzute de Regulamentul general privind protecția datelor. Transferul de date cu caracter personal către țări terțe sau organizații internaționale este permis în următoarele situații și condiții[771]:

- Transferul este necesar pentru atingerea obiectivelor directivei.

- Datele cu caracter personal sunt transferate unui operator dintr-o țară terță sau unei organizații internaționale care este o autoritate competentă în sensul directivei, deși există o derogare de la această normă în cazuri individuale și specifice[772].

- Transferul către țări terțe sau organizații internaționale al datelor cu caracter personal primite în cadrul cooperării transfrontaliere necesită autorizarea din partea statului membru din care provin datele, deși se prevăd excepții în cazuri de urgență.

- Comisia Europeană a adoptat o decizie privind caracterul adecvat al nivelului de protecție a datelor, au fost stabilite garanții adecvate sau se aplică derogarea pentru transferuri în situații specifice.

- Transferurile ulterioare ale datelor cu caracter personal către o altă țară terță sau organizație internațională necesită autorizarea prealabilă din partea autorității

771 *Ibidem*, articolul 35.

772 *Ibidem*, articolul 39.

competente inițiale, care va ține seama, printre altele, de gravitatea infracțiunii și de nivelul de protecție a datelor din țara de destinație a transferului internațional secundar[773].

În conformitate cu directiva, transferurile de date cu caracter personal pot avea loc dacă se îndeplinește una din cele trei condiții specificate. Prima condiție este adoptarea de către Comisia Europeană a unei decizii privind caracterul adecvat al nivelului de protecție, în temeiul directivei. Decizia se poate aplica întregului teritoriu al unei țări terțe, anumitor sectoare determinate dintr-o țară terță sau unei organizații internaționale. Cu toate acestea, transferul se poate efectua numai dacă se asigură un nivel adecvat de protecție și dacă sunt îndeplinite condițiile definite în directivă[774]. În astfel de cazuri, transferul datelor cu caracter personal nu face obiectul autorizării din partea statului membru[775]. Comisia Europeană trebuie să monitorizeze evoluțiile care ar putea afecta funcționarea deciziilor privind caracterul adecvat al nivelului de protecție. În plus, decizia trebuie să includă un mecanism de revizuire periodică. De asemenea, Comisia poate abroga, modifica sau suspenda o decizie în cazul în care informațiile disponibile indică faptul că condițiile din țara terță sau din organizația internațională nu mai asigură un nivel adecvat de protecție. În acest caz, Comisia trebuie să inițieze consultări cu țara terță sau cu organizația internațională, în vederea remedierii situației.

În absența unei decizii privind caracterul adecvat al nivelului de protecție, transferurile se pot întemeia pe garanții adecvate. Acestea pot fi stabilite într-un instrument cu caracter juridic obligatoriu sau operatorul poate efectua o evaluare a propriilor circumstanțe legate de transferul datelor cu caracter personal și poate concluziona că există garanții adecvate. Evaluarea propriilor circumstanțe ar trebui să ia în considerare eventualele acorduri de cooperare încheiate între Europol sau Eurojust și țara terță sau organizația internațională în cauză, existența obligațiilor de confidențialitate și a limitărilor legate de scop, precum și a asigurărilor că datele nu vor fi folosite pentru nicio formă de tratament crud și inuman (inclusiv pedeapsa cu moartea)[776]. În acest din urmă caz, operatorul trebuie să informeze autoritatea de supraveghere competentă cu privire la tipurile de transferuri din această categorie[777].

773 *Ibidem*, articolul 35 alineatul (1).

774 *Ibidem*, articolul 36.

775 *Ibidem*, articolul 36 alineatul (1).

776 *Ibidem*, considerentul 71.

777 *Ibidem*, articolul 37 alineatul (1).

În cazul în care nu a fost adoptată nicio decizie privind caracterul adecvat al nivelului de protecție și nu au fost stabilite garanții adecvate, transferurile pot fi totuși permise în situațiile specifice descrise în directivă. Acestea includ, printre altele, protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane și prevenirea unei amenințări imediate și grave la adresa securității publice a unui stat membru sau a unei țări terțe[778].

În cazuri individuale și specifice, pot fi efectuate transferuri de către autoritățile competente către destinatari stabiliți în țări terțe care nu sunt autorități competente dacă, pe lângă una dintre cele trei condiții descrise mai sus, sunt îndeplinite și condițiile suplimentare prevăzute la articolul 39 din directivă. În special, transferul trebuie să fie strict necesar pentru executarea unei sarcini de către autoritatea competentă care transferă datele și care este, de asemenea, responsabilă pentru determinarea faptului că niciunul dintre drepturile și libertățile fundamentale ale persoanelor fizice nu prevalează în fața interesului public care justifică transferul. Aceste transferuri trebuie să fie documentate, iar autoritatea competentă care transferă datele trebuie să informeze autoritatea de supraveghere competentă[779].

În sfârșit, în ceea ce privește țările terțe și organizațiile internaționale, directiva impune, de asemenea, elaborarea unor mecanisme de cooperare internațională pentru a facilita asigurarea efectivă a respectării legislației și, astfel, pentru a acorda asistență autorităților de supraveghere a protecției datelor în ceea ce privește cooperarea cu omologii lor străini[780].

Supravegherea independentă și căile de atac disponibile persoanelor vizate

Fiecare stat membru trebuie să garanteze că una sau mai multe autorități naționale independente de supraveghere sunt responsabile pentru consiliere și pentru monitorizarea aplicării dispozițiilor adoptate în temeiul directivei[781]. Autoritatea de supraveghere instituită în temeiul directivei poate fi aceeași cu autoritatea de supraveghere instituită în temeiul Regulamentului general privind protecția datelor, dar statele membre au libertatea de a desemna o autoritate diferită, cu condiția ca aceasta să îndeplinească criteriile de independență. De asemenea, autoritățile de

778 *Ibidem*, articolul 38 alineatul (1).

779 *Ibidem*, articolul 37 alineatul (3).

780 *Ibidem*, articolul 40.

781 *Ibidem*, articolul 41.

supraveghere examinează cererile depuse de orice persoană cu privire la protecția drepturilor și libertăților acesteia legate de prelucrarea datelor cu caracter personal de către autoritățile competente.

În cazul în care exercitarea drepturilor persoanei vizate este refuzată din motive întemeiate, persoana vizată trebuie să aibă dreptul de a contesta refuzul în fața autorității naționale de supraveghere competente și/sau în fața unei instanțe. Dacă o persoană suferă un prejudiciu din cauza unei încălcări a legislației naționale de punere în aplicare a directivei, aceasta are dreptul la despăgubiri din partea operatorului sau a oricărei alte autorități competente în temeiul legislației statului membru în cauză[782]. În general, persoanele vizate trebuie să aibă acces la o cale de atac judiciară pentru orice încălcare a drepturilor lor garantate prin legislația națională de punere în aplicare a directivei[783].

8.3. Alte instrumente juridice specifice privind protecția datelor în contextul aplicării legii

Pe lângă Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale, schimbul de informații deținute de statele membre în domenii specifice este reglementat de o serie de instrumente juridice – cum ar fi Decizia-cadru 2009/315/JAI a Consiliului din 26 februarie 2009 privind organizarea și conținutul schimbului de informații extrase din cazierele judiciare între statele membre, Decizia 2000/642/JAI a Consiliului din 17 octombrie 2000 privind acordurile de cooperare între unitățile de informații financiare ale statelor membre în ceea ce privește schimbul de informații și Decizia-cadru 2006/960/JAI a Consiliului din 18 decembrie 2006 privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre ale Uniunii Europene[784].

782 *Ibidem*, articolul 56.

783 *Ibidem*, articolul 54.

784 Decizia-cadru 2009/315/JAI a Consiliului din 26 februarie 2009 privind organizarea și conținutul schimbului de informații extrase din cazierele judiciare între statele membre, JO 2009 L 93; Decizia 2000/642/JAI a Consiliului din 17 octombrie 2000 privind acordurile de cooperare între unitățile de informații financiare ale statelor membre în ceea ce privește schimbul de informații, JO 2000 L 271; Decizia-cadru 2006/960/JAI a Consiliului din 18 decembrie 2006 privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre ale Uniunii Europene, JO 2006 L 386.

Este important de remarcat faptul că cooperarea transfrontalieră[785] între autoritățile competente implică tot mai mult schimbul de date privind imigrația. Acest domeniu legislativ nu este considerat o parte a sectorului polițienesc și al justiției penale, dar este în multe privințe relevant pentru activitatea autorităților polițienești și judiciare. Același lucru este valabil pentru datele referitoare la mărfurile importate în sau exportate din UE. Eliminarea controalelor la frontierele interne ale UE în cadrul spațiului Schengen a sporit riscul de fraudă, ceea ce impune necesitatea ca statele membre să își intensifice cooperarea, în special prin consolidarea schimbului transfrontalier de informații în vederea eficientizării depistării și urmăririi penale a încălcărilor legislației vamale naționale și a UE. În plus, în ultimii ani, s-a înregistrat o creștere a numărului de infracțiuni grave, a criminalității organizate și a terorismului, care pot implica deplasări internaționale, și a devenit evidentă necesitatea intensificării cooperării transfrontaliere în sectorul polițienesc și al aplicării legii în multe cazuri[786].

Decizia Prüm

Un exemplu important de cooperare transfrontalieră instituționalizată prin schimbul de date deținute la nivel național este Decizia 2008/615/JAI a Consiliului – împreună cu dispozițiile de punere în aplicare ale acesteia – privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (Decizia Prüm), prin care Tratatul de la Prüm a fost integrat în dreptul european în anul 2008[787]. Tratatul de la Prüm a fost un acord internațional de cooperare polițienească semnat în 2005 de Austria, Belgia, Franța, Germania, Luxemburg, Țările de Jos și Spania[788].

Decizia Prüm urmărește acordarea de asistență statelor membre în vederea îmbunătățirii schimbului de informații în scopul prevenirii și combaterii criminalității

785 Comunicare a Comisiei către Parlamentul European și Consiliu – Consolidarea cooperării în domeniul asigurării respectării legii în UE: modelul european de schimb de informații (EIXM), COM(2012) 735 final din 7 decembrie 2012, Bruxelles.

786 Vezi Propunerea de directivă a Parlamentului European și a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, COM(2011) 32 final din 2 februarie 2011, Bruxelles, p. 1.

787 Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere, JO 2008 L 210.

788 Convenția dintre Regatul Belgiei, Republica Federală Germania, Regatul Spaniei, Republica Franceză, Marele Ducat al Luxemburgului, Regatul Țărilor de Jos și Republica Austria privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului, a criminalității transfrontaliere și a migrației ilegale.

în trei domenii: terorism, criminalitate transfrontalieră și migrație ilegală. În acest scop, decizia cuprinde dispoziții privind:

- accesul automatizat la profilurile ADN, la datele dactiloscopice și la anumite date naționale de înmatriculare a vehiculelor;
- furnizarea de date în legătură cu evenimente majore de dimensiune transfrontalieră;
- furnizarea de informații în vederea prevenirii infracțiunilor de terorism;
- alte măsuri de intensificare a cooperării polițienești transfrontaliere.

Bazele de date care sunt puse la dispoziție în temeiul Deciziei Prüm sunt reglementate în întregime de legislația națională, iar schimbul de date este reglementat în plus de decizie, a cărei compatibilitate cu Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale va trebui evaluată. Organele competente pentru supravegherea acestor fluxuri de date sunt autoritățile naționale de supraveghere a protecției datelor.

Decizia-cadru 2006/960/JAI – Inițiativa suedeză

Decizia-cadru 2006/960/JAI[789] (Inițiativa suedeză) reprezintă un alt exemplu de cooperare transfrontalieră în ceea ce privește schimbul de date deținute la nivel național de autoritățile de aplicare a legii. Inițiativa suedeză se concentrează în mod specific asupra schimbului de informații și date operative și prevede norme specifice de protecție a datelor la articolul 8.

Potrivit acestui instrument, utilizarea informațiilor și a datelor operative comunicate trebuie să facă obiectul dispozițiilor naționale privind protecția datelor din statul membru care primește informațiile, în conformitate cu aceleași norme care s-ar aplica în cazul în care datele în cauză ar fi colectate în statul membru respectiv. Articolul 8 prevede în continuare că, atunci când furnizează informații și date operative, autoritatea competentă de aplicare a legii poate impune condiții care sunt conforme cu legislația sa națională cu privire la utilizarea lor de către autoritatea competentă de aplicare a legii destinatară. Aceste condiții se pot aplica și difuzării rezultatelor

789 Decizia-cadru 2006/960/JAI a Consiliului din 18 decembrie 2006 privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre ale Uniunii Europene, JO 2006 L 386.

cercetării penale sau operațiunilor de colectare a datelor operative în materie penală pentru care s-a solicitat schimbul de informații și date operative. Cu toate acestea, atunci când legislația națională prevede derogări de la limitările de utilizare (de exemplu, în favoarea autorităților judiciare, a instituțiilor legislative etc.), informațiile și datele operative pot fi utilizate numai după consultarea prealabilă a statului membru emitent.

Informațiile și datele operative furnizate pot fi utilizate:

- în scopurile pentru care au fost transmise;
- pentru a preveni un pericol imediat și grav pentru siguranța publică.

Prelucrarea în alte scopuri poate fi autorizată, dar numai cu acordul prealabil al statului membru emitent.

Inițiativa suedeză mai prevede că datele cu caracter personal prelucrate trebuie să fie protejate în conformitate cu instrumentele internaționale, cum ar fi:

- Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal[790];
- Protocolul adițional din 8 noiembrie 2001 la respectiva convenție, cu privire la autoritățile de control și fluxul transfrontalier al datelor[791];
- Recomandarea nr. R(87) 15 a Comitetului de Miniștri al Consiliului Europei către statele membre de reglementare a utilizării datelor cu caracter personal în sectorul polițienesc[792].

790 Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, ETS nr. 108.

791 Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor, ETS nr. 108.

792 Recomandarea nr. R(87) 15 a Comitetului de Miniștri al Consiliului Europei către statele membre de reglementare a utilizării datelor cu caracter personal în sectorul polițienesc (adoptată de Comitetul de Miniștri la 17 septembrie 1987, în cadrul celei de a 410-a reuniuni a miniștrilor adjuncți).

Directiva UE privind PNR

Datele din registrul cu numele pasagerilor (PNR) conțin informațiile referitoare la pasagerii transportului aerian colectate și păstrate în sistemele de rezervare și de control al plecării operate de transportatorii aerieni în scopuri comerciale proprii. Aceste date conțin diferite tipuri de informații, precum datele călătoriei, itinerariul călătoriei, informații despre bilete, date de contact, agenția de turism la care s-a rezervat zborul, mijloacele de plată utilizate, numărul locului și informații despre bagaje[793]. Prelucrarea datelor PNR poate ajuta autoritățile de aplicare a legii să identifice suspecții cunoscuți sau potențiali și să efectueze evaluări pe baza tiparelor de călătorie și a altor indicatori care sunt asociați în mod obișnuit cu activități infracționale. Analiza datelor PNR permite, de asemenea, urmărirea retrospectivă a itinerariilor de călătorie și a contactelor persoanelor suspectate că au fost implicate în activități infracționale, ceea ce permite autorităților de aplicare a legii să identifice rețelele infracționale[794]. UE a încheiat unele acorduri cu țări terțe pentru schimbul de date PNR, astfel cum s-a explicat la secțiunea 7. În plus, prin intermediul Directivei (UE) 2016/681 privind utilizarea datelor PNR pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave[795] (Directiva UE privind PNR), a fost introdusă prelucrarea datelor PNR în UE. Această directivă prevede obligația transportatorilor aerieni de a transmite datele PNR autorităților competente și stabilește garanții stricte de protecție a datelor în cadrul prelucrării și al colectării acestor date. Directiva UE privind PNR se aplică zborurilor internaționale către și dinspre UE, dar și zborurilor din interiorul Uniunii, în cazul în care un stat membru decide astfel[796].

Datele PNR colectate trebuie să conțină doar informațiile permise de Directiva UE privind PNR. Acestea trebuie păstrate de o singură unitate de informații, într-un loc sigur din fiecare stat membru. Datele PNR trebuie să fie depersonalizate la șase luni după transmiterea lor de către transportatorul aerian și trebuie să fie păstrate pentru o perioadă de maximum cinci ani[797]. Datele PNR fac obiectul schimbului între statele

793 Propunere de directivă a Parlamentului European și a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, COM(2011) 32 final din 2 februarie 2011, Bruxelles, p. 1.

794 Comisia Europeană (2015), Fișă informativă privind combaterea terorismului la nivelul UE, o prezentare generală a acțiunilor, măsurilor și inițiativelor Comisiei, Bruxelles, 11 ianuarie 2015.

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

796 Directiva UE privind PNR, L 119, p. 132, articolul 1 alineatul (1) și articolul 2 alineatul (1).

797 *Ibidem*, articolul 12 alineatele (1) și (2).

membre, respectiv între statele membre și Europol; schimbul cu țările terțe este posibil numai de la caz la caz.

Transmiterea și prelucrarea datelor PNR și drepturile garantate persoanelor vizate trebuie să fie în conformitate cu Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale și trebuie să asigure nivelul înalt de protecție a vieții private și a datelor cu caracter personal impus de Cartă, de Convenția 108 modernizată și de Convenția europeană a drepturilor omului.

Autoritățile naționale independente de supraveghere care sunt competente în temeiul Directivei privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale sunt, de asemenea, responsabile pentru consiliere și pentru monitorizarea aplicării dispozițiilor adoptate de statele membre în temeiul Directivei UE privind PNR.

Păstrarea datelor din telecomunicații

Directiva privind păstrarea datelor[798] – declarată nulă la 8 aprilie 2014 prin Hotărârea CJUE pronunțată în cauza *Digital Rights Ireland* – impunea furnizorilor de servicii de comunicații să păstreze metadatele disponibile, în scopul specific al combaterii infracțiunilor grave, pentru o perioadă de cel puțin șase luni, dar nu mai mult de 24 de luni, indiferent dacă furnizorul mai avea nevoie de aceste date în scopuri de facturare sau în scopuri tehnice de furnizare a serviciului.

Păstrarea datelor din telecomunicații intervine în mod evident asupra dreptului la protecția datelor[799]. Caracterul justificat al acestei ingerințe a fost contestat în cadrul mai multor proceduri judiciare din statele membre ale UE[800].

798 Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE, JO 2006 L 105.

799 Avizul Autorității Europene pentru Protecția Datelor privind Raportul de evaluare al Comisiei către Consiliu și Parlamentul European referitor la Directiva privind păstrarea datelor (Directiva 2006/24/CE), 31 mai 2011.

800 Curtea Constituțională Federală a Germaniei (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 martie 2010; Curtea Constituțională a României, nr. 1258, 8 octombrie 2009; Curtea Constituțională a Republicii Cehe (*Ústavní soud České republiky*), 94/2011 Coll., 22 martie 2011.

Exemplu: În cauzele *Digital Rights Ireland* și *Kärntner Landesregierung și alții*[801], grupul Digital Rights și domnul Seitlinger au introdus acțiuni în fața Înaltei Curți din Irlanda, respectiv în fața Curții Constituționale din Austria, contestând legalitatea măsurilor naționale care permiteau păstrarea datelor colectate din telecomunicații electronice. Digital Rights a solicitat instanței irlandeze să constate nulitatea Directivei 2006/24/CE și a părții din dreptul penal intern referitoare la infracțiunile de terorism. În mod similar, domnul Seitlinger și peste 11 000 de alți reclamanți au contestat o dispoziție din legislația austriacă privind telecomunicațiile care transpunea Directiva 2006/24/CE și au solicitat anularea acestei dispoziții.

În cadrul examinării acestor cereri de pronunțare a unor decizii preliminare, CJUE a anulat Directiva privind păstrarea datelor. Potrivit CJUE, datele care puteau fi reținute în temeiul directivei, considerate în ansamblu, furnizau informații precise despre persoanele fizice. În continuare, CJUE a examinat gravitatea ingerinței în drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal. Curtea a constatat că păstrarea datelor îndeplinește un obiectiv de interes public, și anume combaterea criminalității grave, și, prin urmare, apărarea siguranței publice. Cu toate acestea, CJUE a constatat că legiuitorul UE a încălcat principiul proporționalității prin adoptarea directivei. Deși directiva ar putea fi adecvată pentru atingerea obiectivului urmărit, aceasta conține „o ingerință în [drepturile] fundamentale [la respectarea vieții private și la protecția datelor cu caracter personal], care este de o mare amploare și de o gravitate deosebită [...], fără ca o astfel de ingerință să fie încadrată în mod precis de dispoziții care să permită garantarea faptului că ea este limitată efectiv la strictul necesar”.

În absența unei reglementări specifice în materie, păstrarea datelor este permisă ca o derogare de la norma privind confidențialitatea datelor din telecomunicații în temeiul Directivei 2002/58/CE (Directiva asupra confidențialității și comunicațiilor electronice)[802], ca măsură preventivă, dar trebuie să fie efectuată exclusiv în scopul combaterii infracțiunilor grave. Păstrarea datelor în acest context trebuie să se limiteze la strictul necesar în ceea ce privește categoriile de date păstrate, mijloacele de

801 Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții și Kärntner Landesregierung și alții*, punctul 65.

802 Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), JO 2002 L 201.

comunicare preconizate, persoanele vizate și durata de păstrare a datelor. Autoritățile naționale pot obține acces la datele păstrate cu condiția îndeplinirii unor cerințe stricte, inclusiv a efectuării unei examinări prealabile de către o autoritate independentă. Datele trebuie păstrate în interiorul UE.

Exemplu: Ulterior pronunțării hotărârii CJUE în cauzele conexate *Digital Rights Ireland* și *Kärntner Landesregierung și alții*[803], CJUE a fost sesizată cu alte două cauze, având ca obiect obligațiile generale impuse în Suedia și în Regatul Unit furnizorilor de servicii de comunicații electronice de a păstra datele din telecomunicații în temeiul Directivei privind păstrarea datelor (anulată). În cauzele *Tele2 Sverige* și *Home Department/Tom Watson și alții*[804], CJEU a statuat că reglementarea națională care prevedea păstrarea generalizată și nediferențiată a datelor, fără a impune nicio legătură între datele care trebuiau păstrate și o amenințare la adresa siguranței publice și fără a preciza nicio condiție – de exemplu, perioada păstrării datelor, zona geografică, grupul de persoane susceptibile de a fi implicate în săvârșirea unei infracțiuni grave –, a depășit limitele strictului necesar și nu putea fi considerată justificată într-o societate democratică, astfel cum prevede Directiva 2002/58/CE coroborată cu Carta drepturilor fundamentale a UE.

Perspective

În ianuarie 2017, Comisia Europeană a publicat o propunere de regulament privind respectarea vieții private și protecția datelor cu caracter personal în domeniul comunicațiilor electronice, menit să abroge și să înlocuiască Directiva 2002/58/CE[805]. Propunerea menționată nu include dispoziții specifice privind păstrarea datelor. Totuși, aceasta prevede că statele membre pot restricționa prin lege, în temeiul regulamentului, anumite obligații și drepturi, dacă o astfel de restricție constituie o măsură necesară și proporțională pentru a proteja anumite interese publice, inclusiv securitatea națională, apărarea, siguranța publică, prevenirea, investigarea, depistarea

803 Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții și Kärntner Landesregierung și alții*.

804 Hotărârea CJUE [MC] din 21 decembrie 2016 în cauzele conexate C-203/15 și C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen și Secretary of State for the Home Department/Tom Watson și alții*.

805 Propunere de regulament al Parlamentului European și al Consiliului privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice și de abrogare a Directivei 2002/58/CE (Regulamentul privind viața privată și comunicațiile electronice), COM(2017) 10 final din 10 ianuarie 2017, Bruxelles.

sau urmărirea penală a infracțiunilor sau executarea pedepselor[806]. Prin urmare, statele membre pot să mențină sau să creeze cadre naționale în materie de păstrare a datelor care prevăd măsuri de păstrare specifice, în măsura în care astfel de cadre sunt conforme cu legislația Uniunii, ținând seama de jurisprudența CJUE referitoare la interpretarea Directivei asupra confidențialității și comunicațiilor electronice și de Carta drepturilor fundamentale a UE[807]. La momentul redactării prezentului manual, discuțiile privind adoptarea regulamentului erau în curs de desfășurare.

Acordul-cadru UE-SUA privind protecția datelor cu caracter personal transferate în scopuri de aplicare a legii

La 1 februarie 2017 a intrat în vigoare Acordul UE-SUA privind protecția informațiilor cu caracter personal în ceea ce privește prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor[808]. Acordul-cadru UE-SUA urmărește să asigure un nivel ridicat de protecție a datelor pentru cetățenii UE, consolidând în același timp cooperarea dintre autoritățile de aplicare a legii din UE și din SUA. Acesta completează acordurile existente între UE și SUA și între statele membre și SUA la nivelul autorităților de aplicare a legii, contribuind, de asemenea, la instituirea unor norme clare și armonizate privind protecția datelor pentru viitoarele acorduri în acest domeniu. În această privință, acordul vizează stabilirea unui cadru juridic durabil pentru facilitarea schimbului de informații.

Acordul nu constituie în sine un temei juridic adecvat pentru schimbul de date cu caracter personal, dar oferă, în schimb, garanții adecvate de protecție a datelor pentru persoanele în cauză. Acesta acoperă toate operațiunile de prelucrare a datelor cu caracter personal necesare pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor, inclusiv a terorismului[809].

806 *Ibidem*, considerentul 26.

807 Vezi expunerea de motive a Propunerii de regulament privind viața privată și comunicațiile electronice, COM(2017) 10 final, punctul 1.3.

808 Vezi Comunicatul de presă 305/16 din 2 iunie 2016 al Consiliului UE intitulat „Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign 'Umbrella agreement'" („Consolidarea drepturilor la protecția datelor pentru cetățenii UE în ceea ce privește cooperarea în domeniul aplicării legii: UE și SUA semnează un acord-cadru").

809 Acord între Statele Unite ale Americii și Uniunea Europeană privind protecția informațiilor cu caracter personal în ceea ce privește prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor, 18 mai 2016, traducere, nr. 8557/16, articolul 3 alineatul (1). Vezi, de asemenea, Notificarea Comisiei din 26 mai 2010 privind negocierile pentru acordul UE-SUA privind protecția datelor, MEMO/10/216, și Comunicatul de presă al Comisiei Europene din 26 mai 2010 privind standardele ridicate de respectare a vieții private stabilite de acordul UE-SUA privind protecția datelor, IP/10/609.

Acordul stabilește garanții multiple pentru a asigura faptul că datele cu caracter personal sunt utilizate numai în scopurile specificate în acord. În special, oferă următoarele măsuri de protecție cetățenilor UE:

- limitări privind utilizarea datelor: datele cu caracter personal pot fi utilizate numai în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor;
- protecția împotriva discriminării arbitrare și nejustificate;
- transferurile ulterioare: orice transfer ulterior către o țară terță sau organizație internațională din afara SUA și din afara UE trebuie să facă obiectul unui acord prealabil al autorității competente a țării care a transferat inițial datele;
- calitatea datelor: datele cu caracter personal trebuie păstrate ținându-se seama de exactitatea, relevanța, oportunitatea și caracterul complet al acestora;
- securitatea prelucrării, inclusiv notificarea încălcărilor securității datelor cu caracter personal;
- prelucrarea datelor sensibile este permisă numai cu aplicarea garanțiilor adecvate, în acord cu legea;
- perioade de păstrare: datele cu caracter personal nu pot fi păstrate mai mult timp decât este necesar sau adecvat;
- drepturi de acces și de rectificare: orice persoană are dreptul de acces la datele sale cu caracter personal, sub rezerva anumitor condiții, și va putea solicita rectificarea datelor în cazul în care sunt inexacte;
- deciziile automatizate necesită garanții adecvate, inclusiv posibilitatea de a solicita o intervenție umană;
- supravegherea eficace, inclusiv cooperarea dintre autoritățile de supraveghere din UE și SUA;
- căi de atac judiciare și asigurarea respectării: cetățenii UE au dreptul[810] de a introduce acțiuni în fața instanțelor din SUA în cazul în care autoritățile din

810 Legea SUA privind căile de atac judiciare a fost promulgată de președintele Obama la 24 februarie 2016.

această țară refuză accesul sau rectificarea datelor sau divulgă în mod ilegal datele lor cu caracter personal.

În temeiul acordului-cadru, s-a instituit și un sistem de informare a autorităților de supraveghere competente din statul membru al persoanelor afectate cu privire la orice încălcare a protecției datelor, după caz. Garanțiile juridice prevăzute de acord garantează egalitatea de tratament a cetățenilor UE în SUA în cazul în care există o încălcare a securității datelor cu caracter personal[811].

8.3.1. Protecția datelor în agențiile UE din sectorul judiciar și al aplicării legii

Europol

Europol, agenția UE de aplicare a legii, are sediul la Haga și deține unități naționale Europol (UNE) în fiecare stat membru. Europol a fost înființată în 1998; statutul său juridic actual ca instituție UE se întemeiază pe Regulamentul privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Regulamentul Europol)[812]. Obiectivul Europol este acela de a oferi asistență în ceea ce privește prevenirea și investigarea criminalității organizate, a terorismului și a altor infracțiuni grave, astfel cum sunt enumerate în anexa I la Regulamentul Europol, care afectează două sau mai multe state membre. Acest lucru se realizează prin schimbul de informații și prin caracterul de centru de informații al UE, agenția furnizând analize ale datelor operative și evaluări ale amenințărilor.

Pentru a-și atinge obiectivele, Europol a înființat sistemul informațional Europol, care pune la dispoziția statelor membre o bază de date pentru schimbul de informații și date operative în materie penală prin intermediul UNE. Sistemul informațional

811 Autoritatea Europeană pentru Protecția Datelor a emis un aviz privind acordul UE-SUA, recomandând, printre altele, următoarele modificări: 1) adăugarea formulării „în scopurile specifice pentru care au fost transferate" la articolul care se referă la păstrarea datelor pe o perioadă care să nu depășească ceea ce este necesar și adecvat; și 2) excluderea transferului în bloc al datelor sensibile, care era posibil în temeiul acordului. Vezi Avizul 1/2016 al Autorității Europene pentru Protecția Datelor, *Aviz preliminar referitor la Acordul între Statele Unite ale Americii și Uniunea Europeană privind protecția informațiilor cu caracter personal în ceea ce privește prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor*, punctul 35.

812 Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului, JO 2016 L 135.

Europol poate fi utilizat pentru a pune la dispoziție date referitoare la persoane suspectate sau condamnate pentru o infracțiune care intră în sfera de competență a Europol sau la persoane despre care există indicii concrete că vor comite astfel de infracțiuni. Europol și UNE pot introduce date direct în sistemul informațional Europol și pot prelua date din acesta. Doar partea care a introdus un anumit set de date în sistem le poate modifica, corecta sau șterge. Organismele UE, țările terțe și organizațiile internaționale pot, de asemenea, să furnizeze informații Europol.

Informațiile, inclusiv datele cu caracter personal, pot fi obținute de către Europol și din surse accesibile publicului, cum ar fi internetul. Transferurile de date cu caracter personal către organismele UE sunt permise numai dacă acest lucru este necesar pentru îndeplinirea misiunii Europol sau a organismului UE destinatar. Transferurile de date cu caracter personal către țări terțe sau organizații internaționale sunt permise numai dacă Comisia Europeană decide că țara sau organizația internațională în cauză asigură un nivel adecvat de protecție a datelor (prin adoptarea unei „decizii privind caracterul adecvat al nivelului de protecție") sau dacă există un acord internațional sau de cooperare. Europol poate primi și prelucra date cu caracter personal de la părți private și persoane particulare cu condiția strictă ca aceste date să fie transferate de o UNE în conformitate cu legislația sa națională, de un punct de contact dintr-o țară terță sau de o organizație internațională cu care există o cooperare consacrată printr-un acord de cooperare sau de o autoritate a unei țări terțe sau a unei organizații internaționale care face obiectul unei decizii privind caracterul adecvat al nivelului de protecție sau cu care UE a încheiat un acord internațional. Toate schimburile de informații sunt realizate printr-o aplicație de rețea pentru schimbul securizat de informații (SIENA).

Ca răspuns la noile evoluții, în cadrul Europol au fost înființate centre specializate. În 2013 s-a înființat în cadrul Europol Centrul european de combatere a criminalității informatice[813]. Acesta funcționează ca centru de informații al UE privind criminalitatea informatică, contribuind la accelerarea reacției în cazul infracțiunilor online, dezvoltând și implementând capacități criminalistice digitale și furnizând bune practici în legătură cu anchetele din domeniul criminalității informatice. Centrul se axează pe acte de criminalitate informatică:

- comise de grupuri organizate cu scopul de a genera profituri considerabile din infracțiuni, cum ar fi frauda online;

813 Vezi, de asemenea, Avizul Autorității Europene pentru Protecția Datelor referitor la Comunicarea Comisiei Europene către Consiliu și Parlamentul European privind instituirea unui Centru european de combatere a criminalității informatice, Bruxelles, 29 iunie 2012.

- care aduc prejudicii grave victimelor lor, cum ar fi exploatarea sexuală a minorilor pe internet;

- îndreptate împotriva infrastructurii și a sistemelor informatice critice din UE.

Centrul european de combatere a terorismului (CECT) a fost înființat în ianuarie 2016 pentru a oferi sprijin operativ statelor membre în cadrul investigațiilor legate de infracțiunile de terorism. Acesta efectuează o verificare încrucișată în timp real a datelor operative în baza de date existentă a Europol, punând rapid în evidență legăturile financiare, și analizează toate detaliile disponibile ale anchetelor pentru a contribui la elaborarea unei imagini structurate a unei rețele teroriste[814].

Centrul european privind introducerea ilegală de migranți (EMSC) a fost înființat în februarie 2016, în urma unei reuniuni a Consiliului din noiembrie 2015, pentru a sprijini statele membre în urmărirea și destructurarea rețelelor infracționale implicate în introducerea ilegală de migranți. Acesta funcționează ca un centru de informare care sprijină birourile din Catania (Italia) și Pireu (Grecia) ale grupului operativ la nivel regional al Uniunii Europene, care oferă asistență autorităților naționale în mai multe domenii, inclusiv schimbul de date operative, anchetele penale și urmărirea penală a rețelelor infracționale de trafic de persoane[815].

Regimul de protecție a datelor care reglementează activitățile Europol este consolidat și se bazează pe principiile Regulamentului privind protecția datelor de către instituțiile UE[816] și este, de asemenea, coerent cu dispozițiile Directivei privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale, ale Convenției 108 modernizate și ale Recomandării privind sectorul polițienesc.

Este permisă prelucrarea datelor cu caracter personal care vizează victimele unei infracțiuni penale, martorii sau alte persoane care pot furniza informații privind infracțiunile penale sau care vizează persoanele care nu au împlinit vârsta de 18 ani în cazul în care acest lucru este strict necesar și proporțional pentru prevenirea sau combaterea criminalității care se încadrează în obiectivele Europol[817]. Este interzisă prelucrarea datelor cu caracter personal sensibile, cu excepția cazului în care acest

814 Vezi pagina web a Europol despre CECT.

815 Vezi pagina web a Europol despre EMSC.

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

817 Regulamentul Europol, articolul 30 alineatul (1).

lucru este strict necesar și proporțional pentru prevenirea sau combaterea criminalității care se încadrează în obiectivele Europol și dacă datele respective completează alte date cu caracter personal prelucrate de Europol[818]. În ambele cazuri, numai Europol are acces la datele în cauză[819].

Stocarea datelor este permisă numai pentru o perioadă de timp necesară și proporțională, iar continuarea acesteia face obiectul unei analize din trei în trei ani; dacă nu se decide stocarea în continuare a datelor, acestea sunt șterse în mod automat[820].

Europol este autorizată, în anumite condiții, să transfere în mod direct date cu caracter personal către un organism UE sau către o autoritate dintr-o țară terță sau o organizație internațională[821]. Încălcările securității datelor care sunt susceptibile să producă efecte negative grave asupra drepturilor și libertăților persoanelor vizate afectate trebuie să fie comunicate fără întârziere acestor persoane[822]. La nivelul statelor membre se desemnează autorități naționale de supraveghere care au sarcina de a monitoriza prelucrarea datelor cu caracter personal de către Europol[823].

AEPD răspunde de monitorizarea și asigurarea protecției drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către Europol, precum și de consilierea Europol și a persoanelor vizate cu privire la toate aspectele care se referă la prelucrarea datelor cu caracter personal. În acest scop, AEPD acționează ca organism care investighează plângeri și colaborează îndeaproape cu autoritățile naționale de supraveghere[824]. AEPD și autoritățile naționale de supraveghere se reunesc cel puțin de două ori pe an în cadrul Consiliului de cooperare, care are rol consultativ[825]. Statele membre au obligația de a înființa prin lege o autoritate de supraveghere care are competența de a monitoriza caracterul legal al transferului, al extragerii și al oricărei comunicări de date cu caracter personal efectuate de statul membru în cauză către Europol[826]. De

818 *Ibidem*, articolul 30 alineatul (2).

819 *Ibidem*, articolul 30 alineatul (3).

820 *Ibidem*, articolul 31.

821 *Ibidem*, articolul 24, respectiv articolul 25.

822 *Ibidem*, articolul 35.

823 Regulamentul Europol, articolul 42.

824 *Ibidem*, articolele 43 și 44.

825 *Ibidem*, articolul 45.

826 *Ibidem*, articolul 42 alineatul (1).

asemenea, statele membre trebuie să se asigure că autoritatea națională de supraveghere poate acționa cu deplină independență în cadrul îndeplinirii sarcinilor și atribuțiilor sale în temeiul Regulamentului Europol[827]. În scopul verificării legalității prelucrării datelor, al automonitorizării și al asigurării integrității și securității datelor, Europol ține jurnale sau documente privind activitățile sale de prelucrare a datelor. Aceste jurnale conțin informații privind operațiunile de prelucrare prin sisteme de prelucrare automată, legate de colectarea, modificarea, consultarea, divulgarea, combinarea sau ștergerea datelor[828].

Se pot introduce acțiuni împotriva deciziilor AEPD în fața CJUE[829]. Orice persoană care a suferit un prejudiciu ca urmare a unei operațiuni ilegale de prelucrare a datelor are dreptul de a primi despăgubiri pentru prejudiciul suferit, fie de la Europol, fie de la statul membru răspunzător, prin introducerea unei acțiuni în fața CJUE în primul caz sau în fața instanței naționale competente în al doilea caz[830]. În plus, un grup mixt de control parlamentar specializat (JPSG), instituit împreună de parlamentele naționale și de Parlamentul European, poate monitoriza activitățile Europol[831]. Orice persoană are dreptul de acces la orice date cu caracter personal pe care Europol le poate deține despre această persoană, precum și dreptul de a solicita ca aceste date cu caracter personal să fie verificate, corectate sau șterse. Aceste drepturi pot face obiectul unor derogări și limitări.

827 *Ibidem*, articolul 42 alineatul (1).

828 *Ibidem*, articolul 40.

829 *Ibidem*, articolul 48.

830 *Ibidem*, articolul 50.

831 *Ibidem*, articolul 51.

Eurojust

Eurojust, înființată în 2002, este un organism UE cu sediul la Haga. Acesta promovează cooperarea judiciară în materie de investigare și urmărire penală a infracțiunilor grave care implică cel puțin două state membre[832]. Eurojust are următoarele competențe:

- stimularea și îmbunătățirea coordonării în materie de investigații și urmăriri penale între autoritățile competente ale diferitelor state membre;

- facilitarea executării cererilor și deciziilor privind cooperarea judiciară.

Funcțiile Eurojust sunt îndeplinite de membrii naționali. Fiecare stat membru deleagă la Eurojust un judecător sau un procuror, al cărui statut este reglementat de legislația națională și care este împuternicit cu competențele adecvate pentru a îndeplini sarcinile necesare pentru stimularea și îmbunătățirea cooperării judiciare. În plus, membrii naționali acționează în comun ca un colegiu pentru a îndeplini sarcinile speciale ale Eurojust.

Eurojust poate prelucra date cu caracter personal în măsura în care acest lucru este necesar pentru realizarea obiectivelor sale. Prelucrarea se limitează însă la informații specifice referitoare la persoane care fie sunt suspectate că au comis sau că au participat la comiterea unei infracțiuni care ține de competența Eurojust, fie au fost condamnate pentru o astfel de infracțiune. Eurojust poate prelucra, de asemenea, anumite informații referitoare la martori sau victime ale infracțiunilor care țin de competența Eurojust[833]. În situații excepționale, Eurojust poate prelucra, pentru o perioadă limitată de timp, date cu caracter personal mai extinse cu privire la împrejurările săvârșirii unei infracțiuni, în cazul în care datele respective sunt direct relevante pentru o investigație în curs de desfășurare. În sfera de aplicare a competențelor sale, Eurojust poate coopera cu alte instituții, organisme și agenții ale UE și poate face schimb de date cu caracter personal cu acestea. Eurojust poate, de

832 Decizia 2002/187/JAI a Consiliului din 28 februarie 2002 de instituire a Eurojust în scopul consolidării luptei împotriva formelor grave de criminalitate, JO 2002 L 63; Decizia 2003/659/JAI a Consiliului din 18 iunie 2003 de modificare a Deciziei 2002/187/JAI de instituire a Eurojust în scopul consolidării luptei împotriva formelor grave de criminalitate, JO 2003 L 44; Decizia 2009/426/JAI a Consiliului din 16 decembrie 2008 privind consolidarea Eurojust și de modificare a Deciziei 2002/187/JAI de instituire a Eurojust în scopul consolidării luptei împotriva formelor grave de criminalitate, JO 2009 L 138 (Deciziile Eurojust).

833 Versiunea consolidată a Deciziei 2002/187/JAI a Consiliului, astfel cum a fost modificată prin Decizia 2003/659/JAI a Consiliului și prin Decizia 2009/426/JAI a Consiliului, articolul 15 alineatul (2).

asemenea, să coopereze și să facă schimb de date cu caracter personal cu țări terțe și organizații internaționale.

În ceea ce privește protecția datelor, Eurojust trebuie să garanteze un nivel de protecție cel puțin echivalent cu principiile Convenției 108 modernizate, cu modificările ulterioare. În cazul schimbului de date, trebuie respectate norme și restricții specifice, care sunt puse în aplicare fie în temeiul unui acord de cooperare, fie al unui acord de lucru în conformitate cu Deciziile Eurojust ale Consiliului și cu Normele Eurojust privind protecția datelor[834].

În cadrul Eurojust a fost înființat un organ de control comun, având sarcina de a monitoriza prelucrarea datelor cu caracter personal efectuată de Eurojust. Persoanele fizice pot apela la organul de control comun în cazul în care nu sunt mulțumite de decizia Eurojust referitoare la o cerere de acces sau de blocare a accesului la datele cu caracter personal sau de rectificare ori ștergere a acestora. În cazul în care prelucrează date cu caracter personal în mod ilegal, Eurojust va răspunde în conformitate cu legislația națională a statului membru în care se află sediul central al acestui organism, și anume Țările de Jos, pentru orice prejudiciu cauzat persoanei vizate.

Perspective

Comisia Europeană a prezentat o propunere de regulament de reformare a Eurojust în iulie 2013. Această propunere a fost însoțită de o propunere de înființare a Parchetului European (vezi mai jos). Acest regulament urmărește să eficientizeze funcțiile și structura Eurojust în acord cu Tratatul de la Lisabona. În plus, obiectivul reformei este de a stabili o distincție clară între sarcinile operative ale Eurojust, asigurate de colegiul Eurojust, și sarcinile sale administrative. Acest lucru va permite statelor membre să se concentreze mai mult pe sarcinile operative. Va fi creat un nou consiliu executiv, care să sprijine colegiul în ceea ce privește îndeplinirea sarcinilor administrative[835].

834 Regulament de procedură privind prelucrarea și protecția datelor cu caracter personal la Eurojust, JO 2005 C 68/01, 19 martie 2005, p. 1.

835 Vezi pagina web dedicată Eurojust a Comisiei Europene.

Parchetul European

Statele membre au competență exclusivă în domeniul urmăririi penale a infracțiunilor de fraudă și de utilizare necorespunzătoare a bugetului UE, care au, de asemenea, posibile implicații transfrontaliere. Importanța investigării, urmăririi penale și deferirii în justiție a făptuitorilor acestor infracțiuni a crescut, în special având în vedere criza economică în curs[836]. Comisia Europeană a propus un regulament privind înființarea unui Parchet European independent (EPPO)[837] cu scopul de a combate infracțiunile care afectează interesele financiare ale UE. EPPO va fi instituit prin intermediul procedurii de cooperare consolidată, care permite unui număr de minimum nouă state membre să stabilească o cooperare avansată într-un domeniu din cadrul structurilor UE fără ca celelalte state membre ale UE să fie implicate[838]. Belgia, Bulgaria, Cehia, Cipru, Croația, Estonia, Finlanda, Franța, Germania, Grecia, Letonia, Lituania, Luxemburg, Portugalia, România, Slovenia, Slovacia și Spania au aderat la cooperarea consolidată; Austria și Italia și-au exprimat intenția de a adera[839].

EPPO va avea competența de a investiga și de a urmări penal infracțiuni de fraudă la nivelul UE și alte infracțiuni care afectează interesele financiare ale UE, cu scopul de a coordona eficient investigațiile și urmăririle penale din cadrul diferitelor ordini juridice naționale și de a îmbunătăți utilizarea resurselor și schimbul de informații la nivel european[840].

EPPO va fi condus de un Procuror European, cu cel puțin câte un procuror european delegat, localizat în fiecare stat membru, responsabil pentru desfășurarea anchetelor și urmăririlor penale în statul membru respectiv.

Propunerea stabilește garanții puternice de protecție a drepturilor persoanelor implicate în investigațiile EPPO, astfel cum sunt prevăzute în dreptul intern, în dreptul UE și în Carta drepturilor fundamentale a UE. Măsurile de cercetare care intervin

836 Vezi Propunerea a Comisiei Europene de regulament al Consiliului de instituire a Parchetului European, COM(2013) 534 final din 17 iulie 2013, Bruxelles, p. 1, și pagina web privind EPPO a Comisiei.

837 Propunerea a Comisiei Europene de regulament al Consiliului de instituire a Parchetului European, COM(2013) 534 final din 17 iulie 2013, Bruxelles.

838 Tratatul privind funcționarea UE, articolul 86 alineatul (1) și articolul 329 alineatul (1).

839 Vezi Comunicatul de presă din 8 iunie 2017 al Consiliului Uniunii Europene (2017), *20 de state membre sunt de acord asupra detaliilor privind crearea unui Parchet European (EPPO)*.

840 Propunerea din 17 iulie 2013 a Comisiei Europene de regulament al Consiliului de instituire a Parchetului European, COM(2013) 534 final din 17 iulie 2013, Bruxelles, p. 1 și p. 51. Vezi, de asemenea, pagina web privind EPPO a Comisiei.

în cea mai mare măsură asupra drepturilor fundamentale vor necesita o autorizare prealabilă din partea unei instanțe naționale[841]. Investigațiile EPPO vor face obiectul controlului jurisdicțional al instanțelor naționale[842].

Regulamentul privind protecția datelor de către instituțiile UE[843] se va aplica prelucrării datelor administrative cu caracter personal efectuate de EPPO. Pentru prelucrarea datelor cu caracter personal legate de aspecte operative, cum ar fi cele din cadrul Europol, EPPO va aplica un regim autonom de protecție a datelor similar cu cel care reglementează activitățile Europol și Eurojust, având în vedere că exercitarea funcțiilor EPPO implică prelucrarea datelor cu caracter personal în colaborare cu autoritățile de aplicare a legii și de urmărire penală de la nivelul statelor membre. Normele de protecție a datelor în cadrul EPPO sunt, prin urmare, aproape identice cu normele prevăzute de Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale. În conformitate cu propunerea de înființare a EPPO, prelucrarea datelor cu caracter personal trebuie să respecte principiile legalității, echității, limitărilor legate de scop, reducerii la minimum a datelor, exactității, integrității și confidențialității. EPPO trebuie să facă, pe cât posibil, o distincție clară între datele cu caracter personal ale diferitelor categorii de persoane vizate, cum ar fi persoanele condamnate pentru o infracțiune, persoanele care sunt doar suspecți, victime și martori. De asemenea, EPPO trebuie să depună eforturi pentru a examina calitatea datelor cu caracter personal prelucrate și pentru a diferenția, pe cât posibil, datele cu caracter personal bazate pe fapte de datele cu caracter personal bazate pe evaluări personale.

Propunerea conține dispoziții privind drepturile persoanelor vizate, în special dreptul de a fi informate, dreptul de acces la datele lor cu caracter personal, dreptul de a obține rectificarea, ștergerea și restricționarea prelucrării, și prevede că aceste drepturi pot fi, de asemenea, exercitate indirect prin intermediul AEPD. Aceasta include, de asemenea, principiile securității prelucrării și responsabilității, impunând ca EPPO să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate adecvat în raport cu riscurile pe care le prezintă prelucrarea, să țină evidența tuturor activităților de prelucrare și să efectueze o evaluare a impactului asupra protecției datelor înainte de prelucrare, în cazul în care un tip de

841 Propunerea din 17 iulie 2013 a Comisiei Europene de regulament al Consiliului de instituire a Parchetului European, COM(2013) 534 final din 17 iulie 2013, Bruxelles, articolul 26 alineatul (4).

842 *Ibidem*, articolul 36.

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

prelucrare (de exemplu, prelucrarea care implică utilizarea de noi tehnologii) poate genera un risc ridicat pentru drepturile persoanelor. În sfârșit, propunerea prevede desemnarea de către colegiu a unui responsabil cu protecția datelor, care trebuie să se implice în mod corespunzător în toate aspectele legate de protecția datelor cu caracter personal și trebuie să asigure respectarea de către EPPO a legislației aplicabile în materie de protecție a datelor.

8.3.2. Protecția datelor în cadrul sistemelor informatice comune de la nivelul UE

Pe lângă schimbul de date între statele membre și înființarea de autorități specializate ale UE pentru combaterea criminalității transfrontaliere – precum Europol, Eurojust și EPPO – au fost înființate mai multe sisteme informatice comune la nivelul UE pentru a permite și a facilita cooperarea și schimbul de date între autoritățile naționale și UE competente în scopurile specificate din domeniile apărării frontierelor, imigrației și azilului și sectorul vamal. Întrucât spațiul Schengen a fost creat inițial printr-un acord internațional care funcționa independent de legislația UE, Sistemul de Informații Schengen (SIS) a fost elaborat pe baza unor acorduri multilaterale și a fost ulterior adus sub incidența legislației UE. Sistemul de informații privind vizele (VIS), Eurodac, Eurosur și Sistemul de informații al vămilor (SIV) au fost create ca instrumente reglementate de legislația UE.

Supravegherea acestor sisteme este asigurată în comun de autoritățile naționale de supraveghere și de AEPD. Pentru a asigura un nivel ridicat de protecție, aceste autorități colaborează în cadrul grupurilor de coordonare a supravegherii (GCS), care au ca obiect supravegherea următoarelor sisteme TI la scară largă: 1) Eurodac; 2) Sistemul de informații privind vizele; 3) Sistemul de Informații Schengen; 4) Sistemul de informații al vămilor și 5) Sistemul de informare al pieței interne[844]. În general, GCS se întrunesc de două ori pe an, sub autoritatea unui președinte ales, și adoptă orientări, discută cazurile transfrontaliere sau adoptă cadre comune pentru inspecții.

Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA)[845], înființată în anul 2012, este responsabilă pentru gestionarea operațională a Sistemului de

844 Vezi pagina web privind coordonarea supravegherii a Autorității Europene pentru Protecția Datelor.

845 Regulamentul (UE) nr. 1077/2011 al Parlamentului European și al Consiliului din 25 octombrie 2011 de instituire a Agenției europene pentru gestionarea operațională a sistemelor informatice la scară largă în spațiul de libertate, securitate și justiție, JO 2011 L 286.

informații Schengen de a doua generație (SIS II), a Sistemului de informații privind vizele (VIS) și a Eurodac. Sarcina de bază a eu-LISA este aceea de a asigura funcționarea eficientă, sigură și continuă a sistemelor informatice. Eu-LISA este responsabilă, de asemenea, pentru adoptarea măsurilor necesare de asigurare a securității sistemelor și a securității datelor.

Sistemul de Informații Schengen

În anul 1985, mai multe state membre ale fostei Comunități Europene au încheiat Acordul între statele Uniunii Economice Benelux, Germania și Franța privind eliminarea treptată a controalelor la frontierele lor comune (Acordul Schengen), cu scopul de a crea, în interiorul spațiului Schengen, o zonă de liberă circulație a persoanelor, nestingherită de controale la frontieră[846]. Pentru a contracara amenințarea la adresa securității publice care ar fi putut fi generată de deschiderea frontierelor, s-au instituit controale intensificate la frontierele externe ale spațiului Schengen, precum și o cooperare strânsă între autoritățile polițienești și judiciare naționale.

Ca urmare a aderării altor state la acordul Schengen, sistemul Schengen a fost în cele din urmă integrat în cadrul juridic al UE prin Tratatul de la Amsterdam[847]. Punerea în aplicare a acestei decizii a avut loc în anul 1999. Cea mai nouă versiune a Sistemului de Informații Schengen, denumită SIS II, a intrat în vigoare la 9 aprilie 2013. Aceasta deservește în prezent toate statele membre ale UE[848], precum și Elveția, Islanda, Liechtenstein și Norvegia[849]. Europol și Eurojust au, de asemenea, acces la SIS II.

SIS II constă într-un sistem central (C-SIS), un sistem național (N-SIS) în fiecare stat membru și o infrastructură de comunicații între sistemul central și sistemele naționale. C-SIS conține anumite date introduse de statele membre cu privire la persoane și obiecte. C-SIS este utilizat de autoritățile naționale de control la frontieră, de organele de poliție, autoritățile vamale, autoritățile responsabile pentru vize și

846 Acord între guvernele statelor Uniunii Economice Benelux, Republicii Federale Germania și Republicii Franceze privind eliminarea treptată a controalelor la frontierele lor comune, JO 2000 L 239.

847 Tratatul de la Amsterdam de modificare a Tratatului privind Uniunea Europeană, a tratatelor de instituire a Comunităților Europene și a altor acte conexe, JO 1997 C 340.

848 Croația, Cipru și Irlanda desfășoară activități pregătitoare pentru integrarea în SIS II, dar nu fac încă parte din acesta. Vezi informațiile privind Sistemul de Informații Schengen disponibile pe site-ul Direcției Generale Migrație și Afaceri Interne a Comisiei Europene.

849 Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație (SIS II), JO 2006 L 381, și Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II), JO 2007 L 205.

autoritățile judiciare din întregul spațiu Schengen. Statele membre utilizează copii naționale ale C-SIS, cunoscute sub numele de Sisteme naționale de informații Schengen (N-SIS), care sunt actualizate în permanență, actualizând astfel C-SIS. Există diferite tipuri de semnalări în SIS:

- persoana nu are dreptul de a intra sau de a rămâne în spațiul Schengen; sau
- persoana sau obiectul este căutat(ă) de autoritățile judiciare sau de autoritățile de aplicare a legii (de exemplu, mandate europene de arestare, cereri de control discret); sau
- persoana a fost raportată ca fiind dispărută; sau
- diverse bunuri, cum ar fi bancnote, autoturisme, autoutilitare, arme de foc și documente de identitate, au fost raportate ca fiind furate sau pierdute.

În cazul unei semnalări, se inițiază activități de urmărire prin intermediul birourilor SIRENE. SIS II are noi funcționalități, cum ar fi posibilitatea de a introduce: date biometrice, precum amprente și fotografii; categorii noi de semnalări, cum ar fi furturi de bărci, aeronave, containere sau mijloace de plată; semnalări îmbunătățite cu privire la persoane și obiecte; copii ale mandatelor europene de arestare (MEA) privind persoanele căutate pentru deținere, predare sau extrădare.

SIS II se bazează pe două acte legislative care se completează reciproc: Decizia SIS II[850] și Regulamentul SIS II[851]. Legiuitorul UE a utilizat temeiuri juridice diferite pentru adoptarea deciziei, respectiv a regulamentului. Decizia reglementează utilizarea SIS II în scopurile vizate de cooperarea polițienească și judiciară în materie penală (fostul pilon trei al UE). Regulamentul se aplică procedurilor de semnalare care se încadrează în domeniul vizelor, azilului, imigrației și altor politici legate de libera circulație a persoanelor (fostul pilon unu). Procedurile de semnalare pentru fiecare pilon trebuiau să fie reglementate prin acte legislative separate, întrucât cele două acte legislative au fost adoptate înainte de Tratatul de la Lisabona și eliminarea structurii pilonilor.

850 Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II), JO 2007 L 205.

851 Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație (SIS II), JO 2006 L 381.

Ambele acte legislative conțin norme privind protecția datelor. Decizia SIS II interzice prelucrarea datelor sensibile[852]. Prelucrarea datelor cu caracter personal intră în domeniul de aplicare al Convenției 108 modernizate[853]. În plus, persoanele au dreptul de a avea acces la datele cu caracter personal introduse în SIS II care le privesc[854].

Regulamentul SIS II reglementează condițiile și procedurile referitoare la introducerea și la prelucrarea semnalărilor privind refuzul intrării sau interdicția de ședere a resortisanților din țări terțe. Acesta stabilește, de asemenea, norme privind schimbul de informații suplimentare și complementare în scopul intrării sau șederii în statele membre[855]. Acest regulament conține, de asemenea, norme privind protecția datelor. Este interzisă prelucrarea categoriilor de date sensibile menționate la articolul 9 alineatul (1) din Regulamentul general privind protecția datelor[856]. Regulamentul SIS II prevede, de asemenea, anumite drepturi pentru persoana vizată:

- dreptul de a avea acces la datele cu caracter personal referitoare la persoana vizată[857];
- dreptul de a obține rectificarea datelor care conțin erori de fapt[858];
- dreptul de a obține ștergerea datelor stocate în mod ilegal[859];
- dreptul persoanei vizate de a fi informată în cazul în care face obiectul unei semnalări. Această informare este realizată în scris și este însoțită de o copie a deciziei naționale care stă la originea semnalării sau de o trimitere la decizia respectivă[860].

Dreptul de a fi informat nu este asigurat dacă: 1) datele cu caracter personal nu au fost obținute de la persoana vizată și comunicarea informației este imposibilă sau implică eforturi disproporționate; 2) persoana vizată deține deja informațiile; sau 3)

852 Decizia SIS II, articolul 56; Regulamentul SIS II, articolul 40.
853 Decizia SIS II, articolul 57.
854 Decizia SIS II, articolul 58; Regulamentul SIS II, articolul 41.
855 Regulamentul SIS II, articolul 2.
856 *Ibidem*, articolul 40.
857 *Ibidem*, articolul 41 alineatul (1).
858 *Ibidem*, articolul 41 alineatul (5).
859 *Ibidem*, articolul 41 alineatul (5).
860 *Ibidem*, articolul 42 alineatul (1).

legislația națională permite restrângerea acestui drept, în special, printre altele, pentru apărarea siguranței naționale sau în scopul prevenirii infracțiunilor[861].

Atât Decizia SIS II, cât și Regulamentul SIS II prevăd că dreptul persoanelor de a avea acces la datele introduse în SIS II se exercită în orice stat membru, în conformitate cu legislația statului membru respectiv[862].

Exemplu: În cauza *Dalea/Franța*[863], reclamantului nu i s-a acordat viză pentru a vizita Franța, deoarece autoritățile franceze au raportat în Sistemul de informații Schengen că reclamantului trebuie să i se refuze intrarea. Reclamantul a solicitat, fără succes, accesul la date și rectificarea sau ștergerea acestora în fața Comisiei pentru Protecția Datelor din Franța și, în cele din urmă, în fața Consiliului de Stat. CEDO a constatat că raportarea reclamantului la Sistemul de informații Schengen s-a realizat în conformitate cu legea și urmărea scopul legitim de protecție a securității naționale. Întrucât solicitantul nu a dovedit prejudiciul efectiv pe care l-a suferit ca urmare a faptului că i-a fost refuzată intrarea în spațiul Schengen și întrucât au fost instituite suficiente măsuri pentru a-l proteja împotriva deciziilor arbitrare, atingerea adusă dreptului acestuia de respectare a vieții private a fost proporțională. Prin urmare, plângerea reclamantului în temeiul articolului 8 a fost declarată inadmisibilă.

Autoritatea națională de supraveghere competentă din fiecare stat membru supraveghează sistemul N-SIS intern. Autoritatea națională de supraveghere trebuie să se asigure că auditarea operațiunilor de prelucrare a datelor în cadrul N-SIS se efectuează cel puțin o dată la patru ani[864]. Autoritățile naționale de control și AEPD cooperează și asigură o supraveghere coordonată a N-SIS, în timp ce AEPD este responsabilă pentru supravegherea C-SIS. Din motive de transparență, trebuie prezentat un raport comun de activitate Parlamentului European, Consiliului și eu-LISA o dată la doi ani. Grupul de coordonare a supravegherii (GCS) al SIS II a fost creat pentru a asigura coordonarea supravegherii SIS și se întrunește de două ori pe an. Acest grup este alcătuit din AEPD și reprezentanți ai autorităților de supraveghere din acele state membre care au implementat SIS II, precum și din Elveția, Islanda, Liechtenstein și Norvegia, întrucât, aceste state fiind membre ale spațiului Schengen, SIS se aplică

861 *Ibidem*, articolul 42 alineatul (2).

862 Regulamentul SIS II, articolul 41 alineatul (1), și Decizia SIS II, articolul 58.

863 Hotărârea CEDO din 2 februarie 2010 în cauza *Dalea/Franța*, nr. 964/07.

864 Regulamentul SIS II, articolul 44 alineatul (2), și Decizia SIS II, articolul 60 alineatul (2).

și în cazul lor[865]. Cipru, Croația și Irlanda nu fac încă parte din SIS II și, prin urmare, participă doar ca observatori la GCS. În contextul GCS, AEPD și autoritățile naționale de control cooperează activ, prin schimb de informații, asistență reciprocă în desfășurarea auditurilor și controalelor, formularea de propuneri armonizate în vederea identificării unor soluții comune pentru eventuale probleme și sensibilizarea cu privire la drepturile legate de protecția datelor[866]. De asemenea, GCS al SIS II adoptă orientări pentru a oferi asistență persoanelor vizate. Un exemplu de astfel de orientări este ghidul menit să ofere asistență persoanelor vizate în ceea ce privește exercițiul drepturilor lor de acces[867].

Perspective

În 2016, Comisia Europeană a efectuat o evaluare a SIS[868] care arată că au fost instituite mecanisme naționale care permit persoanelor vizate să aibă acces la datele lor cu caracter personal din SIS II, să obțină rectificarea și ștergerea acestora sau să obțină despăgubiri în cazul unor date inexacte. Pentru a îmbunătăți eficiența și eficacitatea SIS II, Comisia Europeană a prezentat trei propuneri de regulamente:

- un regulament privind instituirea, funcționarea și utilizarea SIS în domeniul controalelor la frontiere, care va abroga Regulamentul SIS II;

- un regulament privind instituirea, funcționarea și utilizarea SIS în domeniul cooperării polițienești și judiciare în materie penală, care va abroga, printre altele, Decizia SIS II;

- un regulament privind utilizarea SIS în scopul returnării resortisanților țărilor terțe aflați în situație de ședere ilegală.

Este important de remarcat faptul că propunerile permit prelucrarea altor categorii de date biometrice pe lângă fotografii și amprente digitale, care fac parte deja din actualul regim SIS II. Amprentele faciale, amprentele palmare și profilurile ADN vor

865 Vezi pagina web privind Sistemul de informații Schengen a Autorității Europene pentru Protecția Datelor.

866 Regulamentul SIS II, articolul 46, și Decizia SIS II, articolul 62.

867 Vezi GCS al SIS II, *The Schengen Information System. A guide for exercising the right of access* („Sistemul de informații Schengen. Ghid pentru exercițiul dreptului de acces"), disponibil pe site-ul AEPD.

868 Raport al Comisiei către Parlamentul European și Consiliu privind evaluarea Sistemului de informații Schengen de a doua generație (SIS II) în conformitate cu articolul 24 alineatul (5), articolul 43 alineatul (3) și articolul 50 alineatul (5) din Regulamentul (CE) nr. 1987/2006 și cu articolul 59 alineatul (3) și articolul 66 alineatul (5) din Decizia 2007/533/JAI, COM(2016) 880 final din 21 decembrie 2016, Bruxelles.

fi, de asemenea, stocate în baza de date SIS. În plus, în timp ce Regulamentul SIS II și Decizia SIS II prevăd posibilitatea de a căuta în sistem amprentele digitale pentru a identifica o persoană, propunerile prevăd că această căutare este obligatorie în cazul în care identitatea persoanei nu poate fi stabilită în niciun alt mod. Imaginile faciale, fotografiile și amprentele palmare vor fi folosite pentru a căuta în sistem și pentru a identifica persoanele, atunci când acest lucru devine posibil din punct de vedere tehnic. Noile norme privind atributele biometrice prezintă riscuri deosebite pentru drepturile persoanelor. În avizul său privind propunerile Comisiei[869], AEPD a precizat că datele biometrice sunt extrem de sensibile, iar introducerea lor într-o astfel de bază de date pe scară largă ar trebui să se întemeieze pe o evaluare bazată pe dovezi privind necesitatea includerii acestora în SIS. Cu alte cuvinte, trebuie demonstrată necesitatea prelucrării noilor atribute. De asemenea, AEPD a considerat că este necesar să se clarifice mai bine ce tip de informații pot fi incluse în profilul ADN. Întrucât profilul ADN poate include informații sensibile (cel mai notabil exemplu ar fi informațiile care dezvăluie problemele de sănătate), profilurile ADN stocate în SIS ar trebui să conțină „doar informațiile minime strict necesare pentru identificarea persoanelor dispărute și să excludă în mod explicit informațiile privind sănătatea, originea rasială și orice alte informații sensibile”[870]. Cu toate acestea, propunerile instituie garanții suplimentare pentru a limita colectarea și prelucrarea ulterioară a datelor la ceea ce este strict necesar și obligatoriu din punct de vedere operațional și pentru a restricționa accesul la datele respective la persoanele care au o nevoie operațională de a prelucra datele cu caracter personal[871]. De asemenea, propunerile împuternicesc eu-LISA să furnizeze statelor membre, la intervale regulate, rapoarte privind calitatea datelor, pentru a examina periodic semnalările în vederea asigurării calității datelor[872].

Sistemul de informații privind vizele

Sistemul de informații privind vizele (VIS), exploatat, de asemenea, de către eu-LISA, a fost dezvoltat pentru a sprijini punerea în aplicare a unei politici a UE comune

869 Avizul 7/2017 al AEPD din 2 mai 2017 privind noul temei juridic al Sistemului de informații Schengen.

870 *Ibidem*, punctul 22.

871 Propunere de regulament al Parlamentului European și al Consiliului privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare a Regulamentului (UE) nr. 515/2014 și de abrogare a Regulamentului (CE) nr. 1986/2006, a Deciziei 2007/533/JAI a Consiliului și a Deciziei 2010/261/UE a Comisiei, COM(2016) 883 final din 21 decembrie 2016, Bruxelles.

872 *Ibidem*, p. 15.

privind vizele[873]. VIS permite statelor Schengen să facă schimb de date privind solicitanții de vize printr-un sistem complet centralizat care conectează consulatele și ambasadele statelor Schengen situate în țări din afara UE cu punctele de trecere a frontierei externe din toate statele Schengen. VIS prelucrează datele privind cererile de viză de scurtă ședere pentru vizitarea sau tranzitarea spațiului Schengen. VIS permite autorităților de frontieră să verifice, cu ajutorul datelor biometrice, în special a amprentelor digitale, dacă persoana care prezintă o viză este titularul de drept al acesteia și să identifice persoanele fără documente sau persoanele care dețin documente false.

Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS) stabilește condițiile și procedurile de transfer al datelor cu caracter personal cu privire la cererile de viză de scurtă ședere. De asemenea, reglementează deciziile luate în legătură cu aceste cereri, printre care decizia de anulare, retragere sau prelungire a vizei[874]. Regulamentul VIS vizează în principal datele referitoare la solicitant, la vizele acestuia, fotografiile, amprentele digitale, legăturile cu cereri anterioare, dosarele de cerere ale persoanelor care însoțesc solicitantul sau datele referitoare la persoanele care îl invită pe solicitant[875]. Accesul la VIS în vederea introducerii, modificării sau ștergerii datelor este limitat exclusiv la autoritățile responsabile în domeniul vizelor, în timp ce accesul pentru consultarea datelor se acordă autorităților responsabile în domeniul vizelor și autorităților competente pentru controalele la punctele de trecere a frontierei externe, controalele în materie de imigrație și de azil.

În anumite condiții, autoritățile polițienești naționale competente și Europol pot solicita accesul la datele introduse în VIS în scopul prevenirii, depistării sau cercetării

873 Decizia Consiliului din 8 iunie 2004 de instituire a Sistemului de Informații privind vizele (SIV), JO 2004 L 213; Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS), JO 2008 L 218; Decizia 2008/633/JAI a Consiliului din 23 iunie 2008 privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave, JO 2008 L 218.

874 Regulamentul VIS, articolul 1.

875 Articolul 5 din Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS), JO 2008 L 218.

infracțiunilor de terorism și a altor infracțiuni[876]. Întrucât VIS a fost conceput ca instrument de sprijinire a punerii în aplicare a politicii comune în materie de vize, principiul limitărilor legate de scop – care, după cum se explică la capitolul 3.2, impune ca datele cu caracter personal să fie prelucrate numai în scopuri determinate, explicite și legitime, să fie adecvate și relevante și să nu depășească ceea ce este necesar în raport cu scopurile în care sunt prelucrate – ar fi încălcat dacă VIS s-ar transforma într-un instrument de aplicare a legii. Din acest motiv, autorităților naționale de aplicare a legii și Europol nu li se acordă acces generalizat la baza de date VIS. Accesul poate fi acordat numai de la caz la caz și trebuie să fie însoțit de garanții stricte. Condițiile și garanțiile pentru accesul la VIS și consultarea acestuia de către aceste autorități au fost reglementate prin Decizia 2008/633/JAI a Consiliului[877].

În plus, Regulamentul VIS prevede drepturile persoanelor vizate. Acestea sunt:

- Dreptul de a fi informat de statul membru responsabil cu privire la identitatea și datele de contact ale operatorului de date responsabil pentru prelucrarea datelor cu caracter personal în statul membru respectiv, scopurile pentru care datele cu caracter personal ale persoanei vizate în cauză vor fi prelucrate în VIS, categoriile de persoane cărora le pot fi transmise datele (destinatarii datelor) și perioada de păstrare a datelor. În plus, solicitanții de vize trebuie să fie informați cu privire la caracterul obligatoriu al colectării datelor lor cu caracter personal în VIS pentru examinarea cererii, iar statele membre trebuie, de asemenea, să îi informeze cu privire la existența dreptului lor de acces la datele care îi privesc și a dreptului de a solicita rectificarea sau ștergerea acestor date și cu privire la procedurile care le permit să își exercite aceste drepturi[878].

- Dreptul persoanelor vizate de a avea acces la datele înregistrate în VIS care le privesc[879].

- Dreptul de a obține rectificarea datelor inexacte[880].

- Dreptul de a obține ștergerea datelor stocate în mod ilegal[881].

876 Decizia 2008/633/JAI a Consiliului din 23 iunie 2008 privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave, JO 2008 L 218.

877 *Ibidem*.

878 Regulamentul VIS, articolul 37.

879 *Ibidem*, articolul 38 alineatul (1).

880 *Ibidem*, articolul 38 alineatul (2).

881 *Ibidem*, articolul 38 alineatul (2).

GCS al VIS a fost înființat pentru a asigura supravegherea VIS. Acesta este compus din reprezentanți ai AEPD și ai autorităților naționale de supraveghere, care se reunesc de două ori pe an. Grupul este format din reprezentanți proveniți din cele 28 de state membre ale UE și din Elveția, Islanda, Liechtenstein și Norvegia.

Eurodac

Eurodac este abrevierea pentru „Sistemul dactiloscopic european”[882]. Este vorba despre un sistem centralizat care conține datele dactiloscopice ale resortisanților țărilor terțe și ale apatrizilor care solicită azil într-unul dintre statele membre ale UE[883]. Sistemul a intrat în funcțiune în ianuarie 2003, odată cu adoptarea Regulamentului (CE) nr. 2725/2000 al Consiliului; o reformare a acestuia a intrat în vigoare în 2015. Scopul său este, în primul rând, de a contribui la determinarea statului membru care ar trebui să fie responsabil pentru examinarea unei anumite cereri de azil în temeiul Regulamentului (CE) nr. 604/2013. Acest regulament stabilește criteriile și mecanismele de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid (Regulamentul Dublin III)[884]. Datele cu caracter personal din Eurodac servesc în principal scopul de a facilita aplicarea Regulamentului Dublin III[885].

Autoritățile naționale de aplicare a legii și Europol au posibilitatea de a compara amprentele digitale legate de anchete penale cu amprentele conținute în Eurodac, dar numai în scopul prevenirii, depistării sau investigării infracțiunilor de terorism

882 Vezi pagina web privind Eurodac a Autorității Europene pentru Protecția Datelor.

883 Regulamentul (CE) nr. 2725/2000 al Consiliului din 11 decembrie 2000 privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Convenției de la Dublin, JO 2000 L 316; Regulamentul (CE) nr. 407/2002 al Consiliului din 28 februarie 2002 de stabilire a anumitor norme de punere în aplicare a Regulamentului (CE) nr. 2725/2000 privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Convenției de la Dublin, JO 2002 L 62 (Regulamentele Eurodac); Regulamentul (UE) nr. 603/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid și privind cererile autorităților de aplicare a legii din statele membre și a Europol de comparare a datelor Eurodac în scopul asigurării respectării aplicării legii și de modificare a Regulamentului (UE) nr. 1077/2011 de instituire a Agenției europene pentru gestionarea operațională a sistemelor informatice la scară largă, în spațiul de libertate, securitate și justiție (Regulamentul de reformare a Eurodac), JO 2013 L 180, p. 1.

884 Regulamentul (UE) nr. 604/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid, JO 2013 L 180 (Regulamentul Dublin III).

885 Regulamentul de reformare a Eurodac, JO 2013 L 180, p. 1, articolul 1 alineatul (1).

sau a altor infracțiuni grave. Întrucât Eurodac a fost conceput ca instrument de sprijinire a punerii în aplicare a politicii UE în domeniul azilului, iar nu ca instrument de aplicare a legii, autoritățile de aplicare a legii nu au acces la această bază de date decât în cazuri specifice, în circumstanțe specifice și în condiții stricte[886]. Pentru utilizarea ulterioară a datelor în scopul aplicării legii se aplică Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale, în timp ce datele utilizate în scopul principal al facilitării aplicării Regulamentului Dublin III sunt protejate în temeiul Regulamentului general privind protecția datelor. Este interzis transferul ulterior al datelor cu caracter personal obținute de un stat membru sau de Europol în temeiul Regulamentului de reformare a Eurodac către orice țară terță, organizație internațională sau entitate privată constituită pe teritoriul sau în afara UE[887].

Eurodac constă într-o unitate centrală, exploatată de eu-LISA, pentru stocarea și compararea amprentelor digitale și un sistem pentru transmiterea de date electronice între statele membre și baza de date centrală. Statele membre prelevă și transmit amprentele digitale ale fiecărei persoane cu vârsta de cel puțin 14 ani care solicită azil pe teritoriul lor și ale fiecărui resortisant al unei țări terțe sau apatrid cu vârsta de cel puțin 14 ani care este reținut pentru trecerea neautorizată a frontierei externe a acestora. Statele membre pot, de asemenea, să preleve și să transmită amprentele digitale ale resortisanților din afara UE sau ale apatrizilor identificați ca locuind pe teritoriul acestora fără permisiune.

Chiar dacă orice stat membru poate consulta Eurodac și poate solicita comparări cu datele dactiloscopice, numai statul membru care a prelevat amprentele digitale și le-a transmis către unitatea centrală are dreptul de a modifica datele prin corectarea sau completarea acestora sau de a le șterge[888]. Eu-LISA păstrează evidența tuturor operațiunilor de prelucrare a datelor pentru a monitoriza protecția datelor și pentru a asigura securitatea datelor[889]. Autoritățile naționale de supraveghere asistă și oferă consiliere persoanelor vizate cu privire la exercitarea drepturilor lor[890]. Colectarea și transmiterea datelor dactiloscopice fac obiectul controlului jurisdicțional al

886 *Ibidem*, articolul 1 alineatul (2).

887 *Ibidem*, articolul 35.

888 *Ibidem*, articolul 27.

889 *Ibidem*, articolul 28.

890 *Ibidem*, articolul 29.

instanțelor naționale[891]. Regulamentul UE privind protecția datelor de către instituțiile UE[892] și supravegherea de către AEPD se aplică activităților de prelucrare privind Eurodac desfășurate de eu-LISA în sistemul central[893]. Dacă o persoană suferă un prejudiciu ca rezultat al unei operațiuni de prelucrare ilicită sau al unui act incompatibil cu Regulamentul Eurodac, respectiva persoană are dreptul la despăgubire din partea statului membru responsabil pentru prejudiciu[894]. Trebuie subliniat totuși că solicitanții de azil sunt o categorie de persoane deosebit de vulnerabile, care au adesea în urmă o călătorie lungă și riscantă. Din cauza vulnerabilității lor și a situației precare în care se află adesea în timp ce li se examinează cererile de azil, exercitarea drepturilor lor, inclusiv a dreptului la despăgubiri, se poate dovedi dificilă în practică.

Pentru a utiliza Eurodac în scopul aplicării legii, statele membre trebuie să desemneze autoritățile care vor avea dreptul să solicite accesul la sistem, precum și autoritățile care vor verifica legalitatea cererilor de comparare a datelor[895]. Accesul autorităților naționale și al Europol la datele dactiloscopice din Eurodac face obiectul unor condiții foarte stricte. Autoritatea solicitantă trebuie să prezinte o cerere electronică motivată numai după ce a comparat datele cu cele disponibile în alte sisteme de informații, cum ar fi bazele de date dactiloscopice naționale și VIS. Trebuie să existe o preocupare preponderentă în materie de securitate publică, prin care să se asigure caracterul proporțional al comparării. Compararea trebuie să fie realmente necesară, să se refere la un caz specific și trebuie să existe motive întemeiate pentru a considera că această comparare va contribui în mod substanțial la prevenirea, depistarea sau investigarea oricăreia dintre infracțiunile în cauză, în special atunci când există o suspiciune întemeiată că suspectul, făptuitorul sau victima unei infracțiuni de terorism sau altei infracțiuni grave se încadrează într-o categorie care face obiectul colectării amprentelor digitale în cadrul sistemului Eurodac. Compararea trebuie efectuată exclusiv cu date dactiloscopice. Europol trebuie, de asemenea, să obțină autorizare din partea statului membru care a colectat datele dactiloscopice.

891 *Ibidem*, articolul 29.

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

893 Regulamentul de reformare a Eurodac, JO 2013 L 180, p. 1, articolul 31.

894 *Ibidem*, articolul 37.

895 Roots, L. (2015), „The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination" („Noul Regulament EURODAC: amprentele digitale ca sursă de discriminare informală"), *Baltic Journal of European Studies, Tallinn University of Technology*, vol. 5, nr. 2, pp. 108-129.

Datele cu caracter personal stocate în Eurodac care se referă la solicitanții de azil sunt păstrate timp de zece ani de la data la care au fost prelevate amprentele digitale, cu excepția cazului în care persoana vizată obține cetățenia unui stat membru al UE. În acest caz, datele trebuie șterse imediat. Datele referitoare la resortisanții străini reținuți pentru trecerea ilegală a frontierei externe sunt stocate timp de 18 luni. Aceste date trebuie șterse imediat în cazul în care persoana vizată primește un permis de ședere, părăsește teritoriul UE sau obține cetățenia unui stat membru. Datele persoanelor cărora li s-a acordat azilul rămân disponibile timp de trei ani pentru comparare în contextul prevenirii, depistării și investigării infracțiunilor de terorism și a altor infracțiuni grave.

Pe lângă toate statele membre ale UE, Elveția, Islanda, Liechtenstein și Norvegia utilizează, de asemenea, Eurodac în temeiul unor acorduri internaționale.

GCS al Eurodac a fost înființat pentru a asigura supravegherea Eurodac. Acesta este compus din reprezentanți ai AEPD și ai autorităților naționale de supraveghere, care se reunesc de două ori pe an. Grupul este format din reprezentanți proveniți din cele 28 de state membre ale UE și din Elveția, Islanda, Liechtenstein și Norvegia[896].

Perspective

În mai 2016, Comisia a emis o propunere privind o nouă reformare a Regulamentului Eurodac, ca parte a unei reforme care vizează îmbunătățirea funcționării sistemului european comun de azil (SECA)[897]. Reformarea propusă este importantă, deoarece va extinde în mod semnificativ sfera de aplicare a bazei inițiale de date Eurodac. Sistemul Eurodac a fost creat inițial pentru a sprijini punerea în aplicare a SECA prin furnizarea de probe dactiloscopice care să permită determinarea statului membru responsabil pentru examinarea unei cereri de azil depuse în UE. Reformarea propusă va extinde sfera de aplicare a bazei de date la facilitarea returnării migranților în situație neregulamentară[898]. Autoritățile naționale vor putea consulta baza de date în scopul

896 Vezi pagina web privind Eurodac a Autorității Europene pentru Protecția Datelor.

897 Propunere de regulament al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac" pentru compararea amprentelor digitale în scopul aplicării eficiente a [Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid], al identificării unui resortisant al unei țări terțe sau a unui apatrid în situație neregulamentară și privind cererile de comparare cu datele Eurodac prezentate de autoritățile de aplicare a legii din statele membre și de Europol în scopul asigurării respectării aplicării legii (reformare), COM(2016) 272 final din 4 mai 2016.

898 Vezi expunerea de motive a propunerii, p. 3.

identificării resortisanților țărilor terțe aflați în UE într-o situație neregulamentară sau care au intrat în UE ilegal, pentru a obține probe care să ajute statele membre cu procesul de returnare a acestor persoane. În plus, în timp ce regimul juridic în vigoare impune doar colectarea și stocarea amprentelor digitale, propunerea introduce prelevarea imaginilor faciale[899] ale persoanelor, care constituie un alt tip de date biometrice. Propunerea vizează, de asemenea, reducerea vârstei minime a copiilor de la care este admisă prelevarea de date biometrice la șase ani[900] în loc de 14 ani, aceasta din urmă fiind vârsta minimă prevăzută de regulamentul din 2013. Domeniul de aplicare extins al propunerii înseamnă că aceasta va constitui o ingerință în drepturile la respectarea vieții private și la protecția datelor mai multor persoane care pot fi incluse în baza de date. Pentru a contrabalansa această ingerință, propunerea și amendamentele propuse de Comisia LIBE[901] a Parlamentului European urmăresc să consolideze cerințele privind protecția datelor. La momentul redactării manualului, discuțiile privind propunerea în cadrul Parlamentului și al Consiliului erau în curs de desfășurare.

Eurosur

Sistemul european de supraveghere a frontierelor (Eurosur)[902] este conceput pentru a consolida controlul frontierelor externe ale spațiului Schengen prin prevenirea, depistarea și combaterea imigrației ilegale și a criminalității transfrontaliere. Scopul acestuia este de a îmbunătăți schimbul de informații și cooperarea operațională între centrele naționale de coordonare și Frontex, agenția UE responsabilă pentru

899 Propunere de regulament al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a [Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid], al identificării unui resortisant al unei țări terțe sau a unui apatrid în situație neregulamentară și privind cererile de comparare cu datele Eurodac prezentate de autoritățile de aplicare a legii din statele membre și de Europol în scopul asigurării respectării aplicării legii (reformare), COM(2016) 272 final din 4 mai 2016, articolul 2 alineatul (1).

900 *Ibidem*, articolul 2 alineatul (2).

901 *Raportul* Parlamentului European referitor la propunerea de regulament al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a [Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid], al identificării unui resortisant al unei țări terțe sau a unui apatrid în situație neregulamentară și privind cererile de comparare cu datele Eurodac prezentate de autoritățile de aplicare a legii din statele membre și de Europol în scopul asigurării respectării aplicării legii (reformare), PE 597.620v03-00, 9 iunie 2017.

902 Regulamentul (UE) nr. 1052/2013 al Parlamentului European și al Consiliului din 22 octombrie 2013 de instituire a Sistemului european de supraveghere a frontierelor (Eurosur), JO 2013 L 295.

dezvoltarea și aplicarea noului concept de gestionare integrată a frontierelor[903]. Obiectivele sale generale sunt:

- reducerea numărului de imigranți în situație neregulamentară care intră nedetectați în UE;
- reducerea numărului de decese în rândul imigranților în situație neregulamentară prin salvarea mai multor vieți pe mare;
- sporirea securității interne a UE în ansamblu prin contribuția la prevenirea criminalității transfrontaliere[904].

Eurosur este operațional din 2 decembrie 2013 în toate statele membre cu frontiere externe, iar din data de 1 decembrie 2014 a devenit operațional și în celelalte state membre. Regulamentul se aplică supravegherii frontierelor externe terestre, maritime și aeriene ale statelor membre. Eurosur face schimb de date cu caracter personal și prelucrează astfel de date într-o măsură foarte limitată, întrucât schimbul de date între statele membre și Frontex se limitează la numerele de identificare ale navelor. Eurosur face schimb de informații operative, cum ar fi localizarea patrulelor și a incidentelor și, ca regulă generală, informațiile comunicate nu pot include date cu caracter personal[905]. În cazurile excepționale în care se fac schimburi de date cu caracter personal în cadrul Eurosur, regulamentul prevede că se aplică integral cadrul juridic general al UE privind protecția datelor[906].

Prin urmare, Eurosur asigură dreptul la protecția datelor, și anume prin faptul că schimburile de date cu caracter personal trebuie să respecte criteriile și garanțiile

903 Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului din 14 septembrie 2016 privind Poliția de frontieră și garda de coastă la nivel european și de modificare a Regulamentului (UE) 2016/399 al Parlamentului European și al Consiliului și de abrogare a Regulamentului (CE) nr. 863/2007 al Parlamentului European și al Consiliului, a Regulamentului (CE) nr. 2007/2004 al Consiliului și a Deciziei 2005/267/CE a Consiliului, JO 2016 L 251.

904 Vezi, de asemenea: Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor analizând crearea unui sistem european de supraveghere a frontierelor (Eurosur), COM(2008) 68 final din 13 februarie 2008, Bruxelles; Documentul de lucru al serviciilor Comisiei intitulat „Evaluarea impactului care însoțește propunerea de regulament al Parlamentului European și al Consiliului de instituire a Sistemului european de supraveghere a frontierelor (Eurosur), SEC(2011) 1536 final, Bruxelles, 12 decembrie 2011, p. 18.

905 Comisia Europeană, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell* („Eurosur: Protejarea frontierelor externe ale spațiului Schengen – protejarea vieților migranților. EUROSUR în câteva cuvinte"), 29 noiembrie 2013.

906 Regulamentul 1052/2013, considerentul 13 și articolul 13.

stabilite de Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale și de Regulamentul general privind protecția datelor[907].

Sistemul de informații al vămilor

Un alt important sistem comun de informații instituit la nivelul UE este Sistemul de informații al vămilor (SIV)[908]. În cadrul instituirii unei piețe interne, toate controalele și formalitățile legate de mărfurile care circulă pe teritoriul UE au fost eliminate, ceea ce a condus la creșterea riscului de fraudă. Acest risc a fost contracarat prin intensificarea cooperării între administrațiile vamale ale statelor membre. Scopul SIV este acela de a asista statele membre în prevenirea, investigarea și urmărirea penală a încălcărilor grave ale legislației vamale și agricole naționale și UE. SIV a fost instituit prin două acte legislative cu temeiuri juridice diferite: Regulamentul (CE) nr. 515/97 al Consiliului se referă la cooperarea dintre diferitele autorități administrative naționale pentru combaterea fraudei în contextul uniunii vamale și al politicii agricole comune, în timp ce Decizia 2009/917/JAI a Consiliului vizează acordarea de asistență pentru prevenirea, investigarea și urmărirea penală a încălcărilor grave ale legislației vamale. Aceasta înseamnă că SIV nu privește doar aplicarea legii.

Informațiile conținute în SIV cuprind date cu caracter personal referitoare la mărfuri, mijloace de transport, societăți comerciale, persoane, articole și lichidități reținute, puse sub sechestru sau confiscate. Categoriile de date care pot fi prelucrate sunt definite în mod clar și includ numele, cetățenia, sexul, locul și data nașterii persoanelor în cauză, motivul introducerii datelor acestora în sistem și numărul de înmatriculare al mijlocului de transport[909]. Aceste informații pot fi utilizate exclusiv în scopuri de observare, informare sau efectuare de controale specifice sau de analize operaționale sau strategice privind persoanele suspectate de încălcarea dispozițiilor vamale.

Accesul la SIV se acordă autorităților naționale din domeniul vamal, fiscal, agricol, polițienesc și al sănătății publice, precum și Europol și Eurojust.

907 *Ibidem*, considerentul 13 și articolul 13.

908 Actul Consiliului din 26 iulie 1995 de elaborare a Convenției privind utilizarea tehnologiei informației în domeniul vamal, JO 1995 C 316, astfel cum a fost modificat prin Regulamentul (CE) nr. 515/97 al Consiliului din 13 martie 1997 privind asistența reciprocă între autoritățile administrative ale statelor membre și cooperarea dintre acestea și Comisie în vederea asigurării aplicării corespunzătoare a legislației din domeniile vamal și agricol și de Decizia 2009/917/JAI a Consiliului din 30 noiembrie 2009 privind utilizarea tehnologiei informației în domeniul vamal, JO 2009 L 323 (Decizia SIV).

909 Vezi Decizia SIV, articolele 24, 25 și 28.

Prelucrarea datelor cu caracter personal trebuie să respecte normele specifice stabilite prin Regulamentul nr. 515/97 și prin Decizia 2009/917/JAI a Consiliului, precum și dispozițiile Regulamentului general privind protecția datelor, Regulamentul privind protecția datelor de către instituțiile europene, Convenției 108 modernizate și Recomandării privind sectorul polițienesc. AEPD este responsabilă pentru supravegherea respectării de către SIV a Regulamentului (CE) nr. 45/2001. AEPD convoacă cel puțin o dată pe an o reuniune cu toate autoritățile naționale de supraveghere a protecției datelor care au competențe în ceea ce privește aspectele de supraveghere legate de SIV.

Interoperabilitatea sistemelor de informații ale UE

Gestionarea migrației, gestionarea integrată a frontierelor externe a UE și combaterea terorismului și a criminalității transfrontaliere reprezintă provocări importante și devin din ce în ce mai complexe într-o lume globalizată. În ultimii ani, UE a lucrat la o nouă abordare cuprinzătoare pentru protejarea și menținerea securității fără a compromite valorile și libertățile fundamentale ale Uniunii. În cadrul acestor eforturi, este esențial schimbul eficient de informații între autoritățile naționale de aplicare a legii și între statele membre și agențiile UE relevante[910]. Fiecare dintre sistemele existente de informații ale UE pentru gestionarea frontierelor și securitatea internă are obiective, structură instituțională, persoane vizate și utilizatori specifici. UE lucrează la depășirea deficiențelor funcționale legate de gestionarea fragmentată a datelor în UE între diferitele sisteme de informații, cum ar fi SIS II, VIS și Eurodac, prin explorarea potențialului de interoperabilitate al acestora[911]. Obiectivul principal este să se asigure faptul că autoritățile polițienești, vamale și judiciare competente

910 Comunicare a Comisiei către Parlamentul European și Consiliu intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate", COM(2016) 205 final din 6 aprilie 2016, Bruxelles; Comunicare a Comisiei către Parlamentul European, Consiliul European și Consiliu intitulată „Creșterea nivelului de securitate într-o lume a mobilității: îmbunătățirea schimbului de informații în cadrul combaterii terorismului și consolidarea frontierelor externe", COM(2016) 602 final, Bruxelles, 14 septembrie 2016; Propunerea din 2016 a Comisiei Europene de regulament al Parlamentului European și al Consiliului privind utilizarea Sistemului de informații Schengen pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală. Vezi, de asemenea, Comunicare a Comisiei către Parlamentul European, Consiliul European și Consiliu intitulată „Al șaptelea raport referitor la progresele înregistrate pentru realizarea unei uniuni a securității efective și reale", COM(2017) 261 final din 16 mai 2017, Bruxelles.

911 Consiliul Uniunii Europene (2005), Programul de la Haga: consolidarea libertății, securității și justiției în Uniunea Europeană, JO 2005 C 53; Comunicare a Comisiei către Parlamentul European și Consiliu intitulată „Prezentare generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție", COM(2010) 385 final; Comunicare a Comisiei către Parlamentul European și Consiliu intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate", COM(2016) 205 final din 6 aprilie 2016, Bruxelles; Decizia Comisiei din 17 iunie 2016 de instituire a Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate, JO 2016 C 257.

dispun în mod sistematic de informațiile necesare pentru a-și îndeplini sarcinile, menținând în același timp un echilibru în ceea ce privește drepturile la respectarea vieții private și la protecția datelor și alte drepturi fundamentale.

Interoperabilitatea este „capacitatea sistemelor de informații de a face schimb de date și de a permite schimbul de informații”[912]. Acest schimb nu trebuie să încalce normele în mod necesar stricte privind accesul și utilizarea garantate de Regulamentul general privind protecția datelor, de Directiva privind protecția datelor destinată autorităților polițienești și autorităților judiciare penale, de Carta drepturilor fundamentale a UE și toate celelalte norme relevante. Nicio soluție integrată de gestionare a datelor nu trebuie să încalce principiul limitărilor legate de scop, al protecției datelor din faza de proiectare sau al protecției implicite a datelor[913].

Pe lângă îmbunătățirea funcționalităților celor trei sisteme principale de informații – SIS II, VIS și Eurodac – Comisia a propus instituirea unui al patrulea sistem centralizat de gestionare a frontierelor care să abordeze resortisanții țărilor terțe: sistemul de intrare/ieșire (EES)[914], a cărui implementare este preconizată pentru 2020 cel târziu[915]. Comisia a emis, de asemenea, o propunere de instituire a unui sistem european de informații și de autorizare privind călătoriile (ETIAS)[916], sistem care va colecta informații privind persoanele care călătoresc fără viză în UE pentru a permite îmbunătățirea gestionării migrației neregulamentare și a controalelor de securitate.

912 Comunicare a Comisiei către Parlamentul European și Consiliu intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”, COM(2016) 205 final din 6 aprilie 2016, Bruxelles, p. 14.

913 *Ibidem*, pp. 4-5.

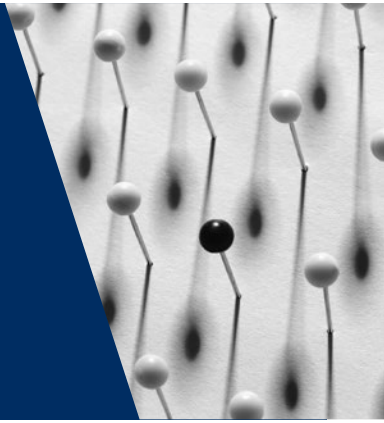
914 Propunere de regulament al Parlamentului European și al Consiliului de instituire a sistemului de intrare/ieșire (EES) pentru înregistrarea datelor de intrare și de ieșire și a datelor referitoare la refuzul intrării în ceea ce îi privește pe resortisanții țărilor terțe care trec frontierele externe ale statelor membre ale Uniunii Europene, de stabilire a condițiilor de acces la EES în scopul asigurării respectării legii și de modificare a Regulamentului (CE) nr. 767/2008 și a Regulamentului (UE) nr. 1077/2011, COM(2016) 194 final din 6 aprilie 2016, Bruxelles.

915 Comunicare a Comisiei către Parlamentul European și Consiliu intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”, COM(2016) 205 final din 6 aprilie 2016, Bruxelles, p. 5.

916 Propunere de regulament al Parlamentului European și al Consiliului de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS) și de modificare a Regulamentelor (UE) nr. 515/2014, (UE) 2016/399, (UE) 2016/794 și (UE) 2016/1624, COM(2016) 731 final din 16 noiembrie 2016.

9

Tipuri specifice de date și normele relevante de protecție a acestora



UE	Aspecte vizate	CoE
Regulamentul general privind protecția datelor Directiva asupra confidențialității și comunicațiilor electronice	**Comunicații electronice**	Convenția 108 modernizată Recomandarea privind serviciile de telecomunicații
Regulamentul general privind protecția datelor, articolul 89	**Relații de muncă**	Convenția 108 modernizată Recomandarea privind datele în contextul relațiilor de muncă Hotărârea CEDO în cauza *Copland/Regatul Unit*, nr. 62617/00, 2007
Regulamentul general privind protecția datelor, articolul 9 alineatul (2) literele (h) și (i)	**Date medicale**	Convenția 108 modernizată Recomandarea privind datele medicale Hotărârea CEDO în cauza *Z/Finlanda*, nr. 22009/93, 1997
Regulamentul privind studiile clinice	**Studii clinice**	
Regulamentul general privind protecția datelor, articolul 6 alineatul (4) și articolul 88	**Statistici**	Convenția 108 modernizată Recomandarea privind datele statistice

UE	Aspecte vizate	CoE
Regulamentul (CE) nr. 223/2009 privind statisticile europene Hotărârea CJUE [MC] în cauza C-524/06, *Huber/Bundesrepublik Deutschland*, 2008	**Statistici oficiale**	Convenția 108 modernizată Recomandarea privind datele statistice
Directiva 2014/65/UE privind piețele instrumentelor financiare Regulamentul (UE) nr. 648/2012 privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții Regulamentul (CE) nr. 1060/2009 privind agențiile de rating de credit Directiva 2007/64/CE privind serviciile de plată în cadrul pieței interne	**Date financiare**	Convenția 108 modernizată Recomandarea 90 (19) utilizată pentru plăți și alte operațiuni conexe Hotărârea CEDO în cauza *Michaud/Franța*, nr. 12323/11, 2012

În mai multe cazuri, s-au adoptat instrumente juridice speciale la nivel european pentru punerea în aplicare, în detaliu, în funcție de situații specifice, a normelor generale ale Convenției 108 modernizate sau ale Regulamentului general privind protecția datelor.

9.1. Comunicații electronice

Principalele elemente

- Recomandarea CoE din 1995 cuprinde norme specifice de protecție a datelor în domeniul telecomunicațiilor, cu referire în special la serviciile de telefonie.
- Prelucrarea datelor cu caracter personal în legătură cu furnizarea de servicii de comunicații la nivelul UE este reglementată de Directiva asupra confidențialității și comunicațiilor electronice.
- Confidențialitatea comunicațiilor electronice se referă nu doar la conținutul unei comunicări, ci și la metadate, cum ar fi informații cu privire la persoanele între care are loc comunicarea, momentul și durata comunicării și datele de localizare, cum ar fi locul de unde au fost comunicate datele.

Rețelele de comunicații prezintă potențial sporit de ingerință nejustificată în sfera personală a utilizatorilor, deoarece oferă posibilități tehnice ample de ascultare și monitorizare a comunicațiilor efectuate în astfel de rețele. Prin urmare, au fost

considerate necesare reglementări speciale de protecție a datelor pentru a aborda riscurile speciale la care sunt supuși utilizatorii de servicii de comunicații.

În anul 1995, **CoE** a emis o Recomandare privind protecția datelor în domeniul telecomunicațiilor, cu referire specială la serviciile de telefonie[917]. În conformitate cu această recomandare, scopurile legate de colectarea și prelucrarea datelor cu caracter personal în contextul telecomunicațiilor ar trebui să se limiteze la următoarele: conectarea unui utilizator la rețea, punerea la dispoziție a serviciului specific de telecomunicații, facturare, verificare, asigurarea funcționării tehnice optime și dezvoltarea rețelei și a serviciului.

S-a acordat, de asemenea, o atenție specială utilizării rețelelor de comunicații pentru trimiterea de mesaje de marketing direct. În general, mesajele de marketing direct nu pot fi direcționate către niciun abonat care a renunțat în mod expres la primirea de mesaje publicitare. Dispozitivele de apelare automată pentru transmiterea de mesaje publicitare pre-înregistrate pot fi utilizate numai în cazul în care un abonat și-a dat consimțământul în mod expres. Legislația națională prevede norme detaliate în acest domeniu.

În **cadrul juridic al UE**, după o primă încercare în 1997, Directiva asupra confidențialității și comunicațiilor electronice a fost adoptată în 2002 și modificată în 2009. Acest lucru s-a făcut în scopul completării și adaptării dispozițiilor directivei anterioare privind protecția datelor la sectorul telecomunicațiilor[918].

Aplicarea Directivei asupra confidențialității și comunicațiilor electronice se limitează la serviciile de comunicații în rețelele electronice publice.

Directiva asupra confidențialității și comunicațiilor electronice distinge trei categorii principale de date generate în cursul unei comunicări:

---

917 Recomandarea Rec(95)4 din 7 februarie 1995 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția datelor cu caracter personal în domeniul serviciilor de telecomunicații.

918 Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), JO 2002 L 201, astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului, JO 2009 L 337.

- datele care constituie conținutul mesajelor trimise în timpul comunicării – aceste date sunt strict confidențiale;

- datele necesare pentru stabilirea și menținerea comunicării – așa-numitele „metadate", denumite „date de transfer" în directivă – cum ar fi informațiile despre participanții la comunicare, ora și durata comunicării;

- în metadate sunt incluse date referitoare în mod specific la localizarea dispozitivului de comunicare – așa-numitele „date de localizare"; aceste date sunt în același timp date care indică localizarea utilizatorilor dispozitivelor de comunicare, în special atunci când este vorba despre utilizatori ai dispozitivelor de comunicații mobile.

Datele de transfer pot fi utilizate de către furnizorul de servicii exclusiv în scopul facturării și furnizării propriu-zise a serviciului. Cu toate acestea, datele respective pot fi divulgate cu consimțământul persoanei vizate, dar exclusiv altor operatori care furnizează servicii cu valoare adăugată, cum ar fi furnizarea de informații cu privire la locul în care se află utilizatorul: unde se află următoarea stație de metrou sau cea mai apropiată farmacie, prognoza meteo pentru localitatea respectivă etc.

În conformitate cu articolul 15 din Directiva asupra confidențialității și comunicațiilor electronice, alte tipuri de acces la datele privind comunicațiile în rețelele electronice trebuie să îndeplinească cerințele privind ingerința justificată în dreptul la protecția datelor, astfel cum este prevăzut la articolul 8 alineatul (2) din Convenția europeană a drepturilor omului și confirmat la articolele 8 și 52 din Carta drepturilor fundamentale a UE. Printre aceste tipuri de acces se poate număra accesul în scopul investigării infracțiunilor.

Modificările din 2009 ale Directivei asupra confidențialității și comunicațiilor electronice[919] au introdus următoarele dispoziții:

- Restricțiile privind trimiterea de e-mailuri în scopuri de marketing direct au fost extinse la serviciile SMS, la serviciile de mesagerie multimedia și la alte tipuri

919 Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului, JO 2009 L 337.

de aplicații similare; e-mailurile de marketing sunt interzise dacă nu s-a obținut consimțământul prealabil. În lipsa unui astfel de consimțământ, doar clienților existenți li se pot trimite e-mailuri de marketing, în cazul în care și-au pus la dispoziție adresa de e-mail și dacă nu au obiecții.

- Statele membre au obligația de a asigura căi de atac judiciare pentru încălcările interdicției referitoare la comunicările nesolicitate[920].

- Instalarea de module cookies – software care monitorizează și înregistrează acțiunile unui utilizator de computer – nu mai este permisă fără acordul utilizatorului computerului. Legislația națională trebuie să reglementeze mai detaliat modul în care trebuie exprimat și obținut consimțământul pentru a asigura un nivel adecvat de protecție[921].

În cazul în care are loc o încălcare a securității datelor ca urmare a accesului neautorizat, a pierderii sau a distrugerii datelor, autoritatea de supraveghere competentă trebuie să fie informată imediat. Abonații trebuie să fie informați în cazul în care ar putea suferi un prejudiciu din cauza unei încălcări a securității datelor[922].

Directiva privind păstrarea datelor[923] solicita furnizorilor de servicii de comunicații să păstreze metadatele. Această directivă a fost însă anulată de CJUE (pentru mai multe detalii, vezi secțiunea 8.3).

Perspective

În ianuarie 2017, Comisia Europeană a adoptat o nouă propunere de regulament privind viața privată și comunicațiile electronice, care să înlocuiască vechea Directivă asupra confidențialității și comunicațiilor electronice. Scopul ar rămâne protecția „drepturilor și libertăților fundamentale ale persoanelor fizice și juridice în ceea ce privește furnizarea și utilizarea serviciilor de comunicații electronice și, în special,

920 Vezi directiva modificată, articolul 13.

921 Vezi *ibidem*, articolul 5; vezi, de asemenea, Avizul 4/2012 din 7 iunie 2012 al Grupului de lucru „Articolul 29" privind exceptarea de la exprimarea consimțământului cu privire la modulele cookie, WP 194, Bruxelles.

922 Vezi, de asemenea, Documentul de lucru 1/2011 din 5 aprilie 2011 al Grupului de lucru „Articolul 29" privind cadrul european actual referitor la încălcările securității datelor cu caracter personal și recomandările pentru evoluțiile politice viitoare, WP 184, Bruxelles.

923 Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE, JO 2006 L 105.

dreptul la respectarea vieții private și a comunicațiilor și la protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal". În același timp, noua propunere urmărește să asigure libera circulație a datelor transmise în cadrul comunicațiilor electronice și a serviciilor de comunicații electronice în cadrul Uniunii[924]. În timp ce Regulamentul general privind protecția datelor se referă în primul rând la articolul 8 din Carta drepturilor fundamentale a UE, regulamentul propus vizează includerea articolului 7 din Cartă în legislația secundară a UE.

Regulamentul ar adapta dispozițiile directivei anterioare la noile tehnologii și realități ale pieței și ar construi un cadru cuprinzător și coerent cu Regulamentul general privind protecția datelor. În acest sens, Regulamentul privind viața privată și comunicațiile electronice ar fi o *lex specialis* în raport cu Regulamentul general privind protecția datelor, adaptându-l la datele transmise în cadrul comunicațiilor electronice care constituie date cu caracter personal. Noul regulament se referă la prelucrarea „datelor transmise în cadrul comunicațiilor electronice", inclusiv a conținutului și a metadatelor din cadrul comunicațiilor electronice care nu sunt neapărat date cu caracter personal. Domeniul de aplicare teritorial este limitat la UE, inclusiv atunci când datele obținute în UE sunt prelucrate în afara acesteia, și se extinde la furnizorii de servicii de comunicații OTT. Aceștia sunt furnizorii de servicii care furnizează conținut, servicii sau aplicații prin internet, fără implicarea directă a unui operator de rețea sau a unui furnizor de servicii internet (ISP). Printre exemplele de astfel de furnizori se numără Skype (apeluri vocale și video), WhatsApp (mesagerie), Google (căutare), Spotify (muzică) sau Netflix (conținut video). Mecanismele de aplicare a Regulamentului general privind protecția datelor se vor aplica noului regulament.

Se preconizează ca Regulamentul privind viața privată și comunicațiile electronice să fie adoptat înainte de 25 mai 2018, moment în care Regulamentul general privind protecția datelor va fi aplicabil în toate cele 28 de state membre. Acest lucru depinde totuși atât de acordul Parlamentului European, cât și de al Consiliului[925].

924 Propunere de regulament al Parlamentului European și al Consiliului privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice și de abrogare a Directivei 2002/58/CE (Regulamentul privind viața privată și comunicațiile electronice), COM(2017) 10 final din 10 ianuarie 2017, articolul 1.

925 Pentru mai multe informații, vezi comunicatul de presă al Comisiei Europene din 10 ianuarie 2017, Comisia propune un nivel înalt al normelor privind respectarea vieții private pentru toate comunicațiile electronice și actualizează normele de protecție a datelor în cadrul instituțiilor UE.

9.2. Datele în contextul relațiilor de muncă

Principalele elemente

- În Recomandarea CoE privind datele în contextul relațiilor de muncă se prevăd norme specifice de protecție a datelor în domeniul relațiilor de muncă.
- În Regulamentul general privind protecția datelor, relațiile de muncă sunt tratate în mod specific numai în contextul prelucrării datelor sensibile.
- Valabilitatea consimțământului, care trebuie să fie exprimat în mod liber, ca temei juridic pentru prelucrarea datelor despre angajați poate fi discutabilă, având în vedere dezechilibrul economic între angajator și angajați. Circumstanțele exprimării consimțământului trebuie să fie evaluate cu atenție.

Prelucrarea datelor în contextul relațiilor de muncă face obiectul legislației generale a UE privind protecția datelor cu caracter personal. Cu toate acestea, un regulament[926] se referă în mod specific la protecția prelucrării datelor cu caracter personal de către instituțiile europene în contextul relațiilor de muncă (printre altele). În Regulamentul general privind protecția datelor, relațiile de muncă sunt menționate în mod specific la articolul 9 alineatul (2), care prevede că datele cu caracter personal pot fi prelucrate în scopul îndeplinirii obligațiilor sau al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă.

În conformitate cu Regulamentul general privind protecția datelor, angajatul ar trebui să aibă posibilitatea de a identifica în mod clar datele în legătură cu care își exprimă în mod liber consimțământul față de prelucrare/stocare și scopurile pentru care sunt stocate aceste date. Înainte de acordarea consimțământului, angajații ar trebui, de asemenea, să fie informați cu privire la drepturile lor și la perioada de timp pentru care vor fi stocate datele. În cazul în care se produce o încălcare a datelor cu caracter personal care ar putea genera un risc ridicat pentru drepturile și libertățile persoanelor fizice, angajatorul trebuie să informeze angajatul cu privire la această încălcare. Articolul 88 din regulament acordă statelor membre posibilitatea de a stabili norme mai detaliate pentru a asigura protecția drepturilor și a libertăților angajaților cu privire la prelucrarea datelor cu caracter personal ale acestora în contextul ocupării unui loc de muncă.

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

Exemplu: În cauza *Worten*[927], datele includeau o evidență a timpului de lucru care conținea perioadele de lucru și de repaus zilnice, ceea ce constituie date cu caracter personal. Legislația națională poate impune unui angajator să pună evidențele timpului de lucru la dispoziția autorităților naționale responsabile pentru monitorizarea condițiilor de muncă. Acest lucru ar permite accesul imediat la datele cu caracter personal relevante. Cu toate acestea, accesul la datele cu caracter personal este necesar pentru a permite autorității naționale să monitorizeze legislația privind condițiile de muncă[928].

În ceea ce privește **CoE**, Recomandarea privind datele în contextul relațiilor de muncă a fost emisă în anul 1989 și revizuită în 2015[929]. Recomandarea se referă la prelucrarea datelor cu caracter personal în contextul relațiilor de muncă, atât în sectorul privat, cât și în cel public. Prelucrarea trebuie să respecte anumite principii și restricții, cum ar fi principiul transparenței și cel referitor la consultarea reprezentanților angajaților înainte de a introduce sisteme de monitorizare la locul de muncă. Recomandarea prevede, de asemenea, că angajatorii ar trebui să aplice măsuri preventive, cum ar fi filtrele, în locul sistemelor de monitorizare a utilizării internetului de către angajați.

Un studiu privind cele mai uzuale probleme specifice legate de protecția datelor în contextul relațiilor de muncă este disponibil într-un document de lucru al Grupului de lucru „Articolul 29”[930]. Grupul de lucru a analizat relevanța consimțământului ca temei juridic pentru prelucrarea datelor în contextul relațiilor de muncă[931]. S-a constatat că dezechilibrul economic între angajatorul care solicită consimțământul și angajatul care trebuie să îl acorde generează adesea îndoieli cu privire la gradul de libertate cu care se poate exprima acest consimțământ. Prin urmare, în momentul evaluării valabilității consimțământului în contextul relațiilor de muncă trebuie analizate cu atenție circumstanțele în care se recurge la consimțământ ca temei juridic al prelucrării datelor.

927 Hotărârea CJUE din 30 mai 2013 în cauza C-342/12, *Worten – Equipamentos para o Lar SA/Autoridade para as Condições de Trabalho (ACT)*, punctul 19.

928 *Ibidem*, punctul 43.

929 Recomandarea Rec(2015)5 a Comitetului de Miniștri al Consiliului Europei către statele membre privind prelucrarea datelor cu caracter personal în contextul relațiilor de muncă, aprilie 2015.

930 Avizul 2/2017 din 8 iunie 2017 al Grupului de lucru „Articolul 29” privind prelucrarea datelor în contextul relațiilor de muncă, WP 249, Bruxelles.

931 Documentul de lucru din 25 noiembrie 2005 al Grupului de lucru „Articolul 29” privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995, WP 114, Bruxelles.

O problemă curentă legată de protecția datelor în mediul de lucru tipic actual este măsura în care comunicațiile electronice ale angajaților pot fi monitorizate în mod legitim la locul de muncă. Se susține adesea că această problemă poate fi rezolvată cu ușurință, prin interzicerea utilizării în scopuri personale a dispozitivelor de comunicații la locul de muncă. Cu toate acestea, o astfel de interdicție generală poate fi disproporționată și nerealistă. Hotărârile CEDO pronunțate în cauzele *Copland/Regatul Unit* și *Bărbulescu/România* prezintă un interes deosebit în acest context.

Exemplu: În cauza *Copland/Regatul Unit*[932], utilizarea telefonului, a e-mailului și a internetului de către angajata unei instituții de învățământ superior a fost monitorizată în secret pentru a se stabili dacă aceasta utiliza excesiv dispozitivele de la locul de muncă în scopuri personale. CEDO a stabilit că apelurile telefonice efectuate de la locul de muncă intrau în domeniul de aplicare al noțiunilor de viață privată și corespondență privată. Prin urmare, apelurile și e-mailurile respective trimise de la locul de muncă, precum și informațiile provenite din monitorizarea utilizării internetului în scopuri personale erau protejate de articolul 8 din Convenția europeană a drepturilor omului. În cazul reclamantei, nu existau dispoziții de reglementare a situațiilor în care angajatorii pot monitoriza utilizarea de către angajați a telefonului, a e-mailului și a internetului. Prin urmare, ingerința în drepturile sale nu era în conformitate cu legea. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Exemplu: În cauza *Bărbulescu/România*[933], reclamantul a fost concediat pentru că a folosit internetul la locul său de muncă în timpul orelor de lucru, încălcând reglementările interne. Angajatorul său i-a monitorizat comunicările. Înregistrările, care prezintă mesaje de natură exclusiv privată, au fost prezentate în cadrul procedurii judiciare a instanței naționale. Constatând că articolul 8 este aplicabil în speță, CEDO a lăsat deschisă întrebarea dacă reglementările restrictive ale angajatorului permiteau ca reclamantul să aibă așteptări rezonabile în ceea ce privește viața privată, dar a considerat totuși că instrucțiunile unui angajator nu pot reduce la zero viața socială privată la locul de muncă.

932 Hotărârea CEDO din 3 aprilie 2007 în cauza *Copland/Regatul Unit*, nr. 62617/00.

933 Hotărârea CEDO [MC] din 5 septembrie 2017 în cauza *Bărbulescu/România*, nr. 61496/08, punctul 121.

Cu privire la fond, statele contractante trebuiau să beneficieze de o marjă largă de apreciere pentru a evalua necesitatea stabilirii unui cadru juridic care să reglementeze condițiile în care un angajator poate reglementa comunicările de altă natură decât profesională ale angajaților săi – în format electronic sau de alt tip – la locul de muncă. Cu toate acestea, autoritățile naționale trebuiau să se asigure că introducerea de către angajator a unor măsuri de monitorizare a corespondenței și a altor comunicări, indiferent de amploarea și de durata acestor măsuri, este însoțită de garanții adecvate și suficiente împotriva abuzurilor. Proporționalitatea și garanțiile procedurale împotriva arbitrarului măsurilor sunt esențiale, iar CEDO a identificat o serie de factori relevanți în speță. Acești factori includ, de exemplu, amploarea monitorizării de către angajator a angajaților și gradul de intruziune în viața privată a acestora din urmă, consecințele pentru angajați și aspectul dacă s-au oferit garanții adecvate. În plus, autoritățile naționale trebuiau să se asigure că un angajat ale cărui comunicări fuseseră monitorizate avea acces la o cale de atac în fața unei instanțe judecătorești competente să determine, cel puțin cu privire la fond, cum au fost respectate criteriile stabilite și dacă măsurile contestate erau legale.

CEDO a constatat în această speță că s-a încălcat articolul 8, deoarece autoritățile naționale nu au acordat o protecție adecvată dreptului reclamantului la respectarea vieții private și a corespondenței și, prin urmare, nu au reușit să asigure un echilibru just între interesele concurente în cauză.

În conformitate cu Recomandarea CoE privind datele în contextul relațiilor de muncă, datele cu caracter personal colectate în scopul angajării ar trebui obținute de la fiecare angajat în mod direct.

Datele cu caracter personal colectate în scopul recrutării trebuie să se limiteze la informațiile necesare pentru evaluarea eligibilității candidaților și a potențialului profesional al acestora.

De asemenea, recomandarea menționează în mod specific date care conțin judecăți cu privire la performanța sau potențialul fiecărui angajat. Datele care conțin judecăți trebuie să se bazeze pe evaluări corecte și oneste, iar modul în care sunt formulate nu trebuie să fie ofensator. Acest lucru este prevăzut de principiul prelucrării echitabile a datelor și de principiul exactității datelor.

Un aspect specific al legislației privind protecția datelor în relația angajator-angajat este rolul reprezentanților angajaților. Acești reprezentanți pot primi datele cu caracter personal ale angajaților numai în măsura în care acest lucru este necesar pentru a le permite să reprezinte interesele angajaților sau dacă aceste date sunt necesare pentru îndeplinirea sau supravegherea obligațiilor prevăzute în contractele colective de muncă.

Datele cu caracter personal sensibile colectate în scopul angajării pot fi prelucrate numai în cazuri specifice și în conformitate cu garanțiile prevăzute de legislația națională. Angajatorii pot solicita angajaților sau candidaților la locuri de muncă informații despre starea lor de sănătate sau pot solicita examene medicale numai în cazurile în care acest lucru este necesar. Scopuri care justifică această necesitate: a stabili dacă persoanele în cauză sunt potrivite pentru locurile de muncă respective; îndeplinirea cerințelor medicinii preventive; protejarea intereselor vitale ale persoanei vizate sau ale altor angajați și persoane fizice; acordarea de prestații sociale; îndeplinirea unor ordine judecătorești. Datele medicale personale nu pot fi colectate din alte surse decât de la angajatul în cauză, cu excepția cazului în care s-a obținut consimțământul expres și în cunoștință de cauză sau dacă legislația națională prevede acest lucru.

În conformitate cu Recomandarea privind datele în contextul relațiilor de muncă, angajații ar trebui să fie informați cu privire la: scopul prelucrării datelor lor cu caracter personal, tipul de date cu caracter personal colectate, entitățile cărora le sunt comunicate datele regulat, precum și scopul și temeiul juridic al acestor divulgări. Comunicațiile electronice pot fi accesate la locul de muncă numai pentru motive de securitate sau alte motive legitime, iar accesul este permis numai după ce angajații au fost informați că angajatorul poate avea acces la acest tip de comunicații.

Angajații trebuie să aibă drept de acces la datele lor din contextul relațiilor de muncă, precum și dreptul la rectificarea sau ștergerea acestor date. În cazul prelucrării datelor care conțin judecăți, angajații trebuie să aibă, în plus, dreptul de a contesta judecata în cauză. Aceste drepturi pot fi însă limitate temporar în scopul efectuării de anchete interne. În cazul în care unui angajat îi este refuzat dreptul de acces, rectificare sau ștergere a datelor sale cu caracter personal din contextul relațiilor de muncă, legislația națională trebuie să prevadă proceduri adecvate pentru contestarea refuzului respectiv.

9.3. Date medicale personale

Element principal

- Datele medicale sunt date sensibile și, prin urmare, beneficiază de protecție specială.

Datele cu caracter personal referitoare la starea de sănătate a persoanei vizate sunt calificate drept date sensibile în conformitate cu articolul 9 alineatul (1) din Regulamentul general privind protecția datelor și cu articolul 6 din Convenția 108 modernizată. La rândul lor, datele medicale fac obiectul unui regim de prelucrare a datelor mai strict decât în cazul datelor fără caracter sensibil. Regulamentul general privind protecția datelor interzice prelucrarea „datelor cu caracter personal privind sănătatea" (înțeleasă ca „toate datele având legătură cu starea de sănătate a persoanei vizate care dezvăluie informații despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei vizate")[934], precum și a datelor genetice și a datelor biometrice, cu excepția cazului în care prelucrarea este autorizată în temeiul articolului 9 alineatul (2). Ambele tipuri de date au fost incluse în lista de „categorii speciale de date"[935].

Exemplu: În cauza *Z/Finlanda*[936], fostul soț al reclamantei, care era infectat cu HIV, a comis o serie de infracțiuni de natură sexuală. Acesta a fost ulterior condamnat pentru ucidere din culpă, pentru motivul că și-a expus cu bună știință victimele riscului de infectare cu HIV. Instanța națională a dispus că hotărârea definitivă și documentele cauzei trebuie să rămână confidențiale timp de 10 ani, în ciuda cererilor din partea reclamantei de acordare a unei perioade mai lungi de confidențialitate. Aceste cereri au fost respinse de către instanța de apel și hotărârea adoptată de instanță menționa atât numele și prenumele reclamantei, cât și ale fostului soț. CEDO a stabilit că această ingerință nu poate fi considerată necesară într-o societate democratică, deoarece protecția datelor medicale este de importanță fundamentală pentru exercitarea dreptului la respectarea vieții private și de familie, în special în ceea ce

934 Regulamentul general privind protecția datelor, considerentul 35.

935 *Ibidem*, articolul 2.

936 Hotărârea CEDO din 25 februarie 1997 în cauza *Z/Finlanda*, nr. 22009/93, punctele 94 și 112; vezi, de asemenea, Hotărârea CEDO din 27 august 1997 în cauza *M.S./Suedia*, nr. 20837/92; Hotărârea CEDO din 10 octombrie 2006 în cauza *L.L./Franța*, nr. 7508/02; Hotărârea CEDO din 17 iulie 2008 în cauza *I/Finlanda*, nr. 20511/03; Hotărârea CEDO din 28 aprilie 2009 în cauza *K.H. și alții/Slovacia*, nr. 32881/04; Hotărârea CEDO din 2 iunie 2009 în cauza *Szuluk/Regatul Unit*, nr. 36936/05.

privește informarea despre infectarea cu HIV, având în vedere stigmatizarea acestei afecțiuni în multe societăți. Prin urmare, CEDO a concluzionat că acordarea accesului la hotărârea instanței de apel, care a descris identitatea și starea medicală a reclamantului, după zece ani de la pronunțarea hotărârii, ar încălca articolul 8 din Convenția europeană a drepturilor omului.

În cadrul **legislației UE**, articolul 9 alineatul (2) litera (h) din Regulamentul general privind protecția datelor permite prelucrarea datelor medicale în cazul în care acest lucru este necesar în scopuri legate de medicina preventivă, de diagnosticare, de administrarea unor îngrijiri sau tratamente ori de gestionarea serviciilor de sănătate. Prelucrarea este permisă numai în cazul în care este efectuată de un cadru medical care are obligația de a păstra secretul profesional sau de către o altă persoană cu obligații echivalente.

În cadrul **legislației CoE**, Recomandarea CoE din 1997 privind datele medicale aplică mai detaliat principiile Convenției 108 legate de prelucrarea datelor în domeniul medical[937]. Normele propuse sunt conforme cu cele ale Regulamentului general privind protecția datelor în ceea ce privește scopurile legitime ale prelucrării datelor medicale, obligațiile necesare privind secretul profesional în cazul persoanelor care utilizează date medicale, precum și drepturile persoanelor vizate privind transparența și accesul la date și rectificarea și ștergerea datelor. În plus, datele medicale care sunt prelucrate în mod legal de către cadrele medicale nu pot fi transferate către autoritățile de aplicare a legii, cu excepția cazului în care „sunt asigurate garanții adecvate pentru a împiedica divulgarea incompatibilă cu respectarea [...] vieții private garantate în temeiul articolului 8 din Convenția europeană a drepturilor omului”[938]. De asemenea, reglementarea națională trebuie să fie „formulată cu suficientă precizie și să ofere o protecție juridică adecvată împotriva caracterului arbitrar”[939].

În plus, Recomandarea privind datele medicale conține dispoziții speciale privind datele medicale ale copiilor nenăscuți și ale persoanelor aflate în incapacitate, precum și privind prelucrarea datelor genetice. Activitatea de cercetare științifică este recunoscută în mod explicit ca justificare pentru conservarea datelor pe o perioadă

937 Recomandarea Rec(97)5 din 13 februarie 1997 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția datelor medicale. Trebuie precizat faptul că această recomandare este în curs de revizuire.

938 Hotărârea CEDO din 6 iunie 2013 în cauza *Avilkina și alții/Rusia*, nr. 1585/09, punctul 53. Vezi, de asemenea, Hotărârea CEDO din 25 noiembrie 2008 în cauza *Biriuk/Lituania*, nr. 23373/03.

939 Hotărârea CEDO din 29 aprilie 2014 în cauza *L.H./Letonia*, nr. 52019/07, punctul 59.

mai lungă decât este necesar, cu toate că acest lucru va necesita, de obicei, anonimizarea acestora. Articolul 12 din Recomandarea privind datele medicale propune reglementări detaliate pentru situațiile în care cercetătorii au nevoie de date cu caracter personal, iar datele anonimizate sunt insuficiente.

Pseudonimizarea poate fi un mijloc adecvat pentru a răspunde nevoilor științifice și, în același timp, pentru a proteja interesele pacienților în cauză. Conceptul de pseudonimizare în contextul protecției datelor este explicat în detaliu la secțiunea 2.1.1.

Recomandarea CoE din 2016 privind datele rezultate din teste genetice se aplică și în domeniul prelucrării datelor în domeniul medical[940]. Această recomandare are o importanță deosebită în domeniul e-sănătății, în care se utilizează TIC pentru a facilita acordarea îngrijirilor medicale. Un exemplu este trimiterea rezultatelor testelor de paternitate ale unui pacient de la un furnizor de servicii medicale la altul. Recomandarea vizează protejarea drepturilor persoanelor ale căror date cu caracter personal sunt prelucrate în scopuri de asigurare împotriva riscurilor legate de sănătatea, integritatea fizică, vârsta sau decesul unei persoane. Asigurătorii trebuie să justifice prelucrarea datelor medicale, iar aceasta ar trebui să fie proporțională cu natura și amploarea riscului acoperit. Prelucrarea acestui tip de date este condiționată de consimțământul persoanei vizate. Asigurătorii ar trebui să pună în aplicare, de asemenea, garanții pentru stocarea datelor medicale.

Studiile clinice – care implică evaluarea efectelor noilor medicamente asupra pacienților aflați în medii de cercetare monitorizate – au implicații considerabile în ceea ce privește protecția datelor. Studiile clinice pentru medicamentele de uz uman sunt reglementate de Regulamentul (UE) nr. 536/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 privind studiile clinice intervenționale cu medicamente de uz uman și de abrogare a Directivei 2001/20/CE (Regulamentul privind studiile clinice)[941]. Principalele elemente ale Regulamentului privind studiile clinice sunt următoarele:

- o procedură simplificată de depunere a cererilor prin portalul UE[942];

940 Recomandarea Rec(2016)8 din 25 octombrie 2016 a Comitetului de Miniștri al Consiliului Europei către statele membre privind prelucrarea datelor medicale personale în scopuri de asigurare, inclusiv a datelor provenite din teste genetice.

941 Regulamentul (UE) nr. 536/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 privind studiile clinice intervenționale cu medicamente de uz uman și de abrogare a Directivei 2001/20/CE (Regulamentul privind studiile clinice), JO 2014 L 158.

942 Regulamentul privind studiile clinice, articolul 5 alineatul (1).

- termene pentru evaluarea cererii pentru un studiu clinic[943];
- participarea la evaluare a unei comisii de etică, în conformitate cu legislația statelor membre (și cu legislația europeană care definește perioadele implicate)[944];
- îmbunătățirea transparenței studiilor clinice și a rezultatelor acestora[945].

Regulamentul general privind protecția datelor precizează că, în scopul acordării consimțământului de a participa la activități de cercetare științifică în cadrul testelor clinice, se aplică Regulamentul (UE) nr. 536/2014[946].

La nivelul UE sunt în curs de dezbatere multe alte inițiative legislative și de altă natură privind datele cu caracter personal din sectorul medical[947].

Dosare electronice de sănătate

Dosarele electronice de sănătate sunt definite drept „o fișă medicală detaliată sau o documentație similară privind starea de sănătate fizică și mentală din trecut și din prezent a unei persoane, care este în formă electronică și oferă acces imediat la aceste date în vederea tratamentului medical sau în alte scopuri strâns legate de acesta”[948]. Dosarele electronice de sănătate sunt versiuni electronice ale istoricului medical al pacienților și pot include date clinice referitoare la aceste persoane, cum ar fi antecedentele medicale, problemele de sănătate și afecțiunile, medicamentele și tratamentele anterioare, precum și rezultatele și rapoartele examenelor și analizelor de laborator. Aceste dosare electronice, care pot varia de la documentații complete la simple extrase sau rezumate, pot fi consultate de medicii generaliști, de farmaciști și de alte cadre medicale. Și conceptul „e-sănătate” are legătură cu aceste dosare de sănătate.

943 *Ibidem*, articolul 5 alineatele (2)-(5).

944 *Ibidem*, articolul 2 alineatul (2) punctul 11.

945 *Ibidem*, articolul 9 alineatul (1) și considerentul 67.

946 Regulamentul general privind protecția datelor, considerentele 156 și 161.

947 Avizul Autorității Europene pentru Protecția Datelor referitor la Comunicarea Comisiei privind „Planul de acțiune privind e-sănătatea 2012-2020 – Asistență medicală inovatoare pentru secolul XXI”, Bruxelles, 27 martie 2013.

948 Recomandarea Comisiei din 2 iulie 2008 privind interoperabilitatea transfrontalieră a sistemelor de evidență electronică a datelor medicale, punctul 3 litera (c).

Exemplu: Domnul A a încheiat o poliță de asigurare cu societatea B, asigurătorul. Acesta din urmă va colecta unele informații medicale de la A, cum ar fi problemele de sănătate sau afecțiunile actuale. Asigurătorul ar trebui să stocheze datele medicale personale ale lui A separat de alte date. De asemenea, asigurătorul trebuie să stocheze datele medicale personale separat de alte date cu caracter personal. Aceasta înseamnă că numai persoana care gestionează cazul lui A va avea acces la datele medicale ale lui A.

Dosarele electronice de sănătate prezintă totuși anumite probleme legate de protecția datelor, cum ar fi accesibilitatea și stocarea adecvată și accesul persoanei vizate la acestea.

Pe lângă instrumentele juridice privind dosarele electronice de sănătate, Comisia Europeană a publicat, la 10 aprilie 2014, o carte verde privind sănătatea mobilă („m-sănătatea"), considerând că m-sănătatea este un domeniu emergent aflat în creștere rapidă, care are potențialul de a transforma asistența medicală și de a spori eficiența și calitatea acesteia. Termenul se referă la practica medicală și de sănătate publică susținută de dispozitive mobile, cum ar fi telefoanele mobile, dispozitivele de monitorizare a pacienților, asistenții personali digitali și alte dispozitive fără fir, precum și aplicații (de exemplu, aplicații de bunăstare) care se pot conecta la dispozitive medicale sau la senzori[949]. Documentul prezintă riscurile privind dreptul la protecția datelor cu caracter personal pe care le poate genera dezvoltarea m-sănătății și prevede că, având în vedere caracterul sensibil al datelor medicale, dezvoltarea ar trebui să conțină garanții de securitate specifice și adecvate pentru datele pacientului, cum ar fi criptarea, și mecanisme adecvate de autentificare a pacienților pentru a atenua riscurile de securitate. Conformitatea cu normele de protecție a datelor cu caracter personal, inclusiv obligația de informare a persoanei vizate, securitatea datelor și principiul prelucrării legale a datelor cu caracter personal sunt esențiale pentru consolidarea încrederii în soluțiile de m-sănătate[950]. În acest scop, sectorul a elaborat un cod de conduită bazat pe contribuții de la o gamă largă de părți interesate, printre care se numără reprezentanți cu expertiză din domeniul protecției datelor, al autoreglementării și al coreglementării, din domeniul TIC și al serviciilor medicale[951]. La momentul redactării manualului, proiectul de cod de conduită a fost

949 Comisia Europeană (2014), *Carte verde privind sănătatea mobilă („m-sănătatea")*, COM(2014) 219 final din 10 aprilie 2014, Bruxelles.

950 *Ibidem*, p. 8.

951 Proiect de cod de conduită privind protecția vieții private pentru aplicațiile mobile de sănătate, 7 iunie 2016.

prezentat Grupului de lucru „Articolul 29” pentru formularea de observații în așteptarea aprobării sale oficiale.

9.4. Prelucrarea datelor în scopuri de cercetare și în scopuri statistice

Principalele elemente

- Datele colectate în scopuri statistice sau de cercetare științifică sau istorică nu pot fi utilizate în niciun alt scop.
- Datele colectate în mod legitim în orice scop pot fi utilizate ulterior în scopuri statistice sau de cercetare științifică sau istorică, cu condiția să existe garanții adecvate. În acest scop, anonimizarea sau pseudonimizarea datelor înaintea transmiterii acestora către părți terțe poate oferi aceste garanții.

Legislația UE permite prelucrarea datelor în scopuri statistice sau de cercetare științifică sau istorică, cu condiția să existe garanții adecvate pentru drepturile și libertățile persoanelor vizate. O astfel de garanție o constituie pseudonimizarea[952]. Legislația UE sau legislația națională pot să prevadă anumite derogări de la drepturile persoanelor vizate dacă drepturile respective sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopului legitim al cercetării[953]. Pot fi introduse derogări de la dreptul de acces al persoanei vizate, de la dreptul la rectificare și la restricționarea prelucrării și de la dreptul la opoziție.

Deși datele colectate în mod legal de un operator, indiferent de scop, pot fi reutilizate de operatorul respectiv în scopuri statistice sau de cercetare științifică sau istorică proprii, datele ar trebui să fie anonimizate sau, după caz, să facă obiectul unor măsuri precum pseudonimizarea înainte de a fi transmise către o parte terță în scopuri statistice sau de cercetare științifică sau istorică, cu excepția cazului în care persoana vizată și-a exprimat consimțământul în acest sens sau dacă acest lucru este prevăzut în mod specific de legislația națională. Datele care fac obiectul pseudonimizării rămân sub incidența Regulamentului general privind protecția datelor, spre deosebire de datele anonime[954].

952 Regulamentul general privind protecția datelor, articolul 89 alineatul (1).

953 *Ibidem*, articolul 89 alineatul (2).

954 *Ibidem*, considerentul 26.

Prin urmare, regulamentul acordă cercetării un tratament special în ceea ce privește normele generale de protecție a datelor, pentru a evita limitarea dezvoltării cercetării și pentru a respecta obiectivul de realizare a unui Spațiu european de cercetare, astfel cum se prevede la articolul 179 din TFUE. Regulamentul prevede o interpretare în sens larg a prelucrării datelor cu caracter personal în scopuri de cercetare științifică, incluzând dezvoltarea tehnologică și activitățile demonstrative, cercetarea fundamentală, cercetarea aplicată și cercetarea finanțată din surse private. De asemenea, RGPD recunoaște importanța compilării datelor în registre în scopuri de cercetare și eventualele dificultăți de identificare pe deplin a scopului ulterior al prelucrării datelor cu caracter personal în scopuri de cercetare științifică la momentul colectării datelor[955]. Din acest motiv, regulamentul permite prelucrarea datelor în aceste scopuri fără consimțământul persoanelor vizate, cu condiția să existe garanții relevante.

Un exemplu important de utilizare a datelor în scopuri statistice sunt statisticile oficiale obținute de birourile statistice naționale și ale UE în conformitate cu dreptul intern și cu dreptul UE în materie de statistici oficiale. În conformitate cu aceste legislații, cetățenii și întreprinderile au, în general, obligația de a divulga date autorităților de statistică relevante. Funcționarii care lucrează în birourile de statistică au obligații speciale de păstrare a secretului profesional, care trebuie să fie respectate cu strictețe, deoarece sunt esențiale pentru asigurarea unui nivel ridicat de încredere al cetățenilor, necesar în cazul în care datele sunt puse la dispoziția autorităților de statistică[956].

Regulamentul (CE) nr. 223/2009 privind statisticile europene (Regulamentul privind statisticile europene) conține norme esențiale pentru protejarea datelor în contextul statisticilor oficiale și, prin urmare, poate fi, de asemenea, considerat relevant pentru dispozițiile privind statisticile oficiale la nivel național[957]. Regulamentul susține prin-

955 *Ibidem*, considerentele 33, 157 și 159.

956 *Ibidem*, articolul 90.

957 Regulamentul (CE) Nr. 223/2009 al Parlamentului European și al Consiliului din 11 martie 2009 privind statisticile europene și de abrogare a Regulamentului (CE, Euratom) nr. 1101/2008 al Parlamentului European și al Consiliului privind transmiterea de date statistice confidențiale Biroului Statistic al Comunităților Europene, a Regulamentului (CE) nr. 322/97 al Consiliului privind statisticile comunitare și a Deciziei 89/382/CEE, Euratom a Consiliului de constituire a Comitetului pentru programele statistice ale Comunităților Europene, JO 2009 L 87, astfel cum a fost modificat prin Regulamentul (UE) 2015/759 al Parlamentului European și al Consiliului din 29 aprilie 2015 de modificare a Regulamentului (CE) nr. 223/2009 privind statisticile europene, JO 2015 L 123.

cipiul conform căruia activitatea statistică oficială necesită un temei juridic suficient de clar[958].

> Exemplu: În cauza *Huber/Bundesrepublik Deutschland*[959], un om de afaceri austriac care s-a mutat în Germania a depus o plângere în care susținea că colectarea și stocarea datelor cu caracter personal ale cetățenilor străini de către autoritățile germane într-un registru central (AZR), inclusiv în scopuri statistice, constituia o încălcare a drepturilor sale prevăzute de Directiva privind protecția datelor. Având în vedere că Directiva 95/46/CE are ca scop asigurarea unui nivel echivalent de protecție a datelor în toate statele membre, CJUE a stabilit că, pentru a asigura un nivel ridicat de protecție în UE, conceptul de necesitate prevăzut la articolul 7 litera (e) nu poate avea un înțeles diferit de la un stat membru la altul. Astfel, acest concept are propriul său înțeles independent în dreptul UE și trebuie interpretat într-un mod care să reflecte pe deplin obiectivul Directivei 95/46/CE. Precizând că în scopuri statistice ar trebui să se solicite doar informații anonime, CJUE a stabilit că registrul german nu era compatibil cu cerința de necesitate prevăzută la articolul 7 litera (e).

În contextul **CoE**, prelucrarea ulterioară a datelor poate fi efectuată în scopuri de cercetare științifică sau istorică sau în scopuri statistice, dacă acest lucru este în interesul public, iar această prelucrare trebuie să facă obiectul unor garanții adecvate[960]. Drepturile persoanelor vizate pot fi, de asemenea, restricționate atunci când se prelucrează date în scopuri statistice, cu condiția să nu existe un risc previzibil de încălcare a drepturilor și libertăților acestora[961].

Recomandarea privind datele statistice din 1997 privește performanța activității statistice în sectoarele public și privat[962].

---

958 Acest principiu urmează să fie detaliat în Codul de practică al Eurostat, care, în conformitate cu articolul 11 din Regulamentul privind statisticile europene, prevede orientări etice cu privire la modul de efectuare a statisticilor oficiale, inclusiv utilizarea prudentă a datelor cu caracter personal.

959 Hotărârea CJUE [MC] din 16 decembrie 2008 în cauza C-524/06, *Heinz Huber/Bundesrepublik Deutschland*; vezi, în special, punctul 68.

960 Convenția 108 modernizată, articolul 5 alineatul (4) litera (b).

961 *Ibidem*, articolul 11 alineatul (2).

962 Recomandarea Rec(97)18 din 30 septembrie 1997 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția datelor cu caracter personal colectate și prelucrate în scopuri statistice.

Datele colectate de un operator în scopuri statistice nu pot fi utilizate în niciun alt scop. Datele colectate în alte scopuri decât cele statistice trebuie să fie disponibile pentru o utilizare ulterioară în scopuri statistice. Recomandarea privind datele statistice permite și comunicarea de date către părți terțe, dar exclusiv în scopuri statistice. În astfel de cazuri, părțile trebuie să ajungă la un acord – consemnat în scris – cu privire la gradul de utilizare ulterioară legitimă în scopuri statistice. Întrucât acest lucru nu poate înlocui consimțământul persoanei vizate – în cazul în care acest consimțământ este necesar – legislația națională trebuie să prevadă garanții adecvate pentru a reduce la minimum riscurile de utilizare incorectă a datelor cu caracter personal, cum ar fi obligația de anonimizare sau pseudonimizare a datelor înainte de a fi divulgate.

Legislația națională trebuie să prevadă obligații speciale de păstrare a secretului profesional pentru profesioniștii din domeniul cercetărilor statistice, cum se întâmplă de obicei în cazul statisticilor oficiale. Acest lucru trebui să se extindă, de asemenea, la intervievatori și la alte persoane care colectează date cu caracter personal, în cazul în care aceștia sunt angajați în colectarea de date de la persoanele vizate sau de la alte persoane.

În cazul în care un studiu statistic efectuat pe baza datelor cu caracter personal nu este autorizat prin lege, trebuie obținut consimțământul persoanelor vizate față de utilizarea datelor lor pentru ca studiul să fie legitim sau acestora trebuie să li se acorde posibilitatea de a obiecta. În cazul în care datele cu caracter personal sunt colectate în scopuri statistice de către intervievatori, persoanele vizate trebuie să fie informate în mod clar dacă divulgarea datelor este sau nu obligatorie în temeiul legislației naționale.

În cazul în care un studiu statistic nu poate fi efectuat cu date anonime, fiind necesare date cu caracter personal, datele colectate în scopul respectiv trebuie să fie anonimizate cât mai curând posibil. Rezultatele studiului statistic nu trebuie, în niciun caz, să permită identificarea persoanelor vizate, cu excepția cazului în care este evident că acest lucru nu prezintă niciun risc.

După realizarea analizei statistice, datele cu caracter personal utilizate trebuie șterse sau anonimizate. În astfel de cazuri, Recomandarea privind datele statistice sugerează ca datele de identificare să fie stocate separat de alte date cu caracter personal. Acest lucru înseamnă, de exemplu, că fie cheia de criptare, fie lista cu sinonimele de identificare trebuie păstrată separat de celelalte date.

9.5. Date financiare

Principalele elemente

- Deși datele financiare nu sunt considerate date sensibile în cadrul Convenției 108 modernizate sau al Regulamentului general privind protecția datelor, prelucrarea acestora necesită anumite garanții specifice în vederea asigurării exactității și securității datelor.
- Sistemele de plată electronică necesită o protecție a datelor încorporată, și anume protecția datelor din faza de proiectare și protecția implicită a datelor.
- În acest domeniu pot apărea probleme specifice de protecție a datelor, cauzate de necesitatea de a dispune de mecanisme adecvate de autentificare.

Exemplu: În cauza *Michaud/Franța*[963], reclamantul, un avocat francez, a contestat obligația care îi revenea în temeiul dreptului francez de a raporta suspiciuni privind posibilele activități de spălare a banilor de către clienții săi. CEDO a considerat că impunerea obligației avocaților de a raporta informații cu privire la o altă persoană, informații care intrau în posesia lor în cadrul discuțiilor cu caracter profesional, constituie o ingerință în dreptul avocaților la respectarea corespondenței și a vieții private, prevăzut la articolul 8 din Convenția europeană a drepturilor omului, întrucât noțiunea respectivă vizează activitățile cu caracter profesional sau de afaceri. Cu toate acestea, ingerința era în conformitate cu legea și urmărea un scop legitim, respectiv prevenirea dezordinii și a criminalității. Întrucât avocații au obligația de a raporta activitățile suspecte doar în circumstanțe foarte limitate, CEDO a constatat că obligația respectivă este proporțională. Curtea a concluzionat că nu s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Exemplu: În cauza *M.N. și alții/San Marino* [964], reclamantul, cetățean italian, a încheiat un contract de fiducie cu o societate anchetată. Aceasta însemna că societatea făcea obiectul descoperirii și sechestrării unor exemplare ale documentelor (electronice). Reclamantul a depus o plângere la instanța din San Marino, susținând că nu există nicio legătură între el și presupusele

963 Hotărârea CEDO din 6 decembrie 2012 în cauza *Michaud/Franța*, nr. 12323/11. Vezi, de asemenea, Hotărârea CEDO din 16 decembrie 1992 în cauza *Niemietz/Germania*, nr. 13710/88, punctul 29, și Hotărârea CEDO din 25 iunie 1997 în cauza *Halford/Regatul Unit*, nr. 20605/92, punctul 42.

964 Hotărârea CEDO din 7 iulie 2015 în cauza *M.N. și alții/San Marino*, nr. 28005/12.

infracțiuni. Cu toate acestea, instanța i-a declarat plângerea inadmisibilă, întrucât reclamantul nu era „parte interesată". CEDO a constatat că, deși reclamantul era în dezavantaj semnificativ în ceea ce privește protecția judiciară în comparație cu o „parte interesată", datele sale au făcut totuși obiectul operațiunilor de descoperire și sechestrare. Prin urmare, Curtea a considerat că s-a încălcat articolul 8.

Exemplu: În cauza *G.S.B./Elveția*[965], detaliile contului bancar al solicitantului au fost transmise autorităților fiscale din SUA pe baza acordului de cooperare administrativă dintre Elveția și SUA. CEDO a constatat că transmiterea datelor nu încalcă articolul 8 din Convenția europeană a drepturilor omului, deoarece ingerința în dreptul reclamantului la respectarea vieții private era prevăzută de lege, urmărea un scop legitim și era proporțională cu interesul public în cauză.

Aplicarea cadrului juridic general privind protecția datelor (astfel cum este stabilit în Convenția 108) în contextul plăților a fost elaborată de **CoE** în Recomandarea Rec(90)19 din 1990[966]. Această recomandare clarifică domeniul colectării și utilizării legale a datelor în contextul plăților, în special al plăților cu cardul. Recomandarea oferă, de asemenea, propuneri detaliate legiuitorilor naționali în ceea ce privește normele de divulgare către părți terțe a datelor privind plățile, termenele de păstrare a datelor, transparență, securitatea datelor și fluxurile transfrontaliere de date, precum și supravegherea și căile de atac. CoE a elaborat, de asemenea, un aviz privind transferul datelor fiscale[967], care oferă recomandări și menționează aspectele care trebuie luate în considerare atunci când se efectuează transferuri de date fiscale.

CEDO permite transmiterea datelor financiare – în mod specific, detaliile contului bancar al unei persoane – în temeiul articolului 8 din Convenția europeană a drepturilor omului, dacă această transmitere este prevăzută de lege, urmărește un scop legitim și este proporțională cu interesul public în cauză[968].

965 Hotărârea CEDO din 22 decembrie 2015 în cauza *G.S.B./Elveția*, nr. 28601/11.

966 Recomandarea R(90)19 din 13 septembrie 1990 a Comitetului de Miniștri al Consiliului Europei privind protecția datelor cu caracter personal utilizate pentru plăți și alte operațiuni conexe.

967 Consiliul Europei, Comitetul consultativ al Convenției 108, Avizul din 4 iunie 2014 privind implicațiile asupra protecției datelor ale mecanismelor de schimburi automate interstatale de date în scopuri administrative și fiscale.

968 Hotărârea CEDO din 22 decembrie 2015 în cauza *G.S.B./Elveția*, nr. 28601/11.

În ceea ce privește **legislația UE**, sistemele de plată electronică în care sunt implicate operațiuni de prelucrare a datelor cu caracter personal trebuie să respecte Regulamentul general privind protecția datelor. Prin urmare, aceste sisteme trebuie să asigure protecția datelor din faza de proiectare și protecția implicită a datelor. Protecția datelor din faza de proiectare obligă operatorul să introducă măsuri tehnice și organizatorice adecvate pentru punerea în aplicare a principiilor de protecție a datelor. Protecția implicită a datelor înseamnă că operatorul trebuie să se asigure că doar datele cu caracter personal necesare pentru un scop specific pot fi prelucrate în mod implicit (vezi secțiunea 4.4). În ceea ce privește datele financiare, CJUE a stabilit că datele fiscale transferate pot constitui date cu caracter personal[969]. Grupul de lucru „Articolul 29" a emis orientări pentru statele membre, inclusiv criterii care să asigure respectarea normelor de protecție a datelor în cazul schimbului automat de date cu caracter personal în scopuri fiscale, efectuat prin mijloace automate[970]. În plus, au fost adoptate o serie de instrumente juridice pentru a reglementa piețele financiare și activitățile instituțiilor de credit și ale firmelor de investiții[971]. Alte instrumente juridice acordă sprijin pentru combaterea utilizărilor abuzive ale informațiilor privilegiate și a manipulărilor pieței[972]. Domeniile principale care au un impact asupra protecției datelor sunt:

- păstrarea înregistrărilor cu privire la tranzacțiile financiare;
- transferul datelor cu caracter personal către țări terțe;

969 CJUE, C-201/14, *Smaranda Bara și alții/Casa Națională de Asigurări de Sănătate și alții*, 1 octombrie 2015, punctul 29.

970 Grupul de lucru pentru protecția datelor instituit în temeiul articolului 29 (2015), Declarația grupului de lucru instituit în temeiul articolului 29 privind schimburile interstatale automate de date cu caracter personal în scopuri fiscale, 14/RO WP 230.

971 Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE, JO 2014 L 173; Regulamentul (UE) nr. 600/2014 al Parlamentului European și al Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Regulamentului (UE) nr. 648/2012, JO 2014 L 173; Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit și a firmelor de investiții, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE, JO 2013 L 176.

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

- înregistrarea convorbirilor telefonice sau a comunicațiilor electronice, inclusiv prerogativa autorităților competente de a solicita înregistrări ale convorbirilor telefonice și ale datelor de transfer;

- divulgarea informațiilor cu caracter personal, inclusiv publicarea sancțiunilor;

- competențele de supraveghere și de investigare ale autorităților competente, inclusiv competența de a efectua inspecții la fața locului și de a pătrunde în incinte private în vederea confiscării de documente;

- mecanismele de raportare a încălcărilor, respectiv regimurile de avertizare în interes public;

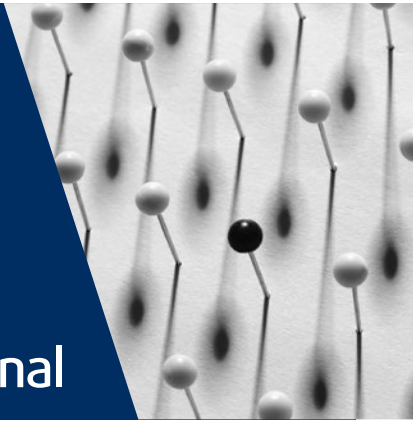
- cooperarea între autoritățile competente ale statelor membre și Autoritatea Europeană pentru Valori Mobiliare și Piețe (ESMA).

Se abordează în mod specific și alte probleme din aceste domenii, inclusiv colectarea de date cu privire la situația financiară a persoanelor vizate[973] sau plățile transfrontaliere prin transferuri bancare, care generează, inevitabil, fluxuri de date cu caracter personal[974].

973 Regulamentul (CE) nr. 1060/2009 al Parlamentului European și al Consiliului din 16 septembrie 2009 privind agențiile de rating de credit, JO 2009 L 302, astfel cum a fost modificat ultima dată prin Directiva 2014/51/UE a Parlamentului European și a Consiliului din 16 aprilie 2014 de modificare a Directivelor 2003/71/CE și 2009/138/CE și a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 1094/2010 și (UE) nr. 1095/2010 în ceea ce privește competențele Autorității europene de supraveghere (Autoritatea Europeană de Asigurări și Pensii Ocupaționale) și ale Autorității europene de supraveghere (Autoritatea Europeană pentru Valori Mobiliare și Piețe), JO 2014 L 153; Regulamentul (UE) nr. 462/2013 al Parlamentului European și al Consiliului din 21 mai 2013 de modificare a Regulamentului (CE) nr. 1060/2009 privind agențiile de rating de credit, JO 2013 L 146.

974 Directiva 2007/64/CE a Parlamentului European și a Consiliului din 13 noiembrie 2007 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 97/7/CE, 2002/65/CE, 2005/60/CE și 2006/48/CE și de abrogare a Directivei 97/5/CE, JO 2007 L 319, astfel cum a fost modificată prin Directiva 2009/111/CE a Parlamentului European și a Consiliului din 16 septembrie 2009 de modificare a Directivelor 2006/48/CE, 2006/49/CE și 2007/64/CE în ceea ce privește băncile afiliate instituțiilor centrale, anumite elemente ale fondurilor proprii, expunerile mari, reglementările privind supravegherea, precum și gestionarea crizelor, JO 2009 L 302.

10 Provocările moderne în domeniul protecției datelor cu caracter personal



Era digitală sau era tehnologiei informației se caracterizează prin utilizarea pe scară largă a computerelor, a internetului și a tehnologiilor digitale. Aceasta implică colectarea și prelucrarea unor cantități mari de date, inclusiv date cu caracter personal. Colectarea și prelucrarea datelor cu caracter personal într-o economie globalizată înseamnă că fluxurile transfrontaliere de date se multiplică. O astfel de prelucrare poate aduce beneficii semnificative și vizibile în viața de zi cu zi: motoarele de căutare facilitează accesul la un volum considerabil de informații și cunoștințe, serviciile de rețele sociale permit oamenilor din întreaga lume să comunice, să își exprime opiniile și să mobilizeze sprijin pentru cauze sociale, ecologice și politice, iar întreprinderile și consumatorii beneficiază de tehnici de marketing eficace și eficiente, care stimulează economia. Tehnologia și prelucrarea datelor cu caracter personal constituie, de asemenea, instrumente indispensabile pentru autoritățile statului în efortul de combatere a criminalității și a terorismului. În mod similar, datele masive – colectarea, stocarea și analiza unor cantități mari de informații pentru a identifica tipare și a prezice comportamente – „pot fi o sursă de valoare semnificativă pentru societate, sporind productivitatea, performanța sectorului public și participarea socială”[975].

În pofida multiplelor avantaje, era digitală ridică, de asemenea, provocări în privința respectării vieții private și a protecției datelor, deoarece se colectează și se prelucrează în moduri tot mai complexe și mai opace cantități uriașe de informații cu caracter personal. Progresul tehnologic a condus la apariția unor seturi de date masive, care pot fi corelate și analizate în detaliu pentru identificarea de tipare sau

975 Consiliul Europei, Comitetul consultativ al Convenției 108, *Orientări privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive*, T-PD(2017)01, Strasbourg, 23 ianuarie 2017.

pentru adoptarea unor decizii pe baza algoritmilor, ceea ce poate oferi o imagine de o profunzime fără precedent asupra comportamentului uman și a vieții private[976].

Noile tehnologii sunt puternice și pot fi deosebit de periculoase dacă ajung în posesia unor persoane rău-intenționate. Autoritățile de stat care desfășoară activități de supraveghere în masă susceptibile de a utiliza aceste tehnologii reprezintă un exemplu al impactului semnificativ pe care tehnologiile respective îl pot avea asupra drepturilor persoanelor fizice. Dezvăluirile lui Edward Snowden din 2013 privind utilizarea programelor de supraveghere pe scară largă a comunicațiilor prin internet și telefonie de către agențiile de informații din unele state au provocat preocupări semnificative cu privire la pericolele pe care le generează activitățile de supraveghere în ceea ce privește viața privată, guvernarea democratică și libertatea de exprimare. Supravegherea în masă, tehnologiile care permit stocarea și prelucrarea globală a informațiilor cu caracter personal și accesul în bloc la date pot aduce atingere substanței înseși a dreptului la respectarea vieții private[977]. În plus, acestea pot avea un efect negativ asupra culturii politice și un efect de descurajare a democrației, creativității și inovării[978]. Teama că statul le poate urmări și analiza în permanență comportamentul și acțiunile poate descuraja cetățenii să își exprime opiniile cu privire la anumite aspecte și poate conduce la atitudini de îngrijorare și timorare[979]. Aceste provocări au determinat o serie de autorități publice, centre de cercetare și organizații ale societății civile să analizeze impactul potențial al noilor tehnologii asupra societății. În 2015, Autoritatea Europeană pentru Protecția Datelor a lansat mai multe inițiative menite să evalueze implicațiile etice ale datelor masive și ale internetului obiectelor. Trebuie menționat faptul că AEPD a înființat un Grup consultativ pentru etică, acesta urmărind stimularea „unei discuții deschise și informate privind etica digitală, care să permită UE să asigure avantajele tehnologiei pentru societate și economie și în același

976 Rezoluția Parlamentului European din 14 martie 2017 referitoare la implicațiile megadatelor asupra drepturilor fundamentale: viața privată, protecția datelor, nediscriminarea, securitatea și impunerea respectării legii (P8_TA-PROV(2017)0076, Strasbourg.

977 Vezi Adunarea Generală a ONU, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (Raportul raportorului special privind promovarea și protejarea drepturilor omului și a libertăților fundamentale în cadrul acțiunilor de combatere a terorismului), Ben Emmerson, A/69/397, 23 septembrie 2014, punctul 59. Vezi, de asemenea, CEDO, *Fișă informativă privind supravegherea în masă*, iulie 2017.

978 Avizul 7/2015 din 19 noiembrie 2015 al AEPD privind *Răspunsul la provocările Big Data*, Bruxelles.

979 Vezi, în special, Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții și Kärntner Landesregierung și alții*, punctul 37.

timp să consolideze drepturile și libertățile persoanelor fizice, în special drepturile acestora la viața privată și protecția datelor"[980].

Prelucrarea datelor cu caracter personal constituie, de asemenea, un instrument puternic atunci când face parte din arsenalul corporațiilor. În prezent, această prelucrare poate dezvălui informații detaliate despre starea de sănătate sau situația financiară a unei persoane, informații care sunt utilizate ulterior de corporații în procesul de adoptare a unor decizii importante pentru persoanele fizice, cum ar fi prima de asigurare de sănătate care ar trebui să li se aplice sau bonitatea. Tehnicile de prelucrare a datelor pot avea, de asemenea, un impact asupra proceselor democratice, atunci când sunt folosite de politicieni sau de corporații pentru a influența alegerile – de exemplu, acțiuni prin care li se adresează conținut personalizat (micro-targeting) alegătorilor. Cu alte cuvinte, deși viața privată a fost percepută inițial ca un drept al persoanelor fizice la protecție împotriva ingerințelor nejustificate ale autorităților publice, în era modernă, aceasta poate fi amenințată și de puterile actorilor privați. Acest lucru ridică întrebări cu privire la utilizarea tehnologiei și a analizei predictive în deciziile care afectează viața de zi cu zi a persoanelor fizice și întărește necesitatea de a se asigura faptul că orice prelucrare a datelor cu caracter personal respectă cerințele privind drepturile fundamentale.

Protecția datelor este legată în mod intrinsec de schimbările tehnologice, sociale și politice. Prin urmare, este imposibil de întocmit o listă exhaustivă a provocărilor viitoare. Prezentul capitol analizează câteva aspecte legate de datele masive, de rețelele sociale online și de piața unică digitală a UE. Nu este vorba despre o evaluare exhaustivă a acestor domenii din perspectiva protecției datelor, ci de sublinierea multitudinii de interacțiuni posibile între activitățile umane noi sau actualizate și protecția datelor.

980 Decizia Autorității Europene pentru Protecția Datelor (AEPD) din 3 decembrie 2015 privind înființarea unui grup consultativ extern cu privire la dimensiunile etice ale protecției datelor („Grupul consultativ pentru etică"), considerentul 5.

10.1. Datele masive, algoritmii și inteligența artificială

Principalele elemente

- Inovațiile disruptive din domeniul TIC creează un nou stil de viață, în care relațiile sociale, afacerile, serviciile private și publice sunt interconectate digital, generând astfel o cantitate din ce în ce mai mare de date, dintre care multe sunt date cu caracter personal.
- Guvernele, întreprinderile și cetățenii acționează tot mai mult într-o economie bazată pe date, în care datele în sine au devenit bunuri de valoare.
- Conceptul de date masive se referă atât la datele în sine, cât și la analizarea acestora.
- Datele cu caracter personal prelucrate prin analize de date masive intră sub incidența legislației UE și a CoE.
- Derogările de la normele și drepturile în materie de protecție a datelor se limitează la anumite drepturi și la situații specifice în care exercițiul unui drept s-ar putea dovedi imposibil sau ar necesita eforturi disproporționate din partea operatorilor de date.
- În general, procesul decizional complet automatizat este interzis, cu excepția unor cazuri specifice.
- Conștientizarea și controlul de către persoanele fizice sunt esențiale pentru asigurarea exercitării drepturilor.

În lumea noastră din ce în ce mai digitizată, fiecare activitate lasă o urmă digitală care poate fi colectată, prelucrată și evaluată sau analizată. Odată cu apariția noilor tehnologii de informare și de comunicare, se colectează și se înregistrează tot mai multe date[981]. Până de curând, nicio tehnologie nu putea analiza sau evalua volume mari de date, nici nu putea formula concluzii utile pe baza acestora. Datele erau pur și simplu prea numeroase pentru a fi evaluate, prea complexe, prea slab structurate și mobile pentru a permite identificarea unor tendințe și obiceiuri.

981 Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, intitulată „Către o economie de succes bazată pe date”, COM(2014) 442 final din 2 iulie 2014, Bruxelles.

10.1.1. Definirea datelor masive, a algoritmilor și a inteligenței artificiale

Datele masive

Termenul „date masive" este un termen tehnic modern care se poate referi la diverse concepte, în funcție de context. Acesta cuprinde în mod obișnuit „capacitatea tehnologică crescândă de a colecta, prelucra și extrage cunoștințe noi și predictive din seturi de date caracterizate prin volum, viteză și varietate mare"[982]. Prin urmare, conceptul de date masive acoperă atât datele în sine, cât și analizarea acestora.

Sursele datelor sunt de diferite tipuri și includ persoanele și datele lor cu caracter personal, mașini sau senzori, informații despre climă, imagini prin satelit, instantanee și videoclipuri digitale sau semnale GPS. O mare parte a datelor și informațiilor sunt însă date cu caracter personal – de la nume la fotografii, adrese de e-mail, detalii bancare, date de urmărire GPS, postări pe site-uri de socializare în rețea, informații medicale sau adresa IP a unui computer[983].

Datele masive se referă, de asemenea, la **prelucrarea**, analiza și evaluarea volumelor de date și a informațiilor disponibile pentru a obține informații utile în scopul analizei volumelor mari de date. Aceasta înseamnă că datele și informațiile colectate pot fi utilizate în alte scopuri decât cele preconizate inițial, de exemplu pentru a determina tendințele statistice sau pentru furnizarea unor servicii personalizate, cum ar fi publicitatea. De fapt, în cazul în care există tehnologii de colectare, prelucrare și evaluare a volumelor mari de date, orice tip de informație poate fi combinată și reevaluată: tranzacțiile financiare, bonitatea, tratamentul medical, consumul privat, activitatea profesională, datele de urmărire și drumul parcurs, utilizarea internetului, a cardurilor electronice și a smartphone-urilor, monitorizarea video sau a comunicațiilor. Analiza datelor masive aduce o nouă dimensiune cantitativă a datelor, care poate

982 Consiliul Europei, Comitetul consultativ al Convenției 108, Orientări privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive, 23 ianuarie 2017, p. 2; Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, intitulată „Către o economie de succes bazată pe date", COM(2014) 442 final din 2 iulie 2014, Bruxelles, p. 4; Recomandarea Y.3600 din 2015 a Uniunii Internaționale a Telecomunicațiilor, intitulată „Big Data – Cloud computing based requirements and capabilities" (Datele masive – cerințe și capabilități bazate pe tehnologia de tip cloud computing).

983 Fișa informativă a Comisiei Europene privind reforma UE în domeniul protecției datelor în contextul datelor masive; Consiliul Europei, Comitetul consultativ al Convenției 108, Orientări privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive, 23 ianuarie 2017, p. 2.

fi evaluată și utilizată în timp real, de exemplu pentru a oferi consumatorilor servicii personalizate.

Algoritmi și inteligență artificială

Inteligența artificială (IA) se referă la inteligența mașinilor care acționează ca „agenți inteligenți". În calitate de agenți inteligenți, cu ajutorul software-ului, anumite dispozitive au capacitatea de a percepe mediul în care se află și de a întreprinde acțiuni pe baza algoritmilor. Termenul IA se aplică în situațiile în care o mașină imită funcțiile „cognitive" – cum ar fi învățarea și rezolvarea problemelor –, asociate în mod normal cu persoanele fizice[984]. Pentru a imita procesul de luare a deciziilor, tehnologiile moderne și software-ul utilizează algoritmi pe baza cărora dispozitivele iau „decizii automate". Cea mai potrivită descriere a unui algoritm este aceea de procedură compusă din mai mulți pași și utilizată pentru calcul, prelucrare de date, evaluare, raționament și luare de decizii automatizate.

În mod similar cu analiza datelor masive, IA și procesele decizionale automatizate ale acesteia necesită compilarea și prelucrarea unor volume mari de date. Aceste date pot proveni de la dispozitivul însuși (temperatura frânelor, a combustibilului etc.) sau din mediul înconjurător. Crearea de profiluri, de exemplu, este un proces care se poate baza pe luarea deciziilor în mod automatizat, pe baza unor modele sau factori prestabiliți.

Exemplu: Crearea de profiluri și publicitatea direcționată

Crearea de profiluri pe baza datelor masive presupune căutarea unor modele care să reflecte „caracteristicile unui anumit tip de personalitate" – de exemplu, situația în care site-urile de cumpărături propun produse care „s-ar putea să vă placă, de asemenea", pe baza informațiilor colectate despre produsele plasate anterior în coșul de cumpărături al unui client. Cu cât sunt disponibile mai multe date, cu atât este mai clar mozaicul. Smartphone-ul, de exemplu, este un chestionar complex, pe care utilizatorul îl completează cu fiecare utilizare, conștient sau inconștient.

984 Stuart Russel și Peter Norvig, *Artificial Intelligence: A Modern Approach (ediția a doua)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, pp. 27, 32-58, 968-972; Stuart Russel și Peter Norvig, *Artificial Intelligence: A Modern Approach (ediția a treia)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, p. 2.

Psihologia modernă – studiul științific al personalității – folosește metoda OCEAN, pe baza căreia determină tipurile de personalitate abordate. Cele cinci caracteristici majore („Big Five") ale personalității sunt: deschiderea (cât de deschisă este persoana la nou), conștiinciozitatea (cât de perfecționistă este persoana), extraversiunea (cât de sociabilă este persoana), agreabilitatea (cât de agreabilă este persoana), nevrozism (cât de vulnerabilă este persoana). Aceste informații creează profilul persoanei în cauză, descriindu-i nevoile și temerile, modul în care se va comporta etc. Profilul este completat apoi cu alte informații despre persoana în cauză, obținute din orice surse disponibile: de la brokeri de date, rețele sociale (inclusiv „aprecierile" postărilor și fotografiile postate), muzica ascultată online sau date GPS și date de urmărire.

Masa profilurilor create prin tehnici de analiză a datelor masive este apoi comparată pentru a identifica tipare similare și pentru a construi grupuri de personalități. Informațiile despre comportamentele și atitudinile anumitor personalități sunt, astfel, inversate. Prin accesul la datele masive și utilizarea acestora, testul de personalitate este inversat, informațiile despre comportament și atitudine fiind utilizate de această dată pentru a descrie personalitatea individului. Prin intermediul informațiilor combinate despre „aprecierile" acordate în rețelele sociale, datele de urmărire, muzica ascultată sau filmele vizionate, se poate forma o imagine clară a personalității cuiva, ceea ce permite întreprinderilor să plaseze mesaje publicitare și/sau informații adaptate „personalității" individului respectiv. Mai presus de toate, aceste informații pot fi prelucrate în timp real[985].

10.1.2. Ponderarea beneficiilor și a riscurilor datelor masive

Tehnicile moderne de prelucrare pot gestiona volume mari de date, pot importa rapid altele noi, asigură prelucrarea în timp real a informațiilor, cu răspunsuri rapide (chiar și în cazul solicitărilor complexe), oferă posibilitatea unor solicitări multiple și simultane și pot analiza diferite tipuri de informații (fotografii, texte sau numere). Aceste inovații tehnologice fac posibile structurarea, prelucrarea și evaluarea

985 Tehnicile de prelucrare și software-ul de nouă generație evaluează informațiile despre ceea ce apreciază o persoană, analizează momentul cumpărăturilor online sau adaugă articole în coșul de cumpărături online în timp real și poate propune, pe baza informațiilor colectate, „produse" de care persoana în cauză ar putea fi interesată.

volumelor de date și informații în timp real[986]. Prin creșterea exponențială a cantității de date disponibile și analizate, se pot obține rezultate care ar fi imposibile în cazul unei analize la scară mai mică. Datele masive au contribuit la dezvoltarea unui nou sector economic, în care pot apărea noi servicii atât pentru întreprinderi, cât și pentru consumatori. Valoarea datelor cu caracter personal ale cetățenilor UE are potențialul de a crește până la aproape 1 trilion EUR pe an până în 2020[987]. Prin urmare, datele masive pot oferi noi **oportunități** – care rezultă din evaluarea volumelor mari de date – pentru noi perspective sociale, economice sau științifice care pot aduce beneficii atât persoanelor fizice, cât și întreprinderilor și guvernelor[988].

Analizele datelor masive pot dezvălui tipare existente între diferite surse și seturi de date, permițând înțelegerea aprofundată în domenii precum știința și medicina. Acesta este, de exemplu, cazul unor domenii precum sănătatea, securitatea alimentară, sistemele inteligente de transport, eficiența energetică sau planificarea urbană. Această analiză în timp real a informațiilor poate fi utilizată pentru a îmbunătăți sistemele implementate. În cercetare se pot obține noi perspective prin combinarea unor volume mari de date cu evaluările statistice, în special în discipline în care, până în prezent, o mare parte a datelor au fost evaluate numai manual. Se pot dezvolta tratamente noi, adaptate pacienților individuali, pe baza comparațiilor cu masa de informații disponibile. Întreprinderile speră că analiza datelor masive le va permite să obțină avantaje concurențiale, să genereze eventuale economii și să creeze noi domenii de activitate prin furnizarea unor servicii direct către clienți, în mod individualizat. Agențiile guvernamentale speră să obțină îmbunătățiri în domeniul justiției penale. Strategia privind piața unică digitală pentru Europa a Comisiei recunoaște

986 Dezvoltarea de programe de calculator pentru procesarea volumelor mari de date este încă într-o fază incipientă. S-au dezvoltat însă recent programe analitice, în special pentru analiza în timp real de date și informații masive, în legătură cu activitățile persoanelor. Posibilitatea de a analiza și procesa în mod structurat volume mari de date a oferit noi moduri de creare de profiluri și de publicitate direcționată. Comisia Europeană, Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor – Către o economie de succes bazată pe date COM(2014) 442 final din 2 iulie 2014, Bruxelles; Fișa informativă a Comisiei Europene privind reforma UE în domeniul protecției datelor în contextul datelor masive și Consiliul Europei, Orientări privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive, 23 ianuarie 2017, p.2.

987 Fișa informativă a Comisiei Europene privind reforma UE în domeniul protecției datelor în contextul datelor masive.

988 Rezoluția privind datele masive a Conferinței internaționale a comisarilor pentru protecția datelor și a vieții private (2014); Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, intitulată „Către o economie de succes bazată pe date", COM(2014) 442 final din 2 iulie 2014, Bruxelles, p. 2; Fișa informativă a Comisiei Europene privind reforma UE în domeniul protecției datelor în contextul datelor masive; Orientările Consiliului Europei privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive, 23 ianuarie 2017, p. 1.

potențialul tehnologiilor bazate pe date, al serviciilor și al datelor masive de a acționa drept catalizator pentru creșterea economică, inovarea și digitalizarea în UE[989].

Cu toate acestea, datele masive generează și **riscuri**, asociate în general cu cele trei atribute ale lor, numite și „cei trei V": volumul, viteza și varietatea datelor prelucrate. Volumul se referă la cantitatea de date prelucrate, varietatea la numărul și diversitatea tipurilor de date, în timp ce viteza se referă la viteza de prelucrare a datelor. Câteva considerații specifice privind protecția datelor apar, în special, atunci când se utilizează analize ale datelor masive pe seturi mari de date pentru a extrage cunoștințe noi și predictive în scopul luării unor decizii privind persoane individuale și/sau grupuri[990]. Riscurile în ceea ce privește protecția datelor și respectarea vieții private legate de datele masive au fost evidențiate în avizele AEPD și ale Grupului de lucru „Articolul 29", în rezoluțiile Parlamentului European și în documentele strategice ale Consiliului Europei[991].

Riscurile pot include utilizarea necorespunzătoare a datelor de către cei care au acces la masa de informații, prin manipulare, discriminare sau oprimarea anumitor persoane sau grupuri din societate[992]. În cazul în care se colectează, se prelucrează și se evaluează volume mari de date sau informații cu caracter personal despre comportamentul individual, exploatarea acestora poate conduce la încălcări semnificative ale drepturilor și libertăților fundamentale, care depășesc dreptul la respectarea vieții private. Nu se poate măsura exact gradul în care pot fi afectate viața privată și datele cu caracter personal. Parlamentul European a identificat lipsa metodologiilor pentru realizarea unei evaluări bazate pe dovezi a impactului total al datelor masive,

989 Rezoluția Parlamentului European din 14 martie 2017 referitoare la implicațiile megadatelor asupra drepturilor fundamentale: viața privată, protecția datelor, nediscriminarea, securitatea și impunerea respectării legii [2016/2225(INI)].

990 Consiliul Europei, Comitetul consultative al Convenției 108, Orientări privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive, 23 ianuarie 2017, p.2.

991 Vezi, de exemplu, Avizul 7/2015 al AEPD privind *Răspunsul la provocările Big Data*; Avizul 8/2016 al AEPD din 23 septembrie 2016, intitulat *Aplicarea coerentă a drepturilor fundamentale în era megadatelor*; Rezoluția Parlamentului European din 14 martie 2017 referitoare la implicațiile megadatelor asupra drepturilor fundamentale: viața privată, protecția datelor, nediscriminarea, securitatea și impunerea respectării legii, P8_TA(2017)0076, Strasbourg; Consiliul Europei, Comitetul consultativ al Convenției 108, Orientări privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive, T-PD(2017)01, Strasbourg, 23 ianuarie 2017.

992 Rezoluția privind datele masive a Conferinței internaționale a comisarilor pentru protecția datelor și a vieții private (2014).

dar există dovezi care sugerează că analiza datelor masive poate avea un impact orizontal semnificativ, atât în sectorul public, cât și în cel privat[993].

Regulamentul general privind protecția datelor include dispoziții privind dreptul de a nu face obiectul unui proces decizional automatizat, inclusiv crearea de profiluri[994]. Respectarea vieții private intră în discuție atunci când exercitarea dreptului la opoziție necesită intervenția umană, permițând persoanelor vizate să își exprime punctul de vedere și să conteste decizia[995]. Acest lucru poate provoca dificultăți în ceea ce privește asigurarea unui nivel adecvat de protecție a datelor cu caracter personal dacă, de exemplu, nu este posibilă intervenția umană sau dacă algoritmii sunt prea complecși și volumul de date implicat este prea mare pentru a oferi persoanelor fizice justificări pentru anumite decizii și/sau informații prealabile în vederea obținerii consimțământului acestora. Un exemplu de utilizare a IA și de proces decizional automatizat poate fi găsit în evoluțiile recente ale evaluării solicitărilor de credite ipotecare sau în procesele de recrutare a angajaților. Cererile și candidaturile în cauză sunt respinse sau refuzate pe baza faptului că solicitanții nu îndeplinesc anumiți parametri sau factori prestabiliți.

10.1.3. Aspecte legate de protecția datelor

În ceea ce privește protecția datelor, aspectele principale se referă, pe de o parte, la volumul și varietatea datelor cu caracter personal prelucrate, iar pe de altă parte, la prelucrare și la rezultatele acesteia. Introducerea algoritmilor și a software-ului complex pentru a transforma datele masive într-o resursă pentru luarea deciziilor afectează în special persoanele fizice și grupurile, mai ales în cazul creării de profiluri sau de categorii și, în cele din urmă, ridică numeroase probleme de protecție a datelor[996].

Identificarea operatorilor și a persoanelor împuternicite de operatori și răspunderea acestora

Datele masive și IA ridică diverse întrebări cu privire la identificarea operatorilor și a persoanelor împuternicite de operatori și la răspunderea acestora: atunci când se

993 Rezoluția Parlamentului European din 14 martie 2017 referitoare la implicațiile megadatelor asupra drepturilor fundamentale: viața privată, protecția datelor, nediscriminarea, securitatea și impunerea respectării legii [2016/2225(INI)].

994 Regulamentul general privind protecția datelor, articolul 22.

995 *Ibidem*, articolul 22 alineatul (3).

996 Consiliul Europei, Comitetul consultativ al Convenției 108, Orientări privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive, 23 ianuarie 2017, p 2.

colectează și se prelucrează astfel de volume mari de date, cine este proprietarul datelor? Când datele sunt prelucrate de mașini inteligente și de software, cine este operatorul? Care sunt responsabilitățile exacte ale fiecărui actor implicat în prelucrare? În ce scop pot fi folosite datele masive?

Problema răspunderii în contextul IA devine cu atât mai dificilă atunci când o IA ia o decizie bazată pe o operațiune de prelucrare a datelor dezvoltată chiar de respectiva IA. Regulamentul general privind protecția datelor oferă un cadru juridic pentru răspunderea operatorului de date și a persoanei împuternicite de operator. Prelucrarea ilegală a datelor cu caracter personal atrage răspunderea operatorului de date și a persoanei împuternicite de operator[997]. Inteligența artificială și procesul decizional automatizat ridică întrebări cu privire la entitatea răspunzătoare pentru încălcările care afectează viața privată a persoanelor vizate în cazurile în care complexitatea și cantitatea datelor prelucrate nu pot fi atribuite cu certitudine. În cazul în care IA și algoritmii sunt considerate produse, acest lucru creează probleme de armonizare între răspunderea personală, care este reglementată de Regulamentul general privind protecția datelor, respectiv răspunderea pentru produse, care nu este reglementată de acesta[998]. Acest lucru necesită norme privind răspunderea care să compenseze decalajul dintre răspunderea personală și răspunderea pentru produse în sectorul roboticii și al IA, inclusiv în cazul proceselor decizionale automatizate, de exemplu[999].

Impactul asupra principiilor protecției datelor

Caracterul, analiza și utilizarea datelor masive descrise mai sus creează anumite dificultăți în ceea ce privește aplicarea unor principii fundamentale tradiționale ale legislației europene privind protecția datelor[1000]. Aceste dificultăți se referă în principal la principiile legalității, reducerii la minimum a datelor, limitărilor legate de scop și transparenței.

997 Regulamentul general privind protecția datelor, articolele 77-79 și considerentul 82.

998 Parlamentul European, „European Civil Law Rules in Robotics" (Normele privind robotica în cadrul dreptului civil european), Direcția Generală Politici Interne, octombrie 2016, p. 14.

999 Discursul lui Roberto Viola din cadrul seminarului pentru mass-media privind legislația europeană în domeniul roboticii organizat de Parlamentul European. (DISCURS 16/02/2017); anunțul Parlamentului European referitor la solicitarea adresată Comisiei de a emite o propunere privind normele de răspundere civilă în domeniul roboticii și al IA.

1000 Consiliul Europei, Orientări privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive, T-PD (2017) 01, Strasbourg, 23 ianuarie 2017.

Principiul reducerii la minimum a datelor impune ca datele cu caracter personal să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Cu toate acestea, modelul de afaceri al datelor masive poate fi antiteza reducerii la minimum a datelor, deoarece necesită tot mai multe date, adesea în scopuri nespecificate.

Același lucru este valabil și pentru principiul limitărilor legate de scop, care prevede că datele trebuie să fie prelucrate în scopuri specificate și că nu pot fi utilizate în scopuri care sunt incompatibile cu scopul inițial al colectării, cu excepția cazului în care o astfel de prelucrare se bazează pe un temei juridic – cum ar fi, printre altele, consimțământul persoanei vizate (vezi secțiunea 4.1.1).

În sfârșit, datele masive creează provocări și în ceea ce privește principiul exactității datelor, deoarece aplicațiile din domeniul datelor masive tind să colecteze date dintr-o gamă largă de surse fără să existe posibilitatea de a verifica și/sau de a menține exactitatea datelor colectate[1001].

Norme și drepturi specifice

Regula generală rămâne aceea potrivit căreia datele cu caracter personal care sunt prelucrate prin analize de date masive intră sub incidența legislației privind protecția datelor. Cu toate acestea, în legislația UE și a CoE au fost introduse norme specifice sau derogări pentru cazuri specifice în legătură cu prelucrarea algoritmică complexă a datelor.

În cadrul legislației CoE, Convenția 108 modernizată acordă noi drepturi persoanelor vizate pentru a le permite un control mai eficient asupra datelor lor cu caracter personal în era datelor masive. Tocmai acesta este cazul, de exemplu, al articolului 9 alineatul (1) literele (a), (c) și (d) din Convenția 108 modernizată, care privește dreptul persoanei vizate de a nu face obiectul unei decizii care o afectează în mod semnificativ și care se bazează exclusiv pe prelucrarea automată a datelor, fără a-i fi luate în considerare opiniile, și dreptul persoanei vizate de a obține, la cerere, informații privind raționamentul care stă la baza prelucrării datelor în cazul în care rezultatele acestei prelucrări i se aplică, precum și dreptul la opoziție. Alte dispoziții ale Convenției 108 modernizate, în special cele referitoare la transparență și obligațiile

1001 Avizul 8/2016 al AEPD din 23 septembrie 2016, intitulat „Aplicarea coerentă a drepturilor fundamentale în era megadatelor", p. 8.

suplimentare, reprezintă elemente care completează mecanismul de protecție instituit prin Convenția 108 modernizată pentru abordarea provocărilor erei digitale.

În temeiul legislației UE, pe lângă cazurile enumerate la articolul 23 din RGPD, trebuie asigurată **transparența** pentru toate operațiunile de prelucrare a datelor cu caracter personal. Acest lucru este deosebit de important în ceea ce privește serviciile de internet și alte tipuri de prelucrare automatizată a datelor, cum ar fi utilizarea algoritmilor pentru luarea deciziilor. În acest caz, caracteristicile sistemelor de prelucrare a datelor trebuie să permită ca persoanele vizate să înțeleagă cu adevărat ce se întâmplă cu datele lor. Pentru a asigura prelucrarea echitabilă și transparentă, Regulamentul general privind protecția datelor impune operatorului să furnizeze persoanei vizate informații pertinente cu privire la logica utilizată în procesul decizional automatizat, inclusiv crearea de profiluri[1002]. În Recomandarea sa privind protecția și promovarea dreptului la libertatea de exprimare și a dreptului la respectarea vieții private în ceea ce privește neutralitatea rețelei, Comitetul de Miniștri al Consiliului Europei a recomandat ca furnizorii de servicii internet „să ofere utilizatorilor informații clare, complete și publice cu privire la orice practici de gestionare a traficului care ar putea afecta accesul utilizatorilor la conținut, aplicații sau servicii și distribuirea acestora”[1003]. Rapoartele privind practicile de gestionare a traficului internet elaborate de autoritățile competente din toate statele membre ar trebui pregătite în mod deschis și transparent și ar trebui să fie puse la dispoziția publicului în mod gratuit[1004].

Operatorii de date trebuie să **comunice** persoanelor vizate – atât în cazul în care datele au fost colectate de la acestea, cât și în cazul opus – nu doar informațiile specifice privind datele colectate și prelucrarea preconizată (vezi secțiunea 6.1.1), ci, dacă este cazul, și existența unor procese decizionale automatizate, comunicându-le „informații pertinente privind logica utilizată”[1005], precum și obiectivele și consecințele potențiale ale unor astfel de procese. Regulamentul general privind protecția datelor clarifică, de asemenea (numai în cazurile în care datele cu caracter personal nu au fost obținute de la persoana vizată), că operatorul nu are obligația de a furniza persoanei vizate aceste informații atunci când „furnizarea acestor

1002 Regulamentul general privind protecția datelor, articolul 13 alineatul (2) litera (f).

1003 Recomandarea CM/Rec(2016)1 din 13 ianuarie 2016 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția și promovarea dreptului la libertatea de exprimare și a dreptului la respectarea vieții private în ceea ce privește neutralitatea rețelei, punctul 5.1.

1004 *Ibidem*, punctul 5.2.

1005 Regulamentul general privind protecția datelor, articolul 13 alineatul (2) litera (f) și articolul 14 alineatul (2) litera (g).

informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate”[1006]. Cu toate acestea, astfel cum a subliniat Grupul de lucru „Articolul 29” în *Orientările privind procesul decizional automatizat și crearea de profiluri în sensul Regulamentului 2016/679*, complexitatea prelucrării nu ar trebui, în sine, să împiedice operatorul de date să furnizeze persoanei vizate explicații clare despre obiectivele prelucrării datelor și analizele utilizate[1007].

Drepturile persoanelor vizate de a avea **acces** la datele lor cu caracter personal, de a obține **rectificarea** și **ștergerea** acestora, precum și dreptul de a obține **restricționarea** prelucrării nu includ o derogare similară. Cu toate acestea, obligația operatorului de date de a informa persoana vizată cu privire la orice rectificare sau ștergere a datelor sale cu caracter personal (vezi secțiunea 6.1.4) poate fi, de asemenea, suspendată atunci când informarea „se dovedește a fi imposibilă sau ar implica eforturi disproporționate”[1008].

Persoanele vizate au, de asemenea, dreptul la **opoziție**, în conformitate cu articolul 21 din RGPD (vezi secțiunea 6.1.6), față de orice prelucrare a datelor lor cu caracter personal, inclusiv în cazul unor analize de date masive. Deși operatorii de date pot fi scutiți de această obligație în cazul în care pot demonstra interese legitime preponderente, aceștia nu pot beneficia de o astfel de derogare în cazul prelucrării în scopuri de marketing direct.

În cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare în interes public, de cercetare științifică sau istorică ori în scopuri statistice, operatorii de date se pot prevala de derogări specifice de la aceste drepturi[1009].

În ceea ce privește **crearea de profiluri și procesele decizionale automatizate**, RGPD a introdus norme specifice: articolul 22 alineatul (1) prevede că persoana vizată „are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată [...] care produce efecte juridice care privesc persoana vizată”. După cum se subliniază în orientările Grupului de lucru „Articolul 29”, acest articol stabilește o interdicție generală privind procesele decizionale complet automatizate[1010]. Operatorii de date pot

1006 *Ibidem*, articolul 14 alineatul (5) litera (b).

1007 Orientările din 3 octombrie 2017 ale Grupului de lucru „Articolul 29” privind procesul decizional automatizat și crearea de profiluri în sensul Regulamentului 2016/679, WP 251, Bruxelles, 3 octombrie 2017, p. 14.

1008 Regulamentul general privind protecția datelor, articolul 19.

1009 *Ibidem*, articolul 89 alineatele (2) și (3).

1010 Orientările din 3 octombrie 2017 ale Grupului de lucru „Articolul 29” privind procesul decizional automatizat și crearea de profiluri în sensul Regulamentului 2016/679, WP 251, Bruxelles, 3 octombrie 2017, p. 9.

fi exceptați de la aplicarea acestei interdicții numai în trei cazuri specifice, și anume atunci când decizia este: 1) necesară pentru executarea unui contract între persoana vizată și un operator de date; 2) autorizată prin dreptul Uniunii sau dreptul intern; sau 3) are la bază consimțământul explicit[1011].

Controlul individual

Complexitatea și lipsa de transparență care caracterizează analizele de date masive pot impune necesitatea regândirii controlului individual asupra datelor cu caracter personal. Acest lucru ar trebui adaptat la contextul social și tehnologic dat, ținând seama de lipsa de cunoștințe a persoanelor despre acest subiect. Prin urmare, protecția datelor în contextul datelor masive ar trebui să adopte o concepție mai amplă despre controlul asupra utilizării datelor, potrivit căreia controlul individual evoluează într-un proces mai complex de evaluări multiple ale impactului riscurilor legate de utilizarea datelor[1012].

Calitatea unei aplicații din domeniul datelor masive depinde de cât de bine poate prevedea aceasta dorințele sau comportamentul persoanelor în cauză (sau al consumatorilor). Modelele actuale de predicție bazate pe analizele de date masive sunt în curs de perfecționare. Evoluțiile recente presupun nu doar utilizarea datelor pentru a clasifica personalitățile (cu alte cuvinte, comportamentul și atitudinile), ci și evaluarea comportamentului prin analizarea tiparului vocii, a intensității cu care se introduc mesajele sau a temperaturii corpului. Toate aceste informații pot fi utilizate în timp real prin comparare cu cunoștințele extrase din evaluările de date masive, pentru a evalua, de exemplu bonitatea solicitantului în cadrul unei întâlniri cu reprezentantul unei bănci. Evaluarea nu se face pe baza meritelor persoanei care solicită creditul, ci mai degrabă pe baza caracteristicilor comportamentale extrase din analiza și evaluarea datelor masive: de exemplu, faptul că solicitantul vorbește cu voce puternică sau pe un ton măgulitor, limbajul corpului sau temperatura corpului.

Crearea de profiluri și publicitatea direcționată pot să nu constituie neapărat o problemă dacă persoanele **sunt conștiente** că fac obiectul unor reclame personalizate. Crearea de profiluri devine o problemă atunci când este folosită pentru a manipula persoanele: de exemplu, vizarea anumitor personalități sau grupuri de oameni în campaniile politice. De exemplu, grupurile de alegători indeciși pot fi abordate prin mesaje politice adaptate la „personalitatea" și atitudinile lor. O altă problemă

1011 Regulamentul general privind protecția datelor, articolul 22 alineatul (2).

1012 Consiliul Europei, Comitetul consultativ al Convenției 108, Orientări privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive, T-PD(2017)01, Strasbourg, 23 ianuarie 2017.

ar putea fi utilizarea creării de profiluri pentru a refuza accesul la produse și servicii anumitor persoane. O măsură care poate oferi protecție împotriva utilizării abuzive a datelor masive și a informațiilor cu caracter personal este pseudonimizarea (vezi secțiunea 2.1.1)[1013]. În cazul în care datele cu caracter personal sunt cu adevărat anonime, adică nu există informații care să lase urme prin care se poate restabili legătura cu persoana vizată, aceste cazuri nu intră sub incidența Regulamentului general privind protecția datelor. Consimțământul persoanelor vizate și al persoanelor fizice în cadrul prelucrării datelor masive reprezintă, de asemenea, o provocare pentru legislația privind protecția datelor. Aici se include consimțământul de a primi anunțuri personalizate și de a face obiectul creării de profiluri, care pot fi justificate prin motive legate de „îmbunătățirea experienței clientului", sau consimțământul față de utilizarea volumelor mari de date cu caracter personal pentru a rafina și dezvolta instrumente analitice bazate pe informații. Conștientizarea sau lipsa de conștientizare a prelucrării datelor masive ridică mai multe întrebări în legătură cu mijloacele prin care persoanele vizate își pot exercita drepturile, dat fiind că prelucrarea datelor masive se poate baza atât pe informații pseudonimizate, cât și anonimizate care fac obiectul unor algoritmi. În timp ce datele pseudonimizate intră sub incidența Regulamentului general privind protecția datelor, acest regulament nu se aplică datelor anonimizate. Controlul individual al persoanelor vizate asupra prelucrării datelor lor cu caracter personal și conștientizarea acestei prelucrări sunt esențiale în domeniul datelor masive: în lipsa acestora, persoanele vizate nu vor avea o idee clară despre cine este operatorul de date sau persoana împuternicită de operator, ceea ce le împiedică să își exercite drepturile în mod eficient.

10.2. Web 2.0 și web 3.0: rețelele sociale și internetul obiectelor

Principalele elemente

- Serviciile de networking social (SNS) sunt platforme de comunicare online care permit persoanelor să se alăture unor rețele de utilizatori cu care au diverse lucruri în comun sau să creeze astfel de rețele noi.
- Internetul obiectelor se referă la conectarea obiectelor la internet și la interconectarea obiectelor între ele.

1013 *Ibidem*, p. 2.

- Consimțământul persoanelor vizate este cel mai uzual temei juridic al prelucrării legale a datelor de către operatorii de date din domeniul rețelelor sociale.
- Utilizatorii rețelelor sociale sunt, în general, protejați de „excepția privind activitățile domestice"; totuși, această derogare poate fi suspendată în contexte specifice.
- Furnizorii de rețele sociale nu sunt protejați de „excepția privind activitățile domestice".
- Protejarea vieții private din faza de proiectare și protejarea implicită a vieții private sunt esențiale pentru a asigura securitatea datelor în acest domeniu.

10.2.1. Definirea web 2.0 și web 3.0

Serviciile de networking social

Inițial, internetul a fost conceput ca o rețea destinată interconectării computerelor și transmiterii de mesaje, cu capacități limitate de schimb de date, site-urile oferind doar posibilitatea vizualizării pasive a conținutului de către utilizatori[1014]. În era web 2.0, internetul a fost transformat într-un forum în care utilizatorii interacționează, colaborează și generează conținut. Această eră se caracterizează prin succesul remarcabil și utilizarea pe scară largă a serviciilor de networking social, care reprezintă acum o parte esențială a vieții de zi cu zi a milioane de oameni.

Serviciile de networking social (SNS) sau „platformele de comunicare socială" pot fi definite în sens larg drept „platforme de comunicare online care permit persoanelor să se alăture unor rețele de utilizatori cu care au diverse lucruri în comun sau să creeze astfel de rețele noi"[1015]. Pentru a se alătura unei rețele sau pentru a crea o rețea, persoanele fizice sunt invitate să furnizeze date cu caracter personal și să își creeze un profil. SNS permit utilizatorilor să genereze „conținut" digital, care poate varia de la fotografii și înregistrări video până la linkuri la ziare și postări personale în care se exprimă opinii. Prin intermediul acestor platforme de comunicare online, utilizatorii pot interacționa și comunica cu alți utilizatori. Este important de menționat faptul că majoritatea SNS populare nu percep comisioane pentru înregistrare. În loc să solicite utilizatorilor să plătească pentru a se alătura rețelei, furnizorii SNS generează cea mai mare parte a veniturilor din publicitatea direcționată. Agențiile de publicitate pot beneficia foarte mult de pe urma informațiilor cu caracter personal dezvăluite zi de zi pe aceste site-uri. Dispunând de informații despre vârsta, sexul,

1014 Comisia Europeană (2016), *Dezvoltarea internetului obiectelor în Europa*, SWD(2016) 110 final.

1015 Avizul 5/2009 din 12 iunie 2009 al Grupului de lucru „Articolul 29" privind platformele de comunicare socială online, WP 163, Bruxelles, p. 4.

localizarea și interesele utilizatorilor, anunțurile acestor agenții pot ajunge la persoanele „potrivite".

Comitetul Miniștrilor din cadrul Consiliului Europei a adoptat o Recomandare privind protecția drepturilor omului în ceea ce privește serviciile de networking social[1016], care conține o secțiune dedicată protecției datelor și care a fost completată în 2018 de o altă recomandare, referitoare la rolurile și responsabilitățile intermediarilor serviciilor de internet[1017].

Exemplu: Nora este foarte fericită pentru că partenerul ei de viață a cerut-o în căsătorie. Vrea să împărtășească vestea cea bună cu prietenii și familia ei și decide să publice o postare plină de emoție pe o platformă de comunicare socială, în care să își exprime bucuria, schimbându-și totodată statutul relației în „logodită". În zilele următoare, când se conectează la contul ei, Nora vede reclame la rochii de mireasă și la florării. De ce se întâmplă acest lucru?

Când creează anunțuri pe Facebook, societățile care comercializează rochii de mireasă și flori selectează anumiți parametri pentru a putea ajunge la persoane precum Nora. Dacă profilul Norei indică faptul că este o femeie logodită care locuiește la Paris, aproape de zona în care se află magazinele cu rochii de mireasă și florăriile care publică anunțurile, Nora vede imediat aceste anunțuri.

Internetul obiectelor

Internetul obiectelor reprezintă următorul pas în dezvoltarea internetului: era web 3.0. Odată cu internetul obiectelor, dispozitivele pot fi conectate și pot interacționa cu alte dispozitive prin internet. Acest lucru permite ca obiectele și persoanele să fie interconectate prin intermediul rețelelor de comunicații și să trimită rapoarte despre starea lor și/sau despre starea mediului înconjurător[1018]. Internetul obiectelor și dispozitivele conectate sunt deja o realitate și se așteaptă ca prezența acestora să crească substanțial în următorii ani, odată cu crearea și dezvoltarea în continuare

1016 Recomandarea CM/Rec(2012)4 din 4 aprilie 2012 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția drepturilor omului în ceea ce privește serviciile de networking social.

1017 Recomandarea CM/Rec(2018)2 din 7 martie 2018 a Comitetului de Miniștri al Consiliului Europei către statele membre privind rolurile și responsabilitățile intermediarilor serviciilor de internet.

1018 Comisia Europeană, *Documentul de lucru al serviciilor Comisiei intitulat „Dezvoltarea internetului obiectelor în Europa"*, SWD(2016) 110 din 19 aprilie 2016.

a dispozitivelor inteligente care vor conduce la crearea de orașe inteligente, case inteligente și întreprinderi inteligente.

Exemplu: Internetul obiectelor poate oferi beneficii deosebite în domeniul serviciilor medicale. Întreprinderile au creat deja dispozitive, senzori și aplicații care permit monitorizarea stării de sănătate a unui pacient. Prin utilizarea unui buton de alarmă la purtător și a altor senzori fără fir amplasați în locuință, se poate urmări activitatea cotidiană a persoanelor în vârstă care locuiesc singure și se pot genera alerte dacă sunt detectate perturbări semnificative ale programului zilnic. Senzorii de detectare a căderii, de exemplu, sunt folosiți pe scară largă de către persoanele în vârstă. Acești senzori pot detecta căderile cu precizie și pot informa medicul și/sau familia persoanei cu privire la cădere.

Exemplu: Barcelona este unul dintre cele mai cunoscute exemple de oraș inteligent. Din 2012, orașul a pus în aplicare utilizarea tehnologiilor inovatoare, cu scopul de a crea un sistem inteligent de transport public, de gestionare a deșeurilor, de parcare și de iluminat stradal. Pentru a îmbunătăți gestionarea deșeurilor, de exemplu, orașul utilizează pubele inteligente. Acestea permit monitorizarea nivelurilor de deșeuri pentru a optimiza traseele de colectare. Când pubelele sunt aproape pline, acestea transmit, prin rețeaua de comunicații mobile, semnale care sunt direcționate către aplicația software utilizată de societatea de gestionare a deșeurilor. Societatea respectivă poate astfel să planifice ruta optimă de colectare a deșeurilor, ordonând după prioritate și/sau organizând colectarea doar pentru pubelele care trebuie într-adevăr golite.

10.2.2. Ponderarea beneficiilor și a riscurilor

Extinderea foarte amplă și succesul înregistrat de SNS în ultimul deceniu sugerează că aceste servicii oferă **beneficii semnificative**. De exemplu, publicitatea direcționată (astfel cum este descrisă în exemplul evidențiat) reprezintă un mod deosebit de inovator prin care întreprinderile pot ajunge la clienți, oferindu-le o piață mai specifică. De asemenea, ar putea fi în interesul consumatorilor să li se prezinte anunțuri mai relevante și mai interesante pentru ei. Un aspect mai important însă este faptul că serviciile de networking social și platformele de comunicare socială pot avea un impact pozitiv asupra societății și asupra implementării schimbărilor. Acestea oferă

utilizatorilor posibilitatea de a comunica, de a interacționa, de a organiza grupuri și evenimente pe teme care îi privesc.

În mod similar, se preconizează că internetul obiectelor va aduce beneficii semnificative economiei; acesta face parte din strategia UE de dezvoltare a unei piețe unice digitale. Se estimează că numărul de conexiuni din cadrul internetului obiectelor va ajunge la șase miliarde în UE până în 2020. Se estimează că această extindere a conectivității va aduce beneficii economice importante, prin dezvoltarea de servicii și aplicații inovatoare, creșterea calității serviciilor medicale, o mai bună înțelegere a nevoilor consumatorilor și creșterea eficienței.

În același timp, având în vedere cantitatea uriașă de informații cu caracter personal generate de utilizatorii platformelor de comunicare socială și prelucrate ulterior de operatorii de servicii, extinderea SNS este însoțită de **preocupări tot mai mari** cu privire la modalitățile în care se poate asigura protecția vieții private și a datelor cu caracter personal. SNS pot amenința dreptul la respectarea vieții private și dreptul la libertatea de exprimare. Printre aceste amenințări se pot număra următoarele: „lipsa garanțiilor legale și procedurale în cadrul proceselor care pot duce la excluderea unor utilizatori; protejarea necorespunzătoare a copiilor și a tinerilor împotriva conținutului sau a comportamentelor nocive; lipsa de respect față de drepturile celorlalți; lipsa setărilor implicite care să protejeze viața privată; lipsa de transparență cu privire la scopurile pentru care se colectează și se prelucrează datele cu caracter personal”[1019]. Legislația europeană în materie de protecție a datelor a încercat să răspundă provocărilor legate de protecția vieții private/datelor în contextul platformelor de comunicare socială. Principii precum consimțământul, protejarea vieții private/datelor din faza de proiectare și implicită, precum și drepturile persoanelor fizice sunt deosebit de importante în contextul platformelor de comunicare socială și a serviciilor de networking social.

În contextul internetului obiectelor, volumul vast de date cu caracter personal generate de diferitele dispozitive interconectate implică, de asemenea, riscuri pentru respectarea vieții private și protecția datelor. Deși transparența este un principiu important al legislației europene privind protecția datelor, din cauza multitudinii de dispozitive conectate nu este întotdeauna clar cine poate colecta, accesa și utiliza datele colectate de la dispozitivele conectate prin internetul obiectelor[1020].

1019 Recomandarea Rec(2012)4 din 4 aprilie 2012 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția drepturilor omului în ceea ce privește serviciile de networking social.

1020 Autoritatea Europeană pentru Protecția Datelor (2017), *Înțelegerea internetului obiectelor*.

Cu toate acestea, în conformitate cu legislația UE și a CoE, principiul transparenței stabilește obligația operatorilor de a informa într-un limbaj clar și simplu persoanele vizate cu privire la modul în care sunt utilizate datele lor. Riscurile, normele, garanțiile și drepturile legate de prelucrarea datelor lor cu caracter personal trebuie să le fie prezentate în mod clar persoanelor în cauză. Dispozitivele conectate prin internetul obiectelor și volumul mare de operații de prelucrare și de date implicat ar putea, de asemenea, să creeze dificultăți în ceea ce privește cerința obținerii unui consimțământ clar și în cunoștință de cauză față de prelucrarea datelor – în cazurile în care prelucrarea respectivă se bazează pe consimțământ. Deseori, persoanele fizice nu înțeleg partea tehnică a prelucrării respective și, prin urmare, nici consecințele consimțământului lor.

O altă preocupare majoră este securitatea, având în vedere că dispozitivele conectate sunt deosebit de vulnerabile la riscurile de securitate. Dispozitivele conectate au niveluri diferite de securitate. Deoarece funcționează în afara infrastructurii TI standard, aceste dispozitive ar putea să nu dispună de capacitatea de prelucrare și de stocare adecvată pentru a accepta software de securitate sau utilizarea unor tehnici precum criptarea, pseudonimizarea sau anonimizarea în vederea protejării informațiilor cu caracter personal ale utilizatorilor.

Exemplu: În Germania, autoritățile de reglementare au decis să interzică o jucărie conectată la internet în urma unor preocupări grave cu privire la impactul jucăriei asupra respectării vieții private a copiilor. Autoritățile de reglementare au considerat că o păpușă conectată la internet pe nume Cayla se putea transforma într-un adevărat dispozitiv de spionaj. Păpușa funcționa prin transmiterea întrebărilor audio ale copilului care se juca cu ea către o aplicație de pe un dispozitiv digital, care convertea mesajul audio în text și căuta pe internet răspunsul. Aplicația trimitea apoi răspunsul către păpușă, care i-l exprima verbal copilului. Prin intermediul păpușii, se puteau înregistra și transmite aplicației comunicațiile copilului și ale adulților din apropiere. Dacă producătorii păpușii nu adoptau măsuri de securitate adecvate, păpușa ar fi putut fi folosită de oricine pentru a asculta conversațiile în cauză.

10.2.3. Aspecte legate de protecția datelor

Consimțământul

În Europa, prelucrarea datelor cu caracter personal este legală numai dacă este permisă de legislația europeană privind protecția datelor. Pentru furnizorii SNS, consimțământul persoanelor vizate furnizează, în general, temeiul juridic al prelucrării datelor. Consimțământul trebuie să fie acordat în mod liber și să fie specific, în cunoștință de cauză și lipsit de ambiguitate (vezi secțiunea 4.1.1)[1021]. „Acordat în mod liber" înseamnă, în esență, că persoanele vizate trebuie să aibă capacitatea de a-și exercita libertatea de alegere în mod efectiv și autentic. Consimțământul este „specific" și „în cunoștință de cauză" atunci când este inteligibil și se referă în mod clar și precis la întregul domeniu de aplicare și la toate scopurile și consecințele prelucrării datelor. În contextul platformelor de comunicare socială, este discutabil dacă consimțământul poate fi acordat în mod liber, specific și în cunoștință de cauză pentru toate tipurile de prelucrare efectuate de operatorul SNS și de părțile terțe.

Exemplu: Pentru a se alătura unui SNS și a avea acces la acesta, persoanele trebuie adesea să accepte diferite tipuri de prelucrare a datelor lor cu caracter personal, de multe ori fără a li se oferi precizările necesare sau opțiuni alternative. Un exemplu ar fi necesitatea de a acorda consimțământul pentru primirea unor reclame bazate pe comportament în vederea înregistrării în SNS. Astfel cum arată Grupul de lucru „Articolul 29" în avizul său privind conceptul de consimțământ, „având în vedere importanța pe care au dobândit-o unele rețele sociale, anumite categorii de utilizatori (cum ar fi adolescenții) vor accepta primirea de reclame bazate pe comportament pentru a evita riscul de a fi excluși parțial din interacțiunile sociale. Utilizatorul ar trebui să fie pus în poziția de a-și exprima în mod liber și specific consimțământul față de primirea reclamelor bazate pe comportament independent de accesul său la serviciul de networking social"[1022].

În conformitate cu Regulamentul general privind protecția datelor, datele cu caracter personal ale copiilor sub 16 ani nu pot fi, în principiu, prelucrate în temeiul consimțământului acestora[1023]. Dacă este necesar consimțământul față de

1021 Regulamentul general privind protecția datelor, articolele 4 și 7; Convenția 108 modernizată, articolul 5.

1022 Avizul 15/2011 din 13 iulie 2011 al Grupului de lucru „Articolul 29" privind conceptul de consimțământ, WP 187, Bruxelles, 13 iulie 2011, p. 18.

1023 Vezi Regulamentul general privind protecția datelor, articolul 8. Statele membre ale UE pot stabili prin lege o vârstă mai mică, cu condiția ca aceasta să nu fie mai mică de 13 ani.

prelucrare, acesta trebuie să fie acordat de părintele sau tutorele copilului. Copiii trebuie să beneficieze de o protecție specifică datorită faptului că pot fi mai puțin conștienți de riscurile și consecințele implicate de prelucrarea datelor. Acest lucru este foarte important în contextul platformelor de comunicare socială, deoarece copiii sunt mai vulnerabili la unele dintre efectele negative pe care le poate implica utilizarea unor astfel de platforme de comunicare, cum ar fi comportamentul agresiv pe internet, urmărirea cibernetică sau furtul de identitate.

Securitatea și protecția vieții private/datelor din faza de proiectare și implicită

Prelucrarea datelor cu caracter personal implică în mod inerent riscuri de securitate, având în vedere posibilitatea constantă de încălcare a securității care duce la distrugerea, pierderea, modificarea, accesul neautorizat sau divulgarea accidentale sau ilegale ale datelor cu caracter personal prelucrate. Conform legislației europene privind protecția datelor, operatorii și persoanele împuternicite de operatori au obligația de a pune în aplicare măsuri tehnice și organizatorice adecvate pentru a preveni orice ingerință neautorizată în operațiunile de prelucrare a datelor. Furnizorii de servicii de networking social care intră sub incidența normelor europene de protecție a datelor trebuie, de asemenea, să respecte această obligație.

Principiile protecției vieții private/datelor din faza de proiectare și implicite impun operatorilor să asigure securitatea în proiectarea produselor lor și să aplice în mod automat setările adecvate de protecție a vieții private și a datelor. Aceasta înseamnă că, atunci când o persoană decide să se alăture unei rețele sociale, furnizorul de servicii nu poate să pună automat toate informațiile despre noul utilizator al serviciului la dispoziția tuturor celorlalți utilizatori. Când o persoană se alătură serviciului, setările de protecție implicită a vieții private și a datelor trebuie să fie de așa natură încât informațiile să fie disponibile numai contactelor alese de persoana respectivă. Extinderea accesului la persoane din afara acestei liste ar trebui să fie posibilă numai după ce utilizatorul a modificat manual setările de protecție implicită a vieții private și a datelor. Acest lucru poate avea, de asemenea, un impact în cazurile în care se produce o încălcare a securității datelor în pofida măsurilor de securitate puse în aplicare. În astfel de situații, furnizorii serviciului trebuie să informeze utilizatorii afectați în cazul în care încălcarea poate genera un risc ridicat pentru drepturile și libertățile persoanei vizate[1024].

1024 *Ibidem*, articolul 34.

Protecția vieții private/datelor din faza de proiectare și implicită sunt deosebit de importante în contextul SNS, deoarece, pe lângă riscurile accesului neautorizat implicat în majoritatea tipurilor de prelucrare, schimbul de informații cu caracter personal pe platformele de comunicare socială prezintă riscuri suplimentare de securitate. Acestea se datorează adesea faptului că utilizatorii nu înțeleg *cine* are acces la informațiile lor și cum pot folosi aceste persoane informațiile. Odată cu utilizarea pe scară largă a platformelor de comunicare socială, numărul incidentelor și al victimelor furturilor de identitate a crescut.

Exemplu: Furtul de identitate este fapta prin care o persoană obține informații, date sau documente aparținând unei alte persoane (victima) și apoi folosește aceste informații pentru a se substitui victimei, cu scopul de a obține bunuri și servicii în numele victimei. Să luăm exemplul unui utilizator pe nume Paul, care are un cont pe o platformă web de comunicare socială. Paul este profesor și membru activ al comunității sale, o persoană foarte deschisă, care nu își face multe griji legate de setările de confidențialitate și de protecție a datelor din contul său de pe platforma de comunicare socială. Are o listă mare de contacte, care cuprinde inclusiv oameni pe care nu îi cunoaște personal. Deoarece lucrează într-o școală mare și a devenit foarte popular de când antrenează echipa de fotbal a școlii, se gândește că persoanele necunoscute din lista de contacte sunt probabil părinți ai elevilor sau diverși prieteni ai școlii. Adresa de e-mail a lui Paul și ziua lui de naștere sunt afișate în contul său de pe platforma de comunicare socială. În plus, Paul postează în mod regulat fotografii cu câinele său Toby, însoțite de comentarii precum „Eu și Toby la alergarea de dimineață". Paul nu s-a gândit că una dintre întrebările de securitate cu ajutorul cărora și-a protejat contul de e-mail sau de telefon mobil a fost „Cum se numește animalul tău de companie?". Folosind informațiile disponibile în profilul lui Paul de pe platforma de comunicare socială, Nick reușește să spargă conturile lui Paul.

Drepturile persoanelor fizice

Furnizorii SNS trebuie să respecte drepturile persoanelor fizice (vezi secțiunea 6.1), inclusiv dreptul de a fi informate cu privire la scopul prelucrării și la modul în care datele cu caracter personal pot fi utilizate în scopuri de marketing direct. Persoanele fizice trebuie, de asemenea, să aibă dreptul de acces la datele cu caracter personal pe care le-au generat pe platforma de comunicare socială și dreptul de a solicita ștergerea acestora. Chiar și atunci când persoanele și-au exprimat consimțământul

față de prelucrarea datelor cu caracter personal și au încărcat informații online, ar trebui să poată solicita să fie „uitate" în cazul în care nu mai doresc să utilizeze serviciile rețelei sociale. Dreptul la portabilitatea datelor le permite utilizatorilor să primească o copie a datelor cu caracter personal pe care le-au comunicat furnizorului de servicii de netwoking social, într-un format structurat, utilizat în mod curent și care poate fi citit automat și să transfere datele lor de la un furnizor de servicii de netwoking social la altul[1025].

Operatori

O întrebare dificilă care apare adesea în contextul platformelor de comunicare socială este problema identității operatorului, cu alte cuvinte, cine este persoana care are obligația și responsabilitatea de a respecta normele de protecție a datelor. Furnizorii de servicii de netwoking social sunt considerați operatori în temeiul legislației europene privind protecția datelor. Acest lucru este evident având în vedere definiția largă a „operatorului" și faptul că acești furnizori de servicii determină scopul și mijloacele de prelucrare a datelor cu caracter personal împărtășite de persoanele fizice. În conformitate cu legislația UE, în cazul în care furnizează servicii persoanelor vizate în UE, operatorii trebuie să respecte dispozițiile Regulamentului general privind protecția datelor, chiar dacă nu sunt stabiliți în UE.

Pot totuși utilizatorii serviciilor de networking social să fie considerați operatori? În cazul în care persoanele fizice prelucrează date cu caracter personal „în cadrul unei activități exclusiv personale sau domestice", nu se aplică normele de protecție a datelor. Acest lucru este cunoscut în legislația europeană privind protecția datelor drept „excepția privind activitățile domestice". Cu toate acestea, în unele cazuri, utilizatorii unui serviciu de networking social nu pot beneficia de excepția privind activitățile domestice.

Utilizatorii își partajează în mod voluntar informațiile cu caracter personal online. Însă informațiile partajate online includ adesea informațiile cu caracter personal ale altor persoane.

Exemplu: Paul are un cont pe o platformă de comunicare socială foarte populară. Paul își dorește să devină actor și își folosește contul pentru a publica fotografii, înregistrări video și postări care îi pun în evidență

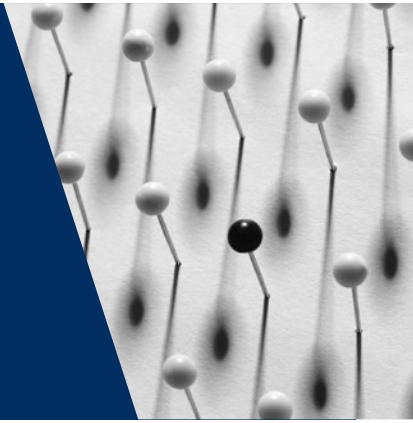
1025 Regulamentul general privind protecția datelor, articolul 21.

pasiunea pentru artă. Popularitatea este importantă pentru viitorul său; de aceea, a decis că profilul său ar trebui să fie disponibil nu doar listei sale de prieteni, ci tuturor utilizatorilor de internet, indiferent dacă sunt membri ai rețelei sau nu. Poate Paul să posteze fotografii și înregistrări video în care apare și prietena lui, Sarah, fără consimțământul ei? Fiind învățătoare, Sarah nu dorește ca viața ei privată să fie expusă angajatorului său, elevilor ei și părinților acestora. Să ne imaginăm o situație în care Sarah, care nu utilizează platformele de comunicare socială, află de la Nick, un prieten comun al său și al lui Paul, că acesta din urmă a postat online o fotografie cu ea și el de la o petrecere. Într-un astfel de caz, prelucrarea datelor de către Paul nu intră sub incidența legislației UE, deoarece se încadrează în domeniul de aplicare al „excepției privind activitățile domestice".

Cu toate acestea, rămâne crucial ca utilizatorii să fie conștienți și atenți la faptul că încărcarea informațiilor despre alte persoane fără consimțământul acestora poate încălca drepturile acestor persoane la respectarea vieții private și la protecția datelor. Chiar și în cazul în care se aplică excepția privind activitățile domestice – de exemplu, dacă un utilizator are un profil care este accesibil doar unei liste de contacte selectate de respectivul utilizator – publicarea informațiilor cu caracter personal despre alte persoane ar putea totuși să atragă răspunderea utilizatorului. Deși normele de protecție a datelor nu se aplică în cazul în care se aplică excepția privind activitățile domestice, răspunderea poate rezulta din aplicarea altor norme naționale, cum ar fi cele legate de defăimare sau de încălcarea drepturilor personalității. În sfârșit, numai utilizatorii SNS sunt protejați de excepția privind activitățile domestice: operatorii și persoanele împuternicite de operatori care furnizează mijloacele pentru astfel de prelucrări private intră sub incidența legislației UE privind protecția datelor[1026].

Odată cu reformarea Directivei asupra confidențialității și comunicațiilor electronice, normele privind protecția datelor, respectarea vieții private și securitatea aplicabile furnizorilor de servicii de telecomunicații în cadrul juridic actual se vor aplica, de asemenea, comunicațiilor între mașini și serviciilor de comunicații electronice, inclusiv, de exemplu, serviciilor OTT.

1026 *Ibidem*, considerentul 18.



Lecturi suplimentare

Capitolul 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Viena, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. *Four fundamental rights: finding the balance*, *International Data Privacy Law*, vol. 6, nr. 3, pp. 195-209.

EDRi, *An introduction to data protection*, Bruxelles.

Frowein, J. și Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

González Fuster, G. și Gellert, G. (2012), *The fundamental right of data protection in the European Union: in search of an uncharted right*, *International Review of Law, Computers and Technology*, vol. 26 (1), pp. 73-82.

Grabenwarter, C. și Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. și Nouwt, S. (Eds.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. și Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), *EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation*.

Kranenborg, H. (2015), *Google and the Right to be Forgotten*, *European Data Protection Law Review*, vol. 1, nr. 1, pp. 70-79.

Lynskey, O. (2014), *Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order*, *International and Comparative Law Quarterly*, vol. 63, nr. 3, pp. 569-597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Kokott, J. și Sobotta, C. (2013), *The distinction between privacy and data protection in the case law of the CJEU and the ECtHR*, *International Data Privacy Law*, vol. 3, nr. 4, pp. 222-228.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Anvers, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. și Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bruxelles, Emile Bruylant.

Simitis, S. (1997), *Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?*, *Neue Juristische Wochenschrift*, nr. 5, pp. 281-288.

Warren, S. și Brandeis, L. (1890), *The right to privacy*, *Harvard Law Review,* vol. 4, nr. 5, pp. 193-220.

White, R. și Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Capitolul 2

Acquisty, A., și Gross R. (2009), Predicting Social Security numbers from public data, *Proceedings of the National Academy of Science*, 7 iulie 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., și Blondel V. D. (2013), *Unique in the Crowd: the Privacy Bounds of Human Mobility*, *Nature Scientific Reports*, vol. 3, 2013.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. și Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, Londra, Sweet & Maxwell.

Ohm, P. (2010), *Broken promises of privacy: Responding to the surprising failure of anonymization*, *UCLA Law Review*, vol. 57, nr. 6, pp. 1701-1777.

Samarati, P. și Sweeney, L. (1998), Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression, *Technical Report* SRI-CSL-98-04.

Sweeney, L. (2002), K-Anonymity: A Model for Protecting Privacy, *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, nr. 5, pp. 557-570.

Tinnefeld, M., Buchner, B. și Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, München, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice.*

Capitolele 3-6

Brühann, U. (2012), *Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* în: Grabitz, E., Hilf, M. și Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, München, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Curren, L. și Kaye, J. (2010), *Revoking consent: a 'blind spot' in data protection law?*, *Computer Law & Security Review*, vol. 26, nr. 3, pp. 273-283.

Dammann, U. și Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. și Papakonstantinou, V. (2012), *The Police and Criminal Justice Data Protection Directive: Comment and Analysis*, *Computers & Law Magazine of SCL*, vol. 22, nr. 6, pp. 1-5.

De Hert, P. și Papakonstantinou, V. (2012), *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, *Computer Law & Security Review*, vol. 28, nr. 2, pp. 130-142.

Feretti, Federico (2012), *A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously*, *European Review of Private Law*, vol. 20, nr. 2, pp. 473-506.

FRA (Agenția pentru Drepturi Fundamentale a Uniunii Europene) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxemburg, *Oficiul pentru Publicații al Uniunii Europene* (Oficiul pentru Publicații).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (ediție de conferință), Viena, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxemburg, Oficiul pentru Publicații.

Irish Health Information and Quality Authority (2010), *Guidance on Privacy Impact Assessment in Health and Social Care*.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. și Saxby, S. (2011), *30 years on – The review of the Council of Europe Data Protection Convention 108*, *Computer Law & Security Review*, vol. 27, nr. 3, pp. 223-231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*.

Capitolul 7

Autoritatea Europeană pentru Protecția Datelor (2014), *Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies*.

Grupul de lucru „Articolul 29" (2005), Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. și Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Capitolul 8

Blasi Casagran, C. (2016), *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, Londra, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Berlin, Springer.

De Hert, P. și Papakonstantinou, V. (2012), T*he Police and Criminal Justice Data Protection Directive: Comment and Analysis*, *Computers & Law Magazine of SCL*, vol. 22, nr. 6, pp. 1-5.

Drewer, D. and Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime, ERA Forum*, vol. 13, nr. 3, pp. 381-395.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haga, Eurojust.

Europol (2012), *Data Protection at Europol*, Luxemburg, Oficiul pentru Publicații.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Poullet, Y. și De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. și Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, *European Law Review*, vol. 36, nr. 5, pp. 722-776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2.

Capitolul 9

Büllesbach, A., Gijrath, S., Poullet, Y. și Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. și Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. și De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. și Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, *European Law Review*, vol. 36, nr. 5, pp. 722-776.

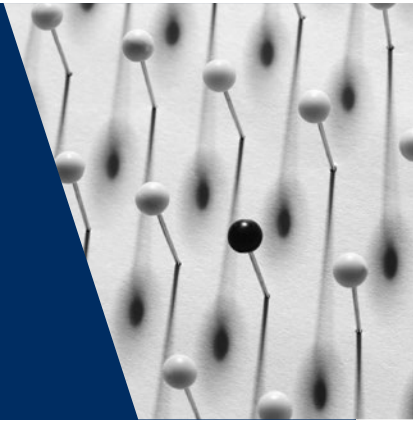
Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, Londra, Sweet & Maxwell.

Capitolul 10

El Emam, K. și Álvarez, C. (2015), *A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques*, *International Data Privacy Law*, vol. 5, nr. 1, pp. 73-87.

Mayer-Schönberger, V. și Cate, F. (2013), *Notice and consent in a world of Big Data*, *International Data Privacy Law*, vol. 3, nr. 2, pp. 67-73.

Rubistein, I. (2013), *Big Data: The End of Privacy or a New Beginning?*, *International Data Privacy Law*, vol. 3, nr. 2, pp. 74-87.



Jurisprudență

Jurisprudență selectată a Curții Europene a Drepturilor Omului

Accesul la datele cu caracter personal
Hotărârea CEDO din 7 iulie 1989 în cauza *Gaskin/Regatul Unit*, nr. 10454/83
Hotărârea CEDO din 25 septembrie 2012 în cauza *Godelli/Italia*, nr. 33783/09
Hotărârea CEDO din 28 aprilie 2009 în cauza *K.H. și alții/Slovacia*, nr. 32881/04
Hotărârea CEDO din 26 martie 1987 în cauza *Leander/Suedia*, nr. 9248/81
Hotărârea CEDO din 18 aprilie 2013 în cauza *M.K./Franța*, nr. 19522/09
Hotărârea CEDO [MC] din 13 februarie 2003 în cauza *Odièvre/Franța*, nr. 42326/98

Ponderarea protecției datelor cu libertatea de exprimare și cu dreptul la informare
Hotărârea CEDO [MC] din 7 februarie 2012 în cauza *Axel Springer AG/Germania*, nr. 39954/08
Hotărârea CEDO din 19 februarie 2015 în cauza *Bohlen/Germania*, nr. 53495/09
Hotărârea CEDO [MC] din 10 noiembrie 2015 în cauza *Coudec și Hachette Filipacchi Associés/Franța*, nr. 40454/07
Hotărârea CEDO [MC] din 8 noiembrie 2016 în cauza *Magyar Helsinki Bizottság/Ungaria*, nr. 18030/11
Hotărârea CEDO din 24 mai 1988 în cauza *Müller și alții/Elveția*, nr. 10737/84
Hotărârea CEDO din 25 ianuarie 2007 în cauza *Vereinigung bildender Künstler/Austria*, nr. 68354/01
Hotărârea CEDO [MC] din 7 februarie 2012 în cauza *Von Hannover/Germania (nr. 2)*, nr. 40660/08 și 60641/08

Hotărârea CEDO [MC] din 27 iunie 2017 în cauza *Satakunnan Markkinapörssi Oy și Satamedia Oy/Finlanda*, nr. 931/13

Ponderarea protecției datelor cu libertatea religioasă
Hotărârea CEDO din 2 februarie 2010 în cauza *Sinan Işık/Turcia*, nr. 21924/05

Provocări legate de protecția datelor online
Hotărârea CEDO din 2 decembrie 2008 în cauza *K.U./Finlanda*, nr. 2872/02

Consimțământul persoanei vizate
Hotărârea CEDO din 13 ianuarie 2015 în cauza *Elberte/Letonia*, nr. 61243/08
Hotărârea CEDO din 2 februarie 2010 în cauza *Sinan Işık/Turcia*, nr. 21924/05
Hotărârea CEDO din 17 februarie 2015 în cauza *Y/Turcia*, nr. 648/10

Corespondență
Hotărârea CEDO [MC] din 16 februarie 2000 în cauza *Amann/Elveția*, nr. 27798/95
Hotărârea CEDO din 28 iunie 2007 în cauza *Association for European Integration and Human Rights și Ekimdzhiev/Bulgaria*, nr. 62540/00
Hotărârea CEDO din 14 martie 2013 în cauza *Bernh Larsen Holding AS și alții/Norvegia*, nr. 24117/08
Hotărârea CEDO din 18 noiembrie 2008 în cauza *Cemalettin Canli/Turcia*, nr. 22427/04
Hotărârea CEDO din 19 mai 2016 în cauza *D.L./Bulgaria*, nr. 7472/14
Hotărârea CEDO din 2 februarie 2010 în cauza *Dalea/Franța*, nr. 964/07
Hotărârea CEDO din 7 iulie 1989 în cauza *Gaskin/Regatul Unit*, nr. 10454/83
Hotărârea CEDO din 27 octombrie 2009 în cauza *Haralambie/România*, nr. 21737/03
Hotărârea CEDO din 18 octombrie 2011 în cauza *Khelili/Elveția*, nr. 16188/07
Hotărârea CEDO din 26 martie 1987 în cauza *Leander/Suedia*, nr. 9248/81
Hotărârea CEDO din 2 august 1984 în cauza *Malone/Regatul Unit*, nr. 8691/79
Hotărârea CEDO [MC] din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95
Hotărârea CEDO [MC] din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04
Hotărârea CEDO din 21 iunie 2011 în cauza *Shimovolos/Rusia*, nr. 30194/09
Hotărârea CEDO din 25 martie 1983 în cauza *Silver și alții/Regatul Unit*, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75
Hotărârea CEDO din 26 aprilie 1979 în cauza *The Sunday Times/Regatul Unit*, nr. 6538/74

Baze de date cu caziere judiciare
Hotărârea CEDO din 22 iunie 2017 în cauza *Aycaguer/Franța*, nr. 8806/12
Hotărârea CEDO din 17 decembrie 2009 în cauza *B.B./Franța*, nr. 5335/06
Hotărârea CEDO din 18 septembrie 2014 în cauza *Brunet/Franța*, nr. 21010/10
Hotărârea CEDO din 18 aprilie 2013 în cauza *M.K./Franța*, nr. 19522/09
Hotărârea CEDO din 13 noiembrie 2012 în cauza *M.M./Regatul Unit*, nr. 24029/07

Securitatea datelor
Hotărârea CEDO din 27 octombrie 2009 în cauza *Haralambie/România*, nr. 21737/03
Hotărârea CEDO din 28 aprilie 2009 în cauza *K.H. și alții/Slovacia*, nr. 32881/04

Baze de date privind ADN-ul
Hotărârea CEDO [MC] din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04

Date GPS
Hotărârea CEDO din 2 septembrie 2010 în cauza *Uzun/Germania*, nr. 35623/05

Date medicale personale
Hotărârea CEDO din 6 iunie 2013 în cauza *Avilkina și alții/Rusia*, nr. 1585/09
Hotărârea CEDO din 25 noiembrie 2008 în cauza *Biriuk/Lituania*, nr. 23373/03
Hotărârea CEDO din 17 iulie 2008 în cauza *I/Finlanda*, nr. 20511/03
Hotărârea CEDO din 29 aprilie 2014 în cauza *L.H./Letonia*, nr. 52019/07
Hotărârea CEDO din 10 octombrie 2006 în cauza *L.L./Franța*, nr. 7508/02
Hotărârea CEDO din 27 august 1997 în cauza *M.S./Suedia*, nr. 20837/92
Hotărârea CEDO din 2 iunie 2009 în cauza *Szuluk/Regatul Unit*, nr. 36936/05
Hotărârea CEDO din 17 februarie 2015 în cauza *Y/Turcia*, nr. 648/10
Hotărârea CEDO din 25 februarie 1997 în cauza *Z/Finlanda*, nr. 22009/93

Identitate
Hotărârea CEDO din 27 aprilie 2010 în cauza *Ciubotaru/Moldova*, nr. 27138/04
Hotărârea CEDO din 25 septembrie 2012 în cauza *Godelli/Italia*, nr. 33783/09
Hotărârea CEDO [MC] din 13 februarie 2003 în cauza *Odièvre/Franța*, nr. 42326/98

Informații privind activitățile profesionale
Hotărârea CEDO din 22 decembrie 2015 în cauza *G.S.B./Elveția*, nr. 28601/11
Hotărârea CEDO din 7 iulie 2015 în cauza *M.N. și alții/San Marino*, nr. 28005/12
Hotărârea CEDO din 6 decembrie 2012 în cauza *Michaud/Franța*, nr. 12323/11
Hotărârea CEDO din 16 decembrie 1992 în cauza *Niemietz/Germania*, nr. 13710/88

Interceptarea comunicărilor
Hotărârea CEDO [MC] din 16 februarie 2000 în cauza *Amann/Elveția*, nr. 27798/95
Hotărârea CEDO din 1 decembrie 2015 în cauza *Brito Ferrinho Bexiga Villa-Nova/Portugalia*, nr. 69436/10
Hotărârea CEDO din 3 aprilie 2007 în cauza *Copland/Regatul Unit*, nr. 62617/00
Hotărârea CEDO din 25 iunie 1997 în cauza *Halford/Regatul Unit*, nr. 20605/92
Hotărârea CEDO din 10 februarie 2009 în cauza *Iordachi și alții/Moldova*, nr. 25198/02
Hotărârea CEDO din 25 martie 1998 în cauza *Kopp/Elveția*, nr. 23224/94
Hotărârea CEDO din 1 iulie 2008 în cauza *Liberty și alții/Regatul Unit*, nr. 58243/00
Hotărârea CEDO din 2 august 1984 în cauza *Malone/Regatul Unit*, nr. 8691/79
Hotărârea CEDO din 18 iulie 2017 în cauza *Mustafa Sezgin Tanrıkulu/Turcia*, nr. 27473/06
Hotărârea CEDO din 3 februarie 2015 în cauza *Pruteanu/România*, nr. 30181/05
Hotărârea CEDO din 2 iunie 2009 în cauza *Szuluk/Regatul Unit*, nr. 36936/05

Obligații pentru persoanele responsabile
Hotărârea CEDO din 17 decembrie 2009 în cauza *B.B./Franța*, nr. 5335/06
Hotărârea CEDO din 17 iulie 2008 în cauza *I/Finlanda*, nr. 20511/03
Hotărârea CEDO din 10 mai 2011 în cauza *Mosley/Regatul Unit*, nr. 48009/08

Date cu caracter personal
Hotărârea CEDO [MC] din 16 februarie 2000 în cauza *Amann/Elveția*, nr. 27798/95
Hotărârea CEDO din 2 septembrie 2010 în cauza *Uzun/Germania*, nr. 35623/05
Hotărârea CEDO din 14 martie 2013 în cauza *Bernh Larsen Holding AS și alții/Norvegia*, nr. 24117/08

Fotografii
Hotărârea CEDO din 11 ianuarie 2005 în cauza *Sciacca/Italia*, nr. 50774/99
Hotărârea CEDO din 24 iunie 2004 în cauza *Von Hannover/Germania*, nr. 59320/00

Dreptul de a fi uitat
Hotărârea CEDO din 6 iunie 2006 în cauza *Segerstedt-Wiberg și alții/Suedia*, nr. 62332/00
Hotărârea CEDO [MC] din 27 iunie 2017 în cauza *Satakunnan Markkinapörssi Oy și Satamedia Oy/Finlanda*, nr. 931/13

Dreptul la opoziție
Hotărârea CEDO din 26 martie 1987 în cauza *Leander/Suedia*, nr. 9248/81

Hotărârea CEDO din 27 august 1997 în cauza *M.S./Suedia*, nr. 20837/92
Hotărârea CEDO din 10 mai 2011 în cauza *Mosley/Regatul Unit*, nr. 48009/08
Hotărârea CEDO [MC] din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95
Hotărârea CEDO din 2 februarie 2010 în cauza *Sinan Işık/Turcia*, nr. 21924/05

Categorii de date sensibile
Hotărârea CEDO din 18 septembrie 2014 în cauza *Brunet/Franța*, nr. 21010/10
Hotărârea CEDO din 17 iulie 2008 în cauza *I/Finlanda*, nr. 20511/03
Hotărârea CEDO din 6 decembrie 2012 în cauza *Michaud/Franța*, nr. 12323/11
Hotărârea CEDO [MC] din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04

Supraveghere și aplicarea legii (rolul diferiților actori, inclusiv al autorităților de supraveghere)
Hotărârea CEDO din 17 iulie 2008 în cauza *I/Finlanda*, nr. 20511/03
Hotărârea CEDO din 2 decembrie 2008 în cauza *K.U./Finlanda*, nr. 2872/02
Hotărârea CEDO din 24 iunie 2004 în cauza *Von Hannover/Germania*, nr. 59320/00
Hotărârea CEDO [MC] din 7 februarie 2012 în cauza *Von Hannover/Germania (nr. 2)*, nr. 40660/08 și 60641/08

Metode de supraveghere
Hotărârea CEDO din 5 noiembrie 2002 în cauza *Allan/Regatul Unit*, nr. 48539/99
Hotărârea CEDO din 28 iunie 2007 în cauza *Association for European Integration and Human Rights și Ekimdzhiev/Bulgaria*, nr. 62540/00
Hotărârea CEDO [MC] din 5 septembrie 2017 în cauza *Bărbulescu/România*, nr. 61496/08
Hotărârea CEDO din 19 mai 2016 în cauza *D.L./Bulgaria*, nr. 7472/14
Hotărârea CEDO din 15 ianuarie 2015 în cauza *Dragojević/Croația*, nr. 68955/11
Hotărârea CEDO din 7 iunie 2016 în cauza *Karabeyoğlu/Turcia*, nr. 30083/10
Hotărârea CEDO din 6 septembrie 1978 în cauza *Klass și alții/Germania*, nr. 5029/71
Hotărârea CEDO [MC] din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95
Hotărârea CEDO din 12 ianuarie 2016 în cauza *Szabó și Vissy/Ungaria*, nr. 37138/14
Hotărârea CEDO din 22 octombrie 2002 în cauza *Taylor-Sabori/Regatul Unit*, nr. 47114/99
Hotărârea CEDO din 2 septembrie 2010 în cauza *Uzun/Germania*, nr. 35623/05
Hotărârea CEDO din 16 iunie 2016 în cauza *Versini-Campinchi și Crasnianski/Franța*, nr. 49176/11
Hotărârea CEDO din 31 mai 2005 în cauza *Vetter/Franța*, nr. 59842/00
Hotărârea CEDO din 18 octombrie 2016 în cauza *Vukota-Bojić/Elveția*, nr. 61838/10

Hotărârea CEDO [MC] din 4 decembrie 2015 în cauza *Roman Zakharov/Rusia*, nr. 47143/06

Supraveghere video
Hotărârea CEDO din 5 octombrie 2010 în cauza *Köpke/Germania*, nr. 420/07
Hotărârea CEDO din 28 ianuarie 2003 în cauza *Peck/Regatul Unit*, nr. 44647/98

Probe de voce
Hotărârea CEDO din 20 decembrie 2005 în cauza *Wisse/Franța*, nr. 71611/01
Hotărârea CEDO din 25 septembrie 2001 în cauza *P.G. și J.H./Regatul Unit*, nr. 44787/98

Jurisprudență selectată a Curții de Justiție a Uniunii Europene

Jurisprudență legată de Directiva privind protecția datelor

Hotărârea CJUE din 4 mai 2017 în cauza C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA „Rīgas satiksme"*

[Principiul prelucrării legale: interes legitim urmărit de o parte terță]

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

[Dreptul la ștergerea datelor cu caracter personal; dreptul la opoziție față de prelucrare]

Hotărârea CJUE [MC] din 21 decembrie 2016 în cauzele conexate C-203/15 și C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen* și *Secretary of State for the Home Department/Tom Watson și alții*

[Confidențialitatea comunicațiilor electronice; furnizori de servicii de comunicare electronică; obligația privind păstrarea generalizată și nediferențiată a datelor de transfer și de localizare; lipsa examinării prealabile de către o instanță sau o autoritate administrativă independentă; Carta drepturilor fundamentale a Uniunii Europene; compatibilitatea cu dreptul UE]

Hotărârea CJUE din 19 octombrie 2016 în cauza C-582/14, *Patrick Breyer/Bundesrepublik Deutschland*

[Definiția „datelor cu caracter personal"; adrese IP; stocarea datelor de către un furnizor de servicii media online; reglementare națională care nu permite luarea în considerare a interesului legitim urmărit de operator]

Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*

[Principiul prelucrării legale; drepturi fundamentale; anularea Deciziei privind „sfera de siguranță"; competențele autorităților de supraveghere independente]

Hotărârea CJUE din 1 octombrie 2015 în cauza C-230/14, *Weltimmo s.r. o./Nemzeti Adatvédelmi és Információszabadság Hatóság*

[Competențele autorităților naționale de supraveghere]

Hotărârea CJUE din 1 octombrie 2015 în cauza C-201/14, *Smaranda Bara și alții/Casa Națională de Asigurări de Sănătate și alții*
[Dreptul de a fi informat cu privire la prelucrarea datelor cu caracter personal]

Hotărârea CJUE din 11 decembrie 2014 în cauza C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*
[Conceptele „prelucrarea datelor" și „operator"]

Hotărârea CJUE din 7 noiembrie 2013 în cauza C-473/12, *Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert și alții*
[Dreptul de a fi informat cu privire la prelucrarea datelor cu caracter personal]

Hotărârea CJUE din 11 martie 2013 în cauza T-462/12 R, *Pilkington Group Ltd/Comisia Europeană*, Ordonanța președintelui Tribunalului

Hotărârea CJUE din 30 mai 2013 în cauza C-342/12, *Worten – Equipamentos para o Lar SA/Autoridade para as Condições de Trabalho (ACT)*
[Conceptul „date cu caracter personal"; evidența timpului de lucru; principiile legate de calitatea datelor și criteriile care conferă legitimitate prelucrării datelor; accesul de către autoritatea națională responsabilă pentru monitorizarea condițiilor de lucru; obligația angajatorului de a pune la dispoziție evidența timpului de lucru, astfel încât să permită consultarea imediată a acesteia]

Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții* și *Kärntner Landesregierung și alții*
[Încălcarea legislației primare a UE de către Directiva privind păstrarea datelor; prelucrarea legală; limitările legate de scop și de stocare]

Hotărârea CJUE [MC] din 8 aprilie 2014 în cauza C-288/12, *Comisia Europeană/Ungaria*
[Legitimitatea încetării mandatului autorității naționale pentru protecția datelor]

Hotărârea CJUE din 17 iulie 2014 în cauzele conexate C-141/12 și C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel* și *Minister voor Immigratie, Integratie en Asiel/M și S*
[Domeniul de aplicare al dreptului de acces al unei persoane vizate; protejarea persoanelor fizice față de prelucrarea datelor cu caracter personal; conceptul „date cu caracter personal"; date referitoare la solicitantul unui permis de ședere și analiza juridică inclusă într-un document administrativ de pregătire a deciziei; Carta drepturilor fundamentale a Uniunii Europene]

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

[Obligațiile furnizorilor de servicii de motoare de căutare de a se abține, la cererea persoanei vizate, de la a afișa datele cu caracter personal în rezultatele de căutare; aplicabilitatea Directivei privind protecția datelor; conceptu „prelucrarea datelor"; sensul termenului „operator"; ponderarea protecției datelor cu libertatea de exprimare; dreptul de a fi uitat]

Hotărârea CJUE [MC] din 16 octombrie 2012 în cauza C-614/10, *Comisia Europeană/ Republica Austria*

[Independența unei autorități naționale de supraveghere]

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

[Punerea în aplicare corectă a articolului 7 litera (f) din Directiva privind protecția datelor – „interesele legitime ale altor persoane" – în legislația națională]

Hotărârea CJUE din 16 februarie 2012 în cauza C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/Netlog NV*

[Obligația furnizorilor de rețele sociale de a împiedica utilizarea ilicită a operelor muzicale și audiovizuale de către utilizatorii rețelei]

Hotărârea CJUE din 24 noiembrie 2011 în cauza C-70/10, *Scarlet Extended SA/ Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*

[Societatea informațională; drepturi de autor; internet; software peer-to-peer; furnizori de servicii internet; instalarea unui sistem de filtrare a comunicațiilor electronice pentru a preveni partajarea de fișiere care încalcă drepturile de autor; absența obligației generale de a monitoriza informațiile transmise]

Hotărârea CJUE din 5 mai 2011 în cauza C-543/09, *Deutsche Telekom AG/ Bundesrepublik Deutschland*

[Necesitatea reînnoirii consimțământului]

Hotărârea CJUE [MC] din 9 noiembrie 2010 în cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*

[Conceptul „date cu caracter personal"; proporționalitatea obligației legale de a publica date cu caracter personal privind beneficiarii unor anumite fonduri agricole ale UE]

Hotărârea CJUE din 7 mai 2009 în cauza C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*
[Dreptul de acces al persoanei vizate]

Hotărârea CJUE [MC] din 9 martie 2010 în cauza C-518/07, *Comisia Europeană/Republica Federală Germania*
[Independența unei autorități naționale de supraveghere]

Hotărârea CJUE [MC] din 16 decembrie 2008 în cauza C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy și Satamedia Oy*
[Conceptul „activități jurnalistice", în sensul articolului 9 din Directiva privind protecția datelor]

Hotărârea CJUE [MC] din 16 decembrie 2008 în cauza C-524/06, *Heinz Huber/Bundesrepublik Deutschland*
[Legitimitatea deținerii de date privind cetățenii străini într-un registru statistic]

Hotărârea CJUE [MC] din 29 ianuarie 2008 în cauza C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*
[Conceptul „date cu caracter personal"; obligația furnizorilor de servicii de acces la internet de a dezvălui identitatea utilizatorilor de programe de schimb de fișiere KaZaA unei asociații de protecție a proprietății intelectuale]

Hotărârea CJUE din 6 noiembrie 2003 în cauza C-101/01, *Proces penal/Bodil Lindqvist*
[Categorii speciale de date cu caracter personal]

Hotărârea CJUE din 20 mai 2003 în cauzele conexate C-465/00, C-138/01 și C-139/01, *Rechnungshof/Österreichischer Rundfunk și alții și Christa Neukomm și Joseph Lauermann/Österreichischer Rundfunk*
[Proporționalitatea obligației legale de a publica date cu caracter personal privind salariile angajaților anumitor categorii de instituții asociate sectorului public]

Concluziile avocatului general Kokott din 20 iulie 2017 în cauza C-434/16, *Peter Nowak/Data Protection Commissioner*
[Conceptul de date cu caracter personal; accesul la propria foaie de examinare; corecturile examinatorului]

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

[Trimitere preliminară; spațiul de libertate, securitate și justiție; pașaport biometric; amprente digitale; temei juridic; proporționalitate]

Jurisprudență legată de Directiva (UE) 2016/681

Avizul 1/15 al Curții (Marea Cameră) din 26 iulie 2017

[Temei juridic; proiect de acord între Canada și Uniunea Europeană privind transferul și prelucrarea datelor din registrul cu numele pasagerilor; compatibilitatea proiectului de acord cu articolul 16 din TFUE și cu articolele 7 și 8 și articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene]

Jurisprudență legată de Regulamentul privind protecția datelor de către instituțiile UE

Hotărârea CJUE din 16 iulie 2015 în cauza C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/Autoritatea Europeană pentru Siguranța Alimentară (EFSA), Comisia Europeană*

[Accesul la documente]

Hotărârea CJUE [MC] din 29 iunie 2010 în cauza C-28/08 P, *Comisia Europeană/The Bavarian Lager Co. Ltd.*

[Accesul la documente]

Jurisprudență legată de Directiva 2002/58/CE

Hotărârea CJUE din 15 martie 2017 în cauza C-536/15, *Tele2 (Netherlands) BV și alții/Autoriteit Consument en Markt (ACM)*

[Principiul nediscriminării; punerea la dispoziție a datelor cu caracter personal ale abonaților în scopul furnizării de servicii publice de informații telefonice și de liste de abonați; consimțământul abonatului; diferențiere în funcție de statul membru în care se furnizează serviciile publice de informații telefonice și de liste de abonați]

Hotărârea CJUE [MC] din 21 decembrie 2016 în cauzele conexate C-203/15 și C-698/15, *Tele2 Sverige AB/Post- och telestryrelsen* și *Secretary of State for the Home Department/Tom Watson și alții*

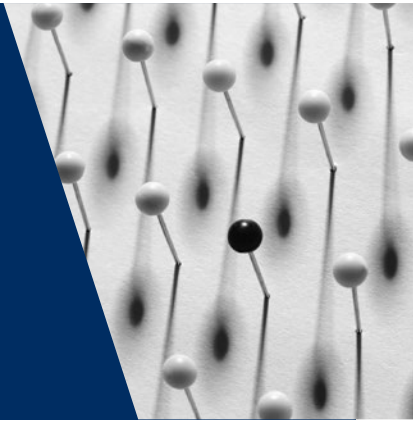
[Confidențialitatea comunicațiilor electronice; furnizori de servicii de comunicare electronică; obligația privind păstrarea generalizată și nediferențiată a datelor de transfer și de localizare; lipsa examinării prealabile de către o instanță sau o autoritate administrativă independentă; Carta drepturilor fundamentale a Uniunii Europene; compatibilitatea cu dreptul UE]

Hotărârea CJUE din 24 noiembrie 2011 în cauza C-70/10, *Scarlet Extended SA/ Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*

[Societatea informațională; drepturi de autor; internet; software peer-to-peer; furnizori de servicii internet; instalarea unui sistem de filtrare a comunicațiilor electronice pentru a preveni partajarea de fișiere care încalcă drepturile de autor; absența obligației generale de a monitoriza informațiile transmise]

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 Sweden AB*

[Drepturi de autor și drepturi conexe; prelucrarea datelor prin internet; încălcarea unui drept exclusiv; cărți audio puse la dispoziție prin internet, pe un server FTP, prin intermediul unei adrese IP alocate de furnizorul de servicii internet; ordin emis împotriva furnizorului de servicii internet, prin care i se impune acestuia să divulge numele și adresa fizică a utilizatorului adresei IP]



Index

Jurisprudența Curții Europene a Drepturilor Omului

Jurisprudența instanțelor naționale

O gamă largă de informații privind Agenția pentru Drepturi Fundamentale a Uniunii Europene este disponibilă pe internet. Acestea pot fi accesate pe pagina de web a FRA la adresa fra.europa.eu

Informații suplimentare privind jurisprudența Curții Europene a Drepturilor Omului sunt disponibile pe pagina de web a Curții: echr.coe.int. Portalul de căutare HUDOC oferă acces la hotărârile și deciziile Curții în limba engleză și/sau franceză, traduceri în limbi suplimentare, rezumate ale hotărârilor, comunicate de presă și alte informații privind activitatea Curții (https://hudoc.echr.coe.int).

Cum se obțin publicațiile Consiliului Europei

Editura Consiliului Europei produce lucrări în toate domeniile de referință ale organizației, inclusiv drepturile omului, științe juridice, sănătate, etică, afaceri sociale, mediu, educație, cultură, sport, tineret și patrimoniu arhitectural. Cărțile și publicațiile electronice din catalogul extins pot fi comandate online (https://book.coe.int).

O sală de lectură virtuală permite utilizatorilor să consulte gratuit fragmente din lucrări importante recent publicate sau textele integrale ale unor documente oficiale.

Informații despre convențiile Consiliului Europei și textul integral al acestora sunt disponibile pe site-ul Biroului pentru Tratate: http://conventions.coe.int

Contactați UE

În persoană

În întreaga Uniune Europeană există sute de centre de informare Europe Direct. Puteți găsi adresa centrului cel mai apropiat de dumneavoastră la: https://europa.eu/european-union/contact_ro

La telefon sau prin e-mail

Europe Direct este un serviciu care vă oferă răspunsuri la întrebările privind Uniunea Europeană. Puteți accesa acest serviciu:
— apelând numărul gratuit 00 800 6 7 8 9 10 11 (unii operatori pot taxa aceste apeluri);
— apelând numărul standard: +32 22999696; sau
— prin e-mail, la: https://europa.eu/european-union/contact_ro

Găsiți informații despre UE

Online

Informații despre Uniunea Europeană în toate limbile oficiale ale UE sunt disponibile pe site-ul Europa, la: https://europa.eu/european-union/index_ro

Publicații ale UE

Puteți descărca sau comanda publicații ale UE gratuite și contra cost pe site-ul EU Bookshop, la: https://op.europa.eu/ro/publications. Mai multe exemplare ale publicațiilor gratuite pot fi obținute contactând Europe Direct sau centrul dumneavoastră local de informare (a se vedea https://europa.eu/european-union/contact_ro).

Dreptul UE și documente conexe

Pentru accesul la informații juridice din UE, inclusiv la ansamblul legislației UE începând din 1951 în toate versiunile lingvistice oficiale, accesați site-ul EUR-Lex, la: http://eur-lex.europa.eu

Datele deschise ale UE

Portalul de date deschise al UE (http://data.europa.eu/euodp/ro) oferă acces la seturi de date din UE. Datele pot fi descărcate și reutilizate gratuit, atât în scopuri comerciale, cât și necomerciale.

doi:10.2811/582023 TK-05-17-225-RO-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Dezvoltarea rapidă a tehnologiei informației a exacerbat nevoia de protecție solidă a datelor cu caracter personal – un drept garantat atât de instrumentele Uniunii Europene (UE), cât și de instrumentele Consiliului Europei. Protejarea acestui drept important implică provocări noi și semnificative, pe măsură ce progresele tehnologice extind frontierele unor domenii precum supravegherea, interceptarea comunicațiilor și stocarea datelor. Prezentul manual este conceput pentru a familiariza practicienii în domeniul dreptului nespecializați în domeniul protecției datelor cu acest domeniu de drept emergent. Acesta oferă o imagine de ansamblu asupra cadrelor juridice ale UE și Consiliului Europei în vigoare. Manualul explică jurisprudența fundamentală în domeniu, prezentând succint atât hotărârile majore ale Curții de Justiție a Uniunii Europene, cât și pe cele ale Curții Europene a Drepturilor Omului. În plus, prezintă scenarii ipotetice care servesc drept ilustrații practice ale diferitelor probleme întâlnite în acest domeniu în continuă evoluție.

AGENȚIA PENTRU DREPTURI FUNDAMENTALE A UNIUNII EUROPENE
Schwarzenbergplatz 11 – 1040 Viena – Austria
Tel. +43 (1) 580 30-0 – Fax +43 (1) 580 30-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

CURTEA EUROPEANĂ A DREPTURILOR OMULUI
CONSILIUL EUROPEI
67075 Strasbourg Cedex – Franța
Tel. +33 (0) 3 88 41 20 18 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int – twitter.com/ECHR_CEDH

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR
Rue Wiertz 60 – 1047 Bruxelles – Belgia
Tel. +32 2 283 19 00
edps.europa.eu – edps@edps.europa.eu – @EU_EDPS

Oficiul pentru Publicații al Uniunii Europene

ISBN 978-92-871-9824-2 (Consiliul Europei)
ISBN 978-92-9474-787-7 (FRA)