MANUAL

Manual de legislație europeană privind protecția datelor

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

Manuscrisul prezentului manual a fost finalizat în luna aprilie 2014.
Actualizările vor fi disponibile în viitor pe site-ul FRA la adresa: fra.europa.eu, pe site.ul Consiliului Europei la adresa: coe.int/dataprotection, și pe site-ul Curții Europene a Drepturilor Omului în meniul de Jurisprudență la adresa: echr.coe.int.

Europe Direct este un serviciu destinat să vă ajute să găsiți răspunsuri la întrebările pe care vi le puneți despre Uniunea Europeană.

Un număr unic gratuit (*):

00 800 6 7 8 9 10 11

(*) Informațiile primite sunt gratuite, la fel ca și cea mai mare parte a apelurilor telefonice (unii operatori și unele cabine telefonice și hoteluri taxează totuși aceste apeluri).

Credite foto (copertă & conținut): © iStockphoto

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

Cuprinsul informațiilor poate fi găsit la finalul prezentei publicații.

Luxemburg: Oficiul pentru Publicații al Uniunii Europene, 2014

ISBN 978-92-871-9938-6 (CoE)
ISBN 978-92-9239-339-7 (FRA)
doi:10.2811/55294

Printed in Belgium

Tipărit pe hârtie reciclată (PCF)

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

Manual de legislație europeană privind protecția datelor

Cuvânt înainte

Prezentul manual de legislație europeană privind protecția datelor este întocmit prin cooperarea dintre Agenția pentru Drepturi Fundamentale a Uniunii Europene (FRA) şi Consiliul Europei alături de Grefa Curții Europene a Drepturilor Omului. Este al treilea dintr-o serie de manuale juridice întocmite prin cooperarea dintre FRA şi Consiliul Europei. În luna martie a anului 2011 a fost publicat primul manual de legislație europeană privind nediscriminarea, iar în luna iunie a anului 2013, cel de al doilea manual de legislație europeană privind azilul, frontierele şi imigrația.

Am hotărât să ne continuăm cooperarea cu privire la un subiect de actualitate, care ne afectează pe toți în fiecare zi, şi anume protecția datelor cu caracter personal. Europa se bucură de unul dintre cele mai protective sisteme în acest domeniu, care se bazează pe Convenția 108 a Consiliului Europei, pe instrumentele Uniunii Europene (UE), precum şi pe jurisprudența Curții Europene a Drepturilor Omului (CEDO) şi a Curții de Justiție a Uniunii Europene (CJUE).

Scopul prezentului manual este acela de a sensibiliza şi de a ameliora cunoaşterea reglementărilor în materie de protecție a datelor în cadrul Uniunii Europene şi în statele membre ale Consiliului Europei, servind drept principal punct de referință pentru cititori. Manualul se adresează profesioniştilor nespecializați din domeniul juridic, judecătorilor, autorităților naționale pentru protecția datelor şi altor persoane care activează în domeniul protecției datelor.

Odată cu intrarea în vigoare a Tratatului de la Lisabona în luna decembrie a anului 2009, Carta Drepturilor Fundamentale a Uniunii Europene a devenit obligatorie din punct de vedere juridic şi, astfel, dreptul la protecția datelor cu caracter personal a fost ridicat la statutul de drept fundamental individual. O mai bună înțelegere a Convenției 108 a Consiliului Europei şi a instrumentelor UE, care au pregătit drumul pentru protecția datelor în Europa, precum şi a jurisprudenței CJUE şi a CEDO este esențială pentru protecția acestui drept fundamental.

Dorim să mulțumim Institutului pentru Drepturile Omului Ludwig Bolzmann pentru contribuția sa la elaborarea acestui manual. De asemenea, adresăm mulțumiri biroului Autorității Europene pentru Protecția Datelor pentru contribuția adusă pe parcursul etapei de redactare. Mulțumim în mod deosebit unității pentru protecția datelor a Comisiei Europene pentru sprijinul acordat pe parcursul întocmirii acestui manual. În cele din urmă, am dori să ne exprimăm recunoştința față de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, care a revizuit traducerea manualului în limba română.

Philippe Boillat
Director General pentru Drepturile omului şi statul de drept Consiliul Europei

Morten Kjaerum
Director al Agenției Europene pentru Drepturi Fundamentale

Cuprins

Abrevieri şi acronime

AELS	Asociația Europeană a Liberului Schimb
AEPD	Autoritatea Europeană pentru Protecția Datelor
BCR	Reguli corporatiste obligatorii
Carta	Carta Drepturilor Fundamentale a Uniunii Europene
CE	Comunitatea Europeană
CEDO	Curtea Europeană a Drepturilor Omului
CETS	Seria Tratatelor Consiliului Europei
CIS	Sistemul de informații al vămilor
CJUE	Curtea de Justiție a Uniunii Europene (denumită Curtea Europeană de Justiție, CEJ, înainte de luna decembrie a anului 2009)
CoE	Consiliul Europei
Convenția 108	Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Consiliul Europei)
CRM	Gestionarea relației cu clienții
C-SIS	Sistemul Central de Informații Schengen
DUDO	Declarația Universală a Drepturilor Omului
EAW	Mandat european de arestare
ECHR	Convenția europeană a drepturilor omului
ENISA	Agenția Uniunii Europene pentru Securitatea Rețelelor şi a Informațiilor
ESMA	Autoritatea Europeană pentru Valori Mobiliare şi Piețe
eTEN	Rețele transeuropene de telecomunicații
eu-LISA	Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă
EuroPriSe	Marca europeană de protecție a vieții private
FRA	Agenția pentru Drepturi Fundamentale a Uniunii Europene

GPS	Sistem de poziționare globală
JSB	Organismul comun de supraveghere
N-SIS	Sistemul Național de Informații Schengen
OCDE	Organizația pentru Cooperare şi Dezvoltare Economică
ONG	Organizație neguvernamentală
ONU	Organizația Națiunilor Unite
PIN	Număr personal de identificare
PNR	Registrul cu numele pasagerilor
SEE	Spațiul Economic European
SEPA	Zona unică de plăți în euro
SIS	Sistemul de Informații Schengen
SWIFT	Societatea pentru Telecomunicații Financiare Interbancare Mondiale
TFUE	Tratatul privind funcționarea Uniunii Europene
TUE	Tratatul privind Uniunea Europeană
TVCI	Televiziune cu circuit închis
UE	Uniunea Europeană
UNE	Unitatea Națională Europol
VIS	Sistemul de informații privind vizele

Modul de utilizare a acestui manual

Prezentul manual oferă o privire de ansamblu asupra legislației aplicabile în domeniul protecției datelor în legătură cu Uniunea Europeană (UE) şi Consiliul Europei (CoE).

Manualul este conceput astfel încât să sprijine practicienii în domeniul dreptului care nu sunt specializați în domeniul protecției datelor; se adresează avocaților, judecătorilor sau altor practicieni, precum şi acelor persoane care lucrează pentru alte organisme, inclusiv organizații neguvernamentale (ONG-uri), care se pot confrunta cu probleme juridice legate de protecția datelor.

Este primul punct de referință atât pentru legislația UE, cât şi pentru Convenția europeană a drepturilor omului (ECHR) cu privire la protecția datelor, explicând modul în care acest domeniu este reglementat în conformitate cu dreptul european şi ECHR, precum şi cu Convenția CoE pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108) şi alte instrumente ale CoE. Fiecare capitol prezintă la început un tabel unic cu dispozițiile juridice aplicabile, inclusiv o selecție de acte importante din jurisprudență, conform celor două sisteme juridice europene separate. Apoi sunt prezentate succesiv legile relevante ale acestor două ordini europene, în măsura în care sunt aplicabile pentru fiecare subiect. Acest lucru permite cititorului să observe punctele de convergență ale celor două sisteme juridice şi aspectele în care acestea diferă.

Tabelele de la începutul fiecărui capitol enumeră subiectele tratate în cadrul acelui capitol şi indică dispozițiile juridice aplicabile şi alte materiale relevante, cum ar fi jurisprudența. Ordinea subiectelor poate fi uşor diferită față de structura textului din cadrul capitolului, dacă se consideră că se favorizează astfel prezentarea concisă a conținutului capitolului. Tabelele vizează atât legislația CoE, cât şi dreptul european. Acest lucru ar trebui să ajute utilizatorii să găsească informațiile-cheie referitoare la propria situație, în special dacă se află exclusiv sub incidența legislației CoE.

Practicienii din statele non-membre ale UE, dar membre ale CoE şi părți la Convenția europeană a drepturilor omului şi la Convenția 108 pot accesa informațiile relevante pentru țara lor prin consultarea directă a secțiunilor privind CoE. Practicienii din statele membre ale UE vor trebui să acceseze ambele secțiuni, întrucât aceste state se află sub incidența ambelor ordini juridice. Persoanele care au nevoie de informații suplimentare despre un anumit aspect au la dispoziție o listă de trimiteri la materiale mai specializate în secțiunea „Lecturi suplimentare” din manual.

Legislația CoE este prezentată prin scurte trimiteri la o selecție de cazuri ale Curții Europene a Drepturilor Omului (CEDO). Acestea au fost alese dintr-un număr mare de hotărâri şi decizii CEDO existente cu privire la aspecte legate de protecția datelor.

Legislația UE este disponibilă în măsurile legislative adoptate, în dispozițiile relevante ale tratatelor şi în Carta Drepturilor Fundamentale a Uniunii Europene, astfel cum sunt interpretate în jurisprudența Curții de Justiție a Uniunii Europene [CJUE, denumită Curtea Europeană de Justiție (CEJ) înainte de anul 2009].

Jurisprudența descrisă sau citată în prezentul manual oferă exemple de o importanță semnificativă atât pentru jurisprudența CEDO, cât şi pentru cea a CJUE. Orientările de la sfârşitul prezentului ghid sunt destinate să ajute cititorul în căutarea online a jurisprudenței.

În plus, ilustrații practice cu scenarii ipotetice sunt oferite în casete de text pentru o mai bună exemplificare a aplicării în practică a normelor europene privind protecția datelor, în special acolo unde nu există o jurisprudență CEDO sau CJUE specifică pe tema respectivă.

Manualul începe cu o scurtă descriere a rolului celor două sisteme juridice, rol stabilit prin legislația Convenției europene a drepturilor omului şi dreptul UE (capitolul 1). Capitolele 2-8 tratează următoarele aspecte:

- terminologia în domeniul protecției datelor;
- principiile-cheie ale legislației europene privind protecția datelor;
- normele legislației europene privind protecția datelor;
- drepturile persoanei vizate şi aplicarea acestora;
- fluxurile transfrontaliere de date;
- protecția datelor în contextul poliției şi justiției penale;
- alte legi europene specifice privind protecția datelor.

1

Contextul şi cadrul legislației europene privind protecția datelor

UE	Aspecte vizate	CoE
Dreptul la protecția datelor		
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*), MO 1995 L 281		Convenția europeană a drepturilor omului, articolul 8 (dreptul la respectarea vieții private și de familie, a domiciliului și a corespondenței) Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108)
Echilibrarea drepturilor		
CJUE, Cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert /Land Hessen*, 2010	**În general**	
CJUE, C-73/07, *Tietosuojavaltuutettu/ Satakunnan Markkinapörssi Oy și Satamedia Oy*, 2008	**Libertatea de exprimare**	CEDO, *Axel Springer AG/ Germania*, 2012 CEDO, *Mosley/Regatul Unit*, 2011
	Libertatea artelor și științelor	CEDO, *Vereinigung bildender Künstler/Austria*, 2007
CJUE, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, 2008	**Protecția proprietății**	
CJUE, C-28/08 P, *Comisia Europeană/The Bavarian Lager Co. Ltd*, 2010	**Accesul la documente**	CEDO, *Társaság a Szabadságjogokért/Ungaria*, 2009

1.1. Dreptul la protecția datelor

Puncte-cheie

- În conformitate cu articolul 8 din Convenția europeană a drepturilor omului, dreptul de protecție împotriva colectării şi utilizării datelor cu caracter personal face parte din dreptul la respectarea vieții private şi de familie, a domiciliului şi a corespondenței.
- Convenția 108 a CoE este primul instrument internațional obligatoriu din punct de vedere juridic care tratează în mod explicit protecția datelor.
- În temeiul dreptului UE, protecția datelor a fost reglementată pentru prima dată prin Directiva privind protecția datelor.
- În temeiul dreptului UE, protecția datelor a fost recunoscută ca drept fundamental.

Dreptul de a proteja sfera privată a unei persoane fizice împotriva intruziunii din partea altora, în special din partea statului, a fost prevăzut pentru prima dată în cadrul unui instrument juridic internațional în articolul 12 din Declarația Universală a Drepturilor Omului (DUDO) din 1948 a Organizației Națiunilor Unite (ONU) privind respectarea vieții private şi de familie[1]. DUDO a influențat dezvoltarea în Europa a altor instrumente pentru drepturile omului.

1.1.1. 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 şi dezvoltării sociale. În acest sens, a adoptat în 1950 Convenția europeană a drepturilor omului (ECHR), care a intrat în vigoare în 1953.

Statele au obligația internațională de a respecta ECHR. 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.

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, Curtea Europeană a Drepturilor Omului (CEDO). CEDO se

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

asigură că statele îşi 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. În anul 2013, Consiliul Europei cuprindea 47 de state membre, 28 dintre acestea fiind şi state membre ale UE. Un reclamant la CEDO nu trebuie să fie resortisant al unuia dintre statele membre. CEDO poate examina şi cauzele interstatale introduse de unul sau mai multe state membre ale CoE împotriva unui alt stat membru.

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 şi de familie, a domiciliului şi a corespondenței şi stabileşte condițiile în baza cărora sunt permise limitări ale acestui drept[2].

Jurisprudența CEDO a examinat numeroase situații în care au apărut aspecte legate de protecția datelor, în special situații cu privire la intercepția comunicărilor[3], diferite forme de supraveghere[4] şi protecția împotriva stocării datelor cu caracter personal de către autoritățile publice[5]. Aceasta a clarificat faptul că articolul 8 din Convenția europeană a drepturilor omului nu numai că obligă statele să nu întreprindă vreo acțiune care ar putea încălca dreptul prevăzut de convenție, ci prevede şi că acestea sunt supuse, în anumite împrejurări, obligațiilor pozitive de a asigura în mod activ respectarea efectivă a vieții private şi de familie[6]. Multe dintre aceste cazuri vor fi analizate în detaliu în capitolele corespunzătoare.

1.1.2. 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 acestora (cu caracter personal). Până la mijlocul anilor 1970, Comitetul de Miniştri al Consiliului Europei a adoptat diferite rezoluții privind protecția datelor cu caracter personal, cu referire la articolul 8 din Convenția europeană a drepturilor

2 CoE, Convenția europeană a drepturilor omului, CETS nr. 005, 1950.

3 A se vedea, 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.

4 A se vedea, 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.

5 A se vedea, de exemplu, Hotărârea CEDO din 26 martie 1987 în cauza *Leander/Suedia*, nr. 9248/81; Hotărârea CEDO din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 şi nr. 30566/04.

6 A se vedea, de exemplu, Hotărârea CEDO din 17 iulie 2008, *I./Finlanda*, nr. 20511/03; Hotărârea CEDO din 2 decembrie 2008 în cauza *K.U./Finlanda*, nr. 2872/02.

omului[7]. În anul 1981, a fost deschisă spre semnare o Convenție pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108)[8]. Convenția 108 a fost, şi rămâne încă, singurul instrument internațional obligatoriu din punct de vedere juridic în domeniul protecției datelor.

Convenția 108 se aplică tuturor prelucrărilor de date efectuate atât în sectorul public, cât şi în cel privat, cum ar fi prelucrările de date efectuate de sistemul judiciar şi autoritățile de aplicare a legii. Aceasta protejează persoanele împotriva abuzurilor care pot însoți colectarea şi prelucrarea datelor cu caracter personal şi, totodată, urmărește să reglementeze fluxul transfrontalier de date cu caracter personal. În ceea ce privește colectarea şi prelucrarea datelor cu caracter personal, principiile stabilite în convenție se referă, în special, la colectarea şi prelucrarea automatizată corectă şi legală a datelor, stocarea în scopuri determinate şi legitime, utilizarea numai în scopuri compatibile cu acestea şi păstrarea într-o formă care să permită identificarea persoanelor în cauză pe o durată ce nu o depăşeşte pe cea necesară scopurilor pentru care datele sunt înregistrate. Principiile vizează, de asemenea, calitatea datelor, în special faptul că acestea trebuie să fie adecvate, pertinente şi neexcesive (principiul proporționalității), precum şi exacte

Pe lângă faptul că oferă garanții pentru colectarea şi prelucrarea datelor cu caracter personal, convenția interzice, în absența unor garanții juridice adecvate, prelucrarea datelor „sensibile", precum cele referitoare la originea rasială, opiniile politice, starea de sănătate, convingerile religioase, viața sexuală sau condamnările penale.

Convenția consacră, de asemenea, dreptul unei persoane fizice de a fi informată cu privire la stocarea informațiilor sale cu caracter personal şi, 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.

Deşi convenția prevede libera circulație a datelor cu caracter personal între statele semnatare ale convenției, aceasta impune şi unele restricții asupra fluxurilor de date către statele în care reglementările juridice nu prevăd o protecție echivalentă.

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

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

Pentru a dezvolta în continuare principiile generale şi normele prevăzute de Convenția 108, Comitetul de Miniştri al CoE a adoptat mai multe recomandări fără caracter obligatoriu din punct de vedere juridic (a se vedea capitolele 7 şi 8).

Toate statele membre ale UE au ratificat Convenția 108. În 1999, Convenția 108 a fost modificată pentru a permite UE să devină parte la aceasta.[9] În 2001, a fost adoptat un Protocol adițional la Convenția 108, care introduce dispoziții privind fluxurile transfrontaliere de date către țările care nu sunt parte la convenție, aşa-numitele țări terțe, şi cu privire la înființarea obligatorie a autorităților naționale de supraveghere a protecției datelor[10].

Perspective

Ca urmare a deciziei de modernizare a Convenției 108, o consultare publică desfăşurată în 2011 a făcut posibilă confirmarea celor două obiective principale ale acestei lucrări: sporirea protecției vieții private în domeniul digital şi consolidarea mecanismului de urmărire al convenției.

Convenția 108 este deschisă pentru aderare statelor non-membre ale CoE, inclusiv țărilor din afara Europei. Potențialul convenției ca standard universal şi caracterul său deschis pot servi drept bază pentru promovarea protecției datelor la nivel mondial.

Până în prezent, 45 dintre cele 46 de părți contractante ale Convenției 108 sunt state membre ale CoE. Uruguay, prima țară din afara Europei, a aderat în luna august a anului 2013, iar Maroc, care a fost invitat de Comitetul de Miniştri să adere la Convenția 108, se află în proces de oficializare a aderării.

1.1.3. Legislația Uniunii Europene privind protecția datelor

Dreptul UE este format din tratate şi legislație europeană secundară. Tratatele, şi anume Tratatul privind Uniunea Europeană (TUE) şi Tratatul privind funcționarea Uniunii Europene (TFUE), au fost aprobate de toate statele membre ale UE şi sunt, de asemenea, denumite „legislația europeană primară". Regulamentele, directivele şi

9 CoE, Amendamente la Convenția pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (ETS No. 108), care să permită Uniunii Europene să adere, adoptată de Comitetul de Miniştri, la Strasbourg, la 15 iunie 1999; Art. 23 (2) din Convenția 108, în forma sa modificată.

10 CoE, Protocol adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal privind autoritățile de supraveghere şi fluxurile transfrontaliere de date, CETS nr. 181, 2001.

deciziile UE au fost adoptate de instituțiile UE care au primit această autoritate în baza tratatelor; deseori, acestea sunt denumite „legislația europeană secundară".

Principalul instrument juridic al UE pentru protecția datelor este 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*)[11]. A fost adoptată în anul 1995, într-un moment în care mai multe state membre adoptaseră deja legislații naționale privind protecția datelor. 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.

Întrucât scopul adoptării Directivei privind protecția datelor a fost armonizarea[12] legislației privind protecția datelor la nivel național, directiva își permite un grad de specificitate comparabil cu cel al legislațiilor naționale privind protecția datelor existente (la acel moment). Pentru CJUE, „Directiva 95/46 urmărește să asigure că nivelul de protecție a drepturilor și libertăților persoanelor în ceea ce privește prelucrarea datelor cu caracter personal este echivalent în toate statele membre. [...] Apropierea legislațiilor naționale în acest domeniu nu trebuie să ducă la scăderea protecției pe care o oferă, ci trebuie, dimpotrivă, să încerce să asigure un nivel înalt de protecție în cadrul UE. Așadar, [...] armonizarea acestor reglementări naționale nu se limitează la o minimă concordanță, ci înseamnă o armonizare completă."[13] În consecință, statele membre au limitat doar libertatea de acțiune în momentul implementării directivei

Directiva privind protecția datelor este concepută astfel încât să concretizeze principiile dreptului la viață privată incluse deja în Convenția 108 și să le extindă. Faptul că toate cele 15 state membre ale UE din 1995 erau și părți contractante ale Convenției 108 exclude adoptarea unor norme contradictorii în cadrul acestor două instrumente juridice. Cu toate acestea, Directiva privind protecția datelor se sprijină pe posibilitatea, prevăzută la articolul 11 din Convenția 108, de adăugare a unor instrumente de protecție. În special, introducerea supravegherii independente ca instrument de îmbunătățire a conformității cu normele privind protecția datelor sa dovedit a fi o contribuție importantă la funcționarea eficientă a legislației europene privind

11 Directiva privind protecția datelor, MO 1995 L 281, p. 31.

12 A se vedea, de exemplu, Directiva privind protecția datelor, considerentele 1, 4, 7 și 8.

13 Hotărârea CJUE din 24 noiembrie 2011 în cauzele comune 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*, alineatele 28–29.

protecția datelor (În consecință, această caracteristică a fost preluată în cadrul legislației CoE în 2001 prin Protocolul adițional la Convenția 108).

Aplicarea teritorială a Directivei privind protecția datelor se extinde dincolo de cele 28 de state membre ale UE, incluzând şi statele non-membre ale UE care fac parte din Spațiul Economic European (SEE)[14] – şi anume, Islanda, Liechtenstein şi Norvegia.

CJUE de la Luxemburg are jurisdicția de a stabili dacă un stat membru şi-a îndeplinit obligațiile în conformitate cu Directiva privind protecția datelor şi de a adopta decizii preliminare cu privire la valabilitatea şi interpretarea directivei, pentru a asigura aplicarea eficientă şi uniformă a acesteia în statele membre. O excepție importantă de la aplicabilitatea Directivei privind protecția datelor este aşa-numita excepție referitoare la activitățile domestice, şi anume prelucrarea datelor cu caracter personal de către o persoană fizică în cursul unei activități exclusiv personale sau domestice[15]. Acest tip de prelucrare este considerat, în general, ca făcând parte din libertățile persoanelor fizice.

Corespunzător legislației primare a UE în vigoare la data adoptării Directivei privind protecția datelor, domeniul de aplicare material al directivei se limitează la aspectele pieței interne. În afara domeniului său de aplicare se situează, cel mai important, aspectele legate de cooperarea polițienească şi judiciară în materie penală. Protecția datelor în aceste privințe rezultă din diferite instrumente juridice, care sunt descrise detaliat în capitolul 7.

Având în vedere că Directiva privind protecția datelor se adresa 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 şi organismele UE. Regulamentul (CE) nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile şi organele comunitare şi privind libera circulație a acestor date (*Regulamentul privind protecția datelor de către instituțiile europene*) îndeplineşte această atribuție[16].

În plus, chiar şi în domeniile vizate de Directiva privind protecția datelor, sunt deseori necesare dispoziții mai detaliate privind protecția datelor în scopul obținerii

14 Acordul privind Spațiul Economic European, MO 1994 L 1, care a intrat în vigoare la 1 ianuarie 1994.

15 Directiva privind protecția datelor, articolul 3 alineatul (2) a doua liniuță.

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

clarității necesare pentru echilibrarea altor interese legitime. Două astfel de exemple sunt Directiva 2002/58/CE privind prelucrarea datelor personale şi protejarea confidențialității în sectorul comunicațiilor publice (*Directiva asupra confidențialității și comunicațiilor electronice*)[17] şi Directiva 2006/24/CE privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice şi de modificare a Directivei 2002/58/CE (*Directiva privind păstrarea datelor*)[18] (declarată invalidă la 8 aprilie 2014). Alte exemple vor fi discutate în capitolul 8. Aceste dispoziții trebuie să fie în conformitate cu Directiva privind protecția datelor.

Carta Drepturilor Fundamentale a Uniunii Europene

Tratatele inițiale ale Comunităților Europene nu conțineau referiri la drepturile omului sau la protecția acestora. Întrucât înaintea Curții Europene de Justiție (CEJ) ajungeau la acea vreme cauze în care erau invocate încălcări ale drepturilor omului în domenii din sfera de aplicare a legislației europene, aceasta a elaborat o nouă abordare. Pentru a oferi protecție persoanelor fizice, a inclus drepturile fundamentale în aşanumitele principii generale de drept european. Conform CJUE, aceste principii generale reflectă conținutul protecției drepturilor omului în constituțiile naționale şi 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 şi 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). Această Cartă încorporează întreaga gamă de drepturi civile, politice, economice şi sociale ale cetățenilor europeni, sintetizând tradițiile constituționale şi obligațiile internaționale comune statelor membre. Drepturile descrise în Cartă se împart în şase secțiuni: demnitate, libertate, egalitate, solidaritate, drepturile cetățenilor şi justiție.

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

18 Directiva 2006/24/CE a Parlamentului European şi 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 şi de modificare a Directivei 2002/58/CE, *(Directiva privind păstrarea datelor),* MO 2006 L 105, declarată invalidă la 8 aprilie 2014.

Deşi inițial a fost doar un document politic, Carta a dobândit caracter juridic obligatoriu[19] ca legislație primară a UE [a se vedea articolul 6 alineatul (1) din TUE)] odată cu intrarea în vigoare a Tratatului de la Lisabona la 1 decembrie 2009[20].

Legislația primară a UE include, de asemenea, competența generală a UE de a legifera în materie de protecție a datelor (articolul 16 din TFUE).

Carta nu numai că asigură respectarea vieții private şi familiale (articolul 7), dar stabileşte şi dreptul la protecția datelor (articolul 8), ridicând în mod explicit nivelul acestei protecții la acela de drept fundamental în temeiul legislației europene. Instituțiile UE şi statele membre trebuie să respecte şi să garanteze acest drept, care este, de asemenea, valabil în cazul statelor membre atunci când pun în aplicare legislația 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 privind protecția datelor. Prin urmare, Carta nu numai că menționează explicit dreptul la protecția datelor la articolul 8 alineatul (1), dar face referire şi la principiile-cheie privind protecția datelor la articolul 8 alineatul (2). În cele din urmă, articolul 8 alineatul (3) din Cartă garantează că o autoritate independentă va controla respectarea acestor principii.

Perspective

În luna ianuarie 2012, Comisia Europeană a propus un pachet de reformă privind protecția datelor, declarând că normele actuale privind protecția datelor trebuie modernizate prin prisma evoluțiilor tehnologice rapide şi a globalizării. Pachetul de reformă constă într-o propunere de Regulament general privind protecția datelor[21], destinat să înlocuiască Directiva privind protecția datelor, precum şi într-o nouă Directivă privind protecția datelor[22], care să prevadă protecția datelor în domeniile cooperării polițieneşti şi judiciare în materie penală. La data publicării prezentului manual, discuția referitoare la pachetul de reformă era în plină desfăşurare.

19 UE (2012), Carta Drepturilor Fundamentale a Uniunii Europene, MO 2012 C 326.

20 A se vedea versiunea consolidată a Comunităților Europene (2012), Tratatul privind Uniunea Europeană, MO 2012 C 326; şi versiunea consolidată a Comunităților Europene (2012), TFUE, MO 2012 C 326.

21 Comisia Europeană (2012), *Propunere de regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor)*, COM(2012) 11 final, Bruxelles, 25 ianuarie 2012.

22 Comisia Europeană (2012), *Propunere de directivă 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 (Directiva generală privind protecția datelor)*, COM(2012) 10 final, Bruxelles, 25 ianuarie 2012.

1.2. Echilibrarea drepturilor

Puncte-cheie

- Dreptul la protecția datelor nu este un drept absolut; acesta trebuie echilibrat cu alte drepturi.

Dreptul fundamental la protecția datelor cu caracter personal în temeiul articolului 8 din Cartă „nu este totuşi o prerogativă absolută, ci trebuie să fie luat în considerare în raport cu funcția sa în societate”[23]. Articolul 52 alineatul (1) din Cartă admite, astfel, că pot fi impuse restrângeri ale exercițiului unor drepturi, precum cele consacrate la articolele 7 şi 8 din aceasta, în măsura în care aceste restrângeri sunt prevăzute de lege, respectă substanța acestor drepturi şi libertăți şi, prin respectarea principiului proporționalității, sunt necesare şi răspund efectiv obiectivelor de interes general recunoscute de Uniunea Europeană sau necesității protejării drepturilor şi libertăților altora[24].

În cadrul sistemului Convenției europene a drepturilor omului, protecția datelor este asigurată prin articolul 8 (dreptul la respectarea vieții private şi familiale) şi, la fel ca în cadrul sistemului Cartei, acest drept trebuie să fie aplicat cu respectarea domeniului de aplicare al altor drepturi concurente. În conformitate cu articolul 8 alineatul (2) din Convenția europeană a drepturilor omului, „nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acesta este prevăzut de lege şi constituie, într-o societate democratică, o măsură necesară [...] pentru protecția drepturilor şi a libertăților altora”.

În consecință, atât CEDO, cât şi CJUE au declarat în repetate rânduri că este necesar un exercițiu de echilibrare cu alte drepturi în momentul aplicării şi interpretării articolului 8 din Convenția europeană a drepturilor omului şi articolului 8 din Cartă[25]. Mai multe exemple sugestive vor ilustra modul în care se realizează acest echilibru.

23 A se vedea, de exemplu, Hotărârea CJUE din 9 noiembrie 2010 în cauzele conexate C-92/09 şi C-93/09, *Volker und Markus Schecke GbR şi Hartmut Eifert/Land Hessen*, punctul 48.

24 *Ibidem*, punctul 50.

25 Hotărârea CEDO din 7 februarie 2012 în cauza *Von Hannover/Germania (nr. 2) [T]*, nr. 40660/08 şi 60641/08; Hotărârea CJUE din 24 noiembrie 2011 în cauzele conexate C-468/10 şi C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) şi Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, punctul 48; Hotărârea CJUE din 29 ianuarie 2008 în cauza *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06, punctul 68. A se vedea, de asemenea, Consiliul Europei (2013), jurisprudența Curții Europene a Drepturilor Omului în ceea ce priveşte protecția datelor cu caracter personal, Jurisprudența DP (2013), disponibilă la: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP%202013%20Case%20Law_Eng%20%28final%2018%2007%202013%29.pdf.

1.2.1. Libertatea de exprimare

Unul dintre drepturile care poate intra în conflict cu dreptul la protecția datelor este dreptul la libertatea de exprimare.

Libertatea de exprimare este protejată prin articolul 11 din Cartă („Libertatea de exprimare şi de informare"). Acest drept cuprinde „libertatea de opinie şi libertatea de a primi sau de a transmite informații sau idei fără implicarea autorităților publice şi fără a ține seama de frontiere". Articolul 11 corespunde articolului 10 din Convenția europeană a drepturilor omului. În conformitate cu articolul 52 alineatul (3) din Cartă, în măsura în care prezenta cartă conține drepturi ce corespund unor drepturi garantate prin Convenția europeană a drepturilor omului, „înțelesul şi scopul lor sunt aceleaşi ca şi cele prevăzute de convenția menționată". Prin urmare, limitările care pot fi impuse legal asupra dreptului garantat prin articolul 11 din Cartă nu pot depăşi limitările prevăzute la articolul 10 alineatul (2) din Convenția europeană a drepturilor omului, adică, trebuie să fie prevăzute de lege şi să constituie, într-o societate democratică, o măsură necesară „pentru protecția [...] reputației sau a drepturilor altora". Acest concept se referă la dreptul la protecția datelor.

Relația dintre protecția datelor cu caracter personal şi libertatea de exprimare este reglementată de articolul 9 din Directiva privind protecția datelor, denumit „Prelucrarea datelor cu caracter personal şi libertatea de exprimare"[26]. Potrivit acestui articol, statele membre prevăd derogări şi limitări de la dispozițiile prezentului capitol, ale capitolului IV şi 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.

Exemplu: În cauza *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy* şi *Satamedia Oy*,[27] CJUE a fost solicitată să interpreteze articolul 9 din Directiva privind protecția datelor şi să definească raportul dintre protecția datelor şi libertatea presei. Curtea a trebuit să examineze diseminarea de către Markkinapörssi şi Satamedia a datelor fiscale aparținând unui număr de aproximativ 1,2 milioane de persoane fizice, obținute legal de la autoritățile fiscale finlandeze. În special, Curtea a trebuit să verifice dacă prelucrarea datelor cu caracter personal, puse

26 Directiva privind protecția datelor, articolul 9.

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

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 Satakunnan reprezentau „prelucrare de date cu caracter personal" în sensul articolului 3 alineatul (1) din Directiva privind protecția datelor, Curtea a procedat la interpretarea articolului 9 din directivă. Curtea a remarcat, în primul rând, importanța dreptului la libertatea de exprimare în fiecare societate democratică şi a considerat că noțiunile legate de această libertate, cum ar fi jurnalismul, trebuie interpretate în sens larg. Apoi a observat că, pentru a obține un echilibru între cele două drepturi fundamentale, derogările şi limitările dreptului la protecția datelor trebuie aplicate numai în măsura în care sunt strict necesare. În aceste situații, Curtea a considerat că activități precum cele întreprinse de Markkinapörssi şi Satamedia privind datele incluse în documente care aparțin domeniului public în baza legislației naționale, pot fi clasificate drept „activități jurnalistice" în cazul în care obiectivul acestora este acela de a comunica informații, opinii sau idei publicului, indiferent de suportul utilizat pentru transmiterea acestora. Curtea a hotărât, de asemenea, că aceste activități nu se limitează la activitățile media şi pot fi întreprinse în scopuri lucrative. Cu toate acestea, CJUE a lăsat la aprecierea instanței naționale să stabilească dacă acest lucru este valabil în această situație specială.

În ceea ce priveşte punerea dreptului la protecția datelor în acord cu dreptul la libertatea de exprimare, CEDO a emis o serie de hotărâri de referință.

Exemplu: În cauza *Axel Springer AG/Germania*[28], CEDO a considerat că interdicția impusă de o instanță internă proprietarului unui ziar care dorea să publice un articol cu privire la arestarea şi condamnarea unui actor cunoscut încălca dispozițiile articolului 10 din Convenția europeană a drepturilor omului. CEDO a reiterat criteriile pe care le stabilise în jurisprudența sa atunci când a echilibrat dreptul la libertatea de exprimare cu dreptul la respectarea vieții private:

- în primul rând, dacă evenimentul pe care articolul publicat l-a vizat era de interes general: arestarea şi condamnarea unei persoane constituie un fapt judiciar şi, prin urmare, este de interes public;

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

- în al doilea rând, dacă persoana în cauză era o persoană publică: persoana în cauză era un actor suficient de cunoscut pentru a se califica drept persoană publică şi

- în al treilea rând, modul în care informațiile au fost obținute şi credibilitatea acestora: informațiile au fost oferite de Parchet, iar exactitatea informațiilor din ambele publicații nu a fost contestată între părți.

Prin urmare, CEDO a hotărât că restricțiile de publicare impuse societății nu au fost proporționale în mod rezonabil cu obiectivul legitim de protejare a vieții private a reclamantului. Curtea a concluzionat că articolul 10 din Convenția europeană a drepturilor omului a fost încălcat.

Exemplu: În cauza *Von Hannover/Germania (nr. 2)*[29], CEDO nu a constatat nicio încălcare a dreptului de respectare a vieții private în temeiul articolului 8 din Convenția europeană a drepturilor omului, atunci când Prințesei Caroline de Monaco i-a fost respinsă interdicția împotriva publicării unei fotografii a sa şi a soțului său în timp ce se aflau în vacanță la schi. Fotografia era însoțită de un articol care prezenta, printre altele, şi informații despre starea de sănătate precară a Prințului Rainier. CEDO a concluzionat că instanțele interne au echilibrat atent dreptul la libertatea de exprimare al editurilor cu dreptul reclamanților la respectarea vieții private. Caracterizarea stării de sănătate a prințului Rainier de către instanțele interne drept un eveniment al societății contemporane nu putea fi considerată irațională, iar CEDO a admis că fotografia, analizată prin prisma articolului, contribuie, cel puțin într-o anumită măsură, la o dezbatere de interes general. Curtea s-a pronunțat că nu a existat nicio încălcare a articolului 8 din Convenția europeană a drepturilor omului.

În jurisprudența CEDO, unul dintre criteriile esențiale referitoare la echilibrarea acestor 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*,[30] un săptămânal național a publicat fotografii intime ale reclamantului. Acesta a invocat ulterior încălcarea articolului 8 din Convenția europeană a drepturilor omului, întrucât nu a putut solicita

29 Hotărârea CEDO din 7 februarie 2012 în cauza *Von Hannover/Germania (nr. 2) [T]*, nr. 40660/08 şi 60641/08, punctele 118 şi 124.

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

interzicerea publicării fotografiilor în cauză pe motivul absenței unei cerințe de notificare prealabilă pentru ziar în cazul publicării unui material care poate aduce atingere dreptului unei persoane la viață privată. Deşi difuzarea acestui material a avut, în general, scop de divertisment, şi 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 şi 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. În ceea ce priveşte efectul de intimidare pe care lar putea genera cerința de notificare prealabilă, incertitudinile legate de eficiența acestuia şi marja largă de apreciere în acel domeniu, CEDO a concluzionat că nu este obligatorie existența unei condiții legale de notificare prealabilă, în conformitate cu articolul 8. În consecință, Curtea s-a pronunțat că nu a existat nicio încălcare a articolului 8.

Exemplu: În cauza *Biriuk/Lituania*[31], reclamanta a pretins daune unui cotidian pe motiv că publicase un articol în care relata că aceasta era seropozitivă. Pretinsa informație fusese confirmată de cadrele medicale de la spitalul local. CEDO nu a considerat că articolul în cauză contribuie la o dezbatere de interes general şi a reiterat că protecția datelor cu caracter personal, în special a datelor medicale, are o importanță fundamentală pentru ca o persoană să se poată bucura de dreptul la respectarea vieții private şi familiale, astfel cum se garantează prin articolul 8 din Convenția europeană a drepturilor omului. 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. În consecință, statul nu a asigurat dreptul reclamantei la respectarea vieții sale private. Curtea s-a pronunțat asupra încălcării articolului 8.

1.2.2. Accesul la documente

În conformitate cu articolul 11 din Cartă şi articolul 10 din Convenția europeană a drepturilor omului, libertatea de informare protejează nu numai dreptul de a transmite, ci şi dreptul de a *primi* informații. Se constată din ce în ce mai mult importanța unei guvernări transparente în vederea funcționării unei societăți democratice. În consecință, în ultimele două decenii, dreptul de acces la documentele deținute de

31 Hotărârea CEDO din 25 februarie 2009 în cauza *Biriuk/Lituania*, nr. 23373/03, 25 noiembrie 2008.

autoritățile publice a fost recunoscut ca drept important al fiecărui cetățean european şi 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*)[32]. **În temeiul dreptului european**, dreptul de acces la documente este garantat prin Regulamentul nr. 1049/2001 privind accesul public la documentele Parlamentului European, ale Consiliului şi ale Comisiei (*Regulamentul privind accesul la documente*)[33]. Articolul 42 din Cartă şi articolul 15 alineatul (3) din TFUE au extins acest drept de acces „la documentele instituțiilor, organelor, oficiilor şi agențiilor Uniunii, indiferent de suportul pe care se află aceste documente". În conformitate cu articolul 52 alineatul (2) din Cartă, dreptul de acces la documente se exercită, de asemenea, în condițiile şi cu respectarea limitelor stabilite de articolul 15 alineatul (3) din TFUE. 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. 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 cauza *Comisia/Bavarian Lager*[34], CJUE a definit domeniul de aplicare al protecției datelor cu caracter personal în contextul accesului la documentele instituțiilor UE şi raportul între Regulamentul nr. 1049/2001 (*Regulamentul privind accesul la documente*) şi Regulamentul nr. 45/2001 (*Regulamentul privind protecția datelor*). Bavarian Lager, înființată în anul 1992, importă bere germană îmbuteliată în Regatul Unit, în principal pentru pub-uri şi 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 decis să formuleze o acțiune împotriva Regatului Unit pentru neîndeplinirea obligațiilor, care a condus la modificarea dispozițiilor contestate şi la alinierea acestora la dreptul european. Ulterior, Bavarian Lager a solicitat

32 Consiliul Europei, Comitetul de Miniştri (2002), Recomandarea Rec(2002)2 din 21 februarie 2002 către statele membre privind accesul la documentele oficiale; Consiliul Europei, Convenția din 18 iunie 2009 privind accesul la documentele oficiale, CETS nr. 205. Convenția nu a intrat încă în vigoare.

33 Regulamentul (CE) nr. 1049/2001 al Parlamentului European şi al Consiliului din 30 mai 2001 cu privire la accesul public la documentele Parlamentului European, ale Consiliului şi ale Comisiei, MO 2001 L 145.

34 Hotărârea CJUE din 29 iunie 2010 în cauza *Comisia Europeană/The Bavarian Lager Co. Ltd.*, C-28/08 P, punctele 60, 63, 76, 78 şi 79.

Comisiei, printre alte documente, o copie a procesului-verbal al reuniunii la care au participat reprezentanți ai Comisiei, ai autorităților britanice şi ai *Confédération des Brasseurs du Marché Commun* (CBMC). Comisia a fost de acord să divulge anumite documente cu privire la reuniune, însă a şters cinci nume care apăreau în procesul-verbal, două persoane obiectând în mod expres 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. Întrucât nu a fost mulțumită de această poziție, Bavarian Lager a introdus o acțiune înaintea Tribunalului de Primă Instanță, care a anulat decizia Comisiei prin hotărârea din 8 noiembrie 2007 (cauza T-194/04, *Bavarian Lager/Comisia*), 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 şi nu periclitează în niciun fel viețile private ale acelor persoane.

La apelul Comisiei, CJUE a anulat hotărârea Tribunalului de Primă Instanță. CJUE a considerat că Regulamentul privind accesul la documente instituie „un regim specific şi 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 urmăreşte să obțină acces la documente, inclusiv date cu caracter personal, dispozițiile Regulamentului privind protecția datelor devin aplicabile în ansamblul lor. Potrivit concluziilor ulterioare ale CJUE, Comisia a fost îndreptățită să respingă solicitarea de acces la procesulverbal integral al reuniunii din luna octombrie 1996. În absența consimțământului celor cinci participanți la reuniune, Comisia şi-a respectat suficient îndatorirea de deschidere prin eliberarea unei versiuni a documentului în cauză în care numele acestora erau şterse.

În plus, potrivit CJUE, „întrucât Bavarian Lager nu a oferit nicio motivare expresă şi legitimă şi 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 vreun motiv să se presupună că acest transfer ar putea aduce atingere intereselor legitime ale persoanelor vizate", astfel precum prevede Regulamentul privind protecția datelor.

Potrivit acestei hotărâri, atingerea adusă dreptului la protecția datelor în ceea ce privește accesul la documente necesită o motivare precisă şi întemeiată. Dreptul de acces la documente nu poate anula automat dreptul la protecția datelor[35].

Un aspect specific al unei solicitări de acces a fost tratat în următoarea hotărâre a CEDO.

Exemplu: În cauza *Társaság a Szabadságjogokért/Ungaria*[36], reclamanta, un ONG pentru apărarea drepturilor omului, a solicitat Curții Constituționale accesul la informații privind o cauză aflată pe rol. Fără a se consulta cu membrul Parlamentului care îi adresase cauza, Curtea Constituțională a respins solicitarea de acces în temeiul faptului că plângerile care îi sunt adresate pot fi puse la dispoziția străinilor numai cu aprobarea reclamantului. Instanțele interne au aprobat această respingere pe motiv că protecția acestor date cu caracter personal nu poate fi anulată de alte interese legale, inclusiv accesul la informații publice. Reclamanta a acționat în calitate de „entitate de supraveghere socială", activitățile sale garantând o protecție similară celei oferite presei. În legătură cu libertatea presei, CEDO a considerat în mod consecvent că publicul are dreptul să primească informații de interes general. Informațiile solicitate de reclamantă erau „complete şi disponibile" şi nu necesitau niciun fel de colectare de date. În aceste circumstanțe, statul avea obligația să nu împiedice fluxul de informații solicitat de reclamantă. Pe scurt, CEDO a considerat că barierele destinate să împiedice accesul la informații de interes public pot descuraja acele persoane care lucrează în mass-media sau în domenii asociate în rolul lor vital de „entitate publică de supraveghere". Curtea s-a pronunțat asupra încălcării articolului 10.

În temeiul dreptului european, importanța transparenței este stabilită în mod ferm. Principiul transparenței este consacrat în articolele 1 şi 10 din TUE şi în articolul 15 alineatul (1) din TFUE[37]. Potrivit considerentului 2 din Regulamentul (CE) nr. 1049/2001, aceasta permite cetățenilor să participe îndeaproape la

35 A se vedea totuşi dezbaterile detaliate ale Autorității Europene pentru Protecția Datelor (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, 24 martie 2011, disponibile la: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 Hotărârea CEDO din 14 aprilie 2009 în cauza *Társaság a Szabadságjogokért/Ungaria*, nr. 37374/05; a se vedea punctele 27, 36-38.

37 UE (2012), Versiunile consolidate ale Tratatului privind Uniunea Europeană şi ale TFUE, MO 2012 C 326.

procesul decizional şi garantează faptul că administrația beneficiază de o legitimitate mai mare, este mai eficientă şi răspunzătoare față de cetățeni, într-un sistem democratic[38].

Ca urmare a acestei argumentări, Regulamentul (CE) nr. 1290/2005 al Consiliului privind finanțarea politicii agricole comune şi Regulamentul (CE) nr. 259/2008 al Comisiei de stabilire a normelor de aplicare a Regulamentului (CE) nr. 1290/2005 al Consiliului impun publicarea informațiilor despre beneficiarii anumitor fonduri ale UE din sectorul agricol şi a sumelor primite de fiecare beneficiar[39]. Publicarea ar trebui să contribuie la controlul public al utilizării adecvate a fondurilor publice de către administrație. Proporționalitatea acestei publicări a fost contestată de mai mulți beneficiari.

Exemplu: În cauza *Volker und Markus Schecke şi Hartmut Eifert/Land Hessen*[40], CJUE a trebuit să se pronunțe asupra proporționalității publicării, impusă de legislația UE, a numelor beneficiarilor subvențiilor agricole ale UE şi a sumelor pe care aceştia le-au primit.

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

Curtea a considerat că o astfel de atingere adusă articolelor 7 şi 8 din Cartă este prevăzută de lege şi răspunde unui obiectiv de interes general recunoscut de UE, şi anume, includerea consolidării transparenței în ceea ce priveşte utilizarea fondurilor comunitare. Cu toate acestea, CJUE a considerat că publicarea numelor persoanelor fizice care sunt beneficiare ale unui ajutor al UE pentru agricultură în cadrul acestor două fonduri şi a sumelor exacte primite constituie o măsură

38 Hotărârea CJUE din 6 martie 2003 în cauza *Interporc Im- und Export GmbH/Comisia Comunităților Europene*, C-41/00 P, punctul 39; şi Hotărârea CJUE din 29 iunie 2010 în cauza *Comisia Europeană/The Bavarian Lager Co. Ltd.*, C-28/08 P, punctul 54.

39 Regulamentul (CE) nr. 1290/2005 al Consiliului din 21 iunie 2005 privind finanțarea politicii agricole comune, MO 2005 L 209; şi 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 priveşte publicarea informațiilor referitoare la beneficiarii fondurilor provenite din Fondul European de Garantare Agricolă (FEGA) şi din Fondul European Agricol pentru Dezvoltare Rurală (FEADR), MO 2008 L 76.

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

disproporționată şi nejustificată în conformitate cu articolul 52 alineatul (1) din Cartă. Astfel, Curtea a declarat parțial nulă legislația UE privind publicarea informațiilor referitoare la beneficiarii fondurilor europene pentru agricultură.

1.2.3. Libertatea artelor şi științelor

Un alt drept care să echilibreze dreptul la respectarea vieții private şi protecția datelor este libertatea artelor şi științelor, protejată în mod explicit în temeiul articolului 13 din Cartă. Acest drept decurge în principal din libertatea de gândire şi de exprimare şi se exercită cu respectarea articolului 1 din Cartă (Demnitatea umană). CEDO consideră că libertatea artelor este protejată prin articolul 10 din Convenția europeană a drepturilor omului[41]. Dreptul garantat prin articolul 13 din Cartă poate fi, de asemenea, supus restrângerilor permise de articolul 10 din Convenția europeană a drepturilor omului[42].

Exemplu: În cauza *Vereinigung bildender Künstler/Austria*[43], instanțele austriece au interzis asociației reclamante să continue expunerea unei picturi care conținea fotografii ale capetelor mai multor personalități în poziții obscene. Un parlamentar austriac, a cărui fotografie fusese folosită în tablou, a formulat o acțiune împotriva asociației reclamante, solicitând o decizie care să îi interzică acesteia să expună tabloul. Instanța națională a emis o decizie de interdicție, acceptând cererea acestuia. CEDO a reiterat că articolul 10 din Convenția europeană a drepturilor omului este aplicabil în cazul transmiterii unor idei care insultă, şochează sau perturbă statul sau orice parte a populației. Acele persoane care au creat, realizat, distribuit sau expus lucrări de artă au contribuit la schimbul de idei şi 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 şi folosea fotografii înfățişând numai capetele persoanelor, corpurile fiind pictate într-o manieră nerealistă şi exagerată, care, în mod evident, nu avea ca scop reflectarea sau chiar sugerarea realității, CEDO a susținut 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" şi că „în această calitate [persoana descrisă] trebuie să afişeze o mai mare toleranță în ceea ce priveşte dezaprobarea". Cântărind diferitele interese în cauză, CEDO a constatat că interzicerea pe termen

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

42 Explicații cu privire la Carta Drepturilor Fundamentale, MO 2007 C 303.

43 Hotărârea CEDO din 25 ianuarie 2007 în cauza *Vereinigung bildender Künstler/Austria*, nr. 68345/01; a se vedea în mod special punctele 26 şi 34.

nelimitat a expunerii tabloului este disproporționată. Curtea s-a pronunțat asupra încălcării articolului 10 din Convenția europeană a drepturilor omului.

În ceea ce privește știința, legislația europeană privind protecția datelor cunoaște valoarea specială a științei pentru societate. Prin urmare, restricțiile generale pentru utilizarea datelor cu caracter personal sunt diminuate. Atât Directiva privind protecția datelor, cât și Convenția 108 permit păstrarea datelor pentru cercetare științifică după ce acestea nu mai servesc scopului inițial pentru care au fost colectate. Mai mult, utilizarea ulterioară a datelor cu caracter personal pentru cercetare științifică nu este considerată ca fiind un scop incompatibil. Legislației naționale îi revine atribuția de a elabora dispoziții mai detaliate, inclusiv garanțiile necesare, pentru a pune în acord interesul pentru cercetare științifică și dreptul la protecția datelor (a se vedea și secțiunile 3.3.3 și 8.4).

1.2.4. Protecția proprietății

Dreptul la protecția proprietății este consacrat în articolul 1 din Primul protocol la Convenția europeană a drepturilor omului și în articolul 17 alineatul (1) din Cartă. Un aspect important legat de dreptul la proprietate este protecția proprietății intelectuale, menționată în mod explicit la articolul 17 alineatul (2) din Cartă. Ordinea juridică a UE cuprinde mai multe directive, care vizează protejarea eficientă a proprietății intelectuale, în special dreptul 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[44]. Au existat cazuri în care unele instituții responsabile de 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 titluri de melodii, chiar dacă acestea sunt protejate prin drepturi de autor.

Exemplu: Cauza *Promusicae/Telefónica de España*[45] se referă la refuzul unui furnizor spaniol de acces la internet, Telefónica, de a face cunoscute către Promusicae, o organizație non-profit de producători muzicali și editori de înregistrări

44 Hotărârea CEDO din 10 ianuarie 2013 în cauza *Ashby Donald și alții/Franța*, nr. 36769/08.

45 Hotărârea CJUE din 29 ianuarie 2008 în cauza *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C275/06, punctele 54 și 60.

muzicale şi 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 fişiere care oferea acces la fonograme ale căror drepturi de exploatare erau deținute de membrii Promusicae.

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

CJUE a subliniat faptul că această cauză a ridicat, astfel, întrebarea cu privire la necesitatea de a pune în acord dispozițiile protecției diferitor drepturi fundamentale, şi anume dreptul la respectarea vieții private, şi drepturile la protecția proprietății şi accesul la o cale de atac eficientă.

Curtea a concluzionat că „atunci când transpun directivele susmenționate, statele membre trebuie să se bazeze pe o interpretare a acestor directive care să permită o echilibrare justă între diferitele drepturi fundamentale protejate de ordinea juridică a Comunității. În plus, atunci când implementează măsurile care transpun aceste directive, autoritățile şi instanțele statelor membre trebuie nu numai să interpreteze dreptul național într-o manieră consecventă cu acele directive, dar să se şi asigure că nu se bazează pe o interpretare a acestora care să contravină acelor drepturi fundamentale sau principii generale de drept comunitar, cum ar fi principiul proporționalității[46].”

46 *Ibidem*, punctele 65 şi 68; a se vedea şi Hotărârea CJUE din 16 februarie 2012, *SABAM/Netlog N.V.*, C-360/10.

2

Terminologia în domeniul protecției datelor

UE	Aspecte vizate	CoE
Date cu caracter personal		
Directiva privind protecția datelor, articolul 2 litera (a). CJUE, Cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert /Land Hessen*, 9 noiembrie 2010 CJUE, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06, 29 ianuarie 2008	**Definiție juridică**	Convenția 108, articolul 2 litera (a) CEDO, *Bernh Larsen Holding AS și alții/Norvegia*, nr. 24117/08, 14 martie 2013
Directiva privind protecția datelor, articolul 8 alineatul (1) CJUE, *Bodil Lindqvist*, C-101/01, 6 noiembrie 2003	**Categorii speciale de date cu caracter personal (date sensibile)**	Convenția 108, articolul 6
Directiva privind protecția datelor, articolul 6 alineatul (1) litera (e)	**Date anonimizate și pseudonimizate**	Convenția 108, articolul 5 litera (e) Convenția 108, Raport explicativ, articolul 42
Prelucrarea datelor		
Directiva privind protecția datelor, articolul 2 litera (b) CJUE, *Bodil Lindqvist*, C-101/01, 6 noiembrie 2003	**Definiții**	Convenția 108, articolul 2 litera (c)
Utilizatori de date		
Directiva privind protecția datelor, articolul 2 litera (d)	**Operator**	Convenția 108, articolul 2 litera (d) Recomandare privind crearea de profile, articolul (1) litera (g) *

UE	Aspecte vizate	CoE
Directiva privind protecția datelor, articolul 2 litera (e) CJUE, *Bodil Lindqvist*, C-101/01, 6 noiembrie 2003	**Persoană împuternicită de către operator**	Recomandare privind crearea de profile, articolul (1) litera (h)
Directiva privind protecția datelor, articolul 2 litera (g)	**Destinatar**	Convenția 108, Protocol adițional, articolul 2 alineatul (1)
Directiva privind protecția datelor, articolul 2 litera (f)	**Terț**	
Consimțământ		
Directiva privind protecția datelor, articolul 2 litera (h) CJUE, *Deutsche Telekom AG/Bundesrepublik Deutschland*, C-543/09, 5 mai 2011	**Definiție și cerințe privind consimțământul valabil**	Recomandare privind datele medicale, articolul 6 și diferite recomandări ulterioare

*Notă: *Consiliul Europei, Comitetul de Miniștri (2010), Recomandarea Rec(2010)13 din 23 noiembrie 2010 către statele membre privind protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal în contextul creării de profile (Recomandarea privind crearea de profile).*

2.1. Datele cu caracter personal

Puncte-cheie

- Datele reprezintă date cu caracter personal dacă se referă la o persoană identificată sau, cel puțin, care poate fi identificată, persoana vizată.
- O persoană poate fi identificată în cazul în care se pot obține informații suplimentare fără eforturi excesive, care permit identificarea persoanei vizate.
- 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 și în Directiva privind protecția datelor, care necesită protecție sporită și, prin urmare, sunt supuse unui regim juridic special.
- Datele sunt an onimizate în cazul în care nu mai conțin niciun element de identificare; acestea sunt pseudonimizate în cazul în care elementele de identificare sunt codificate.
- Spre deosebire de datele anonimizate, datele pseudonimizate sunt date cu caracter personal.

2.1.1. Aspecte principale ale conceptului de date cu caracter personal

În temeiul dreptului european, precum și **în temeiul legislației CoE**, „datele cu caracter personal" sunt definite ca fiind informațiile referitoare la o persoană fizică identificată sau identificabilă[47], și anume, informații despre o persoană a cărei identitate este fie clară în mod evident, fie poate fi, cel puțin, stabilită prin obținerea unor informații suplimentare.

În cazul în care datele despre o astfel de persoană sunt prelucrate, această persoană este denumită „persoană vizată".

Persoana

Dreptul la protecția datelor decurge din dreptul la respectarea vieții private. Conceptul de viață privată este asociat ființelor umane. Prin urmare, persoanele fizice sunt beneficiarii principali ai protecției datelor. În plus, potrivit avizului Grupului de lucru Articolul 29, numai *ființele umane* sunt protejate de legislația europeană privind protecția datelor[48].

Jurisprudența CEDO cu privire la articolul 8 din Convenția europeană a drepturilor omului arată că separarea completă a aspectelor legate de viața privată și cea profesională poate fi dificilă[49].

Exemplu: În cauza *Amann/Elveția*[50], autoritățile au interceptat o conversație telefonică de afaceri a reclamantului. Pe baza acestei conversații, autoritățile au întreprins cercetarea reclamantului și au completat o fișă pe numele reclamantului pentru dosarul de securitate națională. Deși interceptarea privea o conversație telefonică de afaceri, CEDO a considerat că stocarea datelor cu privire la această conversație ține de viața privată a reclamantului. A scos în evidență faptul că noțiunea de „viață privată" nu trebuie interpretată în mod restrictiv, în special, întrucât respectarea vieții private cuprinde dreptul de a stabili și

47 Directiva privind protecția datelor, articolul 2 litera (a); Convenția 108, articolul 2 litera (a).

48 Grupul de lucru Articolul 29 (2007), *Avizul 4/2007 privind conceptul de date cu caracter personal*, WP 136, 20 iunie 2007, p. 22.

49 A se vedea, de exemplu, Hotărârea CEDO din 4 mai 2000 în cauza *Rotaru/România* [T], nr. 28341/95, punctul 43; Hotărârea CEDO din 16 decembrie 1992 în cauza *Niemietz/Germania*, 13710/88, punctul 29.

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

dezvolta relații cu alte ființe umane. În plus, nu a existat niciun motiv principial care să justifice excluderea activităților de natură profesională sau de afaceri din noțiunea de „viață privată". Această interpretare generală corespunde cu cea a Convenției 108. CEDO a constatat în continuare că ingerința în cazul reclamantului nu este în conformitate cu legea, deoarece dreptul intern nu conține dispoziții specifice şi detaliate privind colectarea, înregistrarea şi stocarea informațiilor. Astfel, a concluzionat că articolul 8 din Convenția europeană a drepturilor omului a fost încălcat.

Mai mult, în cazul în care şi aspectele legate de viața profesională pot face obiectul protecției datelor, pare discutabil că numai persoanele fizice ar trebui să beneficieze de protecție. Drepturile prevăzute în Convenția europeană a drepturilor omului sunt garantate tuturor, nu doar persoanelor fizice.

Există o jurisprudență a CEDO care se pronunță asupra cererilor entităților juridice care invocă încălcarea dreptului la protecție împotriva utilizării datelor lor, în conformitate cu articolul 8 din Convenția europeană a drepturilor omului. Cu toate acestea, Curtea a examinat cauza în baza dreptului la respectarea domiciliului şi a corespondenței, şi nu în baza vieții private:

Exemplu: Cauza *Bernh Larsen Holding AS și alții/Norvegia*[51] 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" şi a „corespondenței" în sensul articolului 8 din Convenția europeană a drepturilor omului. Cu toate acestea, Curtea a constatat că autoritățile fiscale posedă garanții eficiente şi adecvate împotriva abuzurilor: societățile reclamante au fost notificate cu suficient timp în avans; au fost prezente şi 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" şi a „corespondenței" şi interesul acestora de protejare a vieții private a persoanelor care lucrează pentru ele, pe de o parte, şi interesul public de asigurare a unei inspecții eficiente în scopuri

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

de evaluare fiscală, pe de altă parte. Curtea a concluzionat că articolul 8 a fost încălcat.

Conform Convenției 108, protecția datelor vizează, în principal, protecția persoanelor fizice; cu toate acestea, părțile contractante pot extinde protecția datelor la persoanele juridice, cum ar fi societățile şi asociațiile comerciale care se supun dreptului lor intern. **Legislația europeană privind protecția datelor** nu reglementează, în general, protecția persoanelor juridice cu privire la prelucrarea datelor care le vizează. Autoritățile naționale de reglementare au libertatea de a reglementa acest subiect[52].

Exemplu: În cauza *Volker und Markus Schecke și Hartmut Eifert/Land Hessen*[53], 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 şi 8 din Cartă față de o astfel de identificare decât în măsura în care denumirea persoanei juridice identifică una sau mai multe persoane fizice. [...] Respectarea dreptului la viață privată în raport cu prelucrarea datelor cu caracter personal, recunoscută prin articolele 7 şi 8 din Cartă, se raportează la orice informație privind o persoană fizică identificată sau identificabilă [...]”[54].

Caracterul identificabil al unei persoane

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

- o persoană fizică este identificată prin aceste informații sau
- în cazul în care o persoană fizică, deşi neidentificată, este descrisă în aceste informații într-un mod care face posibilă identificarea persoanei vizate prin efectuarea de cercetări ulterioare.

Ambele tipuri de informații sunt protejate în acelaşi mod, în conformitate cu legislația europeană privind protecția datelor. CEDO a declarat în mod repetat că noțiunea de „date cu caracter personal” în conformitate cu Convenția europeană a drepturilor

52 Directiva privind protecția datelor, considerentul 24.

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

54 *Ibidem,* punctul 52.

omului este aceeaşi cu cea din Convenția 108, în special în ceea ce priveşte condiția de referire la persoane identificate sau identificabile[55].

Definițiile juridice ale datelor cu caracter personal nu clarifică momentul în care o persoană este considerată identificată[56]. Identificarea în mod evident presupune elemente care descriu o persoană într-un mod în care aceasta se poate distinge de toate celelalte persoane şi poate fi recunoscută ca persoană fizică. Numele unei persoane este un prim exemplu de element de descriere. În cazuri excepționale, alte elemente de identificare pot avea un efect similar ca cel al numelui. De exemplu, în cazul persoanelor publice, este suficient să se facă referire la funcția persoanei, de exemplu, Preşedintele Comisiei Europene.

Exemplu: În cauza *Promusicae*[57], CJUE a declarat că „nu se contestă faptul că respectiva comunicare a numelui şi a adreselor anumitor utilizatori ai [unei anumite platforme de partajare de fişiere 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 litera (a) din Directiva 95/46 [...]. Această comunicare de informații care, în opinia Promusicae, sunt stocate de Telefónica – fapt necontestat de aceasta din urmă – constituie o prelucrare de date cu caracter personal, în sensul articolului 2 primul paragraf din Directiva 2002/58, coroborat cu articolul 2 litera (b) din Directiva 95/46".

Deoarece multe dintre nume nu sunt unice, stabilirea identității unei persoane poate necesita elemente de identificare suplimentare pentru a garanta că o persoană nu este confundată cu altcineva. Data şi locul naşterii sunt deseori utilizate. În plus, în unele țări au fost introduse numere personalizate pentru o mai bună diferențiere a cetățenilor. Datele biometrice, cum ar fi amprentele, fotografiile digitale sau scanarea irisului, devin din ce în ce mai importante pentru identificarea persoanelor în era tehnologică.

55 A se vedea Hotărârea CEDO din 16 februarie 2000 în cauza *Amann/Elveția* [T], nr. 27798/95, punctul 65 *et al.*

56 A se vedea şi Hotărârea CEDO din 13 februarie 2003 în cauza *Odièvre/Franța* [T], nr. 42326/98; şi Hotărârea CEDO din 25 septembrie 2012 în cauza *Godelli/Italia*, nr. 33783/09.

57 Hotărârea CJUE din 29 ianuarie 2008 în cauza *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C275/06, punctul 45.

Cu toate acestea, în sensul aplicabilității legislației europene privind protecția datelor, nu este necesară o identificare de înaltă calitate a persoanelor vizate; este suficient ca persoana în cauză să fie identificabilă. O persoană este considerată identificabilă în cazul în care o parte dintre informații conțin elemente de identificare prin intermediul cărora persoana poate fi identificată direct sau indirect[58]. Potrivit considerentului 26 din Directiva privind protecția datelor, criteriul de referință constă în posibilitatea ca utilizatorii previzibili ai informațiilor să dispună de și să administreze mijloace rezonabile de identificare; aceasta include și destinatarii terți (a se vedea 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 nicio bază juridică, 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 date despre persoane anonime. Autoritatea locală nu are autoritatea juridică de a accesa registrul general al vehiculelor pentru a descoperi identitatea proprietarului sau a conducătorului mașinii.

Această argumentare nu este în conformitate cu considerentul 26 din Directiva privind protecția datelor. 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.

În temeiul legislației CoE, identificabilitatea este înțeleasă în mod similar. Articolul 1 alineatul (2) din Recomandarea privind datele de plată[59], de exemplu, stipulează că o

58 Directiva privind protecția datelor, articolul 2 litera (a).

59 CoE, Comitetul de Miniștri (1990), Recomandarea nr. R Rec(90) 19 privind protecția datelor cu caracter personal utilizate pentru plăți și alte operațiuni conexe, 13 septembrie 1990.

persoană nu va fi considerată „identificabilă" în cazul în care identificarea presupune o perioadă de timp, costuri sau forță de muncă excesive.

Autentificarea

Aceasta este o procedură prin care o persoană poate dovedi că are o anumită identitate şi/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 paşaport, cu datele cu care persoana se identifică, de exemplu, la controlul imigrației; 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 o cartelă cu cip sau cheia unui seif bancar. Pe lângă parole sau cartele cu cip, uneori, semnăturile electronice, utilizate împreună cu PIN-ul, sunt un instrument prin care o persoană se poate identifica şi autentifica în cadrul comunicațiilor electronice.

Natura datelor

Orice tip de informații pot fi date cu caracter personal cu condiția ca acestea să facă referire la o persoană.

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

Datele cu caracter personal includ informațiile care aparțin vieții private a unei persoane, precum şi informațiile referitoare la viața profesională sau publică a acesteia.

În cauza *Amann*[60], CEDO a interpretat că noțiunea de „date cu caracter personal" nu se limitează la aspecte ale sferei private a unei persoane (a se vedea secțiunea 2.1.1). Acest înțeles al termenului de „date cu caracter personal"este relevant şi pentru Directiva privind protecția datelor:

60 A se vedea 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*[61], CJUE a susținut că „în 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 convenție, că termenii «viață privată» nu trebuie interpretați în mod restrictiv şi că «niciun motiv de principiu nu permite excluderea activităților profesionale [...] din noțiunea «viață privată»".

Datele pot fi asociate persoanelor şi în cazul în care conținutul informațiilor dezvăluie în mod indirect date despre o persoană. În unele cazuri, acolo unde există o legătură strânsă între un obiect sau un eveniment – de exemplu, un telefon mobil, o mașină, un accident – pe de o parte, şi o persoană – de exemplu, proprietarul, utilizatorul sau victima – pe de altă parte, informațiile despre acel obiect sau eveniment ar trebui, de asemenea, luate în considerare ca fiind date cu caracter personal.

Exemplu: În cauza *Uzun/Germania*[62], reclamantul împreună cu un alt bărbat au fost puşi sub supraveghere prin intermediul unui dispozitiv GPS instalat în mașina celuilalt bărbat pe motivul suspiciunii de implicare în atacuri cu bombă. În speță, CEDO a considerat că supravegherea reclamantului prin intermediul GPS a echivalat cu ingerința în viața sa privată, protejată prin articolul 8 din Convenția europeană a drepturilor omului. Cu toate acestea, supravegherea prin GPS s-a desfăşurat în conformitate cu legea, precum şi proporțional cu scopul legitim de a ancheta mai multe acuzații de tentativă de omor şi, prin urmare, s-a dovedit necesară într-o societate democratică. Curtea a concluzionat că articolul 8 din Convenția europeană a drepturilor omului nu a fost încălcat.

Forma de apariție a datelor

Forma în care datele cu caracter personal sunt stocate sau utilizate nu este relevantă pentru aplicabilitatea legislației privind protecția datelor. Comunicările scrise sau verbale pot conține date cu caracter personal, precum şi imagini[63], inclusiv înregistrări

61 Cauzele conexate C-92/09 şi C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*, 9 noiembrie 2010, punctul 59.

62 Hotărârea CEDO din 2 septembrie 2010 în cauza *Uzun/Germania*, nr. 35623/05.

63 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.

video prin TVCI[64] sau sunete[65]. Informațiile înregistrate pe suport electronic, precum şi informațiile pe suport de hârtie, pot fi date cu caracter personal; chiar şi probele de celule de țesut uman pot constitui date cu caracter personal, întrucât conțin ADN-ul unei persoane.

2.1.2. Categorii speciale de date cu caracter personal

În temeiul dreptului european, precum şi **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 şi necesită o protecție sporită. Prin urmare, prelucrarea acestor categorii speciale de date („date sensibile") trebuie permisă numai împreună cu garanții specifice.

Referitor la definiția datelor sensibile, atât Convenția 108 (articolul 6), cât şi Directiva privind protecția datelor (articolul 8) disting următoarele categorii:

- date cu caracter personal referitoare la originea rasială sau etnică;
- date cu caracter personal referitoare la opiniile politice, convingerile religioase sau de altă natură şi
- date cu caracter personal referitoare la starea de sănătate sau viața sexuală.

> Exemplu: În cauza *Bodil Lindqvist*[66], CJUE a declarat că „precizarea faptului că o persoană s-a rănit la picior şi lucrează cu fracțiune de normă pe motive medicale constituie date cu caracter personal referitoare la starea de sănătate, în sensul articolului 8 alineatul (1) din Directiva 95/46."

Directiva privind protecția datelor include şi „apartenența la un sindicat" în categoria datelor sensibile, întrucât aceste informații pot constitui un indicator puternic al convingerilor sau afilierii politice.

64 Hotărârea CEDO din 28 ianuarie 2003 în cauza *Peck/Regatul Unit*, nr. 44647/98; Hotărârea CEDO din 5 octombrie 2010 în cauza *Köpke/Germania*, nr. 420/07.

65 Directiva privind protecția datelor, considerentele 16 şi 17; Hotărârea CEDO din 25 septembrie 2001 în cauza *P.G. şi J.H./Regatul Unit*, nr. 44787/98, punctele 59 şi 60; Hotărârea CEDO din 20 decembrie 2005 în cauza *Wisse/Franța*, nr. 71611/01.

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

Convenția 108 consideră, de asemenea, datele cu caracter personal referitoare la condamnările penale ca fiind date sensibile.

Articolul 8 alineatul (7) din Directiva privind protecția datelor autorizează statele membre ale UE „să stabilească condițiile în care poate fi prelucrat un număr de identificare sau orice alt identificator cu aplicabilitate generală."

2.1.3. Date anonimizate şi pseudonimizate

Potrivit principiului limitării duratei de păstrare a datelor, inclus în Directiva privind protecția datelor, precum şi în Convenția 108 (şi discutat în detaliu în capitolul 3), datele trebuie păstrate „într-o formă care permite identificarea persoanelor vizate o perioadă nu mai lungă decât este necesar în vederea atingerii scopurilor pentru care au fost colectate sau pentru care vor fi prelucrate ulterior"[67]. În consecință, datele trebuie să devină anonime în cazul în care un operator doreşte să le stocheze după ce devin perimate şi nu mai servesc scopului inițial.

Datele anonimizate

Datele devin anonime în cazul în care toate elementele de identificare sunt eliminate dintr-un set de date cu caracter personal. Niciun element nu poate fi lăsat în informațiile care, prin exercitarea unui efort rezonabil, ar putea servi la reidentificarea persoanei (persoanelor) vizate[68]. În cazul în care datele au fost anonimizate cu succes, acestea nu mai constituie date cu caracter personal.

Dacă datele cu caracter personal nu mai servesc scopului lor inițial, dar urmează a fi păstrate într-o formă personalizată în scopul utilizării istorice, statistice sau ştiințifice, Directiva privind protecția datelor şi Convenția 108 permit această posibilitate cu condiția aplicării unor garanții adecvate împotriva utilizării incorecte[69].

Datele pseudonimizate

Informațiile personale conțin elemente de identificare, cum ar fi numele, data naşterii, sexul şi adresa. Când informațiile personale devin pseudonime, elementele de

67 Directiva privind protecția datelor, articolul 6 alineatul (1) litera (e); Convenția 108, art. 5 litera (e).

68 *Ibidem*, considerentul 26.

69 *Ibidem*, articolul 6 alineatul (1) litera (e); şi Convenția 108, articolul 5 litera (e).

identificare sunt înlocuite cu un pseudonim. Pseudonimizarea se obține, spre exemplu, prin codificarea elementelor de identificare din datele cu caracter personal.

Datele pseudonimizate nu sunt menționate în mod explicit în definițiile juridice ale Convenției 108, şi nici în cele ale Directivei privind protecția datelor. Cu toate acestea, Raportul explicativ al Convenției 108 prevede la articolul 42 că „[c]erința [...] privind limitele de timp pentru stocarea datelor în forma asociată numelui acestora nu înseamnă că după o anumită perioadă de timp datele trebuie să fie separate irevocabil de numele persoanei la care se referă, doar că asocierea între date şi elementele de identificare nu ar trebui să fie posibilă în mod direct". Acesta este un efect care poate fi obținut prin procesul de pseudonimizare a datelor. Pentru toate persoanele care nu dețin o cheie de decodificare, datele devenite pseudonime pot fi identificabile cu dificultate.,Legătura cu o identitate încă există sub forma pseudonimului plus cheia de decodificare. Pentru acele persoane care au dreptul să utilizeze cheia de decodare, reidentificarea este uşor posibilă. Trebuie create garanții speciale împotriva utilizării cheilor de codificare de către persoane neautorizate.

Întrucât pseudonimizarea datelor reprezintă unul dintre cele mai importante mijloace de protecție a datelor la scară largă, în cazul în care reținerea totală de la utilizarea datelor cu caracter personal nu este posibilă, logica şi efectul unei astfel de acțiuni trebuie explicate în detaliu.

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

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

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

„YESz320l este tatăl a patru copii, doi băieți şi două fete".

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

Cu toate acestea, primul exemplu este mai puțin sigur. Dacă afirmația „C. S. 1967, este tatăl a patru copii, doi băieți şi două fete" este utilizată în localitatea de domiciliu

a lui Charles Spencer, domnul Spencer poate fi recunoscut cu uşurință. Metoda de pseudonimizare afectează eficacitatea protecției datelor.

Datele cu caracter personal care conțin elemente de identificare codificate sunt utilizate în diverse contexte ca mijloace de a păstra secretă identitatea unei persoane. Acest lucru este foarte util atunci când operatorii de date trebuie să se asigure că lucrează cu aceleaşi persoane vizate, însă nu trebuie, 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 aceştia sunt tratați şi 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 viața privată încă din stadiul dezvoltării. Aceasta înseamnă că protecția datelor este integrată în structura sistemelor avansate de prelucrare a datelor.

2.2. Prelucrarea datelor

Puncte-cheie

- Termenul „prelucrare” se referă în principal la prelucrarea automată.
- În temeiul dreptului european, prin „prelucrare” se înțelege şi 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.

În temeiul Convenției 108 şi al Directivei privind protecția datelor, protecția datelor se axează în principal pe prelucrarea automată a datelor.

În temeiul **legislației CoE**, definiția prelucrării automate admite, însă, că pot fi necesare unele etape de utilizare manuală a datelor cu caracter personal între operațiunile automate. În mod similar, în temeiul **dreptului european**, prelucrarea automată a datelor este definită prin „operațiuni efectuate asupra datelor cu caracter personal, integral sau parțial, prin mijloace automate”[70].

70 Convenția 108, articolul 2 litera (c) şi Directiva privind protecția datelor, articolul 2 litera (b) şi articolul 3 alineatul (1).

Exemplu: În cauza *Bodil Lindqvist*[71], CJUE a concluzionat că:

„referirea, pe o pagină de internet, la diverse persoane şi identificarea acestora fie după nume, fie prin alte mijloace, de exemplu, prin menționarea numărului de telefon sau a unor informații referitoare la condițiile lor de muncă sau la hobby-uri, constituie «prelucrare de date cu caracter personal integral sau parțial prin mijloace automate» în sensul articolului 3 alineatul (1) din Directiva 95/46."

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

Protecția datelor **în temeiul dreptului european** nu este limitată în niciun fel la prelucrarea automată a datelor. În consecință, în temeiul dreptului european, protecția datelor se aplică în cazul prelucrării datelor cu caracter personal într-un sistem de evidență manual, şi anume, un dosar structurat special[72]. Motivul acestei extinderi a protecției datelor este acela că:

- dosarele pot fi structurate într-un mod care face ca informațiile să fie găsite rapid şi uşor şi
- stocarea datelor cu caracter personal în dosare structurate înlesneşte sustragerea de la restricțiile stabilite de lege pentru prelucrarea automată a datelor[73].

În temeiul legislației CoE, Convenția 108 reglementează în primul rând prelucrarea datelor din fişiere automate de date[74]. Cu toate acestea, prevede şi posibilitatea extinderii protecției la prelucrarea manuală în cadrul legislației interne. Multe părți la Convenția 108 au recurs la această posibilitate şi au făcut declarații în acest sens către Secretarul General al CoE[75]. Extinderea protecției datelor în baza unei astfel de declarații trebuie să caracterizeze toate prelucrările manuale de date şi nu poate fi limitată la prelucrarea în sisteme de evidență manuale[76].

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

72 Directiva privind protecția datelor, articolul 3 alineatul (1).

73 *Ibidem*, considerent 27.

74 Convenția 108, articolul 2 litera (b).

75 A se vedea declarațiile formulate în temeiul Convenției 108, articolul 3 alineatul (2) litera (c).

76 A se vedea formularea din Convenția 108, articolul 3 alineatul (2).

În ceea ce privește natura operațiunilor de prelucrare incluse, conceptul de prelucrare este cuprinzător **atât în temeiul dreptului european, cât și în temeiul legislației CoE**: „«prelucrarea datelor cu caracter personal» [...] înseamnă orice operațiune [...] cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea”[77] care se efectuează asupra datelor cu caracter personal. Termenul „prelucrare” include şi acțiuni prin care datele nu se mai află în responsabilitatea unui operator şi sunt transferate sub răspunderea unui alt operator.

Exemplu: Angajatorii colectează şi prelucrează datele angajaților lor, inclusiv informațiile legate de salariile acestora. Temeiul juridic pentru a acționa astfel în mod legitim este contractul de muncă.

Angajatorii vor trebui să transmită autorităților fiscale datele privind salariile personalului. Acest transfer de date va constitui, de asemenea, „prelucrare” în sensul acestui termen din Convenția 108 şi din directivă. Cu toate acestea, temeiul juridic pentru această dezvăluire nu este contractul de muncă. Trebuie să existe un temei juridic suplimentar pentru operațiunile de prelucrare care au drept rezultat transferul datelor privind salariile de la angajator către autoritățile fiscale. Acest temei juridic este, de obicei, cuprins în dispozițiile legislației fiscale naționale. Fără o astfel de dispoziție, transferul datelor ar constitui prelucrare ilegală.

2.3. Utilizatorii de date cu caracter personal

Puncte-cheie

- Oricine decide să prelucreze datele cu caracter personal ale altor persoane este un „operator” în conformitate cu legislația privind protecția datelor; în cazul în care mai multe persoane iau această decizie împreună, acestea pot fi „operatori comuni”.
- O „persoană împuternicită de către operator” este o entitate separată din punct de vedere juridic, a cărei sarcină este prelucrarea datelor cu caracter personal pe seama operatorului.

77 Directiva privind protecția datelor, articolul 2 litera (b). În mod similar, a se vedea şi Convenția 108, articolul 2 litera (c).

- O persoană împuternicită de către operator devine operator în cazul în care utilizează datele în scop personal, fără a respecta instrucțiunile unui operator.
- Orice persoană care primește date de la un operator este un „destinatar".
- Un „terț" este o persoană fizică sau juridică, care nu acționează în conformitate cu instrucțiunile operatorului (și nu este persoana vizată).
- Un „destinatar terț" este o persoană sau o entitate separată din punct de vedere juridic de operator, dar care primește date cu caracter personal de la operator.

2.3.1. Operatori și persoane împuternicite de către operatori

Cea mai importantă consecință a statutului de operator sau de persoană împuternicită de către operator este responsabilitatea juridică pentru respectarea obligațiilor în conformitate cu legislația privind protecția datelor. Prin urmare, numai aceia care pot fi considerați responsabili în temeiul legislației aplicabile își pot asuma aceste funcții. În sectorul privat, este, de regulă, o persoană fizică sau juridică; în sectorul public, este o autoritate. Alte entități, cum ar fi organe sau instituții fără personalitate juridică, pot fi operatori sau persoane împuternicite de către operator numai în cazul în care există dispoziții juridice speciale în acest sens.

Exemplu: În cazul în care divizia de marketing a societății Sunshine intenționează să prelucreze date pentru un studiu de piață, societatea Sunshine, și nu divizia de marketing, va fi operatorul acestei prelucrări. Divizia de marketing nu poate fi operator, deoarece nu are identitate juridică separată.

În cadrul grupurilor de societăți, societatea-mamă și fiecare societate afiliată, fiind persoane juridice distincte, pot fi considerate operatori separați sau persoane împuternicite de către operator. Ca o consecință a acestui statut de separare din punct de vedere juridic, transferul de date între membrii unui grup de societăți va necesita o bază juridică specială. Nu există niciun privilegiu care să permită schimbul efectiv de date cu caracter personal între persoanele juridice separate din cadrul unui grup.

În acest context trebuie menționat rolul persoanelor fizice. **În temeiul dreptului european**, atunci când prelucrează datele altora în cursul unei activități exclusiv personale sau domestice, persoanele fizice nu intră sub incidența normelor Directivei privind protecția datelor; acestea nu sunt considerate operatori[78].

78 Directiva privind protecția datelor, considerentul 12 și articolul 3 alineatul (2) ultima liniuță.

Cu toate acestea, jurisprudența a constatat că legislația privind protecția datelor nu se aplică, totuşi, în cazul în care o persoană fizică, în timpul utilizării internetului, publică date cu privire la alte persoane.

Exemplu: CJUE a considerat în cauza *Bodil Lindqvist*[79] că:

„referirea, pe o pagină de internet, la diverse persoane şi identificarea acestora fie după nume, fie prin alte mijloace [...] constituie «prelucrare de date cu caracter personal integral sau parțial prin mijloace automate» în sensul articolului 3 alineatul (1) din Directiva 95/46."[80]

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 Directivei privind protecția datelor, deoarece această excepție „trebuie [...] interpretată ca fiind asociată numai activităților desfăşurate 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"[81].

Operatorul

În temeiul dreptului european, operatorul este definit ca fiind persoana care „singură sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal"[82]. Decizia unui operator stabileşte motivul şi metoda prelucrării datelor. **În temeiul legislației CoE**, definiția „operatorului" precizează în plus că un operator decide categoriile de date cu caracter personal care trebuie înregistrate[83].

Convenția 108 face referire în definiția operatorului la un aspect ulterior al controlului, care necesită atenție. Această definiție vizează persoana sau autoritatea competentă conform legii să prelucreze anumite date pentru o anumită finalitate. Cu toate acestea, în cazul în care se presupune că au loc operațiuni de prelucrare ilegale, iar operatorul responsabil trebuie identificat, operator va fi considerată persoana sau entitatea, cum ar fi o societate sau autoritate, care a luat decizia prelucrării datelor,

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

80 *Ibidem*, punctul 27.

81 *Ibidem*, punctul 47.

82 Directiva privind protecția datelor, articolul 2 litera (d).

83 Convenția 108, articolul 2 litera (d).

indiferent dacă era îndreptățită legal să acționeze astfel sau nu[84]. Prin urmare, cererea de ştergere trebuie întotdeauna adresată operatorului „efectiv".

Controlul comun

Definiția „operatorului" din Directiva privind protecția datelor prevede că pot exista şi mai multe entități separate din punct de vedere juridic, care, împreună sau în comun cu altele, acționează în calitate de operator. Înseamnă că acestea decid împreună să prelucreze date pentru un scop comun[85]. Totuşi, acest lucru este posibil din punct de vedere juridic numai în cazul în care există un temei juridic special care să prevadă prelucrarea în comun a datelor pentru un scop comun.

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

Regulamentele nu menționează explicit dacă un control comun presupune ca scopul comun să fie acelaşi pentru fiecare dintre operatori sau dacă este suficient ca scopurile acestora să se suprapună doar parțial. Cu toate acestea, nicio jurisprudență relevantă nu este încă disponibilă la nivel european şi nu există claritate cu privire la consecințele asumării răspunderii. Grupul de lucru Articolul 29 susține o interpretare mai largă a conceptului de control comun cu scopul de a permite o oarecare flexibilitate pentru a satisface complexitatea tot mai mare a realității actuale privind prelucrarea datelor[86]. Un caz care implică Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT) ilustrează poziția Grupului de lucru.

Exemplu: În aşa-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 dezvăluit datele legate de aceste tranzacții bancare, stocate într-un centru de servicii informatice din Statele Unite, Departamentului american al Trezoreriei, fără a i se impune acest lucru în mod explicit

84 A se vedea, de asemenea, Grupul de lucru Articolul 29 (2010), *Avizul 1/2010 privind conceptele de „operator" și „persoană împuternicită de către operator"*, WP 169, Bruxelles, 16 februarie 2010, p. 15.

85 Directiva privind protecția datelor, articolul 2 litera 1(d).

86 Grupul de lucru Articolul 29 (2010), *Avizul 1/2010 privind conceptele de „operator" și „persoană împuternicită de către operator"*, WP 169, Bruxelles, 16 februarie 2010, p. 19.

de către instituțiile bancare europene care au angajat-o. După evaluarea legalității acestei situații, Grupul de lucru Articolul 29 a ajuns la concluzia că instituțiile bancare europene care au angajat SWIFT, precum şi SWIFT, trebuiau să fie considerate operatori comuni responsabili în fața clienților europeni pentru dezvăluirea datelor lor autorităților americane[87]. Prin decizia de a transmite datele, SWIFT şi-a asumat – în mod ilegal – rolul de operator; instituțiile bancare nu şi-au respectat, în mod evident, obligațiile de supraveghere a persoanei împuternicite şi, prin urmare, nu puteau fi absolvite complet de responsabilitatea lor în calitate de operator. Această situație atrage după sine controlul comun.

Persoana împuternicită de către operator

Persoana împuternicită de către operator este definită **în temeiul dreptului european** ca fiind persoana care prelucrează datele cu caracter personal pe seama operatorului[88]. Activitățile încredințate unei persoane împuternicite de către operator pot fi limitate la o sarcină sau la un context foarte specific sau pot fi relativ generale şi cuprinzătoare.

În temeiul legislației CoE, sensul expresiei este acelaşi ca în temeiul dreptului european.

Pe lângă prelucrarea datelor pentru ceilalți, persoanele împuternicite de către operator vor fi şi operatori de date de drept în legătură cu prelucrarea pe care o efectuează în scopuri proprii, de exemplu, gestionarea propriilor angajați, a vânzărilor şi a conturilor.

Exemple: Societatea Everready este specializată în prelucrarea datelor pentru administrarea datelor privind resursele umane pentru alte societăți. În această calitate, Everready este un împuternicit.

Cu toate acestea, în cazul în care Everready prelucrează datele propriilor angajați, aceasta este operatorul care desfăşoară operațiuni de prelucrare a datelor în scopul respectării obligațiilor sale de angajator.

87 Grupul de lucru Articolul 29 (2006), *Avizul 10/2006 privind prelucrarea datelor cu caracter personal de către Societatea Internațională pentru Telecomunicații Financiare Interbancare (SWIFT)*, WP 128, Bruxelles, 22 noiembrie 2006.

88 Directiva privind protecția datelor, articolul 2 litera (e).

Relația între operator și persoana împuternicită de către operator

Aşa cum am văzut, operatorul este definit ca fiind cel care stabileşte scopurile şi mijloacele prelucrării.

Exemplu: Directorul societății Sunshine decide că societatea Moonlight, specializată în analiză de piață, ar trebui să realizeze o analiză de piață privind datele referitoare la clienții Sunshine. Deşi sarcina de a stabili mijloacele de prelucrare va fi delegată astfel societății Moonlight, operator rămâne societatea Sunshine, iar Moonlight va fi doar persoana împuternicită de către operator, deoarece, potrivit contractului, Moonlight poate utiliza datele privind clienții societății Sunshine numai pentru scopurile stabilite de Sunshine.

În cazul în care competența de stabilire a mijloacelor de prelucrare va fi delegată unei persoane împuternicite de către operator, operatorul trebuie să poată interveni, totuşi, în deciziile 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 asigura conformitatea deciziilor acestora cu legislația privind protecția datelor. Prin urmare, un contract care interzice operatorului să intervină în deciziile persoanei împuternicite de el ar putea fi interpretat probabil ca având drept rezultat controlul comun, ambele părți împărțind responsabilitatea juridică a unui operator.

În plus, în cazul în care o persoană împuternicită de către operator nu respectă limitările utilizării datelor, astfel cum este prevăzut de către operator, persoana împuternicită de către operator va fi devenit operator, cel puțin în măsura încălcării instrucțiunilor operatorului. Acest lucru va duce cel mai probabil la transformarea persoanei împuternicite de către operator în operator ilegal. În schimb, operatorul inițial va trebui să explice cum a fost posibil ca persoana împuternicită de el să îşi încalce împuternicirea. Într-adevăr, Grupul de lucru Articolul 29 tinde să admită controlul comun în astfel de cazuri, întrucât acest lucru are ca rezultat cea mai bună protecție a intereselor persoanelor vizate[89]. O consecință importantă a controlului comun trebuie să fie răspunderea solidară pentru daune, permițând persoanelor vizate o gamă mai extinsă de căi de atac.

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

De asemenea, pot exista probleme cu privire la împărțirea responsabilității în cazul în care operatorul este o întreprindere mai mică, iar persoana împuternicită de către operator este o corporație mare, care are puterea de a dicta condițiile în care își oferă serviciile. Totuși, în aceste situații, Grupul de lucru Articolul 29 menține că standardul de responsabilitate nu trebuie coborât din cauza dezechilibrului economic și că trebuie păstrată înțelegerea conceptului de operator[90].

În vederea asigurării clarității și transparenței, detaliile relației dintre un operator și o persoană împuternicită de către operator ar trebui înregistrate într-un contract scris[91]. Inexistența unui astfel de contract constituie o încălcare a obligației operatorului de a oferi o documentație scrisă a responsabilităților reciproce și poate duce la sancțiuni[92].

Este posibil ca persoanele împuternicite de către operator să dorească să delege anumite sarcini altor subcontractanți. Acest lucru este permis din punct de vedere legal și va depinde în detaliu de prevederile contractuale dintre operator și persoana împuternicită de către operator, inclusiv dacă este necesară autorizarea operatorului în fiecare caz în parte sau dacă este suficientă numai o simplă informare.

În temeiul legislației CoE, interpretarea conceptelor de operator și de persoană împuternicită de către operator explicate mai sus este complet aplicabilă, astfel cum o dovedesc recomandările elaborate conform Convenției 108[93].

2.3.2. Destinatari și terți

Diferența între 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.

Un „terț" este o persoană diferită din punct de vedere juridic de un operator. Prin urmare, dezvăluirea datelor către un terț va necesita întotdeauna un temei juridic specific. Potrivit articolului 2 litera (f) din Directiva privind protecția datelor, un terț

90 Grupul de lucru Articolul 29 (2010), *Avizul 1/2010 privind conceptele de „operator" și „persoană împuternicită de către operator"*, WP 169, Bruxelles, 16 februarie 2010, p. 26.

91 Directiva privind protecția datelor, articolul 17 alineatele (3) și (4).

92 Grupul de lucru Articolul 29 (2010), *Avizul 1/2010 privind conceptele de „operator" și „persoană împuternicită de către operator"*, WP 169, Bruxelles, 16 februarie 2010, p 27.

93 A se vedea, de exemplu, Recomandarea privind crearea de profile, articolul 1.

este „persoana fizică sau juridică, autoritatea publică, agenția sau orice organism, altul decât persoana vizată, operatorul, persoana împuternicită şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite, sunt autorizate să prelucreze date". Aceasta înseamnă că persoanele care lucrează pentru o organizație diferită din punct de vedere juridic de operator – chiar dacă aparține aceluiaşi grup sau societăți de tip holding – vor fi (sau vor aparține unui) „terț". Pe de altă parte, sucursalele unei bănci care prelucrează conturile clienților sub autoritatea directă a sediului lor central nu pot fi considerate „terți"[94].

„Destinatar" este un termen cu semnificație mai largă decât „terț". În sensul articolului 2 litera (g) din Directiva privind protecția datelor, destinatar înseamnă „persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism căruia îi sunt transmise datele, indiferent dacă este sau nu terț". Acest destinatar poate fi o persoană din afara operatorului sau a persoanei împuternicite de către operator – în acest caz un terț – sau cineva din cadrul operatorului sau al persoanei împuternicite de către operator, cum ar fi un angajat sau o altă divizie din cadrul aceleiaşi societăți sau autorități.

Diferența între destinatari şi terți este importantă numai datorită condițiilor pentru dezvăluirea legală a datelor. Angajații unui operator sau ai unei persoane împuternicite de către operator pot fi, fără nicio altă dispoziție juridică, destinatari ai datelor cu caracter personal, în cazul în care sunt implicați în operațiunile de prelucrare ale operatorului sau persoanei împuternicite de către operator. Pe de altă parte, un terț, separat din punct de vedere juridic de operator şi de persoana împuternicită de către operator, nu este autorizat să utilizeze datele cu caracter personal prelucrate de operator, cu excepția cazului în care există temeiuri juridice într-o anumită situație. Prin urmare, „destinatarii terți" ai datelor vor avea întotdeauna nevoie de un temei juridic pentru primirea legală a datelor cu caracter personal.

Exemplu: Angajatul unei persoane împuternicite de către operator, care utilizează datele cu caracter personal în limita atribuțiilor încredințate de angajator, este destinatarul datelor, însă nu terț, deoarece utilizează datele în numele şi în conformitate cu instrucțiunile persoanei împuternicite de către operator.

Cu toate acestea, în cazul în care acelaşi angajat decide să utilizeze datele, pe care le poate accesa în calitate de angajat al persoanei împuternicite de către operator, în scopuri proprii şi le vinde unei alte societăți, atunci se consideră că angajatul a acționat în calitate de terț. Acesta nu mai respectă ordinele

94 Grupul de lucru Articolul 29 (2010), *Avizul 1/2010 privind conceptele de „operator" și „persoană împuternicită de către operator"*, WP 169, Bruxelles, 16 februarie 2010, p. 31.

persoanei împuternicite de către operator (angajatorul). În calitate de terț, angajatul are nevoie de un temei juridic pentru a achiziționa și a vinde datele. În acest exemplu, angajatul, în mod cert, nu posedă un astfel de temei juridic și, prin urmare, acțiunile sale sunt ilegale.

2.4. Consimțământul

Puncte-cheie

- Ca temei juridic pentru prelucrarea datelor cu caracter personal, consimțământul trebuie să fie liber, informat și specific.
- Consimțământul trebuie să fie acordat în mod neechivoc. Consimțământul poate fi acordat fie explicit, fie implicit, acționând într-un mod care nu lasă loc de îndoială asupra faptului că persoana vizată este de acord cu prelucrarea datelor sale.
- Prelucrarea datelor sensibile pe bază de consimțământ necesită un consimțământ explicit.
- Consimțământul poate fi retras în orice moment.

Consimțământ înseamnă „orice manifestare de voință, liberă, specifică și informată din partea persoanei vizate”[95]. În numeroase cazuri, constituie temeiul juridic pentru prelucrarea legitimă a datelor (a se vedea secțiunea 4.1).

2.4.1. Elementele unui consimțământ valabil

Dreptul european stabilește trei elemente necesare pentru ca un consimțimânt să fie valabil, care au ca scop garantarea intenției efective a persoanelor vizate de a accepta utilizarea datelor lor:

- persoana vizată nu trebuie să fie supusă niciunei presiuni atunci când își acordă consimțământul;
- persoana vizată trebuie să fie informată corespunzător cu privire la scopul și consecințele acordării consimțământului și
- domeniul de aplicare al consimțământului trebuie să fie concret în mod rezonabil.

95 Directiva privind protecția datelor, articolul 2 litera (h).

Numai în cazul în care toate aceste trei condiții sunt îndeplinite, consimțământul va fi valabil în sensul legislației privind protecția datelor.

Convenția 108 nu conține o definiție a consimțământului; acesta este lăsat la aprecierea legislației interne. Cu toate acestea, **în temeiul legislației CoE**, elementele unui consimțământ valabil corespund celor explicate mai sus, astfel cum se prevede în recomandările elaborate în conformitate cu Convenția 108[96]. Cerințele privind consimțământul sunt aceleaşi ca pentru o declarație de intenție valabilă, conform dreptului civil european.

Cerințele suplimentare conform dreptului civil pentru un consimțământ valabil, cum ar fi capacitatea juridică, se aplică evident şi în contextul protecției datelor, întrucât aceste cerințe reprezintă condiții juridice prealabile. Consimțământul nevalid al persoanelor lipsite de capacitate juridică va avea ca rezultat absența unui temei juridic pentru prelucrarea datelor acelor persoane.

Consimțământul poate fi acordat fie explicit[97], fie implicit. Primul tip nu lasă loc de îndoială cu privire la intențiile persoanei vizate şi poate fi acordat verbal sau în scris; al doilea tip este dedus din circumstanțe. Orice consimțământ se acordă în mod neechivoc[98]. Aceasta înseamnă că nu trebuie să existe nicio îndoială cu privire la dorința persoanei vizate de a-şi da consimțământul pentru prelucrarea datelor sale. De exemplu, deducerea consimțământului din simpla inactivitate nu poate constitui un consimțământ neechivoc. În cazul în care datele care trebuie prelucrate sunt sensibile, consimțământul explicit este obligatoriu şi trebuie să fie neechivoc.

Consimțământul liber exprimat

Existența consimțământului liber exprimat este valabilă numai „în cazul în care persoana vizată poate exercita o opțiune efectivă şi nu există niciun risc de înşelăciune, intimidare, constrângere sau consecințe negative semnificative dacă nu îşi acordă consimțământul”[99].

96 A se vedea, de exemplu, Convenția 108, Recomandarea privind datele statistice, punctul 6.

97 Directiva privind protecția datelor, articolul 8 alineatul (2).

98 *Ibidem*, articolul 7 litera (a) şi articolul 26 alineatul (1).

99 A se vedea, de asemenea, Grupul de lucru Articolul 29 (2011), *Avizul 15/2011 privind conceptul de „consimțământ”*, WP 187, Bruxelles, 13 iulie 2011, p. 12.

Exemplu: În multe aeroporturi, pasagerii trebuie să treacă prin scanere corporale pentru a putea intra în zona de îmbarcare[100]. Având în vedere că datele persoanelor sunt prelucrate în timpul scanării, această prelucrare trebuie să se conformeze unuia dintre temeiurile juridice în baza articolului 7 din Directiva privind protecția datelor (a se vedea secțiunea 4.1.1). Uneori trecerea prin scanerele corporale este prezentată pasagerilor sub formă de opțiune, ceea ce presupune că prelucrarea poate fi justificată prin consimțământul lor. Cu toate acestea, pasagerii se tem că refuzul de a trece prin scanerele corporale poate crea suspiciune sau poate determina controale suplimentare, cum ar fi percheziționile corporale. Mulți pasageri consimt scanarea deoarece evită, astfel, posibile probleme sau întârzieri. Se presupune că acest consimțământ nu este suficient de liber exprimat.

Prin urmare, un temei juridic solid poate exista numai într-un act al legislatorului, în baza articolului 7 litera (e) din Directiva privind protecția datelor, având ca rezultat obligarea pasagerilor de a coopera ținând seama de interesul public predominant. Această legislație poate prevedea totuşi alegerea între scanare şi control manual, dar numai ca măsuri suplimentare de control la frontieră în circumstanțe speciale. Acestea sunt aspecte prevăzute de Comisia Europeană în două regulamente vizând scanerele de securitate din anul 2011[101].

Consimțământul liber exprimat poate fi amenințat şi în situații de subordonare, în cazul în care există un dezechilibru semnificativ economic sau de altă natură între operatorul care asigură consimțământul şi persoana vizată care acordă consimțământul[102].

Exemplu: O societate mare intenționează să creeze un repertoriu cu numele tuturor angajaților, funcția acestora în cadrul societății şi adresele profesionale,

100 Acest exemplu este luat din *Ibidem*, p. 15.

101 Regulamentul (UE) nr. 1141/2011 al Comisiei din 10 noiembrie 2011 de modificare a Regulamentului (CE) nr. 272/2009 de completare a standardelor de bază comune în domeniul securității aviației civile în ceea ce privește utilizarea scanerelor de securitate în aeroporturile UE, MO 2011 L 293, şi Regulamentul de punere în aplicare (UE) nr. 1147/2011 al Comisiei din 11 noiembrie 2011 de modificare a Regulamentului (UE) nr. 185/2010 de stabilire a măsurilor detaliate de implementare a standardelor de bază comune în domeniul securității aviației în ceea ce privește utilizarea scanerelor de securitate în aeroporturile UE, MO 2011 L 294.

102 A se vedea, de asemenea, Grupul de lucru Articolul 29 (2001), *Avizul 8/2001 privind prelucrarea datelor cu caracter personal în contextul ocupării forței de muncă*, WP 48, Bruxelles, 13 septembrie 2001; şi Grupul de lucru Articolul 29 (2005), *Document de lucru privind interpretarea comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995*, WP 114, Bruxelles, 25 noiembrie 2005.

exclusiv pentru a îmbunătăți comunicațiile interne la nivel de societate. Şeful de personal propune adăugarea în repertoriu a unei fotografii a fiecărui angajat pentru a recunoaşte mai uşor colegii în cadrul întâlnirilor. Reprezentanții angajaților solicită să se facă acest lucru numai dacă angajatul îşi acordă consimțământul.

Într-un astfel de caz, consimțământul angajatului trebuie recunoscut drept temei juridic pentru prelucrarea fotografiilor în repertoriu, deoarece este evident că publicarea unei fotografii în repertoriu nu va avea consecințe negative în sine şi, mai mult, este plauzibil că angajatul nu va suferi efecte negative inițiate de angajator dacă nu va fi de acord cu publicarea fotografiei sale în repertoriu.

Totuşi, aceasta nu înseamnă că niciodată consimțământul nu poate fi valabil în situații în care neacordarea consimțământului ar avea consecințe negative. În cazul în care, de exemplu, neacordarea consimțământului pentru emiterea unui card de client de supermarket rezultă numai în neprimirea reducerilor de preț pentru anumite produse, consimțământul este, totuşi, un temei juridic valid pentru prelucrarea datelor cu caracter personal ale acelor clienți care şi-au dat consimțământul pentru emiterea unui astfel de card. Între societate şi client nu există nicio situație de subordonare şi, în consecință, neacordarea consimțământului nu este un aspect suficient de grav pentru ca persoana vizată să nu mai aibă dreptul la libera alegere.

Pe de altă parte, ori de câte ori produse sau servicii suficient de importante se obțin numai şi numai dacă sunt dezvăluite anumite date cu caracter personal unor terți, consimțământul persoanei vizate pentru dezvăluirea datelor sale nu poate fi considerat, în mod normal, o decizie liberă şi, prin urmare, nu este valabil în temeiul legislației privind protecția datelor.

Exemplu: Consimțământul exprimat de pasagerii unei companii aeriene pentru transferul aşa-numitelor registre cu numele pasagerilor (PNR), şi anume date privind identitatea acestora, obiceiurile alimentare sau problemele de sănătate către autoritățile în domeniul imigrației dintr-o anumită țară străină nu poate fi considerat consimțământ valabil în temeiul legislației privind protecția datelor, întrucât pasagerii care călătoresc nu au de ales dacă doresc să viziteze acea țară. În cazul în care aceste date vor fi transferate legal, este necesar un temei juridic altul decât consimțământul: cel mai probabil o lege specială.

Consimțământul informat

Persoana vizată trebuie să dețină suficiente informații înainte de a lua o decizie. Dacă informațiile furnizate sunt sau nu suficiente se poate stabili numai de la caz la caz. De obicei, consimțământul informat va cuprinde o descriere precisă și ușor de înțeles a scopului pentru care se solicită consimțământul și, în plus, va prezenta consecințele acordării sau neacordării consimțământului. Limbajul utilizat pentru informare trebuie să fie adaptat pentru destinatarii previzibili ai informațiilor.

De asemenea, informațiile trebuie să fie ușor accesibile persoanei vizate. Accesibilitatea și vizibilitatea informațiilor sunt elemente importante. Într-un mediu online, notificările stratificate pot fi o soluție optimă, întrucât, pe lângă o versiune concisă a informațiilor, persoana vizată poate accesa și o versiune mai extinsă a acestora.

Consimțământul specific

Pentru a fi valabil, consimțământul trebuie să fie și specific. Acest lucru este dublat de calitatea informațiilor furnizate cu privire la scopul pentru care se solicită consimțământul. În acest context, așteptările rezonabile ale unei persoane vizate obișnuite vor fi relevante. Consimțământul unei persoane vizate trebuie solicitat din nou atunci când operațiunile de prelucrare urmează a fi adăugate sau modificate într-un mod care nu putea fi prevăzut în mod rezonabil în momentul acordării consimțământului inițial.

Exemplu: În cauza *Deutsche Telekom AG*[103], CJUE a analiza problema dacă un furnizor de servicii de telecomunicații care a trebuit să transmită datele cu caracter personal ale abonaților în temeiul articolului 12 din *Directiva asupra confidențialității și comunicațiilor electronice*[104] trebuia să reînnoiască consimțământul persoanelor vizate, întrucât destinatarii nu au fost stabiliți în momentul acordării consimțământului inițial.

CJUE a considerat că, în temeiul acelui articol, reînnoirea consimțământului înainte de transmiterea datelor nu este necesară, deoarece persoanele vizate au

103 Hotărârea CJUE din 5 mai 2011 în cauza C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*; a se vedea în special punctele 53 și 54.

104 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, MO 2002 L 201 (*Directiva asupra confidențialității și comunicațiilor electronice*).

avut posibilitatea, în baza acestei dispoziții, să consimtă numai în ceea ce privește prelucrarea, și anume, dezvăluirea datelor lor, și nu au putut opta pentru alte directoare în care să poată fi înregistrate aceste date.

Așa cum a evidențiat Curtea, „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”[105]. De asemenea, „însăși publicarea datelor cu caracter personal într-o listă publică de abonați cu o finalitate specifică se poate dovedi prejudiciabilă pentru un abonat”[106], și nu pentru autorul acestei publicări.

2.4.2. Dreptul de retragere a consimțământului în orice moment

Directiva privind protecția datelor nu prevede un drept general de retragere a consimțământului în orice moment. Cu toate acestea, se presupune în mare măsură că un astfel de drept există și că persoana vizată trebuie să aibă posibilitatea de a-l exercita la libera sa apreciere. Nu ar trebui să existe nicio cerință pentru justificarea retragerii și nici un risc de consecințe negative dincolo de încetarea oricăror beneficii care pot rezulta din utilizarea datelor pentru care s-a acordat anterior consimțământul.

Exemplu: Un client este de acord să primească un mesaj publicitar 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 mesajului publicitar. Nu ar trebui impuse niciun fel de consecințe represive, cum ar fi comisioane.

În cazul în care clientul primea o reducere de 5 % din costul unei camere de hotel în schimbul consimțământului de utilizare a datelor sale pentru mesajul publicitar, retragerea ulterioară a consimțământului de a primi mesajul publicitar nu ar trebui să aibă ca rezultat obligația de rambursare a acelor reduceri.

105 Hotărârea CJUE din 5 mai 2011 în cauza *Deutsche Telekom AG/Bundesrepublik Deutschland*, C-543/09; a se vedea în special punctul 61.

106 *Ibidem*, a se vedea în special punctul 62.

3

Principiile-cheie ale legislației europene privind protecția datelor

UE	Aspecte vizate	CoE
Directiva privind protecția datelor, articolul 6 alineatul (1) literele (a) și (b) CJUE, *Huber/Bundesrepublik Deutschland*, C-524/06, 16 decembrie 2008 CJUE, Clauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*, 9 noiembrie 2010	**Principiul prelucrării legale**	Convenția 108, articolul 5 literele (a) și (b) CEDO, *Rotaru/România* [GC], nr. 28341/95, 4 mai 2000 CEDO, *Taylor-Sabori/Regatul Unit*, nr. 47114/99, 22 octombrie 2002 CEDO, *Peck/Regatul Unit*, nr. 44647/98, 28 ianuarie 2003 CEDO, *Khelili/Elveția*, nr. 16188/07, 18 octombrie 2011 CEDO, *Leander/Suedia*, nr. 9248/81, 26 martie 1987
Directiva privind protecția datelor, articolul 6 alineatul (1) litera (b)	**Principiul limitării și specificității scopului**	Convenția 108, articolul 5 litera (b)
	Principiile calității datelor:	
Directiva privind protecția datelor, articolul 6 alineatul (1) litera (c)	**Pertinența datelor**	Convenția 108, articolul 5 litera (c)
Directiva privind protecția datelor, articolul 6 alineatul (1) litera (d)	**Exactitatea datelor**	Convenția 108, articolul 5 litera (d)
Directiva privind protecția datelor, articolul 6 alineatul (1) litera (e)	**Limitarea duratei de păstrare a datelor**	Convenția 108, articolul 5 litera (e)

UE	Aspecte vizate	CoE
Directiva privind protecția datelor, articolul 6 alineatul (1) litera (e)	**Excepții pentru cercetare științifică și statistici**	Convenția 108, articolul 9 alineatul (3)
Directiva privind protecția datelor, articolul 6 alineatul (1) litera (a)	**Principiul prelucrării corecte**	Convenția 108, articolul 5 litera (a) CEDO, *Haralambie/România*, nr. 21737/03, 27 octombrie 2009 CEDO, *K.H. și alții/Slovacia*, nr. 32881/04, 6 noiembrie 2009
Directiva privind protecția datelor, articolul 6 alineatul (2)	**Principiul responsabilității**	

Principiile prevăzute la articolul 5 din Convenția 108 consacră esența legislației europene privind protecția datelor. Acestea apar și la articolul 6 din Directiva privind protecția datelor ca punct de plecare pentru dispoziții mai detaliate în articolele următoare ale directivei. Orice legislație ulterioară privind protecția datelor la nivelul CoE sau UE trebuie să respecte aceste principii, iar acestea trebuie avute în vedere în momentul interpretării legislației. Orice derogări și restricții cu privire la aceste principii-cheie pot fi prevăzute la nivel național[107]; acestea trebuie să fie prevăzute de lege, să urmărească un scop legitim și să constituie o măsură necesară într-o societate democratică. Toate cele trei condiții trebuie îndeplinite.

3.1. Principiul prelucrării legale

Puncte-cheie

- Pentru a înțelege principiul prelucrării legale, trebuie să se facă referire la condițiile limitărilor legale ale dreptului la protecția datelor din perspectiva articolului 52 alineatul (1) din Cartă și a cerințelor privind intervenția legitimă în temeiul articolului 8 alineatul (2) din Convenția europeană a drepturilor omului.
- În consecință, prelucrarea datelor cu caracter personal este legală numai dacă:
  - este în conformitate cu legea;
  - urmărește un scop legitim și
  - este necesară într-o societate democratică pentru atingerea unui scop legitim.

107 Convenția 108, articolul 9 alineatul (2); Directiva privind protecția datelor, articolul 13 alineatul (2).

În temeiul dreptului european și al legislației CoE privind protecția datelor, principiul prelucrării legale este primul principiu denumit; acesta este exprimat în termeni aproape identici în articolul 5 din Convenția 108 şi articolul 6 din Directiva privind protecția datelor.

Niciuna dintre aceste dispoziții nu conține o definiție a ceea ce constituie „prelucrarea legală". Pentru a înțelege acest termen juridic, este necesar să se facă referire la intervenția legitimă în temeiul Convenției europene a drepturilor omului, astfel cum este interpretată de jurisprudența Convenției europene a drepturilor omului, şi la condițiile limitărilor legale în temeiul articolului 52 din Cartă.

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

Prelucrarea datelor cu caracter personal poate constitui o atingere asupra dreptului la respectarea vieții private a persoanei vizate. Cu toate acestea, dreptul la respectarea vieții private nu este un drept absolut, ci trebuie echilibrat şi conciliat cu alte interese legitime, fie ale altor persoane (interese particulare), fie ale societății, în ansamblu (interese publice).

Condițiile în care intervenția statului este legitimă sunt după cum urmează:

Conformitatea cu legea

Potrivit jurisprudenței CEDO, intervenția 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 şi previzibilă în ceea ce priveşte efectele"[108]. O normă este previzibilă „numai atunci când este redactată cu suficientă precizie, în aşa fel încât să permită oricărei persoane fizice – care, la nevoie, poate apela la consultanță de specialitate – să îşi corecteze conduita"[109]. „Gradul de precizie impus «legii» în legătură cu acest aspect va depinde de finalitatea specifică"[110].

108 Hotărârea CEDO din 16 februarie 2000 în cauza *Amann/Elveția* [T], nr. 27798/95, punctul 50; a se vedea şi Hotărârea CEDO din 25 martie 1998 în cauza *Kopp/Elveția*, nr. 23224/94, punctul 55 şi Hotărârea CEDO din 10 februarie 2009 în cauza *Iordachi şi alții/Moldova*, nr. 25198/02, punctul 50.

109 Hotărârea CEDO din 16 februarie 2000 în cauza *Amann/Elveția* [T], nr. 27798/95, punctul 56; a se vedea, 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 şi alții/Regatul Unit*, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, punctul 88.

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

Exemplu: În cauza *Rotaru/România*[111], CEDO a constatat o încălcare a articolului 8 din Convenția europeană a drepturilor omului, întrucât România a permis colectarea, înregistrarea şi arhivarea în fişiere secrete a unor informații care aduc atingere securității naționale, fără a stabili limitări ale exercitării acestor puteri, care au rămas 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. Având în vedere aceste deficiențe, Curtea a concluzionat că legislația internă nu respectă cerința de previzibilitate în temeiul articolului 8 din Convenția europeană a drepturilor omului şi că articolul fusese încălcat.

Exemplu: În cauza *Taylor-Sabori/Regatul Unit*[112], reclamantul fusese ținta măsurilor de supraveghere ale poliției. Utilizând o „clonă" a pager-ului acestuia, poliția a putut intercepta mesajele care îi erau trimise. Ulterior, reclamantul a fost arestat şi acuzat de conspirație la trafic de substanțe controlate. O parte a dosarului de acuzare consta 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 personal de telecomunicații. Prin urmare, intervenția asupra drepturilor sale nu a fost „în conformitate cu legea". CEDO a concluzionat că articolul 8 din Convenția europeană a drepturilor omului a fost încălcat.

Urmărirea unui scop legitim

Scopul legitim poate fi oricare dintre interesele publice numite sau drepturile şi libertățile altora.

Exemplu: În cauza *Peck/Regatul Unit*[113], reclamantul a încercat să se sinucidă pe stradă tăindu-şi venele de la mâini, neştiind că o cameră TVCI îl filmase în timpul tentativei. După ce poliția, care urmărea camerele TVCI, l-a salvat, autoritatea

111 Hotărârea CEDO din 4 aprilie 2000 în cauza *Rotaru/România* [T], nr. 28341/95, punctul 57; a se vedea, 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; şi Hotărârea CEDO din 31 mai 2005 în cauza *Vetter/Franța*, nr. 59842/00.

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

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

poliţienească a transmis înregistrarea camerei TVCI către mass-media, care a publicato fără să ascundă faţa 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 articolul 8 din Convenția europeană a drepturilor omului a fost încălcat.

Măsură necesară într-o societate democratică

CEDO a declarat că „noțiunea de necesitate presupune ca intervenția să corespundă unei nevoi sociale presante şi, în special, să fie proporțională cu scopul legitim urmărit”[114].

Exemplu: În cauza *Khelili/Elveția*[115], în timpul unui control, poliția a constatat că reclamanta avea asupra sa un card pe care scria: „Plăcută, atractivă, spre 40 de ani, doresc să cunosc un domn pentru ieşiri ocazionale în oraş. 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 în permanență. Reclamanta a solicitat ştergerea 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 şi generală, nu era susținută prin fapte concrete, întrucât aceasta nu fusese condamnată niciodată pentru prostituție ilegală şi, prin urmare, nu se putea considera că îndeplineşte „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 şi având în vedere seriozitatea atingerii asupra drepturilor reclamantei, Curtea a hotărât că reținerea cuvântului „prostituată” în evidențele poliţieneşti o perioadă îndelungată nu este necesară într-o societate democratică. Curtea a concluzionat că articolul 8 din Convenția europeană a drepturilor omului a fost încălcat.

114 Hotărârea CEDO din 11 iulie 1985 în cauza *Leander/Suedia*, nr. 9248/81, punctul 58.

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

Exemplu: În cauza *Leander/Suedia*[116], 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 stabilite în legislația națională pentru protejarea intereselor persoanelor vizate – de exemplu, controale exercitate de Parlament şi Cancelarul Justiției – au determinat CEDO să concluzioneze că sistemul suedez de control al personalului îndeplinește 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 există nicio încălcare a articolului 8 din Convenția europeană a drepturilor omului.

3.1.2. Condițiile limitărilor legale în temeiul Cartei UE

Structura şi modul de redactare a Cartei sunt diferite de cele ale Convenției europene a drepturilor omului. Carta nu vorbeşte despre interferențe cu drepturile garantate, însă conține o dispoziție privind limitarea (limitările) exercitării drepturilor şi libertăților recunoscute de Cartă.

În conformitate cu articolul 52 alineatul (1), limitările exercitării drepturilor şi libertăților recunoscute de Cartă şi, în consecință, ale exercitării dreptului la protecția datelor cu caracter personal, cum ar fi prelucrarea datelor cu caracter personal, sunt admisibile numai dacă:

- sunt prevăzute de lege;
- respectă esența dreptului la protecția datelor;
- sunt necesare, sub rezerva principiului proporționalității şi
- îndeplinesc obiective de interes general recunoscute de Uniune sau nevoia de protejare a drepturilor şi libertăților altora.

116 Hotărârea CEDO din 11 iulie 1985 în cauza *Leander/Suedia*, nr. 9248/81, punctele 59 şi 67.

Exemple: În cauza *Volker und Markus Schecke*[117], 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 opera o distincție pe baza unor criterii relevante, cum ar fi perioadele în care acele persoane au primit un astfel de ajutor, frecvența acestui ajutor sau natura şi valoarea acestuia, Consiliul şi Comisia au depăşit limitele impuse de principiul proporționalității.

Prin urmare, CJUE a considerat necesar să declare invalide anumite dispoziții ale Regulamentului (CE) nr. 1290/2005 al Consiliului şi să declare Regulamentul nr. 259/2008 invalid în totalitate[118].

În pofida formulării diferite, condițiile prelucrării legale din articolul 52 alineatul (1) din Cartă amintesc de articolul 8 alineatul (2) din Convenția europeană a drepturilor omului. Într-adevăr, condițiile enumerate la articolul 52 alineatul (1) din Cartă trebuie considerate conforme cu cele prevăzute la articolul 8 alineatul (2) din Convenția europeană a drepturilor omului, întrucât prima teză a articolului 52 alineatul (3) din Cartă prevede că, „în măsura în care prezenta cartă conține drepturi care corespund unor drepturi garantate prin Convenția europeană pentru apărarea drepturilor omului şi a libertăților fundamentale, înțelesul şi întinderea lor sunt aceleaşi ca şi cele prevăzute de convenția menționată".

Cu toate acestea, conform ultimei teze a articolului 52 alineatul (3), „această dispoziție nu împiedică dreptul Uniunii să asigure o protecție mai extinsă". În contextul comparării articolului 8 alineatul (2) din Convenția europeană a drepturilor omului cu prima teză a articolului 52 alineatul (3), aceasta nu poate însemna decât că aceste condiții de intervenție legitimă în conformitate cu articolul 8 alineatul (2) din Convenția europeană a drepturilor omului reprezintă cerințele minime pentru limitările legale ale dreptului la protecția datelor, potrivit Cartei. În consecință, prelucrarea legală a datelor cu caracter personal presupune ca, în temeiul dreptului european, cel puțin condițiile articolului 8 alineatul (2) din Convenția europeană a drepturilor omului să fie îndeplinite; cu toate acestea, dreptul european poate stabili dispoziții suplimentare pentru cazuri specifice.

117 Hotărârea CJUE din 9 noiembrie 2010 în cauzele conexate C-92/09 şi C-93/09, *Volker und Markus Schecke GbR (C-92/09) și Hartmut Eifert (C-93/09)/Land Hessen*, punctele 89 şi 86.

118 Regulamentul (CE) nr. 1290/2005 al Consiliului din 21 iunie 2005 privind finanțarea politicii agricole comune, MO 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 priveşte publicarea informațiilor referitoare la beneficiarii fondurilor provenite din Fondul European de Garantare Agricolă (FEGA) şi Fondul European Agricol pentru Dezvoltare Rurală (FEADR), MO 2008 L 76.

Corespondența între principiul prelucrării legale în temeiul dreptului european şi dispozițiile relevante ale Convenției europene a drepturilor omului este promovată şi prin articolul 6 alineatul (3) din TUE, care prevede că „drepturile fundamentale, astfel cum sunt garantate prin Convenția europeană pentru apărarea drepturilor omului şi a libertăților fundamentale [...], constituie principii generale ale dreptului Uniunii".

3.2. Principiul limitării şi specificității scopului

Puncte-cheie

- Scopul prelucrării datelor trebuie să fie definit în mod vizibil înainte de începerea prelucrării.
- În temeiul dreptului european, scopul prelucrării trebuie definite în mod explicit; în temeiul legislației CoE, acest aspect este de responsabilitatea legislației interne.
- Prelucrarea în scopuri nedefinite nu este în conformitate cu legislația privind protecția datelor.
- Utilizarea ulterioară a datelor pentru un alt scop necesită un temei juridic suplimentar în cazul în care scopul prelucrării este incompatibil cu cel inițial.
- Transferul de date către terți constituie un scop nou care necesită un temei juridic suplimentar.

În esență, principiul limitării şi specificității scopului înseamnă că legitimitatea prelucrării datelor cu caracter personal va depinde de scopul prelucrării[119]. Scopul trebuie să fie menționat şi evidențiat de operator înainte de începerea prelucrării datelor[120]. **În temeiul dreptului european**, acest lucru trebuie realizat fie printr-o declarație, altfel spus, printr-o notificare, către autoritatea de supraveghere competentă, fie, cel puțin, prin documentare internă care trebuie pusă la dispoziție de operator pentru a fi verificată de autoritățile de supraveghere şi accesată de persoana vizată.

Prelucrarea datelor cu caracter personal în scopuri nedefinite şi/sau nelimitate este ilegală.

119 Convenția 108, articolul 5 litera (b); Directiva privind protecția datelor, articolul 6 alineatul (1) litera (b).

120 A se vedea, de asemenea, Grupul de lucru Articolul 29 (2013), *Avizul 3/2013 privind limitarea scopului*, WP 203, Bruxelles, 2 aprilie 2013.

Orice scop nou de prelucrare a datelor trebuie să aibă propriul temei juridic special şi nu se poate baza pe faptul că datele au fost dobândite sau prelucrate inițial în alt scop legitim. În schimb, prelucrarea legitimă este limitată la scopul specificat inițial şi orice scop nou de prelucrare va necesita un nou temei juridic separat. Dezvăluirea datelor către terți va trebui analizată cu deosebită atenție, deoarece dezvăluirea va constitui, de regulă, un nou scop şi, prin urmare, va necesita un temei juridic diferit de cel pentru care au fost colectate datele.

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; şi cerințe alimentare speciale, cum ar fi alimente de tip kosher sau halal. În cazul în care companiilor aeriene li se solicită să transfere aceste date, care sunt incluse în registrele cu numele pasagerilor, către autoritățile în domeniul imigrației de la locul 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, transferul acestor date către o autoritate din domeniul imigrației va necesita un temei juridic nou şi separat.

Atunci când analizează întinderea şi limitele unui anumit scop, Convenția 108 şi Directiva privind protecția datelor recurg la conceptul de compatibilitate: utilizarea datelor în scopuri compatibile este permisă în baza temeiului juridic inițial. Cu toate acestea, semnificația „compatibilității" nu este definită şi lasă loc pentru interpretare de la caz la caz.

Exemplu: Vânzarea datelor privind clienții societății Sunshine obținute în timpul gestionării relației cu clienții (CRM) către o societate de marketing direct, societatea Moonlight, care doreşte să utilizeze aceste date pentru a oferi asistență campaniilor de marketing ale unor terțe societăți, constituie un scop nou, care nu este compatibil cu CRM, scopul inițial al societății Sunshine pentru colectarea datelor privind clienții. Prin urmare, vânzarea datelor către societatea Moonlight necesită un nou temei juridic.

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

Directiva privind protecția datelor declară în mod explicit că „prelucrarea ulterioară a datelor în scopuri istorice, statistice sau științifice nu este incompatibilă în măsura în care statele membre prevăd garanțiile adecvate”[121].

Exemplu: Societatea Sunshine a colectat și stocat date CRM 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.

În cazul în care aceleași date ar fi transmise unui terț, societatea Starlight, în scopuri exclusiv statistice, transferul ar fi permis în absența unui temei juridic suplimentar, dar numai în măsura în care sunt instituite garanții adecvate, cum ar fi ascunderea identității persoanelor vizate, întrucât identitățile nu sunt, de obicei, necesare în scopuri statistice.

3.3. Principiile calității datelor

Puncte-cheie

- Principiile calității datelor trebuie implementate de operator în cadrul tuturor operațiunilor de prelucrare.
- Principiul limitării duratei de păstrare a datelor face necesară ștergerea datelor imediat ce acestea nu mai servesc scopului pentru care au fost colectate.
- Excepțiile de la principiul limitării duratei de păstrare a datelor trebuie stabilite prin lege și necesită garanții speciale pentru protejarea datelor persoanelor vizate.

3.3.1. Principiul pertinenței datelor

Vor fi prelucrate numai datele care sunt „adecvate, pertinente și neexcesive în raport cu scopurile pentru care sunt colectate și/sau ulterior prelucrate”[122]. Categoriile de date alese pentru prelucrare trebuie să fie necesare pentru a atinge scopul

121 Un exemplu de astfel de dispoziții naționale este Legea austriacă privind protecția datelor (*Datenschutzgesetz*), Monitorul Oficial Federal I nr. 165/1999, punctul 46, disponibil în limba engleză la: www.dsk.gv.at/DocView.axd?CobId=41936.

122 Convenția 108, articolul 5 litera (c) și Directiva privind protecția datelor, articolul 6 alineatul (1) litera (c).

general declarat al operațiunilor de prelucrare, iar un operator ar trebui să limiteze colectarea de date strict la acele informații direct relevante pentru scopul specific urmărit de prelucrare.

În societatea contemporană, principiul pertinenței datelor are un argument suplimentar: prin utilizarea tehnologiei speciale de îmbunătățire a vieții private, uneori se poate evita complet utilizarea datelor cu caracter personal sau se pot folosi date pseudonimizate, ajungându-se astfel la o soluție adecvată pentru viața privată. Acest lucru este potrivit în special pentru sistemele de prelucrare mai extinse.

Exemplu: Consiliul local al unui oraş oferă o cartelă cu cip utilizatorilor frecvenți ai sistemului public de transport în schimbul unei taxe. Cartela poartă numele utilizatorului în formă scrisă pe suprafața cartelei şi, de asemenea, în format electronic, în cip. Ori de câte ori persoana foloseşte autobuzul sau tramvaiul, cartela cu cip trebuie validată cu ajutorul dispozitivelor de citire instalate, de exemplu, în autobuze şi tramvaie. Datele citite de dispozitiv sunt comparate electronic cu o bază de date care conține numele persoanelor care au cumpărat cartela de călătorie.

Acest sistem nu aderă la principiul pertinenței în mod optim: verificarea permisiunii unei persoane de a utiliza facilitățile de transport se poate realiza fără compararea datelor cu caracter personal de pe cipul cartelei cu baza de date. Ar fi suficientă, de exemplu, o imagine electronică specială, cum ar fi un cod de bare, în cipul cartelei care, la validarea cu ajutorul dispozitivului de citire, ar confirma valabilitatea cartelei. Un astfel de sistem nu înregistrează cine, când şi ce facilitate de transport a folosit. Nu sunt colectate date cu caracter personal, ceea ce reprezintă soluția optimă în sensul principiului pertinenței, întrucât acest principiu are ca rezultat obligația de a reduce la minim colectarea de date.

3.3.2. Principiul exactității datelor

Un operator care deține informații cu caracter personal nu va utiliza aceste informații fără a lua măsuri pentru a se asigura cu suficientă certitudine că datele sunt exacte şi actualizate.

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

Exemplu: O societate care comercializează mobilă a colectat date privind identitatea şi adresa unui client pentru transmiterea unei facturi. Şase luni mai târziu, aceeaşi societate doreşte să înceapă o campanie de marketing şi doreşte să intre în contact cu foştii clienți. Pentru a-i contacta, societatea doreşte să acceseze registrul național al rezidenților, care poate conține adresele actualizate, întrucât rezidenții sunt obligați prin lege să informeze registrul cu privire la adresa lor curentă. Accesul la datele incluse în acest registru este limitat la persoanele şi entitățile care pot oferi un motiv întemeiat.

În această situație, societatea nu poate utiliza argumentul conform căruia datele trebuie păstrate exacte şi actualizate pentru a susține că este îndreptățită să colecteze datele privind noile adrese ale tuturor foştilor săi clienți din registrul rezidenților. Datele au fost colectate în timpul facturării; pentru acest scop, adresa de la momentul vânzării este relevantă. Nu există niciun temei juridic pentru colectarea datelor privind noile adrese, întrucât marketingul nu reprezintă un interes care să surclaseze dreptul la protecția datelor şi, prin urmare, nu poate justifica accesarea datelor din registru.

Pot exista cazuri în care actualizarea datelor stocate să fie interzisă prin lege, întrucât scopul stocării datelor este, în principal, acela de a documenta evenimente.

Exemplu: Un raport medical de operare nu trebuie modificat, altfel spus, „actualizat", chiar dacă ulterior se dovedeşte că observațiile menționate în raport sunt greşite. În astfel de situații, pot fi făcute numai completări la observațiile raportului, atât timp cât acestea sunt marcate în mod clar ca fiind contribuții efectuate ulterior.

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

Exemplu: Dacă o persoană doreşte să încheie un contract cu o instituție bancară, atunci banca va verifica în mod normal bonitatea potențialului client. În acest sens există baze de date speciale, care conțin date privind istoricul de credibilitate al unor persoane particulare. Dacă o astfel de bază de date furnizează date incorecte sau care nu mai sunt de actualitate cu privire la o persoană, această persoană se poate confrunta cu probleme grave. Prin urmare, operatorii unor

astfel de baze de date depun eforturi deosebite pentru a respecta principiul exactității.

Mai mult, datele asociate unor suspiciuni, şi nu unor fapte, cum ar fi cercetările penale, pot fi colectate şi stocate atât timp cât operatorul are un temei juridic pentru colectarea acestor informații şi are suficiente justificări pentru formarea unei astfel de suspiciuni.

3.3.3. Principiul limitării duratei de păstrare a datelor

Articolul 6 alineatul (1) litera (e) din Directiva privind protecția datelor şi, de asemenea, articolul 5 litera (e) din Convenția 108 obligă statele membre să se asigure că datele cu caracter personal sunt „păstrate într-o formă care permite identificarea persoanelor vizate o perioadă nu mai lungă decât este necesar în vederea atingerii scopurilor pentru care au fost colectate datele sau pentru care vor fi prelucrate ulterior". Prin urmare, datele trebuie şterse după atingerea acestor scopuri.

În cauza *S. și Marper*, CEDO a concluzionat că principiile fundamentale ale instrumentelor relevante ale Consiliului Europei, precum şi dreptul şi practica celorlalte părți contractante impun proporționalitatea păstrării datelor în raport cu scopul colectării şi limitarea duratei de păstrare, în special în sectorul polițienesc[123].

Cu toate acestea, limitarea duratei de păstrare a datelor personale se aplică numai datelor păstrate într-o formă care permite identificarea persoanelor vizate. Prin urmare, păstrarea legală a datelor care nu mai sunt necesare se poate realiza prin anonimizare sau pseudonimizare.

În Directiva privind protecția datelor, păstrarea datelor pentru viitoare utilizări ştiințifice, istorice sau statistice este exceptată în mod explicit de la principiul limitării duratei de păstrare a datelor[124]. Cu toate acestea, o astfel de stocare şi utilizare continuă a datelor cu caracter personal trebuie să fie însoțită de garanții speciale, în conformitate cu legislația națională.

123 Hotărârea CEDO din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 şi 30566/04; a se vedea, de exemplu, şi Hotărârea CEDO din 13 noiembrie 2012 în cauza *M.M./Regatul Unit*, nr. 24029/07.

124 Directiva privind protecția datelor, articolul 6 alineatul (1) litera (e).

3.4. Principiul prelucrării corecte

Puncte-cheie

- Prelucrarea corectă înseamnă transparența prelucrării, în special față de persoanele vizate.
- Operatorii trebuie să informeze persoanele vizate înainte de a le prelucra datele, cel puțin cu privire la scopul prelucrării şi la identitatea şi adresa operatorului.
- Cu excepția cazului în care legea permite în mod special acest lucru, prelucrarea datelor nu se realizează în secret sau pe ascuns.
- Persoanele vizate au dreptul să își acceseze datele indiferent de locul în care sunt prelucrate acestea.

Principiul prelucrării corecte guvernează în principal relația dintre operator şi persoana vizată.

3.4.1. Transparența

Acest principiu stabileşte obligația operatorului de a informa persoanele vizate cu privire la modul în care le sunt utilizate datele.

Exemplu: În cauza *Haralambie/România*[125], reclamantul a solicitat accesul la un dosar pe care organizația serviciilor secrete l-a păstrat cu privire la persoana sa, însă solicitarea a fost onorată abia după cinci ani. CEDO a reiterat că persoanele care fac obiectul dosarelor personale deținute de autoritățile publice au un interes vital în a le putea accesa. Autoritățile aveau datoria de a asigura o procedură eficientă pentru obținerea accesului la aceste informații. CEDO a considerat că nici cantitatea dosarelor transferate şi nici deficiențele sistemului de arhivare nu justifică o întârziere de cinci ani în acordarea accesului reclamantului la dosarele care îl privesc. Autoritățile nu au asigurat reclamantului o procedură eficientă şi accesibilă pentru a-i permite să obțină accesul la dosarele personale într-o perioadă de timp rezonabilă. Curtea a concluzionat că articolul 8 din Convenția europeană a drepturilor omului a fost încălcat.

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

Operațiunile de prelucrare trebuie să fie explicate persoanelor vizate într-o manieră accesibilă, care să garanteze că aceştia înțeleg ceea ce se va întâmpla cu datele lor. O persoană vizată are dreptul, de asemenea, să i se comunice de către un operator, la cerere, dacă îi sunt prelucrate datele şi, dacă da, care sunt acestea.

3.4.2. Stabilirea unei relații de încredere

Operatorii ar trebui să dovedească, față de persoanele vizate şi de publicul larg, că prelucrarea de date se va efectua în mod legal şi transparent. Operațiunile de prelucrare nu trebuie realizate în secret şi nu trebuie să aibă efecte negative imprevizibile. Operatorii trebuie să asigure informarea clienților sau a cetățenilor cu privire la utilizarea datelor acestora. Mai mult decât atât, operatorii trebuie să acționeze, în măsura în care este posibil, astfel încât să satisfacă prompt dorințele persoanelor vizate, în special în cazurile în care consimțământul acestora constituie temeiul juridic pentru prelucrarea datelor.

Exemplu: În cauza *K.H. și alții/Slovacia*[126], reclamantele au fost opt femei de etnie romă care au fost tratate în două spitale din estul Slovaciei în timpul sarcinii şi naşterii. Ulterior, niciuna dintre acestea nu a mai putut rămâne însărcinată, în ciuda încercărilor repetate. Instanțele naționale au ordonat spitalelor să permită reclamantelor şi reprezentanților acestora să consulte şi să realizeze extrase de mână ale evidențelor medicale, dar au respins cererea acestora de a fotocopia documentele, invocând motivul prevenirii abuzurilor. Obligațiile absolute ale statului în temeiul articolului 8 din Convenția europeană a drepturilor omului includ neapărat obligația de a pune la dispoziția persoanelor vizate copii ale dosarelor cu datele acestora. Statul avea îndatorirea de a stabili aranjamentele pentru copierea dosarelor cu datele personale sau, după caz, de a prezenta motive convingătoare pentru refuzul de a acționa în consecință. În cazul reclamantelor, instanțele interne au justificat interzicerea realizării unor copii ale evidențelor medicale în principal prin nevoia de a proteja informațiile relevante împotriva abuzurilor. Cu toate acestea, CEDO nu a înțeles modul în care reclamantele, cărora li s-a acordat oricum accesul la dosarele lor medicale complete, ar fi putut abuza de informații care le priveau. Mai mult, riscul unui astfel de abuz ar fi putut fi prevenit prin alte mijloace decât refuzul fotocopierii dosarelor reclamantelor, cum ar fi prin limitarea numărului de persoane îndreptățite să acceseze dosarele. Statul nu a putut demonstra existența unor motive suficient

126 Hotărârea CEDO din 6 noiembrie 2009 în cauza *K.H. și alții/Slovacia*, nr. 32881/04.

de convingătoare pentru a respinge accesul efectiv al reclamantelor la informațiile privind starea lor de sănătate. Curtea a concluzionat că articolul 8 a fost încălcat.

În legătură cu serviciile de internet, caracteristicile sistemelor de prelucrare a datelor trebuie să permită persoanelor vizate să înțeleagă efectiv ce se întâmplă cu datele lor.

Prelucrarea corectă înseamnă, de asemenea, că operatorii sunt pregătiți să depășească cerințele juridice minime obligatorii de serviciu pentru persoanele vizate, în cazul în care interesele legitime ale persoanelor vizate impun acest lucru.

3.5. Principiul responsabilității

Puncte-cheie

- Responsabilitatea presupune implementarea activă a unor măsuri de către operatori pentru promovarea și garantarea protecției datelor în timpul activităților lor de prelucrare.
- Operatorii sunt responsabili pentru conformitatea operațiunilor lor de prelucrare cu legislația privind protecția datelor.
- Operatorii trebuie să poată demonstra în orice moment conformitatea cu dispozițiile privind protecția datelor persoanelor vizate, publicului larg și autorităților de supraveghere.

Organizația pentru Cooperare și Dezvoltare Economică (OCDE) a adoptat în 2013 orientări privind viața privată care au scos în evidență faptul că operatorii au un rol important în aplicarea protecției datelor. Orientările elaborează un principiu al responsabilității în sensul că „un operator de date trebuie să fie responsabil pentru conformitatea cu măsurile care dau efect principiilor [materiale] susmenționate”[127].

Întrucât Convenția 108 nu face nicio referire la responsabilitatea operatorilor, lăsând acest subiect, în esență, în seama dreptului intern, articolul 6 alineatul (2) din Directiva privind protecția datelor menționează că operatorii trebuie să asigure conformitatea cu principiile referitoare la calitatea datelor incluse la alineatul 1.

127 OCDE (2013), *Orientări privind reglementarea protecției vieții private și a fluxurilor transfrontaliere de date cu caracter personal*, articolul 14.

Exemplu: Un exemplu legislativ pentru evidențierea principiului responsabilității este modificarea din 2009[128] la Directiva privind protecția vieții private în sectorul comunicațiilor electronice 2002/58/CE. Potrivit articolului 4 din forma sa modificată, directiva impune obligația de punere în aplicare a unei politici de securitate, şi anume de „a asigura punerea în aplicare a unei politici de securitate în ceea ce priveşte prelucrarea datelor cu caracter personal". Astfel, în ceea ce priveşte dispozițiile de securitate ale acestei directive, legiuitorul a decis că este necesară introducerea unei cerințe explicite pentru elaborarea şi punerea în aplicare a unei politici de securitate.

În conformitate cu avizul Grupului de lucru Articolul 29[129], esența responsabilității este obligația operatorului de a:

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

- pregăti documentația care dovedeşte persoanelor vizate şi autorităților de supraveghere ce măsuri au fost luate în vederea respectării normelor de protecție a datelor.

Principul responsabilității obligă astfel operatorii să demonstreze activ conformitatea şi să nu aştepte ca persoanele vizate sau autoritățile de supraveghere să scoată în evidență deficiențele.

128 Directiva 2009/136/CE a Parlamentului European şi a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal şi drepturile utilizatorilor cu privire la rețelele şi serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale şi protejarea confidențialității în sectorul comunicațiilor publice şi a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului, MO 2009 L 337, p. 11.

129 Grupul de lucru Articolul 29, *Avizul 3/2010 privind principiul responsabilității*, WP 173, Bruxelles, 13 iulie 2010.

4

Normele legislației europene privind protecția datelor

UE	Aspecte vizate	CoE
Norme privind prelucrarea legală a datelor nesensibile		
Directiva privind protecția datelor, articolul 7 litera (a)	**Consimțământ**	Recomandarea privind crearea de profile, articolul 3.4 litera (b) și articolul 3.6
Directiva privind protecția datelor, articolul 7 litera (b)	**Relație (pre) contractuală**	Recomandarea privind crearea de profile, articolul 3.4 litera (b)
Directiva privind protecția datelor, articolul 7 litera (c)	**Obligațiile legale ale operatorului**	Recomandarea privind crearea de profile, articolul 3.4 litera (a)
Directiva privind protecția datelor, articolul 7 litera (d)	**Interesele vitale ale persoanei vizate**	Recomandarea privind crearea de profile, articolul 3.4 litera (b)
Directiva privind protecția datelor, articolul 7 litera (e) și articolul 8 alineatul (4) CJUE, C-524/06, *Huber/Bundesrepublik Deutschland*, 16 decembrie 2008	**Interesul public și exercitarea autorității oficiale**	Recomandarea privind crearea de profile, articolul 3.4 litera (b)
Directiva privind protecția datelor, articolul 7 (f), articolul 8 alineatele (2) și (3) CJUE, 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*, 24 noiembrie 2011	**Interesele legitime ale altora**	Recomandarea privind crearea de profile, articolul 3.4 litera (b)

UE	Aspecte vizate	CoE
Norme privind prelucrarea legală a datelor sensibile		
Directiva privind protecția datelor, articolul 8 alineatul (1)	Interdicție generală de prelucrare	Convenția 108, articolul 6
Directiva privind protecția datelor, articolul 8 alineatele (2)(4)	Excepțări de la interdicția generală	Convenția 108, articolul 6
Directiva privind protecția datelor, articolul 8 alineatul (5)	Prelucrarea datelor privind condamnările penale	Convenția 108, articolul 6
Directiva privind protecția datelor articolul 8 alineatul (7)	Numere de identificare pentru prelucrare	
Norme privind prelucrarea securizată		
Directiva privind protecția datelor, articolul 17	Obligația de a asigura prelucrarea securizată	Convenția 108, articolul 7 CEDO, *I./Finlanda*, nr. 20511/03, 17 iulie 2008
Directiva privind protecția vieții private în sectorul comunicațiilor electronice, articolul 4 alineatul (2)	Notificări privind încălcarea securității datelor	
Directiva privind protecția datelor, articolul 16	Obligația de confidențialitate	
Norme privind transparența prelucrării		
	Transparența în general	Convenția 108, articolul 8 (a)
Directiva privind protecția datelor, articolele 10 și 11	Informare	Convenția 108, articolul 8 litera (a)
Directiva privind protecția datelor, articolele 10 și 11	Excepții de la obligația de informare	Convenția 108, articolul 9
Directiva privind protecția datelor, articolele 18 și 19	Notificare	Recomandarea privind crearea de profile, articolul 9.2 litera (a)
Norme privind promovarea conformității		
Directiva privind protecția datelor, articolul 20	Verificare prealabilă	
Directiva privind protecția datelor, articolul 18 alineatul (2)	Responsabili de protecția datelor cu caracter personal	Recomandarea privind crearea de profile, articolul 8.3
Directiva privind protecția datelor, articolul 27	Coduri de conduită	

Principiile au, în mod necesar, caracter general. Aplicarea lor unor situații concrete lasă o anumită marjă de interpretare şi alegere a mijloacelor. În temeiul **legislației CoE**, este la latitudinea părților la Convenția 108 să clarifice această marjă de interpretare în cadrul legislațiilor lor interne. Situația în temeiul **dreptului european** este diferită: pentru stabilirea protecției datelor în cadrul pieței interne, s-a considerat necesară elaborarea unor norme detaliate la nivel european pentru armonizarea nivelului de protecție a datelor din cadrul legislațiilor naționale ale statelor membre. Directiva privind protecția datelor stabileşte, în temeiul principiilor prevăzute la articolul 6, un nivel de norme detaliate care trebuie aplicate fidel în legislația națională. Aşadar, următoarele observații privind normele detaliate de protecție a datelor la nivel european vizează în mod predominant dreptul european.

4.1. Normele privind prelucrarea legală

Puncte-cheie

- Datele cu caracter personal pot fi prelucrate legal dacă:
  - prelucrarea se bazează pe consimțământul persoanei vizate sau
  - interesele vitale ale persoanelor vizate necesită prelucrarea datelor lor sau
  - interesele legitime ale altora constituie motivul prelucrării, însă numai în măsura în care nu prevalează interesele de protejare a drepturilor fundamentale ale persoanelor vizate.
- Prelucrarea legală a datelor sensibile cu caracter personal se supune unui regim special, mai strict.

Directiva privind protecția datelor conține două seturi diferite de norme pentru prelucrarea legală a datelor: unul pentru date nesensibile, la articolul 7, şi unul pentru date sensibile, la articolul 8.

4.1.1. Prelucrarea legală a datelor nesensibile

Capitolul II din Directiva 95/46, intitulat „Condițiile generale de legalitate a prelucrării datelor cu caracter personal", prevede că, sub rezerva excepțiilor permise în temeiul articolului 13, toate prelucrările de date cu caracter personal trebuie să fie conforme, în primul rând, cu principiile referitoare la calitatea datelor prevăzute la articolul 6 din Directiva privind protecția datelor şi, în al doilea rând, cu unul dintre criteriile privind

legitimitatea prelucrării datelor enumerate la articolul 7[130]. Astfel se explică situațiile care legitimează prelucrarea datelor nesensibile cu caracter personal.

Consimțământul

În temeiul legislației CoE, consimțământul nu este prevăzut la articolul 8 din Convenția europeană a drepturilor omului şi nici în Convenția 108. Este, totuşi, menționat în jurisprudența CEDO şi în mai multe recomandări ale Consiliului Europei. **În temeiul dreptului european**, consimțământul, ca temei pentru prelucrarea legitimă a datelor, este stabilit ferm la articolul 7 litera (a) din Directiva privind protecția datelor şi este menționat în mod explicit şi în articolul 8 din Cartă.

Relația contractuală

Un alt temei pentru prelucrarea legitimă a datelor cu caracter personal **în temeiul dreptului european**, enumerat la articolul 7 litera (b) din Directiva privind protecția datelor, este legat de „[necesitatea] pentru executarea unui contract la care subiectul datelor este parte". Această dispoziție reglementează şi relațiile precontractuale. De exemplu: o parte intenționează să încheie un contract, însă nu a făcut-o încă, posibil din cauza unor verificări rămase de finalizat. În cazul în care una dintre părți trebuie să prelucreze date în acest scop, această prelucrare este legitimă în măsura în care „există posibilitatea luării unor măsuri, la cererea persoanei vizate, înainte de încheierea contractului".

În temeiul legislației CoE, „protecția drepturilor şi libertăților altora" este prevăzută la articolul 8 alineatul (2) din Convenția europeană a drepturilor omului ca motiv pentru intervenția legitimă în dreptul la protecția datelor.

Obligațiile legale ale operatorului

Dreptul european menționează în continuare în mod explicit un alt criteriu privind legitimizarea prelucrării datelor, şi anume „necesitatea îndeplinirii unei obligații legale care îi revine operatorului" [articolul 7 litera (c) din Directiva privind protecția datelor]. Această dispoziție se referă la operatorii care îşi desfăşoară activitatea în

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

sectorul privat; obligațiile legale ale operatorilor de date din sectorul privat intră sub incidența articolului 7 litera (e) din directivă. Există multe cazuri în care operatorii din sectorul privat sunt obligați prin lege să prelucreze date despre alte persoane, de exemplu, medicii şi spitalele au obligația legală de a stoca date privind tratamentul pacienților pentru mai mulți ani, angajatorii trebuie să prelucreze datele angajaților din motive de securitate socială şi fiscală, iar întreprinderile trebuie să prelucreze datele clienților din motive de impozitare.

În contextul transferului obligatoriu al datelor privind pasagerii de către companiile aeriene către autoritățile străine privind controlul imigrației, a apărut întrebarea dacă obligațiile legale în temeiul *legislației* străine ar putea constitui sau nu un temei legal pentru prelucrarea datelor în temeiul dreptului european (acest aspect este discutat în detaliu în secţiunea 6.2).

Obligațiile legale ale operatorului servesc drept temei juridic pentru prelucrarea legitimă a datelor şi **în temeiul legislației CoE.** Astfel cum a fost 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 în articolul 8 alineatul (2) din Convenția europeană a drepturilor omului. Exemplul de mai sus este, prin urmare, relevant şi pentru legislația CoE.

Interesele vitale ale persoanei vizate

În temeiul dreptului european, articolul 7 litera (d) din Directiva privind protecția datelor prevede că prelucrarea datelor cu caracter personal este legală dacă este „necesară în scopul protejării interesului vital al persoanei vizate". Acest interes, strâns legat de supraviețuirea persoanei vizate, poate constitui baza utilizării legitime a datelor privind starea de sănătate sau despre persoane dispărute, de exemplu.

În temeiul legislației CoE, interesul vital al persoanei vizate nu este menționat în articolul 8 din Convenția europeană a drepturilor omului ca motiv pentru intervenția legitimă asupra dreptului la protecția datelor. Cu toate acestea, în unele recomandări ale CoE care completează Convenția 108 în anumite domenii, interesul vital al persoanei vizate este menționat explicit ca bază pentru prelucrarea legitimă a datelor[131]. Interesul vital al persoanei vizate este evident considerat implicit setului de motive

131 Recomandarea privind crearea de profile, articolul 3.4 litera (b).

care justifică prelucrarea datelor: protecția drepturilor fundamentale nu ar trebui să pună niciodată în pericol interesul vital al persoanei protejate.

Interesul public și exercitarea autorității oficiale

Având în vedere multitudinea de modalități posibile de organizare a afacerilor publice, articolul 7 litera (e) din **Directiva privind protecția datelor** prevede că datele cu caracter personal pot fi prelucrate legal dacă acest lucru „este necesar pentru aducerea la îndeplinire a unei sarcini de interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul sau terțul căruia îi sunt comunicate datele [...].[132].

Exemplu: În cauza *Huber/Bundesrepublik Deutschland*[133], domnul Huber, resortisant austriac cu reşedința în Germania, a solicitat Oficiului Federal pentru Migrație şi Refugiați să șteargă datele sale din Registrul Central al Cetățenilor Străini („AZR"). Registrul, care conține date cu caracter personal ale resortisanților UE care nu sunt cetățeni germani, dar au reşedința în Germania de mai mult de trei luni, este utilizat în scopuri statistice şi de autoritățile judiciare şi de aplicare a legii atunci când cercetează şi urmăresc penal activitățile infracționale sau cele care amenință siguranța publică. Instanța de trimitere a întrebat dacă prelucrarea datelor cu caracter personal care este întreprinsă în cadrul unui registru precum Registrul Central al Cetățenilor Străini, la care au acces şi alte autorități publice, este compatibilă cu dreptul european, având în vedere că nu există un astfel de registru pentru resortisanții germani.

CJUE susține în primul rând că, în temeiul articolului 7 litera (e) din directivă, datele cu caracter personal pot fi prelucrate legal numai dacă este necesar pentru aducerea la îndeplinire a unei sarcini de interes public sau care rezultă din exercitarea autorității publice.

Potrivit Curții, „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 [...] nu poate avea un conținut care să varieze în funcție de statele membre. Este vorba, aşadar, despre o noțiune autonomă de drept comunitar, care trebuie să primească o

132 A se vedea şi Directiva privind protecția datelor, considerentul 32.

133 Hotărârea CJUE din 16 decembrie 2008 în cauza *Huber/Bundesrepublik Deutschland*, C-524/06.

interpretare de natură să reflecte pe deplin obiectul acestei directive, astfel cum este definit la articolul 1 alineatul (1) din aceasta”[134].

Curtea remarcă faptul 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 şi condiții impuse prin Tratat şi 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 şedere, acest registru nu trebuie să conțină informații, altele decât cele necesare în acest scop specific. Curtea concluzionează că acest sistem de prelucrare a datelor cu caracter personal este în conformitate cu dreptul european în cazul în care conține numai datele necesare aplicării acestei legislații, iar structura sa centralizată contribuie la eficientizarea implementării acestei legislații. Instanța națională trebuie să constate dacă aceste condiții sunt îndeplinite în speță. Dacă nu sunt îndeplinite, stocarea şi prelucrarea datelor cu caracter personal într-un registru precum AZR în scopuri statistice nu poate fi considerată, în niciun caz, necesară în sensul articolului 7 litera (e) din Directiva 95/46/CE[135].

În cele din urmă, referitor la aspectul privind utilizarea datelor incluse în registru în scopul combaterii criminalității, Curtea susține că acest obiectiv „are în vedere în mod necesar anchetarea infracțiunilor comise, indiferent de cetățenia autorilor acestora”. Registrul în cauză nu include date personale ale resortisanților statului membru în cauză, iar această diferență de tratament constituie discriminare, interzisă prin articolul 18 din TFUE. În consecință, această dispoziție, astfel cum este interpretată de Curte, „se opune instituirii de către un stat membru, în vederea combaterii criminalității, a unui sistem specific de prelucrare a datelor cu caracter personal care priveşte cetățenii Uniunii care nu sunt resortisanți ai acestui stat membru”[136].

Utilizarea datelor cu caracter personal de către autoritățile care acționează în domeniul public se supune, de asemenea, articolului 8 din Convenția europeană a drepturilor omului.

134 *Ibidem*, punctul 52.

135 *Ibidem*, punctele 54, 58, 59, 66-68.

136 *Ibidem*, punctele 78 şi 81.

Interesele legitime urmărite de operator sau de un terț

Persoana vizată nu este singura cu interese legitime. Articolul 7 litera(f) din Directiva privind protecția datelor prevede că datele cu caracter personal pot fi prelucrate legal dacă „este necesar pentru realizarea interesului legitim urmărit de operator sau de către unul sau mai mulți terți, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protecție [...]".

În cadrul următoarei hotărâri, CJUE s-a pronunțat în mod explicit cu privire la articolul 7 litera (f) din directivă:

Exemplu: În cauza *ASNEF și FECEMD*[137], CJUE a clarificat faptul că legislația națională nu are dreptul să adauge condiții la cele prevăzute în articolul 7 litera (f) din directivă pentru prelucrarea legală a datelor. Aceasta a făcut referire la 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 se regăseau deja în surse publice.

Curtea a remarcat, în primul rând, că Directiva 95/46 este destinată să asigure un nivel echivalent de protecție a drepturilor și libertăților persoanelor cu privire la prelucrarea datelor cu caracter personal în toate statele membre. Apropierea legislațiilor naționale aplicabile în acest domeniu nu trebuie să aibă ca rezultat scăderea protecției pe care o oferă, ci trebuie, dimpotrivă, să aibă drept obiectiv asigurarea unui nivel înalt de protecție în Uniune[138]. În consecință, CJUE a considerat că „din obiectivul constând în asigurarea unui nivel de protecție echivalent în toate statele membre rezultă că articolul 7 din Directiva 95/46 prevede o listă exhaustivă și limitativă de cazuri în care o prelucrare de date cu caracter personal poate fi considerată ca fiind legală". Mai mult decât atât, „statele membre nu pot nici să adauge principii noi privind legitimarea prelucrărilor de date cu caracter personal la articolul 7 din Directiva 95/46, nici să prevadă cerințe suplimentare care să modifice conținutul unuia dintre cele șase principii prevăzute

137 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*.

138 *Ibidem*, punctul 28. A se vedea și Directiva privind protecția datelor, considerentele 8 și 10.

la acest articol”[139]. Curtea 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 de prelucrarea în cauză poate varia în funcție de împrejurarea dacă datele în cauză sunt sau nu deja conținute în surse publice”.

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, Curtea a concluzionat că „articolul 7 litera (f) din Directiva 95/46 trebuie interpretat în sensul că se opune unei reglementări naționale care, în lipsa consimțământului persoanei vizate 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”[140].

Formulări similare sunt disponibile în recomandările CoE. Recomandarea privind crearea de profile confirmă prelucrarea datelor cu caracter personal în scopul creării de profile legitime, în măsura în care prelucrarea este necesară în scopul intereselor legitime ale altora, „cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanelor vizate”[141].

4.1.2. Prelucrarea legală a datelor sensibile

Legislația CoE lasă la aprecierea legislației interne stabilirea protecției adecvate pentru utilizarea datelor sensibile, în timp ce **dreptul european,** în articolul 8 din Directiva privind protecția datelor, conține un regim detaliat pentru prelucrarea unor categorii speciale de date, care dezvăluie: originea rasială sau etnică, opiniile politice,

139 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 30 și 32.

140 *Ibidem*, punctele 40, 44, 48 și 49.

141 Recomandarea privind crearea de profile, articolul 3.4 litera (b).

convingerile religioase sau filozofice, apartenența sindicală, precum și informații privind starea de sănătate sau viața sexuală. Prelucrarea datelor sensibile este, în principiu, interzisă[142]. Cu toate acestea, există o listă exhaustivă de excepțări de la această interdicție, disponibilă la articolul 8 alineatele (2) și (3) din directivă. Aceste excepțări includ consimțământul explicit al persoanei vizate, interesele vitale ale persoanei vizate, interesele legitime ale altora și interesul public.

Spre deosebire de cazul prelucrării datelor nesensibile, o relație contractuală cu persoana vizată nu este considerată ca fiind un temei juridic general pentru prelucrarea legitimă a datelor sensibile. Prin urmare, dacă datele sensibile urmează a fi prelucrate în contextul unui contract încheiat cu persoana vizată, utilizarea acestor date necesită consimțământul explicit distinct al persoanei vizate, în plus față de acordul de a încheia contractul. Cu toate acestea, solicitarea explicită a persoanei vizate pentru produse sau servicii care dezvăluie în mod necesar date sensibile ar trebui considerată la fel de bună ca un consimțământ explicit.

Exemplu: În cazul în care pasagerul unei companii aeriene, în contextul rezervării unui zbor, solicită companiei aeriene să îi pună la dispoziție un scaun cu rotile și alimente de tip kosher, compania aeriană are dreptul să utilizeze aceste date chiar dacă pasagerul nu a semnat o clauză suplimentară de consimțământ prin care să consimtă la utilizarea datelor sale care dezvăluie informații despre starea de sănătate și convingerile religioase.

Consimțământul explicit al persoanei vizate

Prima condiție pentru prelucrarea legală a oricăror date, indiferent dacă sunt date nesensibile sau sensibile, este consimțământul persoanei vizate. În cazul datelor sensibile, acest consimțământ trebuie să fie explicit. Cu toate acestea, legislația națională poate prevedea că acordarea consimțământului pentru utilizarea datelor sensibile nu reprezintă un temei juridic suficient pentru a permite prelucrarea acestora[143], de exemplu, atunci când, în cazuri excepționale, prelucrarea implică riscuri neobișnuite pentru persoana vizată.

Într-un caz special, chiar și consimțământul implicit este recunoscut drept temei juridic pentru prelucrarea datelor sensibile: Articolul 8 alineatul (2) litera (e) din directivă prevede că prelucrarea nu este interzisă atunci când se referă la date care sunt

142 Directiva privind protecția datelor, articolul 8 alineatul (1).

143 *Ibidem,* articolul 8 alineatul (2) litera (a).

făcute publice de către persoanele vizate în mod manifest. Această dispoziție presupune în mod evident că dezvăluirea de către persoana vizată a datelor sale trebuie interpretată ca implicând consimțământul persoanei vizate pentru utilizarea acestor date.

Interesele vitale ale persoanei vizate

La fel ca în cazul datelor nesensibile, datele sensibile pot fi prelucrate datorită intereselor vitale ale persoanei vizate[144].

Pentru ca prelucrarea datelor sensibile să fie legitimă pe această bază, este necesar ca persoana vizată să fie în imposibilitatea de a decide asupra prelucrării, deoarece este inconştientă sau este absentă şi nu a putut fi contactată.

Interesele legitime ale altora

La fel ca în cazul datelor nesensibile, interesele legitime ale altora pot servi drept temei pentru prelucrarea datelor sensibile. Cu toate acestea, pentru datele sensibile şi în conformitate cu articolul 8 alineatul (2) din Directiva privind protecția datelor, acest lucru este valabil numai în următoarelor cazuri:

- prelucrarea este necesară datorită intereselor vitale ale unei alte persoane[145], atunci când persoana vizată este incapabilă fizic sau juridic de a consimți;

- datele sensibile sunt relevante în materie de drept al muncii, cum ar fi datele privind starea de sănătate în contextul unui loc de muncă deosebit de periculos sau datele privind convingerile religioase în contextul sărbătorilor[146];

- în cazul fundațiilor, asociațiilor sau al oricăror alte organisme cu scop nelucrativ şi cu specific politic, filozofic, religios sau sindical, care prelucrează datelor membrilor sau sponsorilor acestora sau ale altor părți interesate (aceste date sunt sensibile deoarece sunt susceptibile să dezvăluie convingerile religioase sau politice ale persoanelor în cauză)[147];

144 *Ibidem*, articolul 8 alineatul (2) litera (c).

145 *Ibidem.*

146 *Ibidem,* articolul 8 alineatul (2) litera (b).

147 *Ibidem,* articolul 8 alineatul (2) litera (d).

- în cazul în care datele sensibile sunt utilizate în contextul procedurilor juridice înaintea unei instanțe sau a unei autorități administrative pentru constatarea, exercitarea sau apărarea unui drept în justiție[148].

- De asemenea, conform articolului 8 alineatul (3) din Directiva privind protecția datelor, atunci când datele medicale sunt utilizate pentru controale medicale și administrarea de tratamente de către furnizorii de asistență medicală, gestionarea acestor servicii se supune acestei exceptări. Ca o garanție specială, persoanele sunt recunoscute drept „furnizori de asistență medicală" numai dacă se supun unor obligații profesionale de confidențialitate specifice.

Interesul public

În plus, în conformitate cu articolul 8 alineatul (4) din Directiva privind protecția datelor, statele membre pot prevedea scopuri suplimentare pentru prelucrarea datelor sensibile, atâta timp cât:

- datele sunt prelucrate pentru un motiv de interes public important;

- se prevede astfel prin legislația internă sau prin decizia autorității de supraveghere și

- legislația internă sau decizia autorității de supraveghere include garanții corespunzătoare în vederea protejării efective a intereselor persoanelor vizate[149].

Un exemplu elocvent îl constituie sistemele electronice de date medicale, care urmează a fi instituite în multe state membre. 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.

Grupul de lucru Articolul 29 a concluzionat că aceste sisteme nu pot fi instituite în conformitate cu normele juridice existente privind prelucrarea datelor pacienților, în baza articolului 8 alineatul (3) din Directiva privind protecția datelor. Cu toate acestea, presupunând că existența acestor sisteme electronice de date medicale constituie un motiv de interes public important, se poate întemeia pe articolul 8

148 *Ibidem*, articolul 8 alineatul (2) litera (e).

149 *Ibidem*, articolul 8 alineatul (4).

alineatul (4) din directivă, necesitând un temei juridic explicit pentru instituirea lor, care să includă şi garanțiile corespunzătoare pentru operarea în siguranță a sistemului[150].

4.2. Normele privind securitatea prelucrării

Puncte-cheie

- Normele privind securitatea prelucrării implică obligarea operatorului şi a persoanei împuternicite de către operator de a implementa măsuri tehnice şi organizatorice adecvate pentru prevenirea unei intervenții neautorizate asupra operațiunilor de prelucrare a datelor.
- Nivelul necesar de securitate a datelor este stabilit de:
  - elementele de securitate disponibile pe piață pentru orice tip specific de prelucrare;
  - costuri şi
  - sensibilitatea datelor prelucrate.
- Prelucrarea securizată a datelor este garantată în plus prin obligația generală a tuturor persoanelor, operatorilor sau persoanelor împuternicite de către operatori de a asigura confidențialitatea datelor.

Obligarea operatorilor şi a persoanelor împuternicite de către operatori de a implementa măsuri adecvate pentru asigurarea securității datelor este, aşadar, prevăzută de **legislația CoE privind protecția datelor,** precum şi **în legislația europeană privind protecția datelor**.

4.2.1. Elementele securității datelor

Potrivit dispozițiilor relevante din **legislația europeană**:

> *„Statele membre prevăd aplicarea obligatorie de către operator a unor măsuri tehnice și organizatorice de protecție adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale,*

150 Grupul de lucru Articolul 29 (2007), *Document de lucru privind prelucrarea datelor medicale cu caracter personal din dosarul electronic de sănătate (DES)*, WP 131, Bruxelles, 15 februarie 2007.

pierderii accidentale, modificării, dezvăluirii sau accesului neautorizat, în special atunci când prelucrarea presupune transmiterea datelor într-o rețea, precum și împotriva oricărei alte forme de prelucrare ilegală"[151].

O dispoziție similară există, de asemenea, în **legislația CoE**:

„Măsuri adecvate de securitate sunt luate pentru protejarea datelor cu caracter personal înregistrate în fișierele automatizate împotriva distrugerii accidentale sau neautorizate, sau a pierderii accidentale, cât și împotriva accesului, modificării sau difuzării neautorizate"[152].

Deseori, există, de asemenea, standarde industriale, naționale şi 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 a explorat posibilitățile de certificare a produselor, în special a produselor software, ca fiind conforme cu legislația europeană privind protecția datelor. Agenția Uniunii Europene pentru Securitatea Rețelelor şi a Informațiilor (ENISA) a fost înființată pentru consolidarea capacității UE, a statelor membre UE şi a comunității de afaceri în vederea prevenirii, abordării şi soluționării problemelor legate de securitatea rețelelor şi a informațiilor[153]. ENISA publică periodic analize ale amenințărilor actuale la adresa securității şi recomandări cu privire la modul în care acestea trebuie abordate.

Securitatea datelor nu se realizează numai prin implementarea echipamentelor corespunzătoare hardware şi software. Aceasta necesită şi 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 şi obligațiile acestora în baza legislației privind protecția datelor, în special obligațiile lor de confidențialitate;

- distribuirea clară a responsabilităților şi sublinierea clară a competențelor în materie de prelucrare a datelor, în special cu privire la deciziile de prelucrare a datelor cu caracter personal şi de transfer al datelor către terți;

151 Directiva privind protecția datelor, articolul 17 alineatul (1).

152 Convenția 108, articolul 7.

153 Regulamentul (CE) nr. 460/2004 al Parlamentului European şi al Consiliului din 10 martie 2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice şi a Datelor, MO 2004 L 77.

- utilizarea datelor cu caracter personal numai în conformitate cu instrucțiunile persoanei competente sau în conformitate cu normele generale puse în aplicare;

- protejarea accesului în spațiile şi la echipamentele hardware şi software ale operatorului sau ale persoanei împuternicite de către operator, inclusiv verificări ale autorizației de acces;

- asigurarea faptului că autorizațiile de acces la date cu caracter personal au fost acordate de către persoana competentă şi necesită documentație adecvată;

- protocoale automatizate privind accesul la date cu caracter personal prin mijloace electronice şi verificări periodice ale acestor protocoale prin intermediul departamentului intern de supraveghere;

- documentarea atentă pentru forme de dezvăluire, altele decât accesul automatizat la date pentru a putea demonstra că nu a fost efectuat niciun transfer ilegal.

Instruirea şi formarea adecvată a membrilor personalului în domeniul securității datelor reprezintă, de asemenea, o măsură importantă de securitate efectivă. Procedurile de verificare trebuie, de asemenea, implementate pentru a garanta că măsurile adecvate nu există numai pe hârtie, ci şi în practică (cum ar fi audituri interne sau externe).

Măsurile de îmbunătățire a nivelului de securitate al unui operator sau persoane împuternicite de către operator includ instrumente, cum ar fi responsabili de protecția datelor cu caracter personal, formarea angajaților în domeniul securității, audituri periodice, teste de penetrate şi mărci de calitate.

Exemplu: În cauza I./*Finlanda*[154], reclamanta nu a putut dovedi că evidențele sale medicale au fost accesate ilegal de către alți angajați ai spitalului în care a lucrat. 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 aşa natură încât nu permitea clarificarea retroactivă a utilizării evidențelor pacienților, acesta prezentând numai cele mai recente cinci consultații, iar aceste informații erau şterse imediat

154 Hotărârea CEDO din 17 iulie 2008 în cauza *I./Finlanda*, nr. 20511/03.

ce dosarul era înapoiat către 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 au acordat importanța cuvenită.

Notificările privind încălcarea securității datelor

Un nou instrument pentru tratarea încălcării securității datelor a fost introdus în legislația privind protecția datelor din mai multe țări europene: obligația furnizorilor de servicii de comunicații electronice de a notifica încălcarea securității datelor posibilelor victime și autorităților de supraveghere. Pentru furnizorii de telecomunicații, aceasta reprezintă o obligație în temeiul dreptului european[155]. Scopul notificărilor privind încălcarea securității datelor transmise persoanelor vizate este acela de a evita orice daune: notificarea încălcărilor securității datelor și a consecințelor posibile ale acestora reduc riscul unor efect negative asupra persoanelor vizate. În cazuri de neglijență gravă, furnizorii pot fi, de asemenea, amendați.

Va fi necesară instituirea în prealabil a unor proceduri interne pentru gestionarea și raportarea eficientă a încălcărilor măsurilor de securitate, întrucât intervalul de timp aferent obligației de raportare către persoanele vizate și/sau autoritățile de supraveghere, conform legislației naționale, este de obicei relativ scurt.

4.2.2. Confidențialitate

În temeiul dreptului european, prelucrarea securizată a datelor este garantată în plus prin obligația generală a tuturor persoanelor, operatorilor sau persoanelor împuternicite de către operatori, de a garanta confidențialitatea datelor.

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.

155 A se vedea Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor electronice, (*Directiva asupra confidențialității și comunicațiilor electronice*), MO 2002 L 201, articolul 4 alineatul (3), 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 se vedea și Directiva 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor electronice și Regulamentul (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului, MO 2009 L 337.

Obligația de confidențialitate asupra datelor clienților impune ca angajatul să aplice cel puțin măsurile de securitate minime înainte de a dezvălui date cu caracter personal. Acest lucru poate fi realizat, de exemplu, prin revenirea cu un apel telefonic la numărul înregistrat în dosarul clientului.

Articolul 16 din Directiva privind protecția datelor tratează confidențialitatea numai în cadrul relației operator-persoană împuternicită de către operator. Obligația operatorilor de a păstra sau nu confidențialitatea datelor, în sensul că nu le pot dezvălui unor terți, este tratată în articolele 7 şi 8 din directivă.

Obligația de confidențialitate nu se extinde asupra situațiilor în care datele sunt aduse la cunoştința unei persoane în calitatea acesteia de persoană fizică, nu de angajat al unui operator sau al unei persoane împuternicite de către operator. În acest caz, articolul 16 din Directiva privind protecția datelor nu se aplică, întrucât utilizarea datelor cu caracter personal de către persoane fizice este, de fapt, exceptată integral de la aplicabilitatea directivei, unde o astfel de utilizare se încadrează în limitele așa-numitei derogări privind activitățile domestice[156]. Derogarea privind activitățile domestice reprezintă utilizarea datelor cu caracter personal „de către o persoană fizică în cursul unei activități exclusiv personale sau domestice"[157]. Având în vedere hotărârea CJUE în cauza *Bodil Lindqvist*[158], această derogare trebuie interpretată, totuşi, în sens restrâns, în special în ceea ce priveşte dezvăluirea datelor. Mai precis, derogarea privind activitățile domestice nu se va extinde la dezvăluirea datelor cu caracter personal către un număr nelimitat de destinatari prin internet (pentru mai multe detalii cu privire la cauză, vă rugăm să consultați secțiunile 2.1.2, 2.2, 2.3.1 şi 6.1).

În temeiul legislației CoE, obligația de confidențialitate este implicită în noțiunea de securitate a datelor prevăzută la articolul 7 din Convenția 108, care tratează securitatea datelor.

Pentru persoanele împuternicite de către operator, confidențialitate înseamnă că pot utiliza datele cu caracter personal încredințate de către operator exclusiv în conformitate cu instrucțiunile acestuia din urmă. Pentru angajații unui operator sau ai unei persoane împuternicite de către operator, confidențialitatea impune utilizarea

156 Directiva privind protecția datelor, articolul 3 alineatul (2) a doua liniuță.

157 *Ibidem*

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

datelor cu caracter personal exclusiv în conformitate cu instrucțiunile superiorilor competenți.

Obligația de confidențialitate trebuie inclusă în orice contract încheiat între operatori şi persoanele împuternicite de către aceştia. În plus, operatorii şi persoanele împuternicite de către operatori vor trebui să adopte măsuri specifice pentru a stabili o obligație juridică de confidențialitate pentru angajații lor, care se obține în mod normal prin includerea unei clauze de confidențialitate în contractul de muncă al angajatului.

Încălcarea atribuțiilor profesionale de confidențialitate se pedepseşte conform dispozițiilor dreptului penal în multe state membre ale UE şi părți la Convenția 108.

4.3. Normele privind transparența prelucrării

Puncte-cheie

- Înainte de a începe prelucrarea datelor cu caracter personal, operatorul trebuie, cel puțin, să informeze persoanele vizate cu privire la identitatea operatorului şi scopul prelucrării datelor, cu excepția cazului în care persoanele vizate dețin deja aceste informații.
- În cazul în care datele sunt colectate de la terți, obligația de informare nu se aplică dacă:
  - prelucrarea datelor este prevăzută prin lege sau
  - furnizarea informațiilor se dovedeşte a fi imposibilă sau ar implica un efort disproporționat.
- Înainte de a începe prelucrarea datelor cu caracter personal, operatorul trebuie, în plus:
  - să notifice autoritatea de supraveghere cu privire la operațiunile de prelucrare avute în vedere sau
  - să asigure documentarea internă a prelucrării cu ajutorul unui responsabil independent de protecția datelor cu caracter personal, în cazul în care legislația națională prevede această procedură.

Principiul prelucrării corecte impune transparența prelucrării. **Legislația CoE** stabileşte, în acest sens, că orice persoană trebuie să poată stabili existența fişierelor de

prelucrare a datelor, finalitatea acestora şi operatorul responsabil[159]. Modul în care se realizează acest lucru este lăsat la aprecierea legislației interne. **Dreptul european** este mai concret, asigurând transparența pentru persoana vizată prin obligarea operatorului de a informa persoana vizată, şi publicul larg, prin intermediul unei notificări.

În conformitate cu ambele sisteme juridice, exceptările şi restricțiile de la obligațiile de transparență ale operatorului pot exista în legislația națională atunci când aceste restricții constituie o măsură necesară pentru protejarea unor interese de ordin public sau pentru protejarea persoanei vizate sau a drepturilor şi libertăților altora, atâta timp cât acest lucru reprezintă o măsură necesară într-o societate democratică[160]. Aceste excepții pot fi necesare, de exemplu, în contextul cercetării penale, dar pot fi justificate şi în alte împrejurări.

4.3.1. Informare

În conformitate cu legislația CoE, precum și cu dreptul european, operatorii prelucrărilor au obligația să informeze în prealabil persoana vizată cu privire la intenția de prelucrare[161]. Această obligație nu depinde de o solicitare din partea persoanei vizate, însă trebuie respectată în mod proactiv de operator, indiferent dacă persoana vizată se arată interesată sau nu de informații.

Conținutul informațiilor

Informațiile trebuie să includă scopul prelucrării, precum şi identitatea şi datele de contact ale operatorului[162]. Directiva privind protecția datelor impune furnizarea de informații suplimentare în măsura în care „ținând seama de circumstanțele specifice în care sunt colectate datele, sunt necesare pentru asigurarea unei prelucrări corecte a datelor cu privire la persoana vizată". Articolele 10 şi 11 din directivă subliniază, printre altele, categoriile de date prelucrate şi destinatarii acestor date, precum şi existența dreptului de acces la date şi a dreptului de rectificare a acestora. În cazul în care datele sunt colectate de la persoanele vizate, informațiile ar trebui să clarifice dacă răspunsurile la întrebări sunt obligatorii sau voluntare, precum şi consecințele posibile ale evitării răspunsului[163].

159 Convenția 108, articolul 8 litera (a).

160 *Ibidem*, articolul 9 alineatul (2) şi Directiva privind protecția datelor, articolul 13 alineatul (1).

161 Convenția 108, articolul 8 litera (a); Directiva privind protecția datelor, articolele 10 şi 11.

162 Convenția 108, articolul 8 litera (a) şi Directiva privind protecția datelor, articolul 10 literele (a) şi (b).

163 Directiva privind protecția datelor, articolul 10 litera (c).

Din perspectiva **legislației CoE**, furnizarea acestor informații poate fi considerată drept o bună practică, în conformitate cu principiul prelucrării corecte, fiind, de asemenea, în această măsură, parte a legislației CoE.

Principiul prelucrării corecte impune ca informațiile să poată fi înțelese ușor de persoanele vizate. Se utilizează un limbaj adecvat destinatarilor. Nivelul și tipul de limbaj va trebui adaptat în funcție de publicul vizat, de exemplu, adulți sau copii, publicul larg sau experți.

Unele persoane vizate vor dori să fie informate exclusiv pe scurt despre modul și motivul pentru care datele lor vor fi prelucrate, în timp ce altele vor solicita explicații detaliate. Echilibrarea acestui aspect al informării corecte este tratată în cadrul unui aviz al Grupului de lucru Articolul 29, care promovează ideea așa-numitelor notificări stratificate[164], permițând persoanei vizate să decidă ce nivel de detaliu preferă.

Termenul de furnizare a informațiilor

Directiva privind protecția datelor conține prevederi ușor diferite în ceea ce privește intervalul în care trebuie furnizate informațiile, în funcție de modul în care sunt colectate datele, de la persoana vizată (articolul 10) sau de la un terț (articolul 11). În cazul în care datele sunt colectate de la persoana vizată, informațiile trebuie furnizate, cel mai târziu, la momentul colectării. În cazul în care datele sunt colectate de la terți, informațiile trebuie furnizate, cel mai târziu, fie la momentul în care operatorul înregistrează datele, fie înaintea dezvăluirii datelor pentru prima dată unui terț.

Excepții de la obligația de informare

În temeiul dreptului european, o excepție generală de la obligația de informare a persoanei vizate există în cazul în care persoana vizată deține deja informațiile[165]. Acest aspect se referă la situațiile în care persoana vizată a fost deja informată, în funcție de împrejurările cazului, că datele sale vor fi prelucrate într-un anumit scop de către un anumit operator.

Articolul 11 din directivă, care se referă la obligația de informare a persoanei vizate atunci când datele nu sunt obținute de la aceasta, prevede, de asemenea, că aceasta nu se aplică, în special în cazul prelucrării în scopuri statistice sau de cercetare istorică ori științifice, dacă:

164 Grupul de lucru Articolul 29 (2004), *Avizul 10/2004 privind dispoziții de informare armonizate*, WP 100, Bruxelles, 25 noiembrie 2004.

165 Directiva privind protecția datelor, articolul 10 și articolul 11 alineatul (1).

- furnizarea acestor informații se dovedeşte imposibilă sau
- ar implica un efort disproporționat sau
- înregistrarea sau dezvăluirea datelor este prevăzută în mod expres prin lege[166].

Numai articolul 11 alineatul (2) din Directiva privind protecția datelor prevede că persoanele vizate trebuie să fie informate cu privire la operațiunile de prelucrare în cazul în care acestea sunt impuse prin lege. Având în vedere ipoteza juridică generală conform căreia legea este cunoscută de cei care i se supun, se poate argumenta că, atunci când datele sunt colectate de la o persoană vizată, în temeiul articolului 10 din directivă, persoana vizată deține informațiile. Dar, având în vedere că această cunoaştere a legii este doar o presupunere, principiul prelucrării corecte ar impune prin articolul 10 ca persoana vizată să fie informată chiar şi atunci când prelucrarea este prevăzută de lege, mai ales pentru că informarea persoanei vizate nu este deosebit de dificilă atunci când datele sunt colectate direct de la aceasta.

În ceea ce privește legislația CoE, Convenția 108 prevede în mod explicit excepții de la articolul 8. Din nou, excepțiile stabilite în articolele 10 şi 11 din Directiva privind protecția datelor pot fi considerate exemple de bune practici pentru excepțiile în temeiul articolului 9 din Convenția 108.

Modalități diferite de furnizare a informațiilor

Metoda ideală de furnizare a informațiilor ar fi adresarea, verbal sau în scris, către fiecare persoană vizată în parte. În cazul în care datele sunt colectate de la persoana vizată, furnizarea informațiilor ar trebui să se întrepătrundă cu operațiunea de colectare. Cu toate acestea, mai ales atunci când datele sunt colectate de la terți, ținând seama de dificultățile practice evidente de contactare a persoanei vizate, informațiile pot fi furnizate şi prin intermediul unei publicații adecvate.

Una dintre cele mai eficiente modalități de furnizare a informațiilor va fi stabilirea 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 semnificativ de populație care nu utilizează internetul, iar politica de informare a unei societăți sau a unei autorități publice ar trebui să țină cont de acest aspect.

166 *Ibidem*, considerentul 40 şi articolul 11 alineatul (2).

4.3.2. Notificare

Legislația națională poate obliga operatorii să notifice autoritatea de supraveghere competentă cu privire la operațiunile lor de prelucrare astfel încât acestea să poată fi publicate. Alternativ, legislația națională poate prevedea ca operatorii să angajeze un responsabil de protecția datelor cu caracter personal, care să răspundă în special de păstrarea unui registru cu operațiunile de prelucrare efectuate de operator[167]. Registrul intern trebuie să fie pus la dispoziția membrilor publicului, la cerere.

Exemplu: O notificare, precum şi documentarea unui responsabil intern de protecția datelor cu caracter personal trebuie să descrie principalele funcții ale prelucrării de date în cauză. Această descriere va include informații despre operator, scopul prelucrării, temeiul juridic al prelucrării, categoriile de date prelucrate, posibilii destinatari terți şi măsura în care sunt prevăzute fluxuri transfrontaliere de date, şi dacă da, care sunt acestea.

Publicarea notificărilor de către autoritatea de supraveghere trebuie să ia forma unui registru special. Pentru îndeplinirea obiectivului, accesul la acest registru ar trebui să fie facil şi gratuit. Acelaşi lucru este valabil pentru documentația păstrată de responsabilul de protecția datelor cu caracter personal al operatorului.

Excepțiile de la obligativitatea de notificare a autorității de supraveghere competente sau de angajare a unui responsabil intern de protecția datelor pot fi prevăzute în legislația națională, operațiunile de prelucrare care nu sunt susceptibile a prezenta un risc specific pentru persoanele vizate fiind enumerate în articolul 18 alineatul (2) din Directiva privind protecția datelor[168].

4.4. Normele privind promovarea conformității

Puncte-cheie

- Prin dezvoltarea principiului responsabilității, Directiva privind protecția datelor menționează mai multe instrumente pentru promovarea conformității:

167 *Ibidem*, articolul 18 alineatul (2) a doua liniuță.

168 *Ibidem*, articolul 18 alineatul (2) prima liniuță.

- verificarea în prealabil de către autoritatea de supraveghere națională a operațiunilor de prelucrare prevăzute;
- responsabilii de protecția datelor cu caracter personal, care vor asigura operatorului expertiză specială în domeniul protecției datelor;
- coduri de conduită care specifică normele privind protecția datelor existente în vederea aplicării într-un anumit sector al societății, în special în sectorul de afaceri.

- Legislația CoE propune instrumente similare pentru promovarea conformității în Recomandarea sa privind crearea de profile.

4.4.1. Verificare prealabilă

Conform articolului 20 din Directiva privind protecția datelor, autoritatea de supraveghere trebuie să verifice operațiunile de prelucrare care pot prezenta riscuri specifice în ceea ce priveşte drepturile şi libertățile persoanelor vizate – cauzate de scopul sau de împrejurările prelucrării – înainte de a începe prelucrarea. Legislația națională trebuie să stabilească operațiunile de prelucrare care se califică pentru verificare prealabilă. O astfel de verificare poate conduce la interzicerea operațiunilor de prelucrare sau la emiterea unui ordin de modificare a caracteristicilor modelului propus al operațiunilor de prelucrare. Articolul 20 din directivă are ca scop asigurarea că nu se dă curs niciunei prelucrări riscante în mod inutil, întrucât autoritatea de supraveghere are autoritatea de a interzice astfel de operațiuni. Condiția prealabilă pentru ca acest mecanism să fie eficient este notificarea efectivă a autorității de supraveghere. Pentru a asigura faptul că operatorii îşi îndeplinesc obligația de notificare, autoritățile de supraveghere trebuie să dispună de puteri coercitive, precum capacitatea de a amenda operatorii.

Exemplu: În cazul în care o societate desfăşoară operațiuni de prelucrare care, în conformitate cu legislația națională, se supun unei verificări prealabile, această societate trebuie să prezinte autorității de supraveghere documentația privind operațiunile de prelucrare planificate. Societatea nu poate da curs operațiunilor de prelucrare înainte de a primi un răspuns favorabil din partea autorității de supraveghere.

În unele state membre, legislația națională prevede în mod alternativ că operațiunile de prelucrare pot fi demarate în cazul în care nu există nicio reacție din partea autorității de supraveghere într-un anumit interval de timp, de exemplu, trei luni.

4.4.2. Responsabili de protecția datelor cu caracter personal

Directiva privind protecția datelor permite ca legislația națională să prevadă posibilitatea operatorilor de a desemna un funcționar să acționeze în calitate de funcționar responsabil pentru protecția datelor cu caracter personal[169]. Misiunea acestuia este aceea de a garanta că drepturile şi libertățile persoanelor vizate nu vor fi afectate în mod negativ prin operațiunile de prelucrare[170].

> Exemplu: În Germania, în conformitate cu secțiunea 4f, subsecțiunea 1 din Legea federală germană privind protecția datelor (*Bundesdatenschutzgesetz*), societățile private sunt obligate să numească un responsabil de protecția datelor cu caracter personal la nivel intern, în cazul în care angajează permanent cel puțin 10 persoane în procesul de prelucrare automatizată a datelor cu caracter personal.

Posibilitatea realizării acestui obiectiv presupune o anumită independență pentru funcția responsabilului în cadrul organizației operatorului, astfel cum se arată în mod explicit în directivă. De asemenea, pentru a sprijini funcționarea eficientă a acestui birou, sunt necesare drepturi de muncă ferme care să îi asigure protecția împotriva unor eventuale situații, precum concedierea nejustificată.

Pentru promovarea conformității cu legislația națională privind protecția datelor, conceptul de responsabili interni de protecția datelor cu caracter personal a fost, de asemenea, adoptat în anumite Recomandări ale Consiliului Europei[171].

4.4.3. Coduri de conduită

Pentru a promova conformitatea, sectorul de afaceri şi alte sectoare pot elabora norme detaliate de reglementare a activităților tipice de prelucrare, care să sistematizeze cele mai bune practici. Expertiza membrilor sectorului respectiv va favoriza identificarea unor soluții practice, care să poată fi urmate. În consecință, statele membre – precum şi Comisia Europeană – sunt încurajate să promoveze elaborarea unor coduri de conduită destinate să contribuie la buna aplicare a dispozițiilor de

169 *Ibidem*, articolul 18 alineatul (2) a doua liniuță.

170 *Ibidem*.

171 A se vedea, de exemplu, Recomandarea privind crearea de profile, articolul 8.3.

drept intern adoptate de statele membre în temeiul directivei, în funcție de particularitățile diferitelor sectoare[172].

Pentru a asigura conformitatea acestor coduri de conduită cu dispozițiile de drept intern adoptate în temeiul Directivei privind protecția datelor, statele membre trebuie să stabilească o procedură de evaluare a codurilor. Această procedură ar necesita, de regulă, implicarea autorității naționale, a asociațiilor profesionale şi a altor organe reprezentând alte categorii de operatori[173].

Proiectele de coduri comunitare şi modificările sau prorogările codurilor comunitare existente pot fi prezentate Grupului de lucru Articolul 29 pentru evaluare. În urma aprobării de către Grupul de lucru, Comisia Europeană poate asigura o publicitate adecvată acestor coduri[174].

Exemplu: Federația Europeană de Marketing Direct şi Interactiv (FEDMA) a elaborat un Cod european de practică pentru utilizarea datelor cu caracter personal în cadrul marketingului direct. Codul a fost prezentat cu succes Grupului de lucru Articolul 29. În anul 2010 a fost adăugată o anexă privind comunicările electronice de marketing[175].

172 A se vedea Directiva privind protecția datelor, articolul 27 alineatul (1).

173 *Ibidem*, articolul 27 alineatul (2).

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

175 Grupul de lucru Articolul 29 (2010), *Avizul 4/2010 privind Codul de conduită european al FEDMA pentru utilizarea datelor cu caracter personal în cadrul marketingului direct*, WP 174, Bruxelles, 13 iulie 2010.

5

Drepturile persoanelor vizate şi punerea în aplicare a acestora

UE	Aspecte vizate	CoE
Dreptul de acces		
Directiva privind protecția datelor, articolul 12 CJUE, C-553/07, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, 7 mai 2009	**Dreptul de acces la datele proprii**	Convenția 108, articolul 8 litera (b)
	Dreptul la rectificare, dreptul de ştergere sau de blocare	Convenția 108, articolul 8 litera (c) CEDO, *Cemalettin Canli/Turcia*, nr. 22427/04, 18 noiembrie 2008 CEDO, *Segerstedt-Wiberg şi alții/Suedia*, nr. 62332/00, 6 iunie 2006 CEDO, *Ciubotaru/Moldova*, nr. 27138/04, 27 aprilie 2010
Dreptul de opoziție		
Directiva privind protecția datelor, articolul 14 alineatul (1) litera (a)	**Dreptul de opoziție ca urmare a situației speciale a persoanei vizate**	Recomandarea privind crearea de profile, articolul 5.3
Directiva privind protecția datelor, articolul 14 alineatul (1) litera (b)	**Dreptul de opoziție față de utilizarea ulterioară a datelor în scopuri de marketing**	Recomandarea privind marketingul direct, articolul 4.1

UE	Aspecte vizate	CoE
Directiva privind protecția datelor, articolul 15	**Dreptul de opoziție față de deciziile automatizate**	Recomandarea privind crearea de profile, articolul 5.5
Supraveghere independentă		
Carta, articolul 8 alineatul (3) Directiva privind protecția datelor, articolul 28 Instituții ale UE, Capitolul V Regulamentul privind protecția datelor CJUE, C-518/07, *Comisia Europeană/ Republica Federală Germania*, 9 martie 2010 CJUE, C-614/10, *Comisia Europeană/ Republica Austria*, 16 octombrie 2012 CJUE, C-288/12, *Comisia Europeană/Ungaria*, 8 aprilie 2014	**Autorități naționale de supraveghere**	Convenția 108, Protocol adițional, articolul 1
Căi de atac și sancțiuni		
Directiva privind protecția datelor, articolul 12	**Cerere către operator**	Convenția 108, articolul 8 litera (b)
Directiva privind protecția datelor, articolul 28 alineatul (4) Regulamentul privind protecția datelor de către instituțiile europene, articolul 32 alineatul (2)	**Cereri depuse la o autoritate de supraveghere**	Convenția 108, Protocol adițional, articolul 1 alineatul (2) litera (b)
Carta, articolul 47	**Instanțe judecătorești (în general)**	Convenția europeană a drepturilor omului, articolul 13
Directiva privind protecția datelor, articolul 28 alineatul (3)	**Instanțe naționale**	Convenția 108, Protocol adițional, articolul 1 alineatul (4)
TFUE, articolul 263 alineatul (4) Regulamentul privind protecția datelor de către instituțiile europene, articolul 32 alineatul (1) TFUE, articolul 267	**CJUE**	
	CEDO	Convenția europeană a drepturilor omului, articolul 34

UE	Aspecte vizate	CoE
Căi de atac şi sancţiuni		
Carta, articolul 47 Directiva privind protecţia datelor, articolele 22 şi 23 CJUE, C-14/83, *Sabine von Colson şi Elisabeth Kamann/Land Nordrhein-Westfalen*, 10 aprilie 1984 CJUE, C-152/84, *M.H. Marshall/Southampton and South-West Hampshire Area Health Authority*, 26 februarie 1986	**Pentru încălcări ale legislaţiei naţionale privind protecţia datelor**	Convenţia europeană a drepturilor omului, articolul 13 (doar pentru statele membre ale CoE) Convenţia 108, articolul 10 CEDO, *K.U./Finlanda*, nr. 2872/02, 2 martie 2008 CEDO, *Biriuk/Lituania*, nr. 23373/03, 25 noiembrie 2008
Regulamentul privind protecţia datelor de către instituţiile europene, articolul 34 alineatul (49) CJUE, C-28/08, *Comisia Europeană/The Bavarian Lager Co. Ltd*, 29 iunie 2010	**Pentru încălcări ale dreptului UE de către instituţiile şi organele UE**	

Eficacitatea normelor juridice, în general, şi a drepturilor persoanelor vizate, în special, depinde într-o măsură considerabilă de existenţa unor mecanisme adecvate pentru punerea în aplicare a acestora. În conformitate cu legislaţia europeană privind protecţia datelor, persoana vizată trebuie să fie împuternicită în temeiul legislaţiei naţionale să îşi protejeze datele personale. De asemenea, trebuie înfiinţate autorităţi independente de supraveghere, conform legislaţiei naţionale, care să asiste persoanele vizate în exercitarea drepturilor lor şi pentru a supraveghea procesul de prelucrare a datelor cu caracter personal. În plus, dreptul de acces la o cale de atac eficientă, astfel cum este garantat prin Convenţia europeană a drepturilor omului şi prin Cartă, prevede punerea la dispoziţie a căilor de atac juridice pentru fiecare persoană.

5.1. Drepturile persoanelor vizate

Puncte-cheie

- Orice persoană are dreptul, în temeiul legislaţiei naţionale, să solicite de la orice operator, informaţii care să indice dacă operatorul respectiv prelucrează datele acesteia.
- În conformitate cu legislaţia naţională, persoanele vizate au dreptul să:
  - îşi acceseze datele personale de la orice operator care prelucrează datele respective;

- solicite rectificarea (sau blocarea, după caz) a datelor personale de către operatorul care se ocupă de prelucrarea datelor acestora, în cazul în care datele respective sunt incorecte;
- solicite ştergerea sau blocarea, după caz, a datelor personale de către operator, în cazul în care acesta prelucrează datele respective în mod ilegal.

- De asemenea, persoanele vizate au dreptul de opoziție față de operatori în cazul:
  - deciziilor automatizate (adoptate pe baza datelor personale prelucrate doar prin mijloace automate);
  - prelucrării datelor acestora, dacă acest lucru conduce la rezultate disproporționate;
  - utilizării datelor acestora în scopuri de marketing direct.

5.1.1. Dreptul de acces

În temeiul dreptului UE, articolul 12 din Directiva privind protecția datelor conține elementele referitoare la dreptul de acces al persoanelor vizate, inclusiv dreptul de a obține de la operator „confirmarea că datele care o privesc sunt sau nu prelucrate, precum şi informații referitoare la scopul prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt comunicate datele", precum şi „rectificarea, ştergerea sau blocarea datelor a căror prelucrare nu respectă dispozițiile prezentei directive, în special datorită caracterului incomplet sau inexact al datelor".

Legislația CoE prevede aceleaşi drepturi, fiind necesar ca acestea să fie prevăzute şi de dreptul intern (articolul 8 din Convenția 108). Într-o serie de recomandări ale CoE, se utilizează termenul „acces", iar diferitele aspecte ale dreptului de acces sunt descrise şi propuse pentru a fi puse în aplicare în dreptul intern, astfel cum este subliniat la alineatul de mai sus.

În conformitate cu articolul 9 din Convenția 108 şi articolul 13 din Directiva privind protecția datelor, obligația operatorilor de a răspunde la o cerere de acces din partea persoanei vizate poate fi restricționată ca urmare a intereselor legale prioritare ale altor entități. Interesele legale prioritare pot implica interese publice, precum securitatea națională, siguranța publică şi urmărirea penală a infracțiunilor, precum şi interese private, care sunt imperative față de interesele privind protecția datelor. Excepțiile sau restricțiile trebuie să fie necesare într-o societate democratică şi proporționale cu scopul urmărit. În cazuri excepționale, de exemplu, în baza unor recomandări medicale, protecția persoanelor vizate poate necesita în sine o

restricționare a transparenței; aceasta implică, în special, limitarea dreptului de acces al fiecărei persoane vizate.

Ori de câte ori datele sunt prelucrate exclusiv în scopul cercetării științifice sau a realizării de statistici, Directiva privind protecția datelor permite restricționarea drepturilor de acces în baza legislației naționale; cu toate acestea, trebuie să se ofere garanții legale adecvate. În special, trebuie să se garanteze că nu sunt luate măsuri sau decizii privind o anumită persoană în contextul prelucrării unor astfel de date şi că „în mod clar, nu există riscuri de încălcare a vieții private persoanei vizate”[176]. Prevederi similare sunt incluse în articolul 9 alineatul (3) din Convenția 108.

Dreptul de acces la datele proprii

În temeiul legislației CoE, dreptul de acces la datele proprii este recunoscut în mod explicit la articolul 8 din Convenția 108. CEDO a susținut în repetate rânduri că alte persoane au şi exercită dreptul de a accesa informații referitoare la datele cu caracter personal ale unei persoane şi că acest drept rezultă din necesitatea de respectare a vieții private[177]. În cauza *Leander*[178], CEDO a concluzionat că dreptul de acces la datele cu caracter personal stocate de autoritățile publice ar putea, totuşi, să fie limitat în anumite circumstanțe.

În temeiul dreptului UE, dreptul de acces la datele proprii este recunoscut în mod explicit la articolul 12 din Directiva privind protecția datelor şi, ca drept fundamental, la articolul 8 alineatul (2) din Cartă.

Articolul 12 litera (a) din directivă prevede obligativitatea statelor membre de a garanta fiecărei persoane vizate dreptul de acces la datele şi informațiile personale. În special, fiecare persoană vizată are dreptul de a obține de la operator confirmarea că datele care o privesc sunt sau nu prelucrate şi informații referitoare cel puțin la:

- scopul prelucrării;
- categoriile de date avute în vedere;

176 Directiva privind protecția datelor, articolul 13 alineatul (2).

177 Hotărârea CEDO din 7 iulie 1989 în cauza *Gaskin/Regatul Unit*, nr. 10454/83; Hotărârea CEDO din 13 februarie 2003, în cauza *Odièvre/Franța* [T], 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.

178 Hotărârea CEDO din 11 iulie 1985 în cauza *Leander/Suedia*, nr. 9248/81.

- datele care fac obiectul prelucrării;
- destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele;
- informațiile disponibile privind sursa datelor care fac obiectul prelucrării;
- în cazul deciziilor automatizate, principiile de funcționare a mecanismului de prelucrare automată a datelor.

Legislația națională poate adăuga informații spre a fi furnizate de operator, de exemplu, invocarea temeiului juridic care autorizează prelucrarea datelor.

Exemplu: Prin accesarea datelor personale, o persoană poate să stabilească dacă datele sunt sau nu exacte. Prin urmare, este absolut necesar ca persoana vizată să fie informată privind categoriile de date prelucrate şi conținutul datelor. Astfel, nu este suficient ca un operator să anunțe doar persoana vizată că prelucrează numele, adresa, data de naştere şi domeniul de interes ale acesteia. Operatorul trebuie, de asemenea, să comunice persoanei vizate faptul că acesta prelucrează „numele: N.N.; o adresă: 1040 Viena, Schwarzenbergplatz 11, Austria; data naşterii: 10.10.1974; şi domeniul de interes (în baza declarației persoanei vizate): muzică clasică." Ultimul element conține, în mod adițional, informații privind sursa datelor.

Informarea persoanei vizate cu privire la datele care fac obiectul prelucrării şi sursa informațiilor disponibile trebuie să fie realizată într-o formă inteligibilă, ceea ce înseamnă că operatorul trebuie să explice, în mod detaliat, persoanei vizate ce anume prelucrează. De exemplu, simpla menționare a unor abrevieri tehnice sau a unor termeni medicali ca răspuns la o cerere de acces nu este, de regulă, suficientă, chiar dacă se stochează numai astfel de abrevieri sau termeni.

Informațiile privind sursa datelor prelucrate de operator trebuie furnizate drept răspuns la o cerere de acces, în măsura în care aceste informații sunt disponibile. Această dispoziție trebuie înțeleasă în lumina principiilor echității şi responsabilității. Un operator nu poate distruge informațiile privind sursa datelor pentru a fi scutit de obligația de a le divulga sau ignora standardul aplicabil şi necesitățile recunoscute de documentare în domeniul în care îşi desfăşoară activitatea. Nedocumentarea sursei datelor prelucrate nu se consideră, de regulă, o îndeplinire a obligațiilor operatorului în ceea ce priveşte dreptul de acces.

În cazul în care se efectuează evaluări automate, se impune explicarea logicii generale a evaluării, inclusiv criteriile specifice care au fost luate în considerare pentru evaluarea persoanei vizate.

Directiva nu specifică în mod clar dacă dreptul de acces la informații se referă la trecut şi, dacă da, la ce perioadă anume din trecut. În acest sens, 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*[179], CJUE i s-a solicitat să stabilească dacă, în conformitate cu articolul 12 litera (a) din directivă, dreptul unei persoane de a avea acces la informații privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal şi conținutul datelor comunicate poate fi limitat la o perioadă de un an anterioară datei de prezentare a cererii de acces.

Pentru a stabili dacă la articolul 12 litera (a) din directivă se prevede un astfel de termen limită, Curtea a hotărât să interpreteze acest articol în lumina scopului directivei. Curtea a concluzionat inițial că dreptul de acces este necesar pentru a permite persoanei vizate să îşi exercite dreptul de a solicita operatorului rectificarea, ştergerea sau blocarea datelor sale [articolul 12 litera (b)] sau să notifice terții cărora le-au fost comunicate datele respective privind rectificarea, ştergerea sau blocarea acestora [articolul 112 litera (c)]. Dreptul de acces este, de asemenea, necesar pentru a permite persoanei vizate să îşi exercite dreptul de opoziție la prelucrarea datelor sale cu caracter personal (articolul 14) sau dreptul său la o cale de atac în cazul în care suferă un prejudiciu (articolele 22 şi 23).

Pentru a asigura efectul practic al dispozițiilor susmenționate, Curtea a hotărât că „dreptul respectiv trebuie să facă referire, în mod obligatoriu, la trecut. Dacă nu se procedează astfel, persoana vizată nu are posibilitatea efectivă de a-şi exercita dreptul de a rectifica, şterge sau bloca datele pe care le consideră a fi deținute ilegal sau inexacte sau de a intenta o acțiune în justiție şi de a obține despăgubiri pentru prejudiciul suferit”.

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

Dreptul la rectificare, dreptul de ștergere și de blocare a datelor

„Orice persoană trebuie să poată beneficia de dreptul de acces la datele cu caracter personal care fac obiectul prelucrării, pentru a se asigura în special de exactitatea datelor şi de legalitatea prelucrării acestora”[180]. În conformitate cu aceste principii, persoanele vizate trebuie să aibă dreptul, în temeiul legislației naționale, de a obține rectificarea, ştergerea sau blocarea datelor acestora de către operator, dacă persoanele respective consideră că prelucrarea datelor nu respectă dispozițiile directivei, în special datorită caracterului inexact sau incomplet al datelor[181].

Exemplu: În cauza *Cemalettin Canli/Turcia*[182], CEDO a constatat încălcarea articolului 8 din Convenția europeană a drepturilor omului prin raportare incorectă de către organele de poliție în cadrul procedurilor penale.

Reclamantul a fost implicat de două ori în proceduri penale în baza unei presupuse apartenențe la organizații ilegale, fără a fi vreodată condamnat. Atunci când reclamantul a fost arestat din nou şi 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 şi înregistrărilor deținute de organele de poliție a fost respinsă. CEDO a concluzionat că informațiile conținute în raportul organelor de poliție au fost prezentate conform articolului 8 din Convenția europeană a drepturilor omului, întrucât informațiile de interes public pot face parte din domeniul „vieții private” atunci când sunt colectate în mod sistematic şi stocate în evidențele autorităților. În plus, raportul organelor de poliției a fost inexact, iar modul de elaborare şi prezentare a acestuia în fața instanței penale nu a respectat legea. Curtea a constatat încălcarea articolului 8.

Exemplu: În cauza *Segerstedt-Wiberg și alții/Suedia*[183], reclamanții au fost afiliați unor partide politice liberale şi comuniste. Aceştia au bănuit că anumite informații despre ei au fost înregistrate în evidențele forțelor de securitate. CEDO a

180 Directiva privind protecția datelor, considerentul 41.

181 *Ibidem*, articolul 12 litera (b).

182 Hotărârea CEDO din 18 noiembrie 2008 în cauza *Cemalettin Canli/Turcia*, nr. 22427/04, punctele 33, 42 şi 43; Hotărârea CEDO din 2 februarie 2010 în cauza *Dalea/Franța*, nr. 964/07.

183 Hotărârea CEDO din 6 iunie 2006 în cauza *Segerstedt-Wiberg și alții/Suedia*, nr. 62332/00, punctele 89 şi 90; a se vedea şi, de exemplu, Hotărârea CEDO din 18 aprilie 2013 în cauza *M.K./Franța*, nr. 19522/09.

constatat că stocarea datelor în cauză a avut un temei juridic şi a urmărit un scop legitim. În cazul unora dintre reclamanți, CEDO a constatat că înregistrarea continuă a datelor a adus o atingere disproporționată vieții private a acestora. De exemplu, în cazul domnului Schmid, autoritățile au înregistrat informații conform 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 ar fi putut urmări niciun interes relevant privind securitatea națională, având în vedere, în special, caracterul istoric al acesteia. CEDO a constatat încălcarea articolului 8 din Convenția europeană a drepturilor omului în cazul a patru dintre cei cinci reclamanți.

În anumite cazuri, este suficient ca persoana vizată să solicite pur şi simplu rectificarea, de exemplu, a ortografiei numelui sau modificarea adresei sau a numărului de telefon. Cu toate acestea, în cazul în care astfel de cereri vizează aspecte juridice, precum identitatea juridică a persoanei vizate sau locul de rezidență exact 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 acestora. 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 registrele secrete[184].

Exemplu: În cauza *Ciubotaru/Moldova*[185], reclamantul nu a avut posibilitatea de a modifica înregistrarea privind originea sa etnică, inclusă în documentele oficiale, din limba moldovenească în limba română întrucât s-a susținut că acesta nu a justificat cererea înaintată. 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 şi 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 şi 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

184 Hotărârea CEDO din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95.

185 Hotărârea CEDO din 27 aprilie 2010 în cauza *Ciubotaru/Moldova*, nr. 27138/04, punctele 51 şi 59.

creat o barieră insurmontabilă privind înregistrarea unei identități etnice alta decât cea înregistrată în cazul părinților acestuia de către autoritățile sovietice. Nepermițând examinarea cererii reclamantului pe baza unor dovezi verificabile în mod obiectiv, statul nu și-a respectat obligația pozitivă de a asigura reclamantului respectarea efectivă a vieții private. Curtea a constatat încălcarea articolului 8 din Convenția europeană a drepturilor omului.

În cadrul unei acțiuni sau proceduri civile desfăşurate înaintea unei autorități publice pentru a 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 şi că o decizie oficială este în curs de adoptare. În această perioadă, operatorul de date nu trebuie să prezinte datele, în special terților, ca fiind certe sau definitive.

O cerere de ştergere sau de eliminare a datelor înaintată de persoana vizată se bazează adeseori pe afirmația că prelucrarea datelor nu are un temei legitim. Astfel de afirmații apar în mod frecvent atunci când consimțământul a fost retras sau în cazul în care anumite date nu mai sunt necesare îndeplinirii scopului colectării de date. Sarcina probei privind justificarea prelucrării datelor revine operatorului de date deoarece acesta este responsabil de legitimitatea prelucrării datelor. 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, procesul trebuie întrerupt.

În cazul în care prelucrarea datelor este contestată în baza afirmației că datele sunt inexacte sau prelucrate în mod ilegal, în conformitate cu principiul prelucrării corecte, persoana vizată poate solicita blocarea datelor care fac obiectul litigiului. Acest lucru nu înseamnă că datele sunt şterse, ci că operatorul trebuie să se abțină de la utilizarea datelor cât timp acestea sunt blocate. Acest lucru este necesar, în special, atunci când continuarea utilizării datelor inexacte sau deținute în mod ilegal ar putea cauza prejudicii persoanei vizate. Legislația națională trebuie să furnizeze mai multe detalii privind situațiile în care poate apărea obligația de a bloca utilizarea datelor şi modalitatea de îndeplinire a acesteia.

De asemenea, persoanele vizate au dreptul să obțină de la operator notificarea terților privind orice blocare, rectificare sau ştergere a datelor, în cazul în care părțile în cauză au primit datele respective înainte de efectuarea acestor operațiuni de prelucrare. Întrucât divulgarea datelor către terți ar fi trebuit documentată de către operator, ar fi posibilă identificarea destinatarilor datelor şi solicitarea ştergerii acestora.

Cu toate acestea, dacă, între timp, datele au fost publicate pe internet, de exemplu, ştergerea acestora în toate cazurile poate fi imposibilă, întrucât destinatarii datelor nu pot fi identificați. În conformitate cu Directiva privind protecția datelor, contactarea destinatarilor datelor în scopul rectificării, ştergerii sau blocării datelor este obligatorie, „cu excepția cazului în care acest lucru se dovedeşte imposibil sau presupune un efort disproporționat”[186].

5.1.2. Dreptul de opoziție

Dreptul de opoziție include dreptul de a se opune deciziilor individuale automatizate, dreptul de opoziție ca urmare a situației particulare a persoanei vizate şi dreptul de a se opune utilizării ulterioare a datelor în scopuri de marketing direct.

Dreptul de opoziție față de deciziile individuale automatizate

Deciziile automatizate sunt decizii adoptate pe baza datelor cu caracter personal prelucrate exclusiv prin mijloace automatizate. Dacă există posibilitatea ca astfel de decizii să afecteze în mod semnificativ viețile persoanelor în cauză, atunci când fac referire, de exemplu, la credibilitatea, randamentul profesional, conduita sau încrederea pe care o prezintă, se impune asigurarea unei protecții speciale pentru a evita consecințele nedorite. Directiva privind protecția datelor prevede că deciziile automatizate nu trebuie să evalueze aspecte importante pentru persoanele vizate şi impune dreptul persoanei în cauză de a revizui decizia automatizată[187].

Exemplu: Un exemplu practic important în care se iau decizii automatizate este evaluarea solvabilității. Pentru a lua o decizie rapidă privind solvabilitatea unui viitor client, anumite date precum profesia şi situația familială sunt colectate de la client şi combinate cu date privind persoana vizată provenind din alte surse, precum sistemele de informații privind creditele. Aceste date sunt introduse în mod automat într-un algoritm de evaluare, care calculează o valoare totală reprezentând solvabilitatea potențialului client. Astfel, angajatul societății poate decide în termen de câteva secunde dacă persoana vizată este sau nu acceptabilă în calitate de client.

Cu toate acestea, în conformitate cu directiva, statele membre prevăd posibilitatea ca o persoană să facă obiectul unei decizii individuale automatizate atunci când

186 Directiva privind protecția datelor, articolul 12 litera (c), ultima parte a tezei.

187 *Ibidem*, articolul 15 alineatul (1).

interesele persoanei vizate, fie nu sunt în joc întrucât decizia a fost luată în favoarea persoanei vizate, fie sunt protejate prin alte mijloace adecvate[188]. Dreptul de opoziție față de deciziile automatizate este, de asemenea, inerent în cadrul **legislației CoE**, astfel cum rezultă din Recomandarea privind crearea de profile[189].

Dreptul de opoziție legat de situația particulară a persoanei vizate

Persoanele vizate nu dețin niciun drept general de a se opune prelucrării propriilor date[190]. Cu toate acestea, articolul 14 litera (a) din Directiva privind protecția datelor, conferă persoanei vizate dreptul de a ridica obiecții din motive imperative şi legitime privind situația particulară a persoanei vizate. Un drept similar a fost recunoscut în Recomandarea CoE privind crearea de profile[191]. Dispozițiile respective vizează stabilirea ponderii corecte între drepturile de protecție a datelor aparținând persoanelor vizate şi drepturile legitime ale altor părți în cadrul procesului de prelucrare a datelor persoanei vizate.

Exemplu: O bancă stochează pe o perioadă de şapte ani datele privind clienții care nu achită împrumuturile. Un client ale cărui date sunt stocate în această bază de date solicită un alt împrumut. Se consultă baza de date, se efectuează o evaluare a situației financiare şi clientului îi este refuzat împrumutul. Cu toate acestea, clientul se poate opune menținerii datelor sale cu caracter personal în baza de date respectivă şi poate solicita ştergerea acestora dacă poate demonstra că plata neachitată a reprezentat o simplă eroare care a fost corectată imediat după ce clientul a luat cunoştință de aceasta.

Rezultatul unei opoziții reuşite este că datele în cauză nu mai pot fi prelucrate de operator. Cu toate acestea, operațiunile de prelucrare a datelor persoanei vizate efectuate înainte de exprimarea opoziției îşi păstrează caracterul legitim.

Dreptul de opoziție față de utilizarea ulterioară a datelor în scopuri de marketing direct

Articolul 14 litera (b) din Directiva privind protecția datelor prevede dreptul specific de opoziție împotriva utilizării datelor unei persoane în scop de marketing direct.

188 *Ibidem*, articolul 15 alineatul (2).

189 Recomandarea privind crearea de profile, articolul 5 alineatul (5).

190 A se vedea, 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 sau Hotărârea CEDO din 26 martie 1987 în cauza *Leander/Suedia*, nr. 9248/81; sau Hotărârea CEDO din 10 mai 2011 în cauza *Mosley/Regatul Unit*, nr. 48009/08.

191 Recomandare privind crearea de profile, articolul 5 alineatul (3).

Acest drept este prevăzut, de asemenea, în Recomandarea CoE privind marketingul direct[192]. Acest tip de opoziție trebuie exprimat înainte ca datele să fie puse la dispoziția terților în scopuri de marketing direct. Prin urmare, persoanei vizate trebuie să i se ofere posibilitatea de a se opune înainte ca datele să fie transferate.

5.2. Supraveghere independentă

Puncte-cheie

- Pentru a asigura o protecție eficientă a datelor, se impune înființarea de autorități independente de supraveghere în conformitate cu legislația națională.
- Autoritățile naționale de supraveghere trebuie să acționeze cu independență deplină, garantată prin legea în baza căreia autoritatea respectivă a fost instituită şi care se reflectă în structura organizatorică specifică a autorității de supraveghere.
- Autoritățile de supraveghere au sarcini specifice, printre care:
  - să monitorizeze şi să promoveze protecția datelor la nivel național;
  - să asigure consiliere persoanelor vizate şi operatorilor, precum şi guvernului şi publicului larg;
  - să răspundă plângerilor şi să asiste persoana vizată în probleme legate de presupusele încălcări ale drepturilor de protecție a datelor;
  - să supravegheze operatorii şi persoanele împuternicite de către operator;
  - să intervină, dacă este necesar, prin
    - avertizarea, mustrarea sau chiar amendarea operatorilor şi a persoanelor împuternicite de către aceştia,
    - solicitarea rectificării, blocării sau ştergerii datelor,
    - impunerea unei interdicții asupra prelucrării;
  - sesizarea instanței.

Directiva privind protecția datelor prevede supravegherea independentă ca mecanism important în asigurarea unei protecții eficiente a datelor. Directiva a introdus

192 CoE, Comitetul de Miniştri (1985), articolul 4 alineatul (1) din Recomandarea Rec(85)20 din 25 octombrie 1985 către statele membre privind protecția datelor cu caracter personal utilizate în scopuri de marketing direct.

un instrument pentru punerea în aplicare a protecției datelor, care nu a fost inclus, inițial, în Convenția 108 sau în Orientările OCDE privind viața privată.

Având în vedere că supravegherea independentă s-a dovedit a fi esențială pentru asigurarea unei protecții eficiente a datelor, o nouă dispoziție a Orientărilor OCDE privind viața privată, revizuite, adoptată în 2013 solicită statelor membre să „înființeze și să mențină autorități care să asigure respectarea legislației privind confidențialitatea, cu guvernanța, resursele și expertiza tehnică necesare pentru exercitarea eficientă a puterilor și luarea de decizii în mod obiectiv, imparțial și consecvent"[193].

În temeiul legislației CoE, Protocolul adițional la Convenția 108 a impus obligativitatea înființării de autorități de supraveghere. Articolul 1 din acest instrument prevede cadrul juridic pentru autoritățile de supraveghere independente, pe care părțile contractante trebuie să îl pună în aplicare în legislația națională. Acesta utilizează formulări similare pentru a descrie atribuțiile și competențele acestor autorități, astfel cum sunt utilizate în Directiva privind protecția datelor. Astfel, autoritățile de supraveghere trebuie să funcționeze, în principiu, în același mod în conformitate atât cu dreptul UE, cât și cu legislația CoE.

În temeiul dreptului UE, competențele și structura organizațională ale autorităților de supraveghere au fost inițial prezentate în articolul 28 alineatul (1) din Directiva privind protecția datelor. Regulamentul privind protecția datelor de către instituțiile europene[194] desemnează AEPD în calitate de autoritate de supraveghere responsabilă de prelucrarea datelor de către instituțiile și organele UE. În prezentarea rolurilor și responsabilităților autorității de supraveghere, acest regulament se bazează pe experiența acumulată de la promulgarea Directivei privind protecția datelor.

Independența autorităților pentru protecția datelor este garantată în baza articolului 16 alineatul (2) din TFUE și a articolului 8 alineatul (3) din Cartă. Această ultimă dispoziție tratează în mod specific controlul exercitat de către o autoritate independentă ca un element esențial al dreptului fundamental de protecție a datelor. De asemenea, Directiva privind protecția datelor prevede obligația statelor membre de a înființa autorități de supraveghere care să monitorizeze punerea în aplicare a

193 OCDE (2013), Orientări privind reglementarea protecției vieții private și a fluxurilor transfrontaliere de date cu caracter personal, punctul 19 litera (c).

194 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, MO 2001 L 8, articolele 41-48.

directivei şi care să acționeze în condiții de independență deplină[195]. Independența trebuie garantată, în mod specific, nu numai prin prevederile legii în temeiul căreia se instituie organul de supraveghere, ci şi prin structura organizațională specifică a autorității în cauză.

În 2010, CJUE a întâmpinat pentru prima dată problema domeniului de aplicare al cerinței de independență a autorităților de supraveghere a protecției datelor[196]. Următoarele exemple ilustrează opinia acesteia.

Exemplu: În cauza *Comisia/Germania*[197], Comisia Europeană a solicitat CJUE să declare că Germania a transpus în mod eronat cerința privind „condițiile de independență deplină" în care trebuie să acționeze autoritățile de supraveghere responsabile de garantarea protecției datelor, neîndeplinindu-şi astfel obligațiile care îi revin conform articolului 28 alineatul (1) din Directiva privind protecția datelor. În opinia Comisiei, problema a constat în faptul că Germania a plasat sub supravegherea statului autoritățile responsabile de monitorizarea prelucrării datelor cu caracter personal în afara sectorului public la nivelul diferitelor landuri (*Länder*).

Examinarea pe fond a cauzei a depins, în opinia Curții, de sfera de aplicare a cerinței de independență prevăzute în dispoziția respectivă şi, prin urmare, de interpretarea acesteia.

Curtea a subliniat că sintagma „în condiții de independență deplină" de la articolul 28 alineatul (1) din directivă trebuie interpretată pe baza formulării efective a dispoziției respective şi a obiectivelor şi structurii Directivei privind protecția datelor[198]. Curtea a accentuat faptul că autoritățile de supraveghere reprezintă „protectorii" drepturilor asociate prelucrării datelor cu caracter personal garantate în directivă şi că înființarea acestora în statele membre este considerată astfel „un element esențial al protecției persoanelor în ceea ce priveşte

195 Directiva privind protecția datelor, articolul 28 alineatul (1), ultima teză; Convenția 108, Protocol adițional, articolul 1 alineatul (3).

196 A se vedea FRA (2010), *Drepturi fundamentale: provocări şi realizări în 2010,* Raport anual 2010, p. 59. FRA a abordat acest aspect în detaliu în raportul privind *Protecția datelor în Uniunea Europeană: rolul autorităților naționale pentru protecția datelor*, publicat în mai 2010.

197 Hotărârea CJUE din 9 martie 2010 în cauza *Comisia Europeană/Republica Federală Germania*, C-518/07, punctul 27.

198 *Ibidem*, punctele 17 şi 29.

prelucrarea datelor cu caracter personal"[199]. Curtea a concluzionat că „în exercitarea atribuțiilor cu care sunt învestite, autoritățile de supraveghere trebuie să acționeze în mod obiectiv şi imparțial. În acest sens, acestea trebuie să acționeze independent de orice influență exterioară, inclusiv de influența directă sau indirectă a statului sau a *landurilor*, şi nu numai de influența organelor supravegheate"[200].

CJUE a constatat, de asemenea, că sensul sintagmei „în condiții de independență deplină" trebuie interpretat având în vedere independența AEPD, astfel cum este definită în Regulamentul privind protecția datelor de către instituțiile europene. Astfel cum a subliniat Curtea, la articolul 44 alineatul (2) din respectivul regulament se clarifică noțiunea de independență adăugând specificația că „AEPD nu solicită şi nici nu primeşte instrucțiuni din partea altcuiva, în îndeplinirea atribuțiilor sale". Această regulă exclude supravegherea de către stat a unei autorități independente de supraveghere a protecției datelor[201].

În consecință, CJUE a constatat că instituțiile germane pentru protecția datelor la nivel de land responsabile de monitorizarea prelucrării datelor cu caracter personal de către alte organisme decât cele publice nu şi-au exercitat atribuțiile în condiții de independență deplină deoarece acestea au făcut obiectul supravegherii de către stat.

Exemplu: În cauza *Comisia/Austria*[202], CJUE a evidențiat probleme similare privind poziția unor membri ai personalului Autorității pentru protecția datelor din Austria (Comisia pentru Protecția Datelor, DSK). Curtea a concluzionat în speță că legislația austriacă nu a permis Autorității pentru protecția datelor din Austria să îşi exercite atribuțiile în condiții de independență deplină, în sensul Directivei privind protecția datelor. Independența APD din Austria nu a fost garantată în mod suficient deoarece Cancelaria Federală asigură forța de muncă a DSK, supraveghează această instituție şi are dreptul de a fi informată în permanență cu privire la activitatea acesteia.

199 *Ibidem*, punctul 23.

200 *Ibidem,* punctul 25.

201 *Ibidem,* punctul 27.

202 Hotărârea CJUE din 16 octombrie 2012 în cauza *Comisia Europeană/Republica Austria*, C-614/10, punctele 59 şi 63.

Exemplu: În cauza *Comisia Europeană/Ungaria,*[203], CJEU a subliniat faptul că „cerința [...] de a asigura că fiecare autoritate de supraveghere este capabilă să ducă la îndeplinire atribuțiile încredințate în deplină independență atrage după sinte obligația statului membru în cauză să permită ca autoritatea să-şi ducă la îndeplinire mandatul". De asemenea, Curtea a reținută că, „prin încetarea anticipată a mandatului Comisarului petnru protecția datelor, Ungaria nu a reuşit să-şi îndeplinească obligațiile potrivit Directivei 95/46/CE [...]."

În temeiul legislației naționale, printre altele, autoritățile de supraveghere dețin competențe şi capacități pentru[204]:

- a informa operatorii şi persoanele privind totalitatea aspectelor legate de protecția datelor;
- a investiga operațiunile de prelucrare a datelor şi de a interveni în mod corespunzător;
- a adresa operatorilor avertismente sau mustrări;
- a dispune rectificarea, blocarea, ştergerea sau distrugerea datelor;
- a interzice temporar sau definitiv prelucrarea;
- a sesiza instanța 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 şi la toate informațiile necesare pentru investigațiile desfăşurate, precum şi la orice sediu în care un operator păstrează informații relevante.

Există diferențe semnificative între jurisdicțiile interne în ceea ce priveşte procedurile şi efectul juridic al constatărilor unei autorități de supraveghere. Acestea pot varia de la recomandări de tipul celor emise de Ombudsman până la decizii cu executare imediată. Astfel, atunci când se analizează eficiența căilor de atac disponibile în cadrul unei jurisdicții, mijloacele de atac trebuie apreciate în contextul asociat acestora.

203 Hotărârea CJUE din 8 aprilie 2014 în cauza *Comisia Europeană/Ungaria*, C-288/12, punctele 50 şi 67.

204 Directiva privind protecția datelor, articolul 28; a se vedea, de asemenea, Convenția 108, Protocol adițional, articolul 1.

5.3. Căi de atac şi sancțiuni

Puncte-cheie

- În conformitate cu Convenția 108 şi Directiva privind protecția datelor, legislația națională trebuie să stabilească căi de atac şi sancțiuni corespunzătoare pentru încălcarea dreptului de protecție a datelor.
  - În conformitate cu dreptul UE, dreptul la o cale de atac eficientă presupune stabilirea în legislația națională a unor proceduri legale împotriva încălcării drepturilor de protecție a datelor, indiferent dacă este posibilă sau nu sesizarea unei autorități de supraveghere.
  - Se impune stabilirea în legislația națională a unor sancțiuni eficiente, echivalente, proporționale şi disuasive.
- Înainte de a sesiza instanțele, reclamantul trebuie să notifice mai întâi operatorul. Obligația de a notifica o autoritate de supraveghere înainte de sesizarea unei instanțe rămâne a fi reglementată în legislația națională.
- În ultimă instanță şi în anumite condiții, persoanele vizate pot să aducă în atenția CEDO cazurile de încălcare a legislației privind protecția datelor.
- De asemenea, persoanele vizate pot sesiza CJUE, însă într-o măsură extrem de limitată.

Drepturile acordate în temeiul legislației privind protecția datelor pot fi exercitate numai de către persoana ale cărei drepturi sunt amenințate, respectiv, persoana care este, sau care cel puțin pretinde că este, persoana vizată. În exercitarea drepturilor lor, aceste persoane pot fi reprezentate de persoane care, în conformitate cu legislația națională, îndeplinesc cerințele impuse. Minorii trebuie să fie reprezentați de către părinții sau tutorii acestora. În fața autorităților de supraveghere, o persoană poate fi reprezentată, de asemenea, de asociații al căror scop legitim este promovarea drepturilor de protecție a datelor.

5.3.1. Cereri adresate operatorului

Drepturile menționate în secțiunea 3.2 trebuie exercitate, în primul rând, în ceea ce privește operatorul. Sesizarea directă a autorității naționale de supraveghere sau a unei instanțe nu ar fi utilă, întrucât autoritatea nu ar putea decât să recomande persoanei respective să se adreseze mai întâi operatorului, în timp ce instanța ar considera cererea inadmisibilă. Cerințele formale privind formularea unei cereri relevante

din punct de vedere legal către operator, în special dacă se impune sau nu să ia forma unei cereri scrise, sunt aspecte ce trebuie reglementate de legislația națională.

Entitatea care a fost sesizată, în calitate de operator, trebuie să răspundă la cerere, chiar dacă aceasta nu este operatorul. În orice caz, trebuie transmis un răspuns persoanei vizate în termenul stabilit în legislația națională, chiar dacă acesta nu conține decât mențiunea că nu există date care fac obiectul prelucrării în ceea ce priveşte solicitantul. În conformitate cu dispozițiile articolului 12 litera (a) din Directiva privind protecția datelor, precum şi cu articolul 8 litera (b) din Convenția 108, la cererea respectivă trebuie să se răspundă „fără întârzieri excesivă". În consecință, legislația națională trebuie să prevadă un termen de răspuns suficient de scurt, dar care să permită operatorului să trateze cererea în mod corespunzător.

Înainte de a răspunde cererii, entitatea sesizată în calitate de operator trebuie să stabilească identitatea solicitantului pentru a constata dacă acesta este într-adevăr persoana care susține că este şi să evite astfel încălcarea gravă a confidențialității. În cazul în care cerințele privind stabilirea identității nu sunt reglementate în mod specific în legislația națională, acestea trebuie stabilite de către operator. Cu toate acestea, principiul prelucrării corecte impune operatorilor să nu stabilească condiții excesiv de împovărătoare în ceea ce priveşte confirmarea identificării (şi autenticitatea cererii, astfel cum s-a discutat în secţiunea 2.1.1).

Legislația națională trebuie să trateze, de asemenea, problema dacă, înainte de a răspunde cererii, operatorii au dreptul de a pretinde solicitantului plata unei taxe: la articolul 12 litera (a) din directivă şi la articolul 8 litera (b) din Convenția 108 se stipulează că răspunsul la cererile de acces trebuie furnizat „fără cheltuieli [...] excesive". Legislația națională din numeroase țări europene prevede ca răspunsurile la cererile formulate în baza legislației privind protecția datelor să fie furnizate gratuit, atât timp cât acest lucru nu implică un efort excesiv şi neobişnuit; la rândul lor, operatorii sunt protejați, în general, prin legislația națională împotriva exercitării abuzive a dreptului de a obține un răspuns la cereri.

Dacă persoana, instituția sau organismul sesizat în calitate de operator nu îşi contestă statutul, entitatea în cauză are obligația, în termenul prevăzut de legislația națională:

- fie să admită cererea şi să notifice solicitantul privind modul în care cererea a fost soluționată, fie

- să informeze solicitantul cu privire la motivul pentru care cererea nu este soluționată.

5.3.2. Cereri înaintate autorității de supraveghere

În cazul în care o persoană, în urma prezentării unei cereri de acces sau formulării unei opoziții față de operator, nu primește un răspuns satisfăcător în timp util, aceasta poate înainta o cerere de asistență autorității naționale de supraveghere a protecției datelor. În cadrul procedurii desfășurate înaintea autorității de supraveghere, trebuie să se clarifice dacă persoana, instituția sau organismul sesizat de solicitant a avut într-adevăr obligația de a răspunde cererii și dacă răspunsul a fost corect și suficient. Autoritatea de supraveghere trebuie să informeze persoana în cauză cu privire la rezultatul procedurii de soluționare a cererii[205]. Efectele juridice ale rezultatelor procedurii desfășurate înaintea autorităților naționale de supraveghere depind de legislația națională: dacă hotărârile emise de autoritate pot fi executate în mod legal, adică de o autoritate publică, sau dacă este necesar să se formuleze o cale de atac înaintea unei instanțe, în cazul în care operatorul nu respectă deciziile (aviz, avertisment etc.) autorității de supraveghere.

În cazul în care se invocă încălcarea drepturilor de protecție a datelor, garantate în conformitate cu articolul 16 din TFUE, de către instituții sau organisme europene, persoana vizată poate depune o plângere la AEPD[206], autoritatea independentă de supraveghere a protecției datelor, în conformitate cu Regulamentul privind protecția datelor de către instituțiile europene, care stabilește responsabilitățile și atribuțiile AEPD. Dacă AEPD nu furnizează un răspuns în termen de șase luni, plângerea se consideră a fi respinsă.

Împotriva hotărârilor emise de o autoritate națională de supraveghere trebuie să existe posibilitatea de a formula o cale de atac înaintea unei instanțe. Această regulă este aplicabilă atât persoanei vizate, cât și operatorilor care au participat la procedura desfășurată înaintea unei autorități de supraveghere.

Exemplu: La 24 iulie 2013, Comisarul pentru informare din Regatul Unit a emis o decizie prin care solicită organelor de poliție din Hertfordshire să suspende

205 Directiva privind protecția datelor, articolul 28 alineatul (4).

206 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, MO 2001 L 8.

utilizarea unui sistem de urmărire a plăcuțelor de înmatriculare ale autovehiculelor considerat a fi ilegal. Datele înregistrate de aparatele de fotografiat au fost stocate atât în bazele de date locale aparținând organelor de poliție, cât şi într-o bază de date centralizată. Fotografiile plăcuțelor de înmatriculare au fost stocate pe o perioadă de doi ani, iar fotografiile autoturismelor timp de 90 de zile. S-a concluzionat că utilizarea excesivă a aparatelor de fotografiat şi a altor forme de supraveghere nu a fost proporțională cu problema care se intenționa a fi soluționată.

5.3.3. Cereri înaintate unei instanțe

În conformitate cu Directiva privind protecția datelor, dacă persoana care a înaintat o cerere unui operator, în conformitate cu legislația privind protecția datelor, nu este mulțumită de răspunsul primit, acesteia trebuie să i se acorde dreptul de a formula o acțiune înaintea unei instanțe naționale[207].

Obligația de a sesiza autoritatea de supraveghere înainte de a formula o acțiune înaintea unei instanțe este reglementată de legislația națională. Cu toate acestea, în majoritatea cazurilor, pentru persoanele care îşi exercită drepturile de protecție a datelor este mai avantajos să sesizeze mai întâi autoritatea de supraveghere, întrucât procedurile privind cererile de asistență adresate acestora se desfăşoară în mod nebirocratic şi gratuit. De asemenea, expertiza documentată în hotărârea autorității de supraveghere (aviz, avertisment etc.) poate ajuta persoana vizată să îşi apere drepturile în fața instanțelor.

În temeiul legislației CoE, încălcările drepturilor de protecție a datelor, despre care se pretinde că au avut loc la nivelul național al unei părți contractante la Convenția europeană a drepturilor omului şi care constituie, în acelaşi timp, o încălcare a articolului 8 din Convenția europeană a drepturilor omului, pot fi, de asemenea, adresate CEDO, după epuizarea tuturor căilor de atac interne disponibile. Invocarea unei încălcări a articolului 8 din Convenția europeană a drepturilor omului înaintea CEDO trebuie să îndeplinească şi alte criterii de admisibilitate (articolele 34-37 din Convenția europeană a drepturilor omului)[208].

207 Directiva privind protecția datelor, articolul 22.

208 Convenția europeană a drepturilor omului, articolele 34-37, disponibilă la: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

Deşi 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 şi-a îndeplinit obligațiile pozitive care îi revin în conformitate cu Convenția europeană a drepturilor omului şi nu a prevăzut, în legislația națională, un nivel corespunzător de protecție împotriva încălcării drepturilor de protecție a datelor.

Exemplu: În cauza *K.U./Finlanda*[209], reclamantul minor a depus o plângere privind postarea unui anunț de natură sexuală la adresa sa pe un site web de anunțuri matrimoniale. Identitatea persoanei care a postat informația nu a fost divulgată de furnizorul de servicii în vederea respectării obligațiilor privind confidențialitatea impuse de legislația din Finlanda. Reclamantul a susținut că legislația finlandeză nu a asigurat un nivel suficient de protecție împotriva unor astfel de acțiuni desfăşurate de o persoană privată, care postează pe internet informații incriminatoare privind reclamantul. CEDO a hotărât că statele nu numai că au obligația de a se abține de la a interveni în mod arbitrar în viața personală 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 şi în ceea ce priveşte relațiile dintre persoane". În cazul reclamantului, pentru a se asigura protecția practică şi eficientă a acestuia, a fost necesar să se ia măsuri eficiente pentru a identifica şi urmări penal autorul infracțiunii. Cu toate acestea, protecția respectivă nu a fost acordată de către stat, iar Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Exemplu: În cauza *Köpke/Germania*[210], reclamanta a fost suspectată de furt la locul de muncă şi, astfel, a fost supusă supravegherii video sub acoperire. CEDO a concluzionat că „niciun aspect nu a indicat că autoritățile naționale nu au stabilit un echilibru corect, în aplicarea marjei de apreciere, între dreptul reclamantei privind respectul față de viața privată a acesteia prevăzut la articolul 8 şi atât interesul angajatorului în protejarea drepturilor de proprietate deținute, cât şi interesul public de bună administrare a justiției". În consecință, cererea a fost declarată inadmisibilă.

Dacă CEDO constată că un stat parte a încălcat oricare dintre drepturile protejate de Convenția europeană a drepturilor omului, statul parte în cauză are obligația de a

209 Hotărârea CEDO din 2 martie 2009 în cauza *K.U./Finlanda*, nr. 2872/02.

210 Hotărârea CEDO din 5 octombrie 2010 în cauza *Köpke/Germania* (dec.), nr. 420/07.

executa hotărârea pronunțată de CEDO. Măsurile de executare trebuie, în primul rând, să pună capăt situațiilor de încălcare şi de înaintarea a unei căi de atac şi, pe cât posibil, consecințelor negative asupra reclamantului. Este, de asemenea, posibil ca pentru executarea hotărârilor judecătoreşti să fie necesară adoptarea de măsuri generale pentru a preveni încălcări similare celor constatate de tribunal, fie prin modificarea legislației sau a jurisprudenței, fie prin aplicarea altor măsuri.

Atunci când CEDO constată o încălcare a Convenției europene a drepturilor omului, la articolul 41 se prevede posibilitatea de a acorda o despăgubire reclamantului pe cheltuiala statului parte.

În temeiul legislației UE[211]**,** victimele încălcărilor legislației naționale privind protecția datelor, care pune în aplicare legislația UE privind protecția datelor, pot, în anumite situații, să îşi prezinte cauzele în fața CJUE. Există două scenarii posibile privind modalitatea în care cererea unei persoane vizate, care invocă încălcarea drepturilor de protecție a datelor sale, poate conduce la proceduri în fața CJUE.

În primul scenariu, persoana vizată este victima directă a unor acte administrative sau normative europene care încalcă dreptul persoanelor la protecția datelor. În conformitate cu articolul 263 alineatul (4) din TFUE:

> *„orice persoană fizică sau juridică poate [...] formula o acțiune împotriva actelor al căror destinatar este sau care o privec direct și individual, precum și împotriva actelor normative care o privesc direct și care nu presupun măsuri de executare."*

În consecință, victimele unei prelucrării ilegale a datelor de către un organism european pot face recurs direct la Tribunalul CJUE, care reprezintă organismul abilitat să pronunțe hotărâri în cauze care au legătură cu Regulamentul privind protecția datelor de către instituțiile europene. De asemenea, există posibilitatea de a sesiza CJUE, în mod direct, atunci când situația juridică a unei entități este afectată în mod direct de o prevedere legală europeană.

Al doilea scenariu se referă la competența CJUE (Curtea de Justiție) de a pronunța hotărâri preliminare, în conformitate cu articolul 267 din TFUE.

211 UE (2007), Tratatul de la Lisabona de modificare a Tratatului privind Uniunea Europeană şi a Tratatului de instituire a Comunității Europene, semnat la Lisabona, 13 decembrie 2007, MO 2007 C 306. A se vedea, de asemenea, versiunile consolidate ale Tratatului privind Uniunea Europeană, MO 2012 C 326 şi ale TFUE, MO 2012 C 326.

În cadrul procedurilor interne, persoanele vizate pot pretinde instanței naționale să solicite clarificări Curții de Justiție privind interpretarea tratatelor europene şi privind interpretarea şi valabilitatea actelor emise de instituțiile, organele, oficiile sau agențiile europene. Aceste clarificări sunt cunoscute sub numele de hotărâri preliminare. Această procedură nu reprezintă o cale de atac directă pentru reclamant, însă permite instanțelor naționale să se asigure că aplică interpretarea corectă a dreptului UE.

Dacă o parte la procedura desfăşurată în fața instanțelor naționale solicită sesizarea CJUE într-o anumită cauză, numai instanțele naționale, acționând ca instanțe de recurs de ultim grad şi ale căror hotărâri nu pot fi atacate, au obligația de a da curs unei astfel de cereri.

Exemplu: În cauza *Kärntner Landesregierung şi alții*[212], Curtea Constituțională a Austriei a adresat întrebări CJUE privind valabilitatea articolelor 3-9 din Directiva 2006/24/CE (*Directiva privind păstrarea datelor*) în conformitate cu articolele 7, 9 şi 11 din Cartă şi dacă anumite dispoziții ale Legii federale privind telecomunicațiile, de transpunere a Directivei privind păstrarea datelor au fost incompatibile cu aspectele prezentate în Directiva privind protecția datelor şi Regulamentul privind protecția datelor de către instituțiile europene.

Domnul Seitlinger, unul dintre reclamanții în procedura desfăşurată în fața Curții Constituționale, a afirmat că utilizează serviciile de telefonie, internet şi e-mail atât în interes de serviciu, cât şi în interes personal. Astfel, informațiile pe care le trimite şi pe care le primeşte sunt transmise utilizând rețelele publice de telecomunicații. În conformitate cu Legea austriacă privind telecomunicațiile din 2003, furnizorul acestuia de servicii de telecomunicații este obligat prin lege să colecteze şi să stocheze datele privind modul în care clientul utilizează rețeaua. Domnul Seitlinger a realizat că această modalitate de colectare şi stocare a datelor sale cu caracter personal nu avea utilitate tehnică în procesul de transmitere a informațiilor de la A la B prin intermediul rețelei. Mai mult decât atât, colectarea şi stocarea datelor respective nu erau sub nicio formă necesare, în vederea facturării. În mod sigur, domnul Seitlinger nu a consimțit asupra acestui mod de utilizare a datelor sale cu caracter personal. Singurul motiv pentru care s-a efectuat colectarea şi stocarea tuturor aceste date suplimentare a fost Legea austriacă privind telecomunicațiile din 2003.

212 Hotărârea CJUE din 8 aprilie 2014 în Cauzele comune *Drepturile Digitale Irlanda și Seiling și ceilalți*, C-293/12 şi C-594/12,.

În consecință, domnul Seitlinger a formulat o acțiune înaintea Curții Constituționale a Austriei, în care a susținut că obligațiile legale impuse furnizorului de servicii de telecomunicații au încălcat drepturile sale fundamentale, în conformitate cu articolul 8 din Carta UE.

CJUE emite o decizie numai privind elementele constitutive ale cererii de hotărâre preliminară formulată în fața acesteia. Instanța națională îşi păstrează competența de a se pronunța în cauza inițială.

În principiu, Curtea de Justiție trebuie să răspundă la întrebările care îi sunt adresate. Aceasta nu poate refuza pronunțarea unei hotărâri preliminare pe motiv că acest răspuns nu ar fi relevant sau furnizat în timp util în cauza inițială. Cu toate acestea, instanța poate refuza furnizarea unui răspuns dacă întrebarea nu se încadrează în sfera sa de competență.

În cele din urmă, dacă se invocă încălcarea drepturilor de protecție a datelor, garantate în temeiul articolului 16 din TFUE, de către o instituție sau organism european în timpul prelucrării datelor cu caracter personal, persoana vizată poate sesiza Tribunalul CJUE [articolul 32 alineatele (1) şi (4) din Regulamentul privind protecția datelor de către instituțiile europene]. Aceeaşi regulă se aplică în cazul deciziilor pronunțate de AEPD privind astfel de încălcări [articolul 32 alineatul (3) din Regulamentul privind protecția datelor de către instituțiile europene].

Chiar dacă Tribunalul CJUE deține competența de a pronunța hotărâri în cauze care au legătură cu Regulamentul privind protecția datelor de către instituțiile europene, în cazul în care o persoană, în calitate de membru al personalului unei instituții sau unui organism european, formulează, totuşi, o cale de atac, aceasta trebuie să înainteze recursul la Tribunalul Funcției Publice a UE.

Exemplu: Cauza *Comisia Europeană/The Bavarian Lager Co. Ltd*[213] ilustrează căile de atac disponibile împotriva activităților sau deciziilor instituțiilor şi organismelor europene în ceea ce priveşte protecția datelor.

Bavarian Lager a solicitat Comisiei Europene să îi acorde accesul la conținutul complet al procesul-verbal al unei reuniuni organizate de Comisie şi despre care se susține că vizează aspecte juridice relevante pentru societate. Comisia a respins cererea

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

de acces a societății pe motiv că primează interesele privind protecția datelor[214]. În conformitate cu articolul 32 din Regulamentul privind protecția datelor de către instituțiile europene, Bavarian Lager a depus o plângere împotriva acestei decizii înaintea CJUE, mai exact, înaintea Tribunalului de Primă Instanță (precursor al Tribunalului). Prin hotărârea pronunțată în cauza *Bavarian Lager/Comisia*, T-194/04, Tribunalul de Primă Instanță a anulat decizia Comisiei de respingere a cererii de acces. Comisia Europeană a atacat această decizie la Curtea de Justiție a CJUE. Curtea de Justiție a pronunțat o hotărâre (în Marea Cameră) prin care a respins hotărârea Tribunalului de Primă Instanță și a confirmat respingerea cererii de acces de către Comisia Europeană.

5.3.4. Sancțiuni

În temeiul legislației CoE, articolul 10 din Convenția 108 prevede ca fiecare parte să stabilească sancțiuni și căi de atac adecvate pentru încălcarea dispozițiilor dreptului intern care pun în aplicare principiile de bază privind protecția datelor prevăzute în Convenția 108215. **În temeiul dreptului UE**, articolul 24 din Directiva privind protecția datelor prevede că statele membre „adoptă măsuri adecvate pentru a asigura aplicarea integrală a dispozițiilor prezentei directive și, în special, stabilește sancțiunile care urmează să fie aplicate în caz de încălcare a dispozițiilor [...]".

Ambele instrumente acordă statelor membre o marjă de apreciere considerabilă în alegerea sancțiunilor și a căilor de atac adecvate. Niciunul dintre cele două instrumente juridice nu furnizează indicații speciale privind natura sau tipul de sancțiuni corespunzătoare și nici nu prezintă exemple de sancțiuni.

Cu toate acestea:

> *„Cu toate că statele membre ale UE beneficiază de o marjă de apreciere în a stabili care sunt cele mai adecvate măsuri pentru protejarea drepturilor care le revin persoanelor fizice în baza dreptului UE, în conformitate cu principiul cooperării loiale prevăzut la articolul 4 alineatul (3) din TUE, trebuie să se*

214 Pentru analiza argumentului, a se vedea: AEPD (2011), documentul *Accesul public la documente conținând date cu caracter personal ulterior hotărârii în cauza* Bavarian Lager, Bruxelles, AEPD, disponibil la: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

215 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.

respecte cerințele minime de eficiență, de echivalență, de proporționalitate și de descurajare"[216].

CJUE a susținut în repetate rânduri că legislația națională nu dispune de independență deplină în stabilirea de sancțiuni.

Exemplu: În cauza *Von Colson și Kamann/Land Nordrhein-Westfalen*[217], CJUE a subliniat că toate statele membre cărora li se adresează o directivă sunt obligate să adopte, în sistemele lor juridice naționale, toate măsurile necesare pentru a asigura efectul deplin al acesteia, în conformitate cu obiectivul pe care îl urmăreşte. Curtea a constatat că, deşi rămâne la latitudinea statelor membre să aleagă căile şi mijloacele prin care să asigure punerea în aplicare a unei directive, independența nu afectează obligația impusă acestora. În special, o cale de atac eficientă trebuie să permită unei persoane să urmărească şi să exercite dreptul în cauză în cea mai mare măsură. Pentru a obține o protecție efectivă şi eficientă, căile de atac trebuie să aibă drept rezultat inițierea unor proceduri penale şi/sau compensatorii care să atragă aplicarea unor sancțiuni cu caracter de descurajare.

În ceea ce priveşte 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 sunt prevăzute numai sub formă de acțiuni disciplinare. În conformitate cu articolul 49 din regulament, „orice neîndeplinire a obligațiilor prevăzute de prezentul regulament, fie aceasta intenționată sau din culpă, atrage după sine sancțiuni disciplinare asupra funcționarului sau agentului Comunităților Europene [...]".

216 FRA(2012), *Avizul Agenției Uniunii Europene pentru Drepturi Fundamentale privind pachetul de reforme propus privind protecția datelor*, 2/2012, Viena, 1 octombrie 2012, p. 27.

217 Hotărârea CJUE din 10 aprilie 1984 în cauza *Sabine von Kolson și Elisabeth Kamann/Land Nordrhein-Westfalen*, C14/83.

6

Fluxuri transfrontaliere de date

UE	Aspecte vizate	CoE
Fluxuri transfrontaliere de date		
Directiva privind protecția datelor, articolul 25 alineatul (1) CJEU, C-101/01, *Bodil Lindqvist*, 6 noiembrie 2003	**Definiție**	Convenția 108, Protocol adițional, articolul 2 alineatul (1)
Libera circulație a datelor		
Directiva privind protecția datelor, articolul 1 alineatul (2)	**Între statele membre ale UE**	
	Între părțile contractante la Convenția 108	Convenția 108, articolul 12 alineatul (2)
Directiva privind protecția datelor, articolul 25	**Către țări terțe cu nivel corespunzător de protecție a datelor**	Convenția 108, Protocol adițional, articolul 2 alineatul (1)
Directiva privind protecția datelor, articolul 26 alineatul (1)	**Către țări terțe în cazuri specifice**	Convenția 108, Protocol adițional, articolul 2 alineatul (2) litera (a)
Flux restricționat de date către țări terțe		
Directiva privind protecția datelor, articolul 26 alineatul (2) Directiva privind protecția datelor, articolul 26 alineatul (4)	**Clauze contractuale**	Convenția 108, Protocol adițional, articolul 2 alineatul (2) litera (b) Ghidul privind elaborarea clauzelor contractuale
Directiva privind protecția datelor, articolul 26 alineatul (2)	**Reguli corporatiste obligatorii**	
Exemple: Acordul PNR între UE și SUA Acordul SWIFT între UE și SUA	**Acorduri internaționale specifice**	

Directiva privind protecția datelor nu prevede doar un flux liber de date între statele membre, ci conține şi dispoziții privind cerințele pentru transferul de date cu caracter personal către țări terțe din afara UE. CoE a recunoscut, de asemenea, importanța punerii în aplicare a normelor privind fluxurile transfrontaliere de date către țările terțe şi a adoptat în anul 2001 Protocolul adițional la Convenția 108. Acest protocol a preluat principalele caracteristici normative privind fluxurile transfrontaliere de date de la părțile la convenție şi statele membre ale UE.

6.1. Natura fluxurilor transfrontaliere de date

Puncte-cheie

- Fluxul transfrontalier de date este un transfer de date cu caracter personal către un destinatar aflat sub o jurisdicție străină.

Articolul 2 alineatul (1) din Protocolul adițional la Convenția 108 descrie fluxul transfrontalier de date ca transferul de date cu caracter personal către un destinatar aflat sub o jurisdicție străină. Articolul 25 alineatul (1) din Directiva privind protecția datelor reglementează „transferul către o țară terță a datelor cu caracter personal care fac obiectul prelucrării sau sunt destinate prelucrării după transfer [...]". Un astfel de transfer de date este permis doar în conformitate cu normele stabilite la articolul 2 din Protocolul adițional la Convenția 108, iar în cazul statelor membre ale UE, de asemenea, la articolele 25 şi 26 din Directiva privind protecția datelor.

Exemplu: În cauza *Bodil Lindqvist*[218], CJUE a constatat că „actul care face trimitere, pe o pagină de internet, la diverse persoane şi le identifică după nume sau prin alte mijloace, de exemplu, prin furnizarea numărului de telefon al acestora sau prin furnizarea de informații referitoare la condițiile de muncă şi pasiunile persoanelor respective, constituie «prelucrarea datelor personale integral sau parțial prin mijloace automatizate», în sensul articolului 3 alineatul (1) din Directiva 95/46".

Pe de altă parte, Curtea a subliniat că directiva stabileşte, de asemenea, norme specifice care au rolul de a permite statelor membre să monitorizeze transferul de date cu caracter personal către țări terțe.

218 Hotărârea CJUE din 6 noiembrie 2003 în cauza *Bodil Lindqvist*, C-101/01, punctele 27, 68 şi 69.

Cu toate acestea, având în vedere, în primul rând, stadiul de dezvoltare a internetului în momentul elaborării directivei şi, în al doilea rând, lipsa din directivă a criteriilor aplicabile utilizărilor internetului, „nu se poate presupune că legiuitorul Comunității a intenționat ca expresia «transfer [de date] către o țară terță» să includă încărcarea [...] unor date pe o pagină de internet, chiar dacă datele sunt accesibile persoanelor din țările terțe care dispun de mijloacele tehnice pentru a le accesa".

În caz contrar, dacă directiva ar fi „interpretată în sensul că transferul de date către o țară terță are loc de fiecare dată când datele cu caracter personal sunt încărcate pe o pagină de internet, transferul ar fi, în mod obligatoriu, un transfer către toate țările terțe în care există mijloacele tehnice necesare pentru accesarea internetului. Astfel, regimul special prevăzut [de directivă] ar deveni, în mod obligatoriu, un regim de aplicare generală, în ceea ce priveşte operațiunile desfăşurate pe internet. În consecință, în cazul în care Comisia ar constata [...] că o singură țară terță nu asigură un nivel de protecție adecvat, statele membre ar fi obligate să împiedice publicarea pe internet a oricăror date cu caracter personal".

Principiul conform căruia simpla publicare a datelor (cu caracter personal) nu este considerată drept flux transfrontalier de date se aplică, de asemenea, şi în cazul registrelor publice online sau mijloacelor de informare în masă, precum ziarele (electronice) şi televiziunea. Numai comunicarea care este direcționată către anumiți destinatari este eligibilă pentru noțiunea de „flux transfrontalier de date".

6.2. Fluxurile libere de date între statele membre sau între părțile contractante

Puncte-cheie

- Transferul de date cu caracter personal către un alt stat membru din Spațiul Economic European sau către o altă parte contractantă la Convenția 108 nu trebuie să fie restricționat.

În conformitate cu articolul 12 alineatul (2) din Convenția 108, **în temeiul legislației CoE** trebuie să existe un flux liber de date cu caracter personal între părțile la convenție. Dreptul intern nu poate restricționa exportul de date cu caracter personal către o parte contractantă, cu excepția cazului în care:

- caracterul specific al datelor impune acest lucru[219] sau

- aplicarea restricției este necesară pentru a evita sustragerea de la prevederile legale interne privind fluxul transfrontalier de date către terți[220].

În temeiul dreptului UE, nu este permisă aplicarea unor restricții sau interdicții asupra fluxului liber de date între statele membre din motive legate de protecția datelor, în conformitate cu articolul 1 alineatul (2) din Directiva privind protecția datelor. Zona de flux gratuit de date a fost extinsă prin Acordul privind Spațiul Economic European (SEE)[221], în baza căruia Islanda, Liechtenstein și Norvegia sunt incluse pe piața internă.

Exemplu: Dacă o societate afiliată unui grup internațional de societăți, având sedii în mai multe state membre ale UE, 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 național din Slovenia.

Cu toate acestea, dacă aceeași societate afiliată din Slovenia dorește să transfere aceleași date cu caracter personal către societatea-mamă din Statele Unite, exportatorul de date sloven trebuie să parcurgă procedurile prevăzute în dreptul sloven în ceea ce privește fluxul transfrontalier de date către țări terțe care nu au un nivel corespunzător de protecție a datelor, cu excepția cazului în care societatea-mamă a aderat la Principiile sferei de siguranță privind protecția vieții private, un cod de conduită voluntar privind asigurarea unui nivel adecvat de protecție a datelor (a se vedea secțiunea 6.3.1)

Fluxurile transfrontaliere de date către statele membre ale SEE în scopuri care nu intră în sfera pieței interne, precum investigarea infracțiunilor, nu fac, totuși, obiectul dispozițiilor Directivei privind protecția datelor și, prin urmare, nu intră sub incidența principiului liberei circulații a datelor. În ceea ce privește legislația CoE, toate zonele sunt incluse în domeniul de aplicare al Convenției 108 și al Protocolului adițional la Convenția 108, deși părțile contractante pot face excepții. Toate statele membre ale SEE sunt, de asemenea, părți la Convenția 108.

219 Convenția 108, articolul 12 alineatul (3) litera (a).

220 *Ibidem*, articolul 12 alineatul (3) litera (b).

221 Decizia 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, MO 1994 L 1.

6.3. Fluxuri libere de date către țări terțe

Puncte-cheie

- Transferul de date cu caracter personal către țări terțe nu este restricționat în conformitate cu dreptul național privind protecția datelor, atunci când:
  - s-a constatat caracterul adecvat al protecției datelor la destinatar sau
  - este necesar pentru interesele specifice ale persoanei vizate sau pentru interesele legitime prioritare ale altor persoane, în special interese publice importante.
- Caracterul adecvat al protecției datelor într-o țară terță înseamnă că principiile de bază ale protecției datelor au fost puse în aplicare în mod eficient în dreptul național al țării respective.
- În temeiul dreptului UE, caracterul adecvat al protecției datelor într-o țară terță este evaluat de Comisia Europeană. În conformitate cu legislația CoE, reglementarea evaluării caracterului adecvat revine dreptului național.

6.3.1. Flux liber de date datorită unei protecții adecvate

Legislația CoE autorizează dreptul intern să permită libera circulație a datelor către state non-contractante dacă statul destinatar sau organizația destinatară asigură un nivel adecvat de protecție pentru transferul de date intenționat[222]. Dreptul intern decide modul de evaluare a nivelului de protecție a datelor într-o țară străină şi autorul evaluării.

În temeiul dreptului UE, fluxul liber de date către țări terțe, cu un nivel adecvat de protecție a datelor, este prevăzut la articolul 25 alineatul (1) din Directiva privind protecția datelor. Cerința privind caracterul adecvat, mai curând decât echivalența, face posibilă utilizarea unor metode diferite de punere în aplicare a protecției datelor. În conformitate cu articolul 25 alineatul (6) din directivă, Comisia Europeană deține competența de a evalua nivelul de protecție a datelor în țări străine în baza unor constatări privind caracterul adecvat şi se consultă, în materie de evaluare, cu Grupul de lucru Articolul 29, care a contribuit substanțial la interpretarea articolelor 25 şi 26[223].

222 Convenția 108, Protocol adițional, articolul 2 alineatul (1).

223 A se vedea, de exemplu, Grupul de lucru Articolul 29 (2003), *Document de lucru privind transferurile de date cu caracter personal către țările terțe: punerea în aplicare a articolului 26 alineatul (2) din Directiva UE privind protecția datelor în cazul regulilor corporatiste obligatorii privind transferurile internaționale de date*, WP 74, Bruxelles, 3 iunie 2003 şi Grupul de lucru Articolul 29 (2005), *Document de lucru privind interpretarea comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995*, WP 114, Bruxelles, 25 noiembrie 2005.

O decizie a Comisiei Europene privind caracterul adecvat are efect obligatoriu. Atunci când Comisia Europeană publică o decizie privind caracterul adecvat, pentru o anumită țară, în *Monitorul Oficial al Uniunii Europene*, toate țările membre ale SEE şi organele acestora sunt obligate să respecte decizia respectivă, ceea ce înseamnă că datele pot circula către țara în cauză fără a fi necesară desfăşurarea de proceduri de verificare sau de autorizare în fața autorităților naționale[224].

De asemenea, Comisia Europeană poate evalua secțiuni ale sistemului juridic al unei țări sau să se limiteze la subiecte specifice. Comisia a luat o decizie privind caracterul adecvat, de exemplu, numai cu privire la dreptul comercial privat al Canadei[225]. Există, de asemenea, mai multe constatări privind caracterul adecvat în cazul transferurilor efectuate în baza acordurilor încheiate între UE şi statele străine. Aceste decizii se referă exclusiv la un singur tip de transfer de date, precum transmiterea registrelor cu numele pasagerilor de către companiile aeriene autorităților de control la frontierele străine, atunci când o companie aeriană efectuează zboruri din UE către anumite destinații transoceanice (a se vedea secțiunea 6.4.3). Practica recentă de transferare a datelor în baza unor acorduri specifice încheiate între UE şi țările terțe, în general, anulează necesitatea adoptării de decizii privind caracterul adecvat, presupunând că acordul în sine oferă un nivel adecvat de protecție a datelor[226].

Una dintre cele mai importante decizii privind caracterul adecvat nu se referă de fapt la un set de prevederi legale[227]. Aceasta vizează, mai curând normele, în genul unui cod de conduită, cunoscute sub denumirea de Principiile sferei de siguranță privind protecția vieții private. Aceste principii au fost elaborate între Uniunea Europeană şi Statele Unite ale Americii pentru societățile comerciale din SUA. Apartenența la

224 Pentru o listă permanent actualizată a țărilor care au primit o decizie privind caracterul adecvat, a se vedea pagina de întâmpinare a Comisiei Europene, Direcția Generală pentru Justiție, disponibilă la: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

225 Comisia Europeană (2002), Decizia 2002/2/CE din 20 decembrie 2001 în conformitate cu Directiva 95/46/CE a Parlamentului European şi a Consiliului privind caracterul adecvat al protecției datelor cu caracter personal asigurat prin legea canadiană referitoare la protecția informațiilor personale şi documentele electronice, MO 2002 L 2.

226 De exemplu, Acordul dintre Statele Unite ale Americii şi Uniunea Europeană privind utilizarea şi transferul de date din registrele cu numele pasagerilor către Departamentul pentru Securitate Internă al Statelor Unite (MO 2012 L 215, pp. 5-14), sau Acordul între Uniunea Europeană şi Statele Unite ale Americii privind prelucrarea şi transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțărilor în scopuri teroriste, MO 2010 L 8, pp. 1116.

227 Comisia Europeană (2000), Decizia 2000/520/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European şi a Consiliului privind caracterul adecvat al protecției oferite de principiile sferei de siguranță privind protecția vieții private şi întrebările de bază aferente publicate de Departamentul de Comerț al SUA, MO 2000 L 215.

Principiile sferei de siguranță privind protecția vieții private se obține prin angajament voluntar declarat în fața Departamentului de Comerț al SUA şi documentat într-o listă publicată de respectivul departament. Având în vedere că unul dintre cele mai importante elemente ale caracterului adecvat este eficiența punerii în aplicare a protecției datelor, Acordul privind sfera de siguranță asigură, de asemenea, un anumit nivel de supraveghere din partea statului: numai societățile care fac obiectul supravegherii Comisiei Federale pentru Comerț din SUA pot deveni părți la Acordul privind sfera de siguranță.

6.3.2. Flux liber de date în cazuri specifice

În temeiul legislației CoE, articolul 2 alineatul (2) din Protocolul adițional la Convenția 108 permite transferul de date cu caracter personal către țări terțe care nu dețin un nivel adecvat de protecție a datelor, atâta timp cât transferul este prevăzut de dreptul național şi este necesar pentru:

- interesele specifice ale persoanei vizate sau
- interese legitime predominante ale altor persoane, în special interese publice importante.

În temeiul dreptului UE, articolul 26 alineatul (1) din Directiva privind protecția datelor conține dispoziții similare cu cele ale Protocolului adițional la Convenția 108.

În conformitate cu directiva, interesele persoanei vizate pot justifica libera circulație a datelor către o țară terță în cazul în care:

- persoana vizată consimte în mod expres asupra exportului de date sau
- persoana vizată încheie – sau se pregăteşte să încheie – o relație contractuală care prevede în mod clar transferul de date către un destinatar din străinătate sau
- s-a încheiat un contract între un operator de date şi un terț în interesul persoanei vizate sau
- transferul este necesar pentru protejarea intereselor esențiale ale persoanei vizate;
- în vederea transferului de date din registrele publice; acesta este un exemplu de interese prioritare ale publicului larg pentru a putea avea acces la informațiile stocate în registrele publice.

Interesele legitime ale altor persoane pot justifica fluxul liber transfrontalier de date[228]:

- datorită unui interes public important, altele decât interesele de siguranță națională sau publică, întrucât acestea nu fac obiectul Directivei privind protecția datelor sau

- pentru a formula, aplica sau apăra cereri legale.

Cazurile menționate mai sus trebuie înțelese drept excepții de la norma potrivit căreia transferul direct de date către alte țări necesită un nivel adecvat de protecție a datelor în țara destinatară. Excepțiile trebuie să fie întotdeauna interpretate în mod restrictiv. Acest aspect a fost subliniat în mod repetat de către Grupul de lucru Articolul 29 în contextul articolului 26 alineatul (1) din Directiva privind protecția datelor, în special atunci când se pretinde că transferul de date se efectuează pe bază de consimțământ[229]. Grupul de lucru Articolul 29 a concluzionat că normele generale cu privire la semnificația juridică a consimțământului se aplică, de asemenea, articolului 26 alineatul (1) din directivă. În cazul în care, în cadrul relațiilor de muncă, de exemplu, nu este clar dacă consimțământul dat de angajați a fost de fapt liber exprimat, transferurile de date nu pot fi efectuate în temeiul articolului 26 alineatul (1) litera (a) din directivă. În astfel de cazuri, se aplică articolul 26 alineatul (2), prin care se solicită autorităților naționale pentru protecția datelor să emită o autorizație pentru transferurile de date.

6.4. Fluxuri restricționate de date către țări terțe

Puncte-cheie

- Înainte de a exporta date către țări terțe care nu asigura un nivel adecvat de protecție a datelor, i se poate solicita operatorului să supună fluxul de date respectiv unei analize efectuate de către autoritatea de supraveghere.

228 Directiva privind protecția datelor, articolul 26 alineatul (1) litera (d).

229 A se vedea în special Grupul de lucru Articolul 29 (2005), *Document de lucru privind interpretarea comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995*, WP 114, Bruxelles, 25 noiembrie 2005.

- Operatorul care intenționează să exporte date trebuie să demonstreze două aspecte în cadrul acestei analize:
  - că există un temei juridic pentru transferul de date către destinatar şi
  - că se aplică măsuri pentru a asigura un nivel adecvat de protecție a datelor la destinatar.
- Măsurile pentru asigurarea unui nivel adecvat de protecție a datelor la destinatar pot include:
  - prevederi contractuale între operatorul care exportă date şi destinatarul din străinătate al datelor sau
  - reguli corporatiste obligatorii aplicabile, de regulă, transferurilor de date în cadrul unui grup multinațional de societăți.
- Transferurile de date către autoritățile străine pot fi, de asemenea, reglementate printr-un acord internațional specific.

Directiva privind protecția datelor şi Protocolul adițional la Convenția 108 autorizează dreptul național să stabilească regimuri pentru fluxurile transfrontaliere de date către țări terțe care nu asigură un nivel adecvat de protecție a datelor, atât timp cât operatorul a luat măsuri speciale pentru a oferi garanții adecvate de protecție a datelor la destinatar şi cu condiția ca operatorul să poată dovedi acest lucru în fața unei autorități competente. Această cerință este menționată explicit numai în Protocolul adițional la Convenția 108; cu toate acestea, cerința este considerată, de asemenea, a fi o procedură standard în conformitate cu Directiva privind protecția datelor.

6.4.1. Clauze contractuale

Atât **legislația CoE**, cât şi **dreptul UE** menționează clauze contractuale între operatorul care exportă date şi destinatarul din țara terță, ca un potențial mijloc de asigurare a unui nivel suficient de protecție a datelor la destinatar.

La **nivelul UE**, Comisia Europeană, cu sprijinul Grupului de lucru Articolul 29, a elaborat clauze contractuale standard care au fost certificate oficial printr-o decizie a Comisiei, ca dovadă a protecției adecvate a datelor[230]. Întrucât deciziile Comisiei sunt în totalitate obligatorii în statele membre, autoritățile naționale responsabile de supravegherea fluxurile transfrontaliere de date trebuie să recunoască aceste clauze

230 Directiva privind protecția datelor, articolul 26 alineatul (4).

contractuale standard în procedurile aplicate[231]. Astfel, dacă operatorul care exportă date şi destinatarul din țara terță sunt de acord şi semnează aceste clauze, acest lucru trebuie să furnizeze autorității de supraveghere dovezi suficiente ale faptului că se oferă garanții adecvate.

Existența unor clauze contractuale standard în cadrul juridic al UE nu interzice operatorilor să formuleze alte clauze contractuale *ad hoc*. Cu toate acestea, aceştia trebuie să asigure acelaşi nivel de protecție prevăzut de clauzele contractuale standard. Cele mai importante caracteristici ale clauzelor 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 desfăşurate de autoritatea națională de supraveghere şi/sau de instanțele operatorului care exportă date.

În prezent, operatorul care exportă date are posibilitatea de a alege între două seturi de clauze standard pentru transferurile de la operator la operator[232]. Pentru transferurile de la operator la împuternicit, există un singur set de clauze contractuale standard[233].

În contextul **legislației CoE**, Comitetul Consultativ al Convenției 108 a elaborat un ghid privind elaborarea clauzelor contractuale[234].

231 TFUE, articolul 288.

232 Setul I este inclus în anexa la Comisia Europeană (2001), Decizia 2001/497/CE a Comisiei din 15 iunie 2001 privind clauzele contractuale standard pentru transferul de date cu caracter personal către țări terțe în temeiul Directivei 95/46/CE, MO 2001 L 181; Setul II este inclus în anexa la Comisia Europeană (2004), 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, MO 2004 L 385.

233 Comisia Europeană (2010), Decizia 2010/87 a Comisiei din 5 februarie 2010 privind clauzele contractuale tip pentru transferul de date cu caracter personal către împuterniciții stabiliți în țări terțe, în temeiul Directivei 95/46/CE a Parlamentului European şi a Consiliului, MO 2010 L 39.

234 CoE, Comitetul Consultativ al Convenției 108 (2002), *Ghid privind elaborarea clauzelor contractuale care reglementează protecția datelor în cadrul transferului de date cu caracter personal către părți terțe care nu au obligația de a asigura un nivel adecvat de protecție a datelor*.

6.4.2. Reguli corporatiste obligatorii

Regulile corporatiste obligatorii (BCR) multilaterale implică, în mod frecvent, mai multe autorități europene pentru protecția datelor[235]. Pentru ca BCR să fie aprobate, proiectul BCR trebuie transmis împreună cu formularele de cerere standardizate la autoritatea principală[236]. Autoritatea principală este identificabilă din formularul de cerere standardizat. Această autoritate informează toate autoritățile de supraveghere din țările membre ale SEE în care sunt stabiliți societățile afiliate grupului, deşi participarea acestora la procesul de evaluare a BCR este voluntară. Cu toate că nu este obligatoriu, toate autoritățile pentru protecția datelor în cauză trebuie să includă rezultatul evaluării în procedurile oficiale de autorizare.

6.4.3. Acorduri internaționale specifice

UE a încheiat acorduri specifice pentru două tipuri de transferuri de date:

Registre cu numele pasagerilor

Datele incluse în registrul cu numele pasagerilor (PNR) sunt colectate de transportatorii aerieni pe parcursul procesului de rezervare şi includ nume, adrese, detalii ale cărților de credit şi numerele locurilor pasagerilor transportului aerian. În conformitate cu legislația SUA, companiile aeriene sunt obligate să furnizeze aceste date Departamentului de Securitate Internă înainte de plecarea pasagerilor. Această regulă se aplică zborurilor către sau dinspre Statele Unite ale Americii.

Pentru a se asigura protecția adecvată datelor PNR şi în conformitate cu prevederile Directivei 95/46/CE, un „pachet PNR"[237] a fost adoptat în 2004. Pachetul includea

235 Conținutul şi structura regulilor corporatiste obligatorii corespunzătoare sunt explicate în cadrul Grupului de lucru Articolul 29 (2008), *Document de lucru de stabilire a unui cadru pentru structura regulilor corporatiste obligatorii*, WP 154, Bruxelles, 24 iunie 2008 şi cadrul Grupului de lucru Articolul 29 (2008), *Document de lucru pentru crearea unui tabel cu elementele și principiile care trebuie incluse în regulile corporatiste obligatorii*, WP 153, Bruxelles, 24 iunie 2008.

236 Grupul de lucru Articolul 29 (2007), *Recomandarea 1/2007 privind cererea standard pentru aprobarea regulilor corporatiste obligatorii pentru transferul de date cu caracter personal*, WP 133, Bruxelles, 10 ianuarie 2007.

237 Decizia Consiliului nr. 496/2004 privind încheierea unui Acord între Comunitatea Europeană şi Statele Unite ale Americii privind prelucrarea şi transferul datelor PNR de la transportatorii aerieni către Departamentul de Securitate Internă al Statelor Unite, Biroul Vamal și de Protecție a Frontierelor, MO 2004 L 183, p. 83 şi Decizia Comisiei nr. 2004/533/CE din 14 mai 2004 privind protecția adecvată a datelor cu caracter personal din registrele nominale ale pasagerilor aerieni transferate către Biroul vamal și de protecție la frontieră al Statelor Unite ale Americii, MO 2004 L 235, pp. 11-22.

caracterul adecvat al prelucrărilor de date efectuate de Departamentul de Securitate Internă din Statele Unite ale Americii (DSI).

Urmare deciziei CJUE de anulare a pachetului PNR[238], UE și Statele Unite ale Americii au semnat două acorduri separate cu un scop dublu: în primul rând, să asigure un temei juridic pentru dezvăluirea datelor PNR către autoritățile din Statele Unite ale Americii, iar, în al doilea rând, să stabilească un nivel adecvat de protecție a datelor în țara destinatară.

Primul acord privind modalitatea de comunicare și de gestionare a datelor între țările UE și Statele Unite ale Americii, semnat în 2012, prezenta o serie de deficiențe și a fost înlocuit, în același an, cu un nou acord pentru a asigura un nivel mai ridicat de securitate juridică[239]. Noul acord oferă îmbunătățiri semnificative. Acesta limitează și clarifică scopurile pentru care pot fi utilizate informațiile, cum ar fi infracțiuni transnaționale grave și terorism și stabilește perioada de păstrare a datelor: după 6 luni datele trebuie depersonalizate și mascate. În cazul în care datele sunt utilizate în mod necorespunzător, orice persoană are dreptul de a formula căi de atac administrative și judiciare, în conformitate cu legislația Statelor Unite. Cetățenii UE au, de asemenea, dreptul de a accesa propriile date PNR și de a solicita rectificarea acestora de către Departamentul pentru Securitate Internă, inclusiv posibilitatea de ștergere, în cazul în care informațiile sunt incorecte.

Acordul, care a intrat în vigoare la data de 1 iulie 2012, rămâne în vigoare pentru o perioadă de șapte ani, până în 2019.

În decembrie 2011, Consiliul Uniunii Europene a aprobat încheierea Acordului actualizat UE – Australia privind prelucrarea și transferul de date PNR[240]. Acordul dintre UE și Australia privind datele PNR reprezintă un pas înainte pe agenda UE, care cuprinde

238 Hotărârea CJUE din 30 mai 2006, cauze comune *Parlamentul European/Consiliul Uniunii Europene*, C-317/04 și C-318/04, punctele. 57, 58 și 59, în care Curtea a decis că atât decizia privind nivelul adecvat, cât și acordul privind prelucrarea datelor sunt excluse din domeniul de aplicare al Directivei.

239 Decizia 2012/472/UE a Consiliului din 26 aprilie 2012 privind încheierea Acordului între Statele Unite ale Americii și Uniunea Europeană privind utilizarea și transferul de date din registrele cu numele pasagerilor către Departamentul pentru Securitate Internă al Statelor Unite, MO 2012 L 215/4. Textul Acordului este anexat la prezenta Decizie, MO 2012 L 215, pp. 5-14.

240 Decizia 2012/381/UE a Consiliului din 13 decembrie 2011 privind încheierea Acordului între Uniunea Europeană și Australia privind prelucrarea și transferul datelor din registrul cu numele pasagerilor (PNR) de către transportatorii aerieni către Serviciul vamal și de protecție a frontierelor din Australia, MO 2012 L 186/3. Textul acordului, care a înlocuit forma anterioară din 2008, este anexat la prezenta decizie, MO 2012 L 186, pp. 4-16.

orientări globale privind PNR[241], realizarea unui sistem PNR al UE[242] şi negocierea unor acorduri cu țările terțe[243].

Date de mesagerie financiară

Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT) cu sediul în Belgia, care este împuternicitul pentru majoritatea transferurilor financiare de la băncile europene, opera cu un centru „în oglindă" în Statele Unite şi a primit solicitarea de a dezvălui date Departamentului de Trezorerie al Statelor Unite în scopuri de cercetare a terorismului[244].

Din perspectiva UE, nu exista niciun temei legal suficient pentru a dezvălui astfel de date efectiv europene, care erau accesibile în Statele Unite doar pentru că unul dintre centrele de prelucrare a datelor aparținând SWIFT îşi avea sediul în Statele Unite ale Americii.

Un acord specific între UE şi Statele Unite, cunoscut sub numele de Acordul SWIFT, a fost încheiat în 2010, pentru a furniza baza legală necesară şi pentru a asigura un nivel adecvat de protecție a datelor[245].

---

241 A se vedea, în special, Comunicarea Comisiei din 21 septembrie 2010 privind o abordare globală a transferului de date din registrul cu numele pasagerilor (PNR) către țări terțe, COM(2010) 492 final, Bruxelles, 21 septembrie 2010. A se vedea Grupul de Lucru Articolul 29 (2010), *Avizul 7/2010 cu privire la Comunicarea Comisiei Europene privind o abordare globală referitoare la transferul de date din registrul cu numele pasagerilor (PNR) către țări terțe*, WP 178, Bruxelles, 12 noiembrie 2010.

242 Propunerea de directivă a Parlamentului European şi a Consiliului privind utilizarea datelor PNR pentru prevenirea, depistarea, cercetarea şi urmărirea penală a infracțiunilor de terorism şi a infracțiunilor grave, COM(2011) 32 final, Bruxelles, 2 februarie 2011.

În luna aprilie 2011, Parlamentul European a solicitat FRA să furnizeze un aviz privind această propunere şi conformitatea acesteia cu Carta Drepturilor Fundamentale a Uniunii Europene. A se vedea: FRA (2011), *Avizul 1/2011 – Registrul cu numele pasagerilor*, Viena, 14 iunie 2011.

243 UE negociază un nou acord PNR cu Canada, care va înlocui acordul din 2006 care este în prezent în vigoare.

244 A se vedea în acest context, Grupul de lucru Articolul 29 (2011), *Avizul 14/2011 privind aspecte de protecție a datelor legate de prevenirea spălării banilor şi a finanțării terorismului*, WP 186, Bruxelles, 13 iunie 2011; Grupul de lucru Articolul 29 (2006), *Avizul 10/2006 privind prelucrarea datelor cu caracter personal de către Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT)*, WP 128, Bruxelles, 22 noiembrie 2006; Comisia pentru protecția vieții private (*Commission de la protection de la vie privée*) din Belgia (2008), *„Procedură de control şi recomandare inițiată în legătură cu societatea SWIFT scrl"*, Decizie, 9 decembrie 2008.

245 Decizia 2010/412/UE a Consiliului din 13 iulie 2010 privind încheierea Acordului dintre Uniunea Europeană şi Statele Unite ale Americii privind prelucrarea şi transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțărilor în scopuri teroriste, MO 2010 L 195, pp. 3 şi 4. Textul acordului este anexat la prezenta decizie, MO 2010 L 195, pp. 5-14.

În conformitate cu acordul respectiv, datele financiare au continuat să fie furnizate de SWIFT Departamentului de Trezorerie al SUA în scopul prevenirii, cercetării, identificării sau urmăririi penale a actelor de terorism sau de finanțare a terorismului. Departamentul de Trezorerie al SUA poate solicita date financiare de la SWIFT, cu condiția ca cererea:

- să identifice cât mai clar posibil datele financiare;
- să demonstreze în mod clar necesitatea datelor;
- să prezinte un caracter cât mai specific pentru a reduce la minimum volumul de date solicitate;
- să nu solicite date referitoare la zona unică de plăți în euro (SEPA).

Europol trebuie să primească o copie a fiecărei cereri formulate de Departamentul de Trezorerie al SUA şi să verifice conformitatea acesteia cu principiile acordului SWIFT[246].. În cazul în care se confirmă conformitatea cu acestea, 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 analiştii care cercetează actele de terorism sau de finanțare a terorismului; datele financiare nu trebuie să fie interconectate cu nicio altă bază de date. În general, datele financiare primite de la SWIFT sunt şterse în termen de maximum cinci ani de la primirea acestora. Datele financiare relevante pentru anumite cercetări sau urmăriri penale pot fi păstrate atât timp cât datele sunt necesare pentru operațiunile respective.

Departamentul de Trezorerie al SUA poate transfera informații din datele primite de SWIFT către autorități specifice responsabile cu aplicarea legii, siguranța publică sau combaterea terorismului din interiorul sau din afara Statelor Unite ale Americii exclusiv în scopul cercetării, identificării, prevenirii sau urmăririi penale a actelor de terorism sau de finanțare a terorismului. 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 supune consimțământului prealabil al autorităților competente din statul membru în cauză. Se pot face excepții

246 Organismul comun de supraveghere independent al Europol a desfăşurat verificări cu privire la activitățile Europol în acest domeniu, rezultate sunt disponibile: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

în cazul în care comunicarea datelor este esențială pentru prevenirea unei amenințări imediate şi grave la adresa securității publice.

Supraveghetori independenți, inclusiv o persoană desemnată de Comisia Europeană, monitorizează conformitatea cu principiile acordului SWIFT.

Persoanele vizate au dreptul de a obține confirmarea din partea autorității competente pentru protecția datelor din UE că drepturile de protecție a datelor lor cu caracter personal au fost respectate. Persoanele vizate au, de asemenea, dreptul la rectificare, dreptul de ştergerea sau de blocare a datelor lor colectate şi stocate de Departamentul de Trezorerie al SUA în temeiul acordului SWIFT. Cu toate acestea, drepturile de acces ale persoanelor vizate pot fi supuse unor restricții legale. Atunci când se refuză accesul, persoana vizată trebuie informată în scris privind refuzul şi dreptul acesteia de a formula căi de atac administrative şi judiciare în Statele Unite ale Americii.

Acordul SWIFT rămâne in vigoare pentru o perioadă de cinci ani, până în luna august 2015, şi se prelungeşte automat cu perioade ulterioare de câte un an, cu excepția cazului în care una dintre părți notifică celeilalte intenția sa de a nu prelungi acordul, cu un preaviz de cel puțin şase luni.

7

Protecția datelor în contextul poliției și cercetării penale

UE	Aspecte vizate	CoE
	În general	Convenția 108
	Poliția	Recomandarea privind sectorul polițienesc
		CEDO, *B.B./Franța*, nr. 5335/06, 17 decembrie 2009
		CEDO, *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04, 4 decembrie 2008
		CEDO, *Vetter/Franța*, nr.59842/00, 31 mai 2005
	Criminalitate informatică	Convenția privind criminalitatea informatică
Protecția datelor în contextul cooperării transfrontaliere între autoritățile polițienești și judiciare		
Decizia-cadru privind protecția datelor	În general	Convenția 108
		Recomandarea privind sectorul polițienesc
Decizia Prüm	Pentru date speciale: amprente, ADN, huliganism etc.	Convenția 108
		Recomandarea privind sectorul polițienesc
Decizia Europol	De către agenții speciale	Convenția 108
Decizia Eurojust		Recomandarea privind datele deținute de poliție
Regulamentul Frontex		
Decizia Schengen II	Prin sisteme de informare comune speciale	Convenția 108
Regulamentul VIS		Recomandarea privind sectorul polițienesc
Regulamentul Eurodac		CEDO, *Dalea/Franța*, nr. 964/07, 2 februarie 2010
Decizia CIS		

Pentru a echilibra interesele persoanelor fizice în ceea ce privește protecția datelor și interesele societăților în ceea ce privește colectarea de date pentru combaterea criminalității și asigurarea siguranței publice și naționale, Consiliul Europei și UE au adoptat instrumente juridice specifice.

7.1. Legislația CoE privind protecția datelor în domeniul poliției și cercetării penale

Puncte-cheie

- Convenția 108 și Recomandarea CoE privind sectorul polițienesc acoperă protecția datelor în toate domeniile de activitate ale poliției.
- Convenția privind criminalitatea informatică (*Convenția de la Budapesta*) este un instrument juridic internațional obligatoriu care acoperă infracțiunile comise împotriva și prin intermediul rețelelor electronice.

La nivel european, Convenția 108 acoperă toate domeniile de prelucrare a datelor cu caracter personal, iar dispozițiile acesteia au scopul de a reglementa prelucrarea datelor cu caracter personal la nivel general. Prin urmare, Convenția 108 se aplică în cazul protecției datelor în domeniul poliției și cercetării penale, deși părțile contractante pot limita aplicarea acesteia.

Atribuțiile juridice ale autorităților polițienești și de cercetare penală necesită de multe ori prelucrarea datelor cu caracter personal care poate avea consecințe grave pentru persoanele în cauză. Recomandarea privind datele deținute de poliție, adoptată de CoE în 1987 cuprinde orientări pentru părțile contractante 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[247].

7.1.1. Recomandarea privind sectorul polițienesc

CEDO a susținut în permanență că stocarea și păstrarea datelor cu caracter personal de către poliție sau de către autoritățile naționale de securitate aduc atingere

247 CoE, Comitetul de Miniștri (1987), Recomandare Rec(87)15 către statele membre de reglementare a utilizării datelor cu caracter personal în sectorul polițienesc, 17 septembrie 1987.

articolului 8 alineatul (1) din Convenția europeană a drepturilor omului. Multe hotărâri ale CEDO tratează motivarea unor astfel de atingeri aduse drepturilor[248].

Exemplu: În cauza *B.B./Franța*[249], CEDO a hotărât că introducerea unui delicvent sexual condamnat într-o bază de date națională judiciară intră sub incidența articolului 8 din Convenția europeană a drepturilor omului. Cu toate acestea, având în vedere că au fost implementate 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 limitat la datele respective, s-a stabilit un echilibru corect între interesele concurente din sectorul privat și din sectorul public aflate în joc. 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*[250], ambii reclamanți au fost acuzați, dar nu și condamnați, pentru infracțiuni penale. Cu toate acestea, amprentele, profilurile ADN și probele celulare ale acestora au fost păstrate și stocate de către poliție. Păstrarea pe termen nelimitat a datelor biometrice era permisă prin lege în cazul în care o persoană era suspectată de o infracțiune penală, 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 în care persoanele achitate aveau doar posibilități limitate de a solicita ștergerea datelor, a adus atingere în mod disproporționat dreptului reclamanților de respectare a vieții private. Curtea a concluzionat că articolul 8 din Convenția europeană a drepturilor omului a fost încălcat.

Multe hotărâri ulterioare ale CEDO tratează motivarea atingerii aduse dreptului la protecția datelor prin supraveghere.

Exemplu: În cauza *Allan/Regatul Unit*[251], conversațiile private ale unui deținut cu un prieten în zona de vizită a penitenciarului și cu un coacuzat într-o celulă au fost înregistrate în secret de către autorități. CEDO a constatat că utilizarea de

248 A se vedea, 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 18 aprilie 2013 în cauza *M.K./Franța*, nr. 19522/09.

249 Hotărârea CEDO din 17 decembrie 2009 în cauza *B.B./Franța*, nr. 5335/06.

250 Hotărârea CEDO din 4 decembrie 2008în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și nr. 30566/04, punctele 119 și 125.

251 Hotărârea CEDO din 5 noiembrie 2002 în cauza, *Allan/Regatul Unit*, nr. 48539/99.

dispozitive de înregistrare audio şi video în celula reclamantului, în zona de vizită a penitenciarului şi în cazul unui coleg de penitenciar 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 sub acoperire, interferența respectivă nu a fost în conformitate cu legea. Curtea a concluzionat că articolul 8 din Convenția europeană a drepturilor omului a fost încălcat.

Exemplu: În cauza *Klass și alții/Germania*[252], reclamanții au susținut că mai multe acte legislative din Germania, care permiteau supravegherea în secret a corespondenței, poştei şi telecomunicațiilor au încălcat articolul 8 din Convenția europeană a drepturilor omului, în special deoarece persoana în cauză nu a fost informată cu privire la măsurile de supraveghere şi nu s-a putut adresa instanțelor de judecată după încheierea acestora. CEDO a constatat că amenințarea de supraveghere aduce atingere, în mod inevitabil, libertății de comunicare între utilizatorii serviciilor poştale şi de telecomunicații. Cu toate acestea, s-a constatat că fuseseră instituite suficiente garanții împotriva abuzului. Puterea legislativă din Germania a acționat în mod justificat prin considerarea măsurilor respective ca fiind necesare într-o societate democratică pentru interesele de securitate națională şi pentru prevenirea tulburărilor sau a infracțiunilor. Curtea a concluzionat că nu a existat nicio încălcare a articolului 8 din Convenția europeană a drepturilor omului.

Având în vedere că prelucrarea datelor de către autoritățile polițieneşti poate avea un impact semnificativ asupra persoanelor în cauză, norme detaliate de protecție a datelor pentru păstrarea bazelor de date din acest domeniu sunt deosebit de necesare. Recomandarea CoE privind sectorul polițienesc a vizat abordarea problemei, oferind orientări cu privire la modul de colectare a datelor în cadrul activității polițieneşti, modul de păstrare a fişierelor de date din domeniu, persoanele cărora trebuie să li se permită accesul la aceste fişiere, inclusiv condițiile pentru transferul de date către autoritățile străine de poliție, modul în care persoanele vizate ar trebui să îşi poată exercita drepturile de protecție a datelor, precum şi modul în care autoritățile independente ar trebui să îşi exercite controlul. Obligația de a asigura un nivel adecvat de securitate a datelor este, de asemenea, luată în considerare.

Recomandarea nu prevede colectarea nediferențiată, pe termen nedeterminat a datelor de către autoritățile polițieneşti. Aceasta limitează colectarea datelor cu

252 Hotărârea CEDO din 6 septembrie 1978 în cauza *Klass și alții/Germania*, nr. 5029/71.

caracter personal de către organele de poliție la minimul necesar pentru prevenirea unui pericol real sau suprimarea 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 consimțământul persoanei vizate, persoana vizată trebuie să fie informată cu privire la colectarea datelor imediat ce divulgarea nu mai împiedică investigațiile. Colectarea de date prin supraveghere tehnică sau prin alte mijloace automatizate ar trebui, de asemenea, să se întemeieze pe dispoziții legale specifice.

Exemplu: În cauza *Vetter/Franța*[253], martori anonimi au acuzat reclamantul de omucidere. Întrucât reclamantul mergea periodic în vizită la un prieten, poliția a instalat dispozitive de ascultare în casa acestuia cu permisiunea judecătorului de instrucție. Pe baza conversațiilor înregistrate, reclamantul a fost arestat și judecat pentru omor. Reclamantul a solicitat ca înregistrările să fie declarate probe inadmisibile, susținând, în special, că nu sunt prevăzute de lege. Pentru CEDO, problema în speță era măsura în care utilizarea de dispozitive de ascultare s-a făcut „conform legii". Ascultarea în incinta locuințelor private, în mod evident, nu intră sub incidența articolelor 100 și urm. din Codul de procedură penală, întrucât dispozițiile respective vizează doar interceptarea liniilor telefonice. Articolul 81 din Cod nu precizează suficient de clar domeniul de aplicare sau modul de exercitare a deciziei autorităților cu privire la permisiunea de monitorizare a conversațiilor personale. În consecință, reclamantul nu a beneficiat de gradul minim de protecție la care cetățenii au dreptul în baza statului de drept într-o societate democratică. Curtea a concluzionat că articolul 8 din Convenția europeană a drepturilor omului a fost încălcat.

Recomandarea concluzionează că, atunci când se stochează date cu caracter personal, trebuie să se facă o distincție clară între: datele administrative și datele deținute de poliție; diferitele tipuri 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.

253 Hotărârea CEDO din 31 mai 2005 în cauza *Vetter/Franța*, nr. 59842/00.

Scopul datelor deținute de poliție ar trebui să fie limitat în mod strict. Acest lucru are consecințe pentru comunicarea datelor deținute de poliție către terți: transferul sau comunicarea acestor date în cadrul sectorului polițienesc ar trebui reglementate în funcție de existența sau nu a unui interes legitim în comunicarea informațiilor. Transferul sau comunicarea acestor date în afara sectorului polițienesc ar trebui permise doar în cazul în care există o obligație sau o autorizație legală clară. Transferul sau comunicarea la nivel internațional ar trebui să se limiteze la autoritățile polițienești străine și să se întemeieze pe dispoziții legale speciale, posibil acorduri internaționale, cu excepția cazului în care sunt necesare pentru prevenirea unui pericol grav și iminent.

Prelucrarea datelor de către poliție 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 în Convenția 108. 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 eficiente, persoana vizată trebuie să aibă dreptul, în temeiul legislației naționale, să facă apel la autoritatea națională de supraveghere a protecției datelor sau la un alt organism independent.

7.1.2. 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[254]. Prezenta convenție este deschisă pentru semnare și statelor non-membre ale CoE și, până la mijlocul anului 2013, patru state din afara CoE – Australia, Republica Dominicană, Japonia și Statele Unite ale Americii – au devenit părți la convenție și alte 12 state non-membre au semnat convenția sau au fost invitate să adere la aceasta.

Convenția privind criminalitatea informatică rămâne tratatul internațional cel mai influent, care tratează încălcări ale legii prin utilizarea internetului sau a altor rețele

254 Consiliul Europei, Comitetul de Miniștri (2001), Convenția privind criminalitatea informatică, CETS nr. 185, Budapesta, 23 noiembrie 2001, intrată în vigoare la 1 iulie 2004.

de informații. Aceasta impune părților actualizarea și armonizarea legislației lor penale împotriva pirateriei și altor încălcări ale securității, inclusiv încălcarea drepturilor de autor, frauda facilitată prin calculator, pornografia infantilă și alte activități informatice ilicite. Convenția prevede, de asemenea, puteri procedurale care vizează căutarea de rețele informatice și interceptarea comunicațiilor în contextul combaterii criminalității informatice. În final, aceasta permite cooperarea internațională eficientă. Un protocol adițional la convenție reglementează incriminarea propagandei rasiste și xenofobe în cadrul rețelelor informatice.

Deși convenția nu este un instrument efectiv de promovare a protecției datelor, aceasta incriminează activitățile care sunt susceptibile de a încălca dreptul unei persoane vizate la protecția datelor. 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[255].

7.2. Legislația UE privind protecția datelor în domeniul poliției și cercetării penale

Puncte-cheie

- La nivelul UE, protecția datelor în domeniul poliției și cercetării penale este reglementată exclusiv în contextul cooperării transfrontaliere între autoritățile polițienești și judiciare.
- Există regimuri speciale de protecție a datelor pentru Oficiul European de Poliție (Europol) și unitatea de cooperare judiciară a UE (Eurojust), care sunt organe ale UE care asistă și promovează aplicarea legii la nivel transfrontalier.
- Regimuri speciale de protecție a datelor există, de asemenea, pentru sistemele comune de informații instituite la nivelul UE pentru schimbul transfrontalier de informații între autoritățile polițienești și judiciare competente. Exemple importante sunt Schengen II, Sistemul de informații privind vizele (VIS) și Eurodac, un sistem centralizat care conține datele dactiloscopice ale resortisanților din țările terțe care solicită azil într-unul din statele membre ale UE.

Directiva privind protecția datelor nu se aplică în sectorul poliției și cercetării penale. Secțiunea 7.2.1 descrie cele mai importante instrumente legale din acest domeniu.

255 *Ibidem*, articolul 15 alineatul (1).

7.2.1. Decizia-cadru privind protecția datelor

Decizia-cadru 2008/977/JAI a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițieneşti şi judiciare în materie penală (*Decizia-cadru privind protecția datelor*)[256] are drept scop asigurarea protecției datelor cu caracter personal ale persoanelor fizice atunci când datele personale ale acestora sunt prelucrate în scopul prevenirii, investigării, depistării şi urmăririi penale a unei infracțiuni sau în scopul executării unei sancțiuni penale. În numele statelor membre sau al UE acționează autorități competente din sectorul poliției şi cercetării penale. Aceste autorități sunt agenții sau organisme ale UE, precum şi autorități din statele membre[257]. Aplicabilitatea deciziei-cadru se limitează la asigurarea protecției datelor în cadrul cooperării transfrontaliere între aceste autorități şi nu se extinde la securitatea națională.

Decizia-cadru privind protecția datelor se bazează în mare măsură pe principiile şi definițiile cuprinse în Convenția 108 şi în Directiva privind protecția datelor.

Datele se utilizează numai de către o autoritate competentă şi exclusiv în scopul pentru care acestea au fost transmise sau puse la dispoziție. Statul membru destinatar trebuie să respecte orice restricții privind schimbul de date prevăzute de legea statului membru care efectuează transferul. Cu toate acestea, utilizarea datelor de către statul destinatar pentru un scop diferit este permisă în anumite condiții. Înregistrarea şi documentarea transferurilor de date este o obligație specifică a autorităților competente pentru a ajuta la clarificarea responsabilităților care decurg din reclamații. Transferul ulterior de date, primite în cadrul cooperării transfrontaliere, către terți necesită acordul statului membru din care provin datele, deşi există excepții în cazuri de urgență.

Autoritățile competente trebuie să ia măsurile de securitate necesare pentru a proteja datele cu caracter personal împotriva oricărei forme de prelucrare ilicită.

Fiecare stat membru trebuie să asigure că una sau mai multe autorități naționale de supraveghere independente sunt responsabile de consilierea şi monitorizarea aplicării dispozițiilor adoptate în conformitate cu Decizia-cadru privind protecția datelor. De asemenea, acestea audiază cererile depuse de orice persoană cu privire la protecția

256 Consiliul Uniunii Europene (2008), Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițieneşti şi judiciare în materie penală (*Decizia-cadru privind protecția datelor*), MO 2008 L 350.

257 *Ibidem*, articolul 2 litera (h).

drepturilor și libertăților acesteia legate de prelucrarea datelor cu caracter personal de către autoritățile competente.

Persoana vizată are dreptul la informații cu privire la prelucrarea datelor sale personale și are dreptul de acces, rectificare, ștergere sau blocare a datelor. În cazul în care exercitarea acestor drepturi este refuzată din motive întemeiate, persoana vizată trebuie să aibă drept de apel la autoritatea națională de supraveghere competentă și/sau la o instanță. În cazul în care o persoană suferă un prejudiciu ca urmare a încălcării legislației naționale de punere în aplicare a Deciziei-cadru privind protecția datelor, persoana respectivă are dreptul la compensații din partea operatorului[258]. În general, persoanele vizate trebuie să aibă acces la o cale de atac legală pentru orice încălcare a drepturilor lor garantate prin legislația națională de punere în aplicare a Deciziei-cadru privind protecția datelor[259].

Comisia Europeană a propus o reformă, care constă într-un Regulament general privind protecția datelor[260] și o Directivă generală privind protecția datelor[261]. Această nouă directivă va înlocui actuala Decizie-cadru privind protecția datelor și va pune în aplicare principiile și normele generale în contextul cooperării polițienești și judiciare în materie penală.

7.2.2. Mai multe instrumente juridice specifice privind protecția datelor în contextul cooperării polițienești și de aplicare a legii transfrontaliere

În plus față de Decizia-cadru privind protecția datelor, schimbul de informații realizat de statele membre în domenii specifice este reglementat printr-o serie de instrumente juridice, cum ar fi Decizia-cadru 2009/315/JAI a Consiliului privind organizarea și conținutul schimbului de informații extrase din cazierele judiciare între statele

258 *Ibidem*, articolul 19.

259 *Ibidem*, articolul 20.

260 Comisia Europeană (2012), *Propunere de regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor)*, COM(2012) 11 final, Bruxelles, 25 ianuarie 2012.

261 Comisia Europeană (2012), *Propunere de directivă 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 libera circulație a acestor date (Directiva generală privind protecția datelor)*, COM(2012) 10 final, Bruxelles, 25 ianuarie 2012.

membre şi Decizia Consiliului privind acordurile de cooperare între unitățile de informații financiare ale statelor membre în ceea ce priveşte schimbul de informații[262].

Este important de reținut că o cooperare transfrontalieră[263] între autoritățile competente implică din ce în ce mai mult schimbul de date privind imigrația. Acest domeniu al legislației nu vizează aspecte legate de poliție şi cercetare penală, dar este în multe privințe relevant pentru activitatea autorităților polițieneşti şi judiciare. Acelaşi lucru este valabil pentru datele referitoare la mărfurile importate în sau exportate din UE. Eliminarea controalelor la frontierele interne în cadrul UE a sporit riscul de fraudă, ceea ce impune ca statele membre să îşi intensifice cooperarea, în special prin consolidarea schimbului transfrontalier de informații în vederea eficientizării depistării şi urmăririi în justiție a încălcărilor legislației vamale naționale şi europene.

Decizia Prüm

Un exemplu important de cooperare transfrontalieră instituționalizată prin schimbul de date deținute la nivel național este Decizia 2008/615/JAI a Consiliului privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului şi a criminalității transfrontaliere (*Decizia Prüm*), prin care Tratatul Prüm a fost integrat în dreptul european în anul 2008[264]. Tratatul Prüm a fost un acord internațional de cooperare polițienească semnat în 2005 de Austria, Belgia, Franța, Germania, Luxemburg, Țările de Jos şi Spania[265].

Scopul Deciziei Prüm este acela de a ajuta statele membre să îmbunătățească schimbul de informații în scopul prevenirii şi combaterii criminalității în trei domenii:

262 Consiliul Uniunii Europene (2009), Decizia-cadru 2009/315/JAI a Consiliului din 26 februarie 2009 privind organizarea şi conținutul schimbului de informații extrase din cazierele judiciare între statele membre, MO 2009 L 93, Consiliul Uniunii Europene (2000), 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 priveşte schimbul de informații, MO 2000 L 271.

263 Comisia Europeană (2012), Comunicarea Comisiei către Parlamentul European şi Consiliu – Consolidarea cooperării între autoritățile responsabile de aplicarea legii în UE: Modelul European de Schimb de Informații (EIXM), COM(2012) 735 final, Bruxelles, 7 decembrie 2012.

264 Consiliul Uniunii Europene (2008), Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului şi a criminalității transfrontaliere, MO 2008 L 210.

265 Convenția între Regatul Belgiei, Republica Federală Germania, Regatul Spaniei, Republica Franceză, Marele Ducat al Luxemburgului, Regatul Țărilor de Jos şi Republica Austria privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului, a criminalității transfrontaliere şi a migrației ilegale; disponibilă la: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

terorism, criminalitate transfrontalieră și migrație ilegală. În acest scop, decizia cuprinde dispoziții privind:

- accesul automatizat la profilurile ADN, 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 teroriste;
- alte măsuri de intensificare a cooperării polițienești transfrontaliere.

Bazele de date care sunt puse la dispoziție în conformitate cu Decizia Prüm sunt reglementate în întregime de legislația națională, dar schimbul de date este reglementat în plus de decizie și, mai recent, de Decizia-cadru privind protecția datelor. Organele competente pentru supravegherea acestor fluxuri de date sunt autoritățile naționale de supraveghere a protecției datelor.

7.2.3. Protecția datelor la Europol și Eurojust

Europol

Europol, agenția Uniunii Europene în materie de aplicare a legii, are sediul la Haga și unități naționale Europol (UNE) în fiecare stat membru. Europol a fost înființată în anul 1998; statutul juridic actual de instituție a UE se bazează pe Decizia Consiliului privind înființarea Oficiului European de Poliție (*Decizia Europol*)[266]. Obiectivul Europol este acela de a asista prevenirea și investigarea criminalității organizate, a terorismului și a altor forme grave de criminalitate, astfel cum sunt enumerate în anexa la Decizia Europol, care afectează două sau mai multe state membre.

Pentru atingerea obiectivelor sale, Europol a înființat Sistemul de Informații Europol, care asigură o bază de date pentru ca statele membre să facă schimb de informații

266 Consiliul Uniunii Europene (2009), Decizia Consiliului din 6 aprilie 2009 privind înființarea Oficiului European de Poliție, MO 2009 L 121 (Europol). A se vedea, de asemenea, propunerea de regulament a Comisiei, care prevede, prin urmare, un cadru juridic pentru un nou Europol, care urmează și substituie Europol, astfel cum a fost înființat prin Decizia 2009/371/JAI a Consiliului din 6 aprilie 2009 privind înființarea Oficiului European de Poliție (Europol) și CEPOL, astfel cum a fost înființat prin Decizia 2005/681/JAI a Consiliului privind înființarea Colegiului European de Poliție (CEPOL), COM(2013) 173 final.

în materie penală și alte informații prin intermediul UNE. Sistemul de informații Europol poate fi utilizat pentru a pune la dispoziție date referitoare la: persoane suspectate sau care au fost condamnate pentru o infracțiune de competența Europol ori persoane cu privire la care există indicii concrete că vor comite astfel de infracțiuni. Europol și UNE pot introduce date direct în Sistemul de informații Europol și pot prelua date din acesta. Doar partea care a introdus datele în sistem poate modifica, corecta sau șterge datele.

În cazul în care este necesar pentru îndeplinirea sarcinilor sale, Europol poate stoca, modifica și utiliza date referitoare la infracțiuni în fișiere de lucru pentru analiză. Fișierele de lucru pentru analiză sunt deschise în vederea asamblării, prelucrării sau utilizării datelor în vederea asistării anchetelor penale concrete coordonate de Europol împreună cu statele membre ale UE.

Ca răspuns la noile dezvoltări, 1 ianuarie 2013, la Europol a fost înființat Centrul european de combatere a criminalității informatice[267]. 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 privind criminalitatea informatică. 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
- care aduc prejudicii grave victimelor lor, cum ar fi exploatarea sexuală a minorilor pe internet;
- îndreptate împotriva infrastructurii critice și a sistemelor informatice din UE.

Regimul de protecție a datelor care reglementează activitățile Europol este îmbunătățit. Decizia Europol prevede în articolul 27 că se aplică principiile prevăzute în Convenția 108 și în Recomandarea privind datele deținute de poliție cu privire la prelucrarea de date automatizate și neautomatizate. Transferul de date între Europol și statele membre trebuie să respecte, de asemenea, normele cuprinse în Decizia-cadru privind protecția datelor.

267 A se vedea, de asemenea, AEPD (2012), *Avizul Autorității Europene pentru Protecția Datelor privind Comunicarea Comisiei Europene către Consiliu și Parlamentul European privind instituirea unui Centru european de combatere a criminalității informatice*, Bruxelles, 29 iunie 2012.

Pentru a asigura conformitatea cu legislația aplicabilă privind protecția datelor și, în special, că drepturile persoanelor fizice nu sunt încălcate prin prelucrarea datelor cu caracter personal, Organismul comun de supraveghere independent al Europol (JSB) evaluează și monitorizează activitățile Europol[268]. Fiecare persoană are dreptul de acces la orice date cu caracter personal pe care Europol le poate deține, în plus față de dreptul de a solicita ca aceste date cu caracter personal să fie verificate, corectate sau șterse. Dacă o persoană nu este mulțumită de decizia Europol în ceea ce privește exercitarea acestor drepturi, aceasta poate apela la Comitetul de Apel al JSB.

În cazul în care s-au adus prejudicii ca urmare a unor erori de drept sau de fapt în ceea ce privește datele stocate sau prelucrate la Europol, partea vătămată poate solicita despăgubiri doar în fața instanței competente a statului membru în care a avut loc evenimentul care a provocat prejudiciul[269]. Europol va despăgubi statul membru în cazul în care prejudiciul este rezultatul neîndeplinirii de către Europol a obligațiilor sale legale.

Eurojust

Eurojust, înființat în anul 2002, este un organism al Uniunii Europene, cu sediul la Haga, care promovează cooperarea în materie judiciară în cadrul anchetelor și urmăririlor penale legate de infracțiuni grave care implică cel puțin două state membre[270]. Eurojust are competența de a:

- stimula și îmbunătăți coordonarea investigațiilor și urmăririlor penale între autoritățile competente din diferite state membre;

- facilita executarea cererilor și deciziilor privind cooperarea judiciară.

Funcțiile Eurojust sunt îndeplinite de membrii naționali. Fiecare stat membru delegă un judecător sau un procuror la Eurojust, al cărui statut se supune legislației naționale

268 Decizia Europol, articolul 34.

269 *Ibidem*, articolul 52.

270 Consiliul Uniunii Europene (2002), Decizia 2002/187/JAI a Consiliului din 28 februarie 2002 de instituire a Eurojust în scopul consolidării luptei împotriva formelor grave de criminalitate, MO 2002 L 63, Consiliul Uniunii Europene (2003), 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, MO 2003 L 44; Consiliul Uniunii Europene (2009), 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, MO 2009 L 138 (*Deciziile Eurojust*).

şi este împuternicit cu competențele adecvate pentru a îndeplini sarcinile necesare pentru stimularea şi 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. Cu toate acestea, prelucrarea se limitează la informații specifice referitoare la persoanele 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 cu privire la martori sau victime ale infracțiunilor penale care intră sub incidența Eurojust[271]. În situații excepționale, Eurojust poate prelucra, pentru o perioadă limitată de timp, date cu caracter personal mai extinse cu privire la împrejurările săvârşirii unei infracțiuni, în cazul în care datele respective sunt direct relevante pentru o investigație în curs de desfăşurare. În sfera de aplicare a competențelor sale, Eurojust poate coopera cu alte instituții, organisme şi agenții ale UE şi poate face schimb de date cu caracter personal cu acestea. Eurojust poate, de asemenea, să coopereze şi să facă schimb de date cu caracter personal cu țări şi organizații terțe.

În ceea ce priveşte protecția datelor, Eurojust trebuie să garanteze un nivel de protecție cel puțin echivalent cu principiile Convenției 108 a Consiliului Europei, cu modificările ulterioare. În cazul schimbului de date, trebuie respectate norme şi restricții specifice, care sunt puse în aplicare fie în baza unui acord de cooperare, fie în baza unui acord de lucru în conformitate cu Deciziile Eurojust ale Consiliului şi Normele Eurojust privind protecția datelor[272].

Un JSB independent a fost înființat la Eurojust, având sarcina de a monitoriza prelucrarea datelor cu caracter personal efectuată de Eurojust. Persoanele fizice pot apela la JSB în cazul în care nu sunt mulțumite de răspunsul Eurojust la o cerere privind accesul la, corectarea, blocarea sau ştergerea datelor cu caracter personal. În cazul în care Eurojust prelucrează date cu caracter personal în mod ilegal, Eurojust îşi va asuma răspunderea, în conformitate cu legislația națională a statului membru în care se află sediul central ale acestuia, Țările de Jos, pentru orice prejudiciu cauzat persoanei vizate.

271 Versiunea consolidată a Deciziei 2002/187/JAI a Consiliului, astfel cum a fost modificată prin Decizia 2003/659/JAI a Consiliului şi prin Decizia 2009/426/JAI a Consiliului, articolul 15 alineatul (2).

272 Regulament de procedură privind prelucrarea şi protecția datelor cu caracter personal la Eurojust, MO 2005, C 68/01, 19 martie 2005, p. 1.

7.2.4. Protecția datelor în cadrul sistemelor informatice comune la nivelul UE

În plus față de schimbul de date între statele membre și înființarea de autorități specializate ale UE pentru combaterea criminalității transfrontaliere, mai multe sisteme informatice comune au fost înființate la nivelul UE pentru a servi drept platformă pentru schimbul de date între autoritățile naționale și europene competente pentru scopurile specificate de aplicare a legii, inclusiv legislația privind imigrația și legislația vamală. Unele dintre aceste sisteme au fost dezvoltate ca urmare a acordurilor multilaterale care au fost ulterior completate de instrumente și sisteme legale europene, cum ar fi Sistemul de Informații Schengen, Sistemului de informații privind vizele, Eurodac, Eurosur sau Sistemul de informații al vămilor.

Agenția europeană pentru gestionarea operațională a sistemelor informatice la scară largă (eu-LISA)[273], înființată în anul 2012, este responsabilă pentru gestionarea operațională pe termen lung a Sistemului de 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. Este, de asemenea, responsabilă pentru adoptarea măsurilor necesare menite să asigure securitatea sistemelor și a 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 comune (*Acordul Schengen*), cu scopul de a crea o zonă pentru libera circulație a persoanelor, nestingherită de controalele efectuate la frontieră pe teritoriul Schengen[274]. 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.

273 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, MO 2011 L 286.

274 Acordul dintre guvernele statelor Uniunii Economice Benelux, Republicii Federale Germania și Republicii Franceze privind eliminarea treptată a controalelor la frontierele lor comune, MO 2000 L 239.

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[275]. 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 plus Islanda, Liechtenstein, Norvegia și Elveția[276]. 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, organele de poliție, autoritățile vamale, autoritățile responsabile de vize și autoritățile judiciare din întreg spațiul Schengen. Statele membre operează copii naționale ale C-SIS, cunoscute sub numele de Sisteme naționale de informații Schengen (N-SIS), care sunt actualizate în permanență, astfel actualizând C-SIS. Se consultă N-SIS și se va emite o alertă în cazul în care:

- persoana nu are dreptul de a intra sau de a rămâne pe teritoriul Schengen; sau
- persoana sau obiectul este urmărit de autoritățile judiciare sau de aplicare a legii; sau
- persoana a fost raportată ca dispărută; sau
- 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 alerte, se vor iniția activități de urmărire prin intermediul Sistemelor naționale de informații Schengen.

SIS II are noi funcționalități, cum ar fi posibilitatea de a introduce: date biometrice, precum amprente și fotografii; sau noi categorii de alerte, cum ar fi furturi de bărci, aeronave, containere sau mijloace de plată; și alerte îmbunătățite cu privire la

275 Comunitățile Europene (1997), Tratatul de la Amsterdam de modificare a Tratatului privind Uniunea Europeană, a Tratatelor de instituire a Comunităților Europene și anumite acte conexe, MO 1997 C 340.

276 Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație, MO 2006 L 381 (*SIS II*) și Consiliul Uniunii Europene (2007), 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*), MO 2007 L 205.

persoane şi obiecte; copii ale mandatelor europene de arestare (MEA) privind persoanele căutate pentru deținere, predare sau extrădare.

Decizia 2007/533/JAI a Consiliului privind înființarea, funcționarea şi utilizarea Sistemului de Informații Schengen de a doua generație (Decizia Schengen II) include Convenția 108: "Datele cu caracter personal prelucrate în temeiul prezentei decizii sunt protejate în conformitate cu Convenția 108 a Consiliului Europei"[277]. În cazul în care utilizarea datelor cu caracter personal de către autoritățile polițieneşti naționale se face în temeiul Deciziei Schengen II, prevederile Convenției 108, precum şi cele ale Recomandării privind datele deținute de poliție, trebuie implementate în legislația națională.

Autoritatea națională de supraveghere competentă din fiecare stat membru supraveghează sistemul N-SIS intern. În special, aceasta trebuie să verifice calitatea datelor pe care statul membru le introduce în C-SIS, prin intermediul N-SIS. Autoritatea națională de supraveghere trebuie să asigure efectuarea unui audit al operațiunilor de prelucrare a datelor în cadrul sistemului N-SIS intern cel puțin o dată la patru ani. Autoritățile de supraveghere naționale şi AEPD cooperează şi asigură supravegherea coordonată a SIS, în timp ce AEPD este responsabilă pentru supravegherea C-SIS. Din motive de transparență, un raport comun de activitate trebuie prezentat Parlamentului European, Consiliului şi eu-LISA la fiecare doi ani.

Drepturile de acces ale persoanelor fizice cu privire la SIS II pot fi exercitate în orice stat membru, întrucât fiecare N-SIS este o copie exactă a C-SIS.

Exemplu: În cauza *Dalea/Franța*[278], 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 şi rectificarea sau ştergerea datelor în fața Comisiei pentru Protecția Datelor din Franța şi, în cele din urmă, în fața Consiliul de Stat. CEDO a constatat că raportarea reclamantului la Sistemul de informații Schengen este în conformitate cu legea şi urmăreşte 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 şi

277 Consiliul Uniunii Europene (2007), Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea şi utilizarea Sistemului de informații Schengen de a doua generație, MO 2007 L 205, articolul 57.

278 Hotărârea CEDO din 2 februarie 2010 în cauza *Dalea/Franța* (dec.), nr. 964/07.

întrucât au fost instituite suficiente măsuri pentru a-l proteja împotriva deciziilor arbitrare, atingerea adusă dreptului acestuia de respectare a vieții private a fost proporționată. Plângerea reclamantului în temeiul articolului 8 a fost, prin urmare, declarată inadmisibilă.

Sistemul de informații privind vizele

Sistemul de informații privind vizele (VIS), operat, de asemenea, de către eu-LISA, a fost dezvoltat pentru a sprijini punerea în aplicare a unei politici europene comune privind vizele[279]. VIS permite statelor Schengen să facă schimb de date privind vizele printr-un sistem care conectează consulatele statelor Schengen situate în țări din afara UE, cu punctele de trecere a frontierei externe ale tuturor statelor Schengen. VIS prelucrează datele privind cererile de viză de scurtă ședere pentru a vizita sau pentru a tranzita spațiul Schengen. VIS permite autorităților de frontieră să verifice, cu ajutorul datelor biometrice, dacă persoana care prezintă o viză este titularul de drept al acesteia și să identifice persoanele fără documente sau persoanele care dețin documente false.

În conformitate cu Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (*Regulamentul VIS*), în VIS pot fi înregistrate doar date alfanumerice referitoare la solicitant, vizele, fotografii, date dactiloscopice, legături către cererile anterioare, precum și dosarele de cerere ale persoanelor care însoțesc solicitantul[280]. Accesul la VIS în vederea introducerii, modificării sau ștergerii datelor este limitat exclusiv la autoritățile responsabile de vize din statele membre, în timp ce accesul pentru consultarea datelor se acordă autorităților responsabile de vize și autorităților competente pentru controalele la punctele de trecere a frontierei externe, controalele în materie de imigrație și azil. În anumite condiții, autoritățile polițienești naționale competente și Europol pot solicita accesul

279 Consiliul Uniunii Europene (2004), Decizia Consiliului din 8 iunie 2004 de instituire a Sistemului de informații privind vizele (VIS), MO 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, MO 2008 L 218 (*Regulamentul VIS*); Consiliul Uniunii Europene (2008), 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, MO 2008 L 218.

280 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*), MO 2008 L 218.

la datele introduse în VIS în scopul prevenirii, depistării și cercetării actelor de terorism și a infracțiunilor penale[281].

Eurodac

Numele Eurodac se referă la dactilograme sau amprente digitale. Acesta este un sistem centralizat care conține datele dactiloscopice ale resortisanților din țările terțe care solicită azil într-unul dintre statele membre ale UE[282]. Sistemul este operațional din luna ianuarie a anului 2003, iar scopul acestuia este de a facilita stabilirea statului membru care trebuie să răspundă de examinarea unei anumite cereri de azil în conformitate cu Regulamentul (CE) nr. 343/2003 al Consiliului de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil cu examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe (*Regulamentul Dublin II*)[283]. Datele cu caracter personal din Eurodac nu pot fi utilizate decât în scopul facilitării aplicării Regulamentului Dublin II; utilizarea în orice alt scop este pasibilă de sancțiuni.

Eurodac constă într-o unitate centrală, operată 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 prelevează și transmit amprentele digitale ale fiecărui resortisant din afara UE sau apatrid cu vârsta de cel puțin 14 de ani, care solicită azil pe teritoriul lor sau care este reținut pentru trecerea neautorizată a frontierei externe a acestora. Statele membre pot, de asemenea, să preleveze și să transmită amprentele digitale ale resortisanților din afara UE sau apatrizilor identificați ca locuind pe teritoriul acestora fără permisiune.

281 Consiliul Uniunii Europene (2008), 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, MO 2008 L 218.

282 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, MO 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, MO 2002 L 62 (*Regulamentele Eurodac*).

283 Regulamentul (CE) nr. 343/2003 al Consiliului din 18 februarie 2003 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe, MO 2003 L 50 (*Regulamentul Dublin II*).

Datele dactiloscopice sunt stocate în baza de date Eurodac numai sub formă pseudonimizată. În cazul unei corespondențe, pseudonimul, împreună cu numele primului stat membru care a transmis datele dactiloscopice, este dezvăluit celui de-al doilea stat membru. Apoi, cel de-al doilea stat membru se va adresa primului stat membru, deoarece, în conformitate cu Regulamentul Dublin II, primul stat membru este responsabil pentru prelucrarea cererii de azil.

Datele cu caracter personal stocate în Eurodac care se referă la solicitanții de azil sunt păstrate timp de 10 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 privind resortisanții străini reținuți pentru trecerea ilegală a frontierei externe sunt stocate timp de doi ani. 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.

Pe lângă toate statele membre ale UE, Islanda, Norvegia, Liechtenstein și Elveția utilizează, de asemenea, Eurodac în baza unor acorduri internaționale.

Eurosur

Sistemul european de supraveghere a frontierelor (*Eurosur*)[284] este conceput pentru a intensifica controlul frontierelor externe Schengen prin detectarea, prevenirea 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 dezvoltarea și aplicarea noului concept de gestionare integrată a frontierelor[285]. Obiectivele sale generale sunt:

- reducerea numărului de imigranți ilegali care intră în UE nedetectați;
- reducerea numărului de decese în rândul imigranților ilegali prin salvarea mai multor vieți pe mare;

284 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), MO 2013 L 295.

285 Regulamentul (UE) nr. 1168/2011 al Parlamentului European și al Consiliului din 25 octombrie 2011 de modificare a Regulamentului (CE) nr. 2007/2004 al Consiliului de instituire a Agenției Europene pentru Gestionarea Cooperării Operative la Frontierele Externe ale Statelor Membre ale Uniunii Europene, MO 2011 L 394 (*Regulamentul Frontex*).

- sporirea securității interne a UE în ansamblu prin contribuția la prevenirea criminalității transfrontaliere[286].

Acest sistem este operațional din 2 decembrie 2013 în toate statele membre cu frontiere externe, iar din data de 1 decembrie 2014 va deveni operațional și în celelalte state. Regulamentul se va aplica în cazul supravegherii frontierelor externe terestre, maritime și frontierelor aeriene ale statelor membre.

Sistemul de informații al vămilor

Un alt important sistem comun de informații înființat la nivelul UE este Sistemul de informații al vămilor (CIS)[287]. În cadrul instituirii unei piețe interne, toate controalele și formalitățile legate de mărfurile care circulă pe teritoriul UE au fost eliminate, ceea ce a crescut riscul de fraudă. Acest risc a fost contracarat prin intensificarea cooperării între administrațiile vamale din statele membre. Scopul CIS este acela de a asista statele membre în prevenirea, anchetarea și urmărirea penală a încălcărilor grave ale legislației vamale și agricole naționale și europene.

Informațiile conținute în CIS cuprind date cu caracter personal privind mărfuri, mijloace de transport, întreprinderi, persoane, bunuri și mijloace băneşti reținute, confiscate sau puse sub sechestru. Aceste informații pot fi utilizate exclusiv în scopul observării, raportării, efectuării anumitor controale specifice ori în scopul analizelor strategice sau operaționale cu privire la persoanele suspectate de încălcarea dispozițiilor vamale.

CIS poate fi accesat de autoritățile naționale vamale, fiscale, agricole, din domeniul sănătății publice, precum și de autoritățile polițieneşti, de Europol și de Eurojust.

---

286 A se vedea, de asemenea: Comisia Europeană (2008), 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, Bruxelles, 13 februarie 2008, Comisia Europeană (2011), Evaluarea impactului care însoțește propunerea de regulament al Parlamentului European și al Consiliului de instituire a Sistemului european de supraveghere a frontierelor (Eurosur), document de lucru al serviciilor Comisiei, SEC (2011) 1536 final, Bruxelles, 12 decembrie 2011, p. 18.

287 Consiliul Uniunii Europene (1995), Actul Consiliului din 26 iulie 1995 de elaborare a Convenției privind utilizarea tehnologiei informației în domeniul vamal, MO 1995 C 316, modificat prin Consiliul Uniunii Europene (2009), Regulamentul nr. 515/97 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, Decizia 2009/917/JAI a Consiliului din 30 noiembrie 2009 privind utilizarea tehnologiei informației în domeniul vamal, 2009 L 323 (*Decizia CIS*).

Prelucrarea datelor cu caracter personal trebuie să respecte normele specifice prevăzute de Regulamentul nr. 515/97 şi de Convenția CIS[288] şi dispozițiile Directivei privind protecția datelor, ale Regulamentului privind protecția datelor de către instituțiile UE, ale Convenției 108 şi ale Recomandării privind datele deținute de poliție. AEPD este responsabilă pentru supravegherea conformității CIS cu dispozițiile Regulamentului (CE) nr. 45/2001 şi va convoca o intâlnire cel puțin o dată pe an cu toate autoritățile de supraveghere competente pentru supravegherea aspectelor referitoare la CIS.

288 *Ibidem.*

8

Alte legislații europene specifice privind protecția datelor

UE	Aspecte vizate	CoE
Directiva privind protecția datelor Directiva privind protecția vieții private în sectorul comunicațiilor electronice	Comunicații electronice	Convenția 108 Recomandarea privind serviciile de comunicații
Directiva privind protecția datelor, articolul 8 alineatul (2) litera (b)	Relații de muncă	Convenția 108 Recomandarea privind relațiile de muncă CEDO, *Copland/Regatul Unit*, nr. 62617/00, 3 aprilie 2007
Directiva privind protecția datelor, articolul 8 alineatul (3)	Date medicale	Convenția 108 Recomandarea privind datele medicale CEDO, *Z./Finlanda*, nr. 22009/93, 25 februarie 1997
Directiva privind studiile clinice	Studii clinice	
Directiva privind protecția datelor, articolul 6 alineatul (1) literele (b) și (e), articolul 13 alineatul (2)	Statistici	Convenția 108 Recomandarea privind datele statistice
Regulamentul (CE) nr. 223/2009 privind statisticile europene CJUE, C-524/06, *Huber/Bundesrepublik Deutschland*, 16 decembrie 2008	Statistici oficiale	Convenția 108 Recomandarea privind datele statistice

UE	Aspecte vizate	CoE
Directiva 2004/39/CE 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 Recomandarea 90(19) utilizată pentru plăți și alte operațiuni conexe CEDO, *Michaud/Franța*, nr. 12323/11, 6 decembrie 2012

În mai multe cazuri, au fost adoptate instrumente juridice speciale la nivel european, care pun în aplicare normele generale ale Convenției 108 sau ale Directivei privind protecția datelor în detaliu, în funcție de situații specifice.

8.1. Comunicații electronice

Puncte-cheie

- Norme specifice privind protecția datelor în domeniul telecomunicațiilor, cu referire în special la serviciile de telefonie, sunt cuprinse în Recomandarea CoE din 1995.
- Prelucrarea datelor cu caracter personal în legătură cu furnizarea de servicii de comunicații la nivelul UE este reglementată în Directiva privind protecția vieții private în sectorul comunicațiilor electronice.
- Confidențialitatea comunicațiilor electronice se referă nu doar la conținutul unei comunicări, ci și la datele de trafic, 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 interferență nejustificată cu sfera personală a utilizatorilor, deoarece acestea oferă posibilități tehnice suplimentare de ascultare și examinare a comunicațiilor efectuate în astfel de rețele. Prin urmare, au fost considerate necesare reglementări speciale privind protecția datelor pentru a trata 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 domeniul serviciilor de telefonie[289]. În conformitate cu această recomandare, scopurile legate de colectarea şi prelucrarea datelor cu caracter personal în contextul telecomunicațiilor ar trebui să se limiteze la: conectarea unui utilizator la rețea, punerea la dispoziție a serviciului specific de telecomunicații, facturare, verificare, asigurarea funcționării tehnice optime şi dezvoltarea rețelei şi a serviciului.

O atenție specială a fost acordată, de asemenea, utilizării rețelelor de comunicații pentru trimiterea de mesaje în scop 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 şi-a dat consimțământul în mod expres. Legislația națională prevede norme detaliate în acest domeniu.

În ceea ce priveşte **cadrul juridic al UE,** după o primă încercare în anul 1997, Directiva privind protecția vieții private în sectorul comunicațiilor electronice (*Directiva asupra confidențialității electronice*) a fost adoptată în anul 2002 şi modificată în anul 2009, în scopul completării şi particularizării dispozițiilor Directivei privind protecția datelor pentru sectorul telecomunicațiilor[290]. Aplicarea Directivei privind protecția vieții private în sectorul comunicațiilor electronice se limitează la serviciile de comunicații în rețelele electronice publice.

Directiva asupra confidențialității electronice distinge trei categorii principale de date generate în cursul unei comunicări:

- datele care constituie conținutul mesajelor trimise în timpul comunicării; aceste date sunt strict confidențiale;

289 CoE, Comitetul de Miniştri (1995), Recomandarea Rec (95)4 către statele membre privind protecția datelor cu caracter personal în domeniul serviciilor de telecomunicații, cu referire specială la serviciile de telefonie, 7 februarie 1995.

290 Directiva 2002/58/CE a Parlamentului European şi a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidențialității în sectorul comunicațiilor publice, MO 2002 L 201 (*Directiva asupra confidențialității şi comunicațiilor electronice*), modificată prin Directiva 2009/136/CE a Parlamentului European şi a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal şi drepturile utilizatorilor cu privire la rețelele şi serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale şi protejarea confidențialității în sectorul comunicațiilor publice şi a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului, MO 2009 L 337.

- datele necesare pentru stabilirea şi menținerea comunicării, aşa-numitele date de trafic, cum ar fi informațiile despre participanții la comunicare, ora şi durata comunicării;

- în datele de trafic sunt incluse date referitoare în mod specific la locația dispozitivului de comunicații, aşa-numite date de localizare; aceste date sunt în acelaşi timp date despre locația *utilizatorilor* dispozitivelor de comunicații şi, în special, despre utilizatorii dispozitivelor de comunicații mobile.

Datele de trafic pot fi utilizate de către furnizorul de servicii exclusiv în scopul facturării şi furnizării propriu-zise a serviciului. Cu toate acestea, în baza acordului persoanei vizate, aceste date pot fi dezvăluite altor operatori care furnizează servicii cu valoare adăugată, cum ar fi furnizarea de informații cu privire la locația utilizatorului, cu privire la următoarea stație de metrou sau farmacie sau prognoza meteo pentru locația respectivă.

Alte forme de acces la date referitoare la comunicațiile în rețelele electronice, cum ar fi accesul în scopul anchetării infracțiunilor, trebuie să îndeplinească, în conformitate cu articolul 15 din Directiva asupra confidențialității electronice, cerințele de interferență justificată în dreptul la protecția datelor, astfel cum sunt prevăzute în articolul 8 alineatul (2) din Convenția europeană a drepturilor omului şi confirmate în articolele 8 şi 52 din Cartă.

Modificările aduse în anul 2009 Directivei asupra confidențialității electronice[291] au introdus următoarele:

- Restricțiile privind trimiterea de e-mailuri în scopuri de marketing direct au fost extinse la servicii de mesaje scurte, servicii de mesagerie multimedia şi alte tipuri de aplicații similare; e-mailurile de marketing sunt interzise dacă nu s-a obținut consimțământul prealabil. În lipsa unui astfel de consimțământ, doar clienților anteriori li se pot trimite e-mailuri de marketing, în cazul în care şi-au pus la dispoziție adresa de e-mail şi dacă nu au obiecții.

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

- Statele membre au obligația de a asigura căi de atac legale pentru încălcările interdicției referitoare la comunicările nesolicitate[292].

- 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 acordul trebuie exprimat și obținut pentru a asigura un nivel adecvat de protecție[293].

În cazul în care are loc o încălcare a securității datelor, ca urmare a accesului neautorizat, pierderii sau distrugerii datelor, autoritatea de supraveghere competentă trebuie să fie informată imediat. Abonații trebuie informați în cazul în care un potențial prejudiciu adus acestora este consecința unei încălcări a securității datelor[294].

Directiva privind păstrarea datelor[295] (declarată invalidă în data de 8 aprilie 2014) obliga furnizorii de servicii de comunicații să păstreze datele de trafic disponibile, în special în scopul combaterii criminalității grave, pentru o perioadă de cel puțin șase, dar nu mai mult de 24 de luni, indiferent dacă furnizorul mai avea sau nu nevoie de datele respective în scopuri de facturare sau de furnizare propriu-zisă a serviciului.

Statele membre ale UE desemnează autorități publice independente, responsabile pentru monitorizarea securității datelor păstrate.

Păstrarea datelor de telecomunicații interferează în mod evident cu dreptul la protecția datelor[296]. Caracterul justificat al acestei interferențe a fost contestat în cadrul mai multor proceduri judiciare din statele membre ale UE[297].

---

292 A se vedea Directiva modificată, articolul 13.

293 A se vedea *Ibidem,* articolul 5; a se vedea, de asemenea, Grupul de lucru Articolul 29 (2012), *Avizul 04/201 2 privind exceptarea de la exprimarea consimțământului cu privire la modulele cookies*, WP 194, Bruxelles, 7 iunie 2012.

294 A se vedea, de asemenea, Grupul de lucru Articolul 29 (2011), *Document de lucru 01/2011 privind cadrul european actual referitor la încălcările securității datelor cu caracter personal și recomandări pentru evoluțiile strategice viitoare*, WP 184, Bruxelles, 5 aprilie 2011.

295 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, MO 2006 L 105.

296 AEPD (2011), *Avizul din 31 mai 2011 privind Raportul de evaluare al Comisiei către Consiliu și Parlamentul European cu privire la Directiva privind păstrarea datelor (Directiva 2006/24/CE)*, 31 mai 2011

297 Germania, Curtea Constituțională Federală (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 martie 2010; România, Curtea Constituțională Federală (*Curtea Constituțională a României*), nr. 1258, 8 octombrie 2009; Republica Cehă, Curtea Constituțională (*Ústavní soud České republiky*), 94/2011 M.O., 22 martie 2011.

Exemplu: În cauza *Drepturi Digitale Irlanda și Seitlinger și alții*[298], CJUE a declarata Directiva privind Păstrarea Datelor invalidă. Potrivit Curții, „interferența vastă şi deosebit de gravă a Directivei cu drepturile fundamentale în cauză nu se circumscrie suficient pentru a se asigura că interferența este de fapt limitată la ceea ce este strict necesară."

O problemă crucială în contextul comunicațiilor electronice este interferența autorităților publice. Mijloacele de supraveghere sau interceptare a comunicațiilor, cum ar fi dispozitivele de ascultare sau de înregistrare, sunt permise numai în cazul în care acest lucru este prevăzut prin lege şi constituie o măsură necesară într-o societate democratică, în interesul: protejării securității statului, siguranței publice, intereselor monetare ale statului sau suprimării infracțiunilor penale ori al protecției persoanei vizate sau a drepturilor şi libertăților altora.

Exemplu: În cauza *Malone/Regatul Unit*[299], reclamantul a fost acuzat de o serie de infracțiuni asociate gestionării necinstite a unor bunuri furate. În timpul procesului, a reieşit că s-a interceptat o conversație telefonică a reclamantului în baza unui mandat emis de Secretarul de Stat al Departamentului de Interne. Chiar dacă modul în care comunicarea reclamantului a fost interceptată a fost legal conform legislației naționale, CEDO a constatat că nu există norme juridice privind domeniul de aplicare şi modul de exercitare a puterii de decizie de către autoritățile publice în domeniul respectiv şi că, prin urmare, atingerea rezultată din existența practicii în cauză nu a fost „în conformitate cu legea". Curtea s-a pronunțat asupra încălcării articolului 8 din Convenția europeană a drepturilor omului.

8.2. Date privind angajarea

Puncte-cheie

- Norme specifice privind protecția datelor în domeniul relațiilor de muncă sunt incluse în Recomandarea CoE referitoare la datele privind angajarea.
- În Directiva privind protecția datelor, relațiile de muncă sunt tratate în mod specific numai în contextul prelucrării datelor sensibile.

298 Hotărârea CJUE din 8 aprilie 2014, în cauzele comune *Drepturile Digitale Irlanda și Seitlinger și ceilalți*, C-293/12 și C-594/12, punctul 65.

299 Hotărârea CEDO din 2 august 1984în cauza *Malone/Regatul Unit*, nr. 8691/79.

- Valabilitatea consimțământului, care trebuie să fi fost liber exprimat, ca temei juridic pentru prelucrarea datelor despre angajați poate fi incertă, având în vedere dezechilibrul economic între angajator şi angajați. Circumstanțele exprimării consimțământului trebuie să fie evaluate cu atenție.

În UE nu există niciun cadru legal specific de reglementare a prelucrării datelor în contextul angajării. În Directiva privind protecția datelor, relațiile de muncă sunt menționate în mod specific numai în articolul 8 alineatul (2) din directivă, care vizează prelucrarea datelor sensibile. În ceea ce priveşte Consiliul Europei, Recomandarea referitoare la datele privind angajarea a fost emisă în anul 1989 şi este în curs de actualizare[300].

Un studiu privind cele mai curente probleme legate de protecția datelor specifice contextului angajării este disponibil într-un document de lucru al Grupului de lucru Articolul 29[301]. Grupul de lucru a analizat semnificația consimțământului ca temei juridic pentru prelucrarea datelor privind angajarea[302]. Grupul de lucru a constatat că dezechilibrul economic între angajatorul care solicită acordul şi angajatul care trebuie să îşi exprime acordul va ridica adesea îndoieli cu privire la măsura în care acordul a fost sau nu liber exprimat. Circumstanțele în care se solicită consimțământul trebuie, prin urmare, luate atent în considerare în momentul evaluării valabilității consimțământului în contextul angajării.

O problemă curentă legată de protecția datelor în mediul de lucru tipic actual este măsura legitimă de monitorizare a comunicațiilor electronice ale angajaților la locul de muncă. Se pretinde adesea că această problemă poate fi rezolvată uşor 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 şi nerealistă. Hotărârea CEDO de mai jos prezintă o importanță deosebită în acest context:

300 Consiliul Europei, Comitetul de Miniştri (1989), Recomandarea Rec(89)2 către statele membre privind protecția datelor cu caracter personal utilizate în scopuri de angajare, 18 ianuarie 1989. A se vedea în continuare Comitetul consultativ pentru Convenția 108, Studiu asupra Recomandării nr. R (89) 2 privind protecția datelor cu caracter personal utilizate în scopuri de angajare şi privind propuneri de revizuire a Recomandării susmenționate, 9 septembrie 2011.

301 Grupul de lucru Articolul 29 (2001), *Avizul 8/2001 privind prelucrarea datelor cu caracter personal în contextul angajării*, WP 48, Bruxelles, 13 septembrie 2001.

302 Grupul de lucru Articolul 29 (2005), *Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995*, WP 114, Bruxelles, 25 noiembrie 2005.

Exemplu: În cauza *Copland/Regatul Unit*[303], utilizarea telefonului, a e-mailului şi a internetului de către angajata unui colegiu a fost monitorizată în secret pentru a stabili dacă aceasta utilizează excesiv dispozitivele colegiului în scopuri personale. CEDO a constatat că apelurile telefonice efectuate de la locul de muncă erau acoperite de noțiunile de viață privată şi corespondență. Prin urmare, apelurile şi e-mailurile respective trimise de la locul de muncă, precum şi informațiile provenite din monitorizarea utilizării internetului în scopuri personale erau protejate de articolul 8 din Convenția europeană a drepturilor omului. În cazul reclamantei, nu există dispoziții de reglementare a situațiilor în care angajatorii pot monitoriza utilizarea de către angajați a telefonului, a e-mailului şi a internetului. Prin urmare, atingerea adusă drepturilor nu este în conformitate cu legea. Curtea s-a pronunțat asupra încălcării articolului 8 din Convenția europeană a drepturilor omului.

În conformitate cu Recomandarea Consiliului Europei referitoare la datele privind angajarea, 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 şi a potențialului profesional al acestora.

De asemenea, recomandarea menționează în mod specific date critice cu privire la performanța sau potențialul fiecărui angajat. Datele critice trebuie să se bazeze pe evaluări corecte şi oneste, iar modul în care sunt formulate nu trebuie să fie ofensator. Acest lucru se impune prin principiile de prelucrare corectă a datelor şi de acuratețe a datelor.

Un aspect specific al legislației privind protecția datelor în relația angajator-angajat este rolul reprezentanților angajaților. Aceşti reprezentanți pot primi datele cu caracter personal ale angajaților numai în măsura în care este necesar pentru a le permite să reprezinte interesele angajaților.

Datele personale sensibile colectate în scopul angajării pot fi prelucrate numai în cazuri speciale şi în conformitate cu garanțiile prevăzute de legislația națională. Angajatorii pot adresa întrebări angajaților sau solicitanților de locuri de muncă cu privire la starea de sănătate sau îi pot supune unei examen medical numai dacă este necesar pentru: determinarea eligibilității acestora pentru angajare; îndeplinirea cerințelor de medicină preventivă; sau a permite acordarea de prestații sociale.

303 Hotărârea CEDO din 3 aprilie 2007 în cauza *Copland/Regatul Unit*, nr. 62617/00.

Datele privind starea de sănătate nu pot fi colectate din alte surse decât de la angajatul în cauză, cu excepția cazului în care s-a obținut consimțământul expres şi informat sau atunci când legislația națională prevede acest lucru.

În conformitate cu Recomandarea privind angajarea, angajații ar trebui informați cu privire la scopul prelucrării datelor lor cu caracter personal, tipul de date cu caracter personal stocate, entitățile către care datele sunt comunicate în mod periodic, precum şi scopul şi temeiul juridic al acestor comunicări. Angajatorii trebuie să îşi informeze, de asemenea, angajații, în prealabil cu privire la introducerea sau adaptarea sistemelor automatizate de prelucrare a datelor cu caracter personal ale angajaților sau de monitorizare a deplasărilor sau productivității angajaților.

Angajații trebuie să aibă drept de acces la datele lor privind angajarea, precum şi drept de rectificare sau ştergere. În cazul prelucrării datelor conținute în sentințe, angajații trebuie să aibă, în plus, dreptul de a contesta hotărârea. 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 ştergere a datelor sale personale privind angajare, legislația națională trebuie să prevadă proceduri adecvate pentru contestarea refuzului respectiv.

8.3. Date medicale

Puncte-cheie

- Datele medicale sunt date sensibile şi, prin urmare, beneficiază de protecție specială.

Datele cu caracter personal privind starea de sănătate a persoanei vizate sunt calificate drept date sensibile în conformitate cu articolul 8 alineatul (1) din Directiva privind protecția datelor şi cu articolul 6 din Convenția 108. La rândul lor, datele medicale sunt supuse unui regim de prelucrare a datelor mai strict decât în cazul datelor nesensibile.

Exemplu: În cauza *Z./Finlanda*[304], fostul soț al reclamantei, care era infectat cu HIV, a comis o serie de infracțiuni de natură sexuală. Acesta a fost ulterior

304 Hotărârea CEDO din 25 februarie 1997 în cauza *Z./Finlanda*, nr. 22009/93, punctele 94 şi 112; a se vedea, 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.

condamnat pentru ucidere din culpă, pe motiv că şi-a expus cu bună ştiință victimele riscului de infectare cu HIV. Instanța națională a dispus că hotărârea definitivă şi 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 Curtea de apel şi hotărârea adoptată de curte menționa atât numele şi prenumele reclamantei, cât şi ale fostului soț. CEDO a constatat că atingerea adusă dreptului nu se consideră o măsură necesară într-o societate democratică, deoarece protecția datelor medicale are o importanță fundamentală pentru exercitarea dreptului de respectare a vieții private şi de familie, în special, în cazul informațiilor despre infecțiile cu HIV, având în vedere stigmatizarea legată de această afecțiune în multe societăți. Prin urmare, Curtea a concluzionat că acordarea accesului la datele de identificare şi privind starea de sănătate a reclamantului, astfel cum se descrie în hotărârea Curții de Apel, după o perioadă de numai 10 ani de la adoptarea hotărârii constituie o încălcare a articolului 8 din Convenția europeană a drepturilor omului.

Articolul 8 alineatul (3) din Directiva privind protecția datelor permite prelucrarea datelor medicale în cazul în care acest lucru este necesar în scopuri legate de medicina preventivă, de diagnosticare, de administrare a unor îngrijirii sau tratamente ori de gestionare a serviciilor de sănătate. Cu toate acestea, prelucrarea este permisă numai în cazul în care aceasta este efectuată de un cadru medical care se supune secretului profesional sau de către o altă persoană care se spune unei obligații echivalente[305].

Recomandarea CoE din 1997 privind datele medicale aplică mai în amănunt principiile Convenției 108 legate de prelucrarea datelor în domeniul medical[306]. Normele propuse sunt în conformitate cu cele ale Directivei privind protecția datelor în ceea ce priveşte scopurile legitime ale prelucrării datelor medicale, obligațiile necesare privind secretul profesional în cazul persoanelor care utilizează date medicale, precum şi drepturile persoanelor vizate privind transparența şi accesul, rectificarea şi ştergerea datelor. În plus, datele medicale care sunt prelucrate în mod legal de către cadrele medicale nu pot fi transferate către autoritățile responsabile de aplicarea legii, cu excepția cazului în care „sunt asigurate garanții adecvate pentru a împiedica

305 A se vedea, de asemenea, Hotărârea CEDO din 25 noiembrie 2008 în cauza *Biriuk/Lituania*, nr. 23373/03.

306 CE, Comitetul de Miniştri (1997), Recomandarea Rec(97)5 către statele membre privind protecția datelor medicale, 13 februarie 1997.

dezvăluirea incompatibilă cu respectarea [...] vieții private garantate în temeiul articolului 8 din Convenția europeană a drepturilor omului"[307].

În plus, Recomandarea privind datele medicale conține dispoziții speciale cu privire la datele medicale ale copiilor nenăscuți şi ale persoanelor aflate în incapacitate şi cu privire la prelucrarea datelor genetice. Activitatea de cercetare ştiințifică este recunoscută în mod explicit ca justificare a conservării datelor pe o perioadă 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 ştiințifice şi, în acelaşi timp, protejează interesele pacienților în cauză. Conceptul de pseudonimizare în contextul protecției datelor este explicat în detaliu la secţiunea 2.1.3.

S-au purtat discuții intense la nivel național şi european cu privire la inițiativele de stocare a datelor privind tratamentul medical al unui pacient într-un dosar electronic de sănătate[308]. Un aspect deosebit legat de sistemele de dosare electronice de sănătate la nivel național este disponibilitatea acestora în străinătate: un subiect de interes deosebit în cadrul UE în contextul asistenței medicale transfrontaliere[309].

Un alt domeniu în curs de dezbatere cu privire la noile dispoziții este acela al studiilor clinice, cu alte cuvinte, testarea de noi medicamente pe pacienți într-un mediu de cercetare documentată; din nou, acest subiect are implicații considerabile cu privire la protecția datelor. Studiile clinice referitoare la produsele medicamentoase de uz uman sunt reglementate prin Directiva 2001/20/CE a Parlamentului European şi a Consiliului din 4 aprilie 2001 de apropiere a actelor cu putere de lege şi a actelor administrative ale statelor membre privind aplicarea bunelor practici clinice în cazul efectuării de studii clinice pentru evaluarea produselor medicamentoase de uz uman (*Directiva privind studiile clinice*)[310]. În luna decembrie a anului 2012, Comisia

307 Hotărârea CEDO din 6 iunie 2013 în cauza *Avilkina și alții/Rusia*, nr. 1585/09, punctul 53 (nefinal).

308 Grupul de lucru Articolul 29 (2007), *Document de lucru privind prelucrarea datelor medicale cu caracter personal din dosarul electronic de sănătate (DES)*, WP 131, Bruxelles, 15 februarie 2007.

309 Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere, MO 2011 L 88.

310 Directiva 2001/20/CE a Parlamentului European și a Consiliului din 4 aprilie 2001 de apropiere a actelor cu putere de lege şi a actelor administrative ale statelor membre privind aplicarea bunelor practici clinice în cazul efectuării de studii clinice pentru evaluarea produselor medicamentoase de uz uman, MO 2001 L 121.

Europeană a propus un regulament de înlocuire a Directivei privind studiile clinice cu scopul de a armoniza şi eficientiza procedurile de investigație[311].

Există multe alte inițiative legislative şi de altă natură în curs la nivelul UE în ceea ce priveşte datele cu caracter personal din sectorul sănătății[312].

8.4. Prelucrarea datelor în scopuri statistice

Puncte-cheie

- Datele colectate în scopuri statistice nu pot fi utilizate în niciun alt scop.
- Datele colectate în mod legitim în orice scop pot fi utilizate ulterior în scopuri statistice, cu condiția ca legislația națională să prevadă garanții corespunzătoare, care trebuie îndeplinite de către utilizatori. În acest scop, anonimizarea sau pseudonimizarea ar trebui avute în vedere înainte de transmiterea către terți.

În Directiva privind protecția datelor, prelucrarea datelor în scopuri statistice este menționată în contextul posibilelor exceptări de la principiile de protecție a datelor. La articolul 6 alineatul (1) litera (b) din directivă, se poate renunța la principiul restrângerii scopului în temeiul legislației naționale în favoarea utilizării ulterioare a datelor în scopuri statistice, deşi legislația națională trebuie să stabilească, de asemenea, toate garanțiile necesare. Articolul 13 alineatul (2) din directivă permite restrângeri ale drepturilor de acces prin legislația națională în cazul în care datele sunt prelucrate exclusiv în scopuri statistice; din nou, legislația națională trebuie să prevadă garanții corespunzătoare. În acest context, Directiva privind protecția datelor stabileşte o cerință specifică conform căreia niciun fel de date obținute sau generate în cadrul cercetării statistice nu pot fi utilizate pentru adoptarea de decizii concrete referitoare la persoanele vizate.

Deşi datele colectate în mod legal de un operator indiferent de scop pot fi reutilizate de operatorul respectiv în scopuri statistice proprii – aşa-numitele statistici secundare – datele trebuie să fie anonimizate sau pseudonimizate, în funcție de context,

311 Comisia Europeană (2012), *Propunere de regulament al Parlamentului European și al Consiliului privind trialurile clinice cu medicamente de uz uman și de abrogare a Directivei 2001/20/CE*, COM(2012) 369 finală, Bruxelles, 17 iulie 2012.

312 AEPD (2013), *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.

înainte de transmiterea acestora către un terț în scopuri statistice, cu excepția cazului în care persoana vizată şi-a exprimat acordul în acest sens sau dacă acest lucru este prevăzut în mod expres prin legislația națională. Acest lucru decurge din cerința privind garanțiile corespunzătoare prevăzută la articolul 6 alineatul (1) litera (b) din Directiva privind protecția datelor.

Cele mai importante cazuri de utilizare a datelor în scopuri statistice sunt statisticile oficiale realizate de birourile de statistică naționale şi europene în temeiul legislației naționale şi europene privind statisticile oficiale. În conformitate cu aceste legislații, cetățenii şi întreprinderile au, de regulă, obligația de a dezvălui date autorităților de statistică. Funcționarii din cadrul birourilor de statistică se supun unor obligații speciale privind secretul profesional, care sunt atent respectate, 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.

Regulamentul (CE) nr. 223/2009 privind statisticele europene (*Regulamentul privind statisticele europene*) conține norme esențiale pentru protejarea datelor în contextul statisticilor oficiale şi, prin urmare, poate fi, de asemenea, considerat relevant pentru dispozițiile privind statisticile oficiale la nivel național[313]. Regulamentul susține principiul conform căruia operațiunile statistice oficiale necesită un temei juridic suficient de explicit[314].

Exemplu: În cauza *Huber/Bundesrepublik Deutschland*[315], CJUE a constatat că, atât colectarea, cât şi stocarea datelor cu caracter personal de către o autoritate în scopuri statistice nu reprezintă, în sine, un motiv suficient pentru ca prelucrarea să fie considerată legală. Legea care prevede prelucrarea datelor cu caracter personal, trebuia, de asemenea, să îndeplinească cerința de necesitate, ceea ce, în speță, nu era valabil.

313 Regulamentul (CE) Nr. 223/2009 al Parlamentului European şi al Consiliului din 11 martie 2009 privind statisticile europene şi de abrogare a Regulamentului (CE, Euratom) nr. 1101/2008 al Parlamentului European şi al Consiliului privind transmiterea de date statistice confidențiale Biroului Statistic al Comunităților Europene, a Regulamentului (CE) nr. 322/97 al Consiliului privind statisticile comunitare şi a Deciziei 89/382/CEE, Euratom a Consiliului de constituire a Comitetului pentru programele statistice ale Comunităților Europene, MO 2009 L 87.

314 Acest principiu urmează a fi 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, disponibil la: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 Hotărârea CJUE din 16 decembrie 2008 în cauza *Huber/Bundesrepublik Deutschland,* C-524/06; a se vedea, în special, punctul 68.

În contextul CoE, Recomandarea privind datele statistice, emisă în anul 1997, face referire la performanța statisticilor în sectorul public şi privat[316]. Această recomandare a introdus principii care coincid cu normele principale ale Directivei privind protecția datelor descrisă mai sus. Sunt furnizate norme mai detaliate cu privire la următoarele aspecte.

Întrucât datele colectate de un operator în scopuri statistice nu pot fi utilizate în alte scopuri, datele care au fost colectate pentru scopuri altele decât statistice vor fi disponibile pentru a fi utilizate ulterior în scopuri statistice. Recomandarea privind datele statistice permite şi comunicarea de date către terți dacă aceasta este exclusiv în scopuri statistice. În astfel de cazuri, părțile trebuie să convină cu privire la şi să înregistreze gradul de utilizare ulterioară legitimă în scopuri statistice. Întrucât acest lucru nu poate substitui consimțământul persoanei vizate, se presupune că legislația națională trebuie să prevadă garanții suplimentare corespunzătoare 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 transmitere.

Persoanele care activează în domeniul cercetărilor statistice trebuie să se supună unor obligații speciale privind secretul profesional – tipic pentru statisticile oficiale – în temeiul legislației naționale. Acest lucru trebui să se extindă, de asemenea, la intervievatori, în cazul în care aceştia 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 prevăzut de lege, persoanele vizate trebuie să fie de acord cu utilizarea datelor lor pentru ca studiul să fie legitim sau acestora trebuie să li se acorde cel puțin oportunitatea de a se opune. În cazul în care datele cu caracter personal sunt colectate în scopuri statistice, prin intervievarea persoanelor, aceste persoane trebuie să fie informate în mod clar dacă divulgarea datelor este sau nu obligatorie în conformitate cu legislația națională. Datele sensibile nu trebuie colectate în aşa fel încât persoana să poată fi identificată, cu excepția cazului în care acest lucru este permis în mod expres de legislația națională.

În cazul în care un studiu statistic nu poate fi efectuat fără date anonime, iar datele cu caracter personal sunt într-adevăr necesare, datele colectate în scopul respectiv trebuie să fie anonimizate cât mai curând posibil. Rezultatele studiului statistic nu

316 Consiliul Europei, Comitetul de Miniştri (1997), Recomandarea Rec(97)18 către statele membre privind protecția datelor personale colectate şi prelucrate în scopuri statistice, 30 septembrie 1997.

trebuie, în niciun fel, să permită identificarea persoanei vizate, cu excepția cazului în care acest lucru, în mod evident, nu prezintă niciun risc.

După finalizarea studiului statistic, datele cu caracter personal utilizate trebuie șterse sau anonimizate. În acest caz, Recomandarea privind datele statistice propune ca datele de identificare să fie păstrate separat de alte date cu caracter personal. Acest lucru înseamnă, spre exemplu, că datele trebuie să fie pseudonimizate, iar cheia de criptare sau lista cu sinonimele de identificare trebuie păstrată separat de datele pseudonimizate.

8.5. Date financiare

Puncte-cheie

- Deși datele financiare nu sunt date sensibile în sensul Convenției 108 sau al Directivei privind protecția datelor, prelucrarea acestora necesită anumite măsuri de protecție în vederea asigurării acurateței și securității datelor.
- Sistemele electronice de plată necesită protecție incorporată a datelor, așa-numitul principiu referitor la viața privată încă din stadiul dezvoltării.
- În acest domeniu, apar probleme specifice privind protecția datelor, determinate de necesitatea de a dispune de mecanisme adecvate de autentificare.

Exemplu: În cauza *Michaud/Franța*[317], reclamantul, un avocat francez, a contestat obligația care îi revine în baza legislației franceze de a raporta suspiciuni privind posibilele activități de spălare de bani de către clienții săi. CEDO a observat că solicitarea avocaților de a raporta autorităților administrative informații cu privire la o altă persoană, care au intrat în posesia acestora prin efectuarea de schimburi de informații cu persoana respectivă, constituie o atingere asupra dreptului avocaților de respectare a corespondenței și a vieții private, în conformitate cu articolul 8 din Convenția europeană a drepturilor omului, întrucât noțiunea respectivă vizează activitățile cu caracter profesional sau de afaceri. Cu toate acestea, atingerea adusă a fost în conformitate cu legea și a urmărit un scop legitim, respectiv prevenirea dezordinii și a criminalității. Întrucât avocații

317 Hotărârea CEDO din 6 decembrie 2012 în cauza *Michaud/Franța*, nr. 12323/11; a se vedea, 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.

se supun obligației de a raporta suspiciuni doar în circumstanțe foarte limitate, CEDO a constatat că obligația respectivă este proporțională și s-a pronunțat asupra neîncălcării articolului 8.

Aplicarea cadrului juridic general privind protecția datelor, astfel cum se prevede în Convenția 108, la contextul plăților a fost elaborată de CoE în Recomandarea Rec(90)19 din 1990[318]. Această recomandare clarifică domeniul colectării legale și al utilizării datelor în contextul plăților, mai ales prin intermediul cardurilor. Recomandarea propune, de asemenea, legislatorilor naționali reglementări detaliate referitoare la limitele de comunicare către terți a datelor privind plata, la termenele de păstrare a datelor, la transparență, securitatea datelor și fluxurile transfrontaliere de date și, în final, la supraveghere și căi de atac. Soluțiile propuse corespund cu ceea ce a fost ulterior furnizat drept cadru general al UE privind protecția datelor în Directiva privind protecția datelor.

O serie de instrumente juridice sunt create pentru reglementarea piețelor instrumentelor financiare și a activităților instituțiilor de credit și a întreprinderilor de investiții[319]. Alte instrumente juridice acordă sprijin în combaterea utilizărilor abuzive ale informațiilor privilegiate și manipulărilor pieței[320]. Cele mai critice probleme în aceste domenii, care au impact asupra protecției datelor sunt:

- păstrarea înregistrărilor cu privire la tranzacțiile financiare;
- transferul datelor cu caracter personal către țări terțe;

318 CoE, Comitetul de Miniștri (1990), Recomandarea Nr. R(90)19 privind protecția datelor cu caracter personal utilizate pentru plăți și alte operațiuni conexe, 13 septembrie 1990.

319 Comisia Europeană (2011), *Propunere de directivă a Parlamentului European și a Consiliului privind piețele instrumentelor financiare, de abrogare a Directivei 2004/39/CE a Parlamentului European și a Consiliului*, COM(2011) 656 final, Bruxelles, 20 octombrie 2011; Comisia Europeană (2011), *Propunere de regulament al Parlamentului European și al Consiliului privind piețele instrumentelor financiare și de modificare a Regulamentului [EMIR] privind instrumentele derivate extrabursiere, contrapărțile centrale și registrele de tranzacții*, COM(2011) 652 final, Bruxelles, 20 octombrie 2011; Comisia Europeană (2011), *Propunere de directivă a Parlamentului European și a Consiliului cu privire la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit și a societăților de investiții și de modificare a Directivei 2002/87/CE a Parlamentului European și a Consiliului privind supravegherea suplimentară a instituțiilor de credit, a întreprinderilor de asigurare și a societăților de investiții care aparțin unui conglomerat financiar*, COM(2011) 453 final, Bruxelles, 20 iulie 2011.

320 Comisia Europeană (2011), *Propunere de regulament al Parlamentului European și al Consiliului privind utilizările abuzive ale informațiilor privilegiate și manipulările pieței (abuzul de piață)*, COM(2011) 651 final, Bruxelles, 20 octombrie 2011; Comisia Europeană (2011), *Propunere de directivă a Parlamentului European și a Consiliului privind sancțiunile penale pentru utilizările abuzive ale informațiilor privilegiate și manipulările pieței*, COM(2011) 654 final, Bruxelles, 20 octombrie 2011.

- înregistrarea convorbirilor telefonice sau a comunicațiilor electronice, inclusiv capacitatea autorităților competente de a solicita înregistrări ale convorbirilor telefonice şi ale datelor de trafic;

- dezvăluirea informațiilor personale, inclusiv publicarea sancțiunilor;

- competențele de supraveghere şi investigare ale autorităților competente, inclusiv competența de a efectua inspecții la fața locului şi competența de a se deplasa la incinte private în vederea confiscării de documente;

- mecanismele de raportare a încălcărilor, respectiv, regimurile privind denunțarea; şi

- cooperarea între autoritățile competente ale statelor membre şi Autoritatea Europeană pentru Valori Mobiliare şi Piețe (AEVMP).

Există şi alte probleme în aceste domenii, care sunt abordate în mod specific, inclusiv colectarea de date cu privire la situația financiară a persoanelor vizate[321] sau plățile transfrontaliere prin transferuri bancare, care generează, inevitabil, fluxuri de date cu caracter personal[322].

321 Regulamentul (CE) Nr. 1060/2009 al Parlamentului European şi al Consiliului din 16 septembrie 2009 privind agențiile de rating de credit, MO 2009 L 302; Comisia Europeană, *Propunere de regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (CE) nr. 1060/2009 privind agențiile de rating de credit*, COM(2010) 289 final, Bruxelles, 2 iunie 2010.

322 Directiva 2007/64/CE a Parlamentului European şi 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 şi 2006/48/CE şi de abrogare a Directivei 97/5/CE, MO 2007 L 319.

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.

EDRi, *An introduction to data protection* (O introducere în protecția datelor), Bruxelles, disponibilă la: www.edri.org/files/paper06_datap.pdf.

Frowein, J. şi Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. şi Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. şi Bates, E. (2009), *Law of the European Convention on Human Rights* (Legea privind Convenția europeană a drepturilor omului), Oxford, Oxford University Press.

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* (Cazuri, materiale şi comentarii cu privire la Convenția europeană a drepturilor omului), Oxford, Oxford University Press.

Nowak, M., Januszewski, K. şi Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights* (Toate drepturile omului pentru toți – Manualul de la Viena cu privire la drepturile omului), Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. şi 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. şi Brandeis, L. (1890), „The right to privacy" („Dreptul la viață privată"), *Harvard Law Review,* Vol. 4, Nr. 5, pp. 193-220, disponibilă la: www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. şi Ovey, C. (2010), *The European Convention on Human Rights* (Convenția europeană a drepturilor omului), Oxford, Oxford University Press.

Capitolul 2

Biroul comisarului pentru informații din Regatul Unit (2012), *Anonymisation: managing data protection risk. Code of practice* (Anonimizarea: administrarea riscului privind protecția datelor. Cod de practică), disponibil la: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law* (Protecția datelor: ghid practic privind legislația Regatului Unit şi a UE), Oxford, Oxford University Press.

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.

Morgan, R. şi Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance* (Strategia privind protecția datelor: punerea în aplicare a respectării protecției datelor), Londra, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization" („Nerespectarea promisiunilor de confidențialitate: reacție la eşecul neprevăzut al anonimizării"), *UCLA Law Review*, Vol. 57, Nr. 6, pp. 1701-1777.

Tinnefeld, M., Buchner, B. şi Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, München, Oldenbourg Wissenschaftsverlag.

Capitolele 3 - 5

Biroul comisarului pentru informații din Regatul Unit, *Privacy Impact Assessment* (Evaluarea impactului asupra vieții private), disponibilă la: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

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. şi 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*, Saarbrücken, Éditions universitaires européennes.

Dammann, U. şi Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Agenția pentru Drepturi Fundamentale a Uniunii Europene) (2010), *Protecția datelor în Uniunea Europeană: rolul autorităților naționale pentru protecția datelor (Consolidarea arhitecturii drepturilor fundamentale în UE II)*, Luxemburg, Oficiul pentru Publicații al Uniunii Europene (Oficiul pentru Publicații).

FRA (2010), *Elaborarea indicatorilor pentru protecția, respectarea și promovarea drepturilor copilului în Uniunea Europeană* (Ediție de conferință), Viena, FRA.

FRA (2011), *Accesul la justiție în Europa: privire de ansamblu asupra provocărilor și oportunităților*, Luxemburg, Oficiul de publicații.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

Capitolul 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. și Nouwt, S. (2009), *Reinventing data protection?* (Reinventarea protecției datelor?), Berlin, Springer.

Kuner, C. (2007), *European data protection law* (Legislația europeană privind protecția datelor), Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law* (Reglementarea fluxului transfrontalier de date și legislația privind confidențialitatea datelor), Oxford, Oxford University Press.

Capitolul 7

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime* (Cadrul Europol privind protecția datelor drept instrument important în lupta împotriva criminalității informatice), Forumul ERA, Vol. 13, Nr. 3, pp. 381-395.

Europol (2012), *Data Protection at Europol* (Protecția datelor la Europol), Luxemburg, Oficiul de publicații, disponibilă la: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime* (Protecția datelor la Eurojust: un regim solid, eficace și adaptat), Haga, Eurojust.

Gutwirth, S., Poullet, Y. și De Hert, P. (2010), *Data protection in a profiled world* (Protecția datelor într-o lume bazată pe profile), Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. și Leenes, R. (2011), *Computers, privacy and data protection: An element of choice* (Computere, confidențialitate și protecția datelor: o chestiune de alegere), Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem* (Distrugerea democrației sub pretextul apărării ei? Directiva privind păstrarea datelor, supravegherea statului şi ecosistemul nostru constituțional), *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* (Rolul Parlamentului European în încheierea acordurilor transatlantice privind transferul de date cu caracter personal după Lisabona), Centrul de drept privind relațiile externe, Documente de lucru CLEER 2013/2, disponibile la: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Capitolul 8

Büllesbach, A., Gijrath, S., Poullet, Y. şi Hacon, R. (2010), *Concise European IT law* (Legislația europeană concisă privind tehnologia informației), Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. şi Poullet, Y. (2012), *European data protection: In good health?* (Protecția datelor în Europa: este sigură?) , Dordrecht, Springer.

Gutwirth, S., Poullet, Y. şi De Hert, P. (2010), *Data protection in a profiled world* (Protecția datelor într-o lume bazată pe profile), Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. şi Leenes, R. (2011), *Computers, privacy and data protection: An element of choice* (Computere, confidențialitate şi protecția datelor: o chestiune de alegere), Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem* (Distrugerea democrației sub pretextul apărării ei? Directiva privind păstrarea datelor, supravegherea statului şi ecosistemul nostru constituțional), *European Law Review*, Vol. 36, Nr. 5, pp. 722-776.

Rosemary, J. şi Hamilton, A. (2012), *Data protection law and practice* (Legislația şi practica privind protecția datelor), Londra, Sweet & Maxwell.

Jurisprudență

Jurisprudență selectată a Curții Europene a Drepturilor Omului

Acces la date cu caracter personal

Cauza *Gaskin/Regatul Unit*, nr. 10454/83, 7 iulie 1989
Cauza *Godelli/Italia*, nr. 33783/09, 25 septembrie 2012
Cauza *K.H. și alții/Slovacia*, nr. 32881/04, 28 aprilie 2009
Cauza *Leander/Suedia*, nr. 9248/81, 26 martie 1987
Cauza *Odièvre/Franța* [T], nr. 42326/98, 13 februarie 2003

Ponderarea protecției datelor cu libertatea de exprimare

Cauza *Axel Springer AG/Germania* [T], nr. 39954/08, 7 februarie 2012
Cauza *Von Hannover/Germania*, nr. 59320/00, 24 iunie 2004
Cauza *Von Hannover/Germania (nr. 2) [T]*, nr. 40660/08 şi nr. 60641/08, 7 februarie 2012

Provocări legate de protecția datelor online

Cauza *K.U./Finlanda*, nr. 2872/02, 2 decembrie 2008

Corespondență

Cauza *Amann/Elveția* [T], nr. 27798/95, 16 februarie 2000
Cauza *Bernh Larsen Holding AS și alții/Norvegia*, nr. 24117/08, 14 martie 2013

Cauza *Cemalettin Canli/Turcia*, nr. 22427/04, 18 noiembrie 2008
Cauza *Dalea/Franța*, nr. 964/07, 2 februarie 2010
Cauza *Gaskin/Regatul Unit*, nr. 10454/83, 7 iulie 1989
Cauza *Haralambie/România*, nr. 21737/03, 27 octombrie 2009
Cauza *Khelili/Elveția*, nr. 16188/07, 18 octombrie 2011
Cauza *Leander/Suedia*, nr. 9248/81, 26 martie 1987
Cauza *Malone/Regatul Unit*, nr. 8691/79, 2 august 1984
Cauza *McMichael/Regatul Unit*, nr. 16424/90, 24 februarie 1995
Cauza *M.G./Regatul Unit*, nr. 39393/98, 24 septembrie 2002
Cauza *Rotaru/România* [T], nr. 28341/95, 4 mai 2000
Cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și nr. 30566/04, 4 decembrie 2008
Cauza *Shimovolos/Rusia*, nr. 30194/09, 21 iunie 2011
Cauza *Turek/Slovacia*, nr. 57986/00, 14 februarie 2006

Baze de date privind cazierele judiciare

Cauza *B.B./Franța*, nr. 5335/06, 17 decembrie 2009
Cauza *M.M./Regatul Unit*, nr. 24029/07, 13 noiembrie 2012

Baze de date privind ADN-ul

Cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și nr. 30566/04, 4 decembrie 2008

Date GPS

Cauza *Uzun/Germania*, nr. 35623/05, 2 septembrie 2010

Date privind starea de sănătate

Cauza *Biriuk/Lituania*, nr. 23373/03, 25 noiembrie 2008
Cauza *I./Finlanda*, nr. 20511/03, 17 iulie 2008
Cauza *L.L./Franța*, nr. 7508/02, 10 octombrie 2006
Cauza *M.S./Suedia*, nr. 34209/96, 27 august 1997
Cauza *Szuluk/Regatul Unit*, nr. 36936/05, 2 iunie 2009
Cauza *Z./Finlanda*, nr. 22009/93, 25 februarie 1997

Identitate

Cauza *Ciubotaru/Moldova*, nr. 27138/04, 27 aprilie 2010
Cauza *Godelli/Italia*, nr. 33783/09, 25 septembrie 2012
Cauza *Odièvre/Franța* [T], nr. 42326/98, 13 februarie 2003

Informații privind activitățile profesionale

Cauza *Michaud/Franța*, nr. 12323/11, 6 decembrie 2012
Cauza *Niemietz/Germania*, nr. 13710/88, 16 decembrie 1992

Interceptarea comunicărilor

Cauza *Amann/Elveția* [T], nr. 27798/95, 16 februarie 2000
Cauza *Copland/Regatul Unit*, nr. 62617/00, 3 aprilie 2007
Cauza *Cotlet/România*, nr. 38565/97, 3 iunie 2003
Cauza *Kruslin/Franța*, nr. 11801/85, 24 aprilie 1990
Cauza *Lambert/Franța*, nr. 23618/94, 24 august 1998
Cauza *Liberty și alții/Regatul Unit*, nr. 58243/00, 1 iulie 2008
Cauza *Malone/Regatul Unit*, nr. 8691/79, 2 august 1984
Cauza *Halford/Regatul Unit*, nr. 20605/92, 25 iunie 1997
Cauza *Szuluk/Regatul Unit*, nr. 36936/05, 2 iunie 2009

Obligații pentru persoanele responsabile

Cauza *B.B./Franța*, nr. 5335/06, 17 decembrie 2009
Cauza *I./Finlanda*, nr. 20511/03, 17 iulie 2008
Cauza *Mosley/Regatul Unit*, nr. 48009/08, 10 mai 2011

Fotografii

Cauza *Sciacca/Italia*, nr. 50774/99, 11 ianuarie 2005
Cauza *Von Hannover/Germania*, nr. 59320/00, 24 iunie 2004

Dreptul de a fi uitat

Cauza *Segerstedt-Wiberg și alții/Suedia*, nr. 62332/00, 6 iunie 2006

Dreptul de opoziție

Cauza *Leander/Suedia*, nr. 9248/81, 26 martie 1987
Cauza *Mosley/Regatul Unit*, nr. 48009/08, 10 mai 2011
Cauza *M.S./Suedia*, nr. 34209/96, 27 august 1997
Cauza *Rotaru/România* [T], nr. 28341/95, 4 mai 2000

Categorii de date sensibile

Cauza *I./Finlanda*, nr. 20511/03, 17 iulie 2008

Cauza *Michaud/Franța*, nr. 12323/11, 6 decembrie 2012
Cauza *S. și Marper/Regatul Unit*, nr. 30562/04 şi nr. 30566/04, 4 decembrie 2008

Supravegherea și aplicarea legii (rolul diferiților actori, inclusiv al autorităților pentru protecția datelor)

Cauza *I./Finlanda*, nr. 20511/03, 17 iulie 2008
Cauza *K.U./Finlanda*, nr. 2872/02, 2 decembrie 2008
Cauza *Von Hannover/Germania*, nr. 59320/00, 24 iunie 2004
Cauza *Von Hannover/Germania (nr. 2) [T]*, nr. 40660/08 şi nr. 60641/08, 7 februarie 2012

Metode de supraveghere

Cauza *Allan/Regatul Unit*, nr. 48539/99, 5 noiembrie 2002
Cauza *Asociația „21 decembrie 1989" și alții/România*, nr. 33810/07 şi nr. 18817/08, 24 mai 2011
Cauza *Bykov/Rusia* [T], nr. 4378/02, 10 martie 2009
Cauza *Kennedy/Regatul Unit*, nr. 26839/05, 18 mai 2010
Cauza *Klass și alții/Germania*, nr. 5029/71, 6 septembrie 1978
Cauza *Rotaru/România* [T], nr. 28341/95, 4 mai 2000
Cauza *Taylor-Sabori/Regatul Unit*, nr. 47114/99, 22 octombrie 2002
Cauza *Uzun/Germania*, nr. 35623/05, 2 septembrie 2010
Cauza *Vetter/Franța*, nr. 59842/00, 31 mai 2005

Supraveghere video

Cauza *Köpke/Germania*, nr. 420/07, 5 octombrie 2010
Cauza *Peck/Regatul Unit*, nr. 44647/98, 28 ianuarie 2003

Probe de voce

Cauza *P.G. și J.H./Regatul Unit*, nr. 44787/98, 25 septembrie 2001
Cauza *Wisse/Franța*, nr. 71611/01, 20 decembrie 2005

Jurisprudență selectată a Curții de Justiție a Uniunii Europene

Jurisprudență pentru Directiva privind protecția datelor

Cauza *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy și Satamedia Oy*, C-73/07, 16 decembrie 2008
[Conceptul de „activități jurnalistice", în sensul articolului 9 Directiva privind protecția datelor]

Cauzele conexate C-92/09 și C-93/09, *Volker și Markus Schecke GbR și Hartmut Eifert/Land Hessen*, 9 noiembrie 2010
[Proporționalitatea obligației legale de a publica date cu caracter personal privind beneficiarii unor anumite fonduri agricole ale UE]

Cauza *Bodil Lindqvist*, C-101/016, noiembrie 2003
[Legitimitatea publicării pe internet de către o persoană fizică a unor date privind viața privată a altor persoane]

Cauza Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González, C-131/12, Referință privind o hotărâre preliminară a Audiencia Nacional (Spain) formulată la 9 martie 2012, 25 mai 2012, pendinte
[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]

Cauza *Comisia Europeană/Regatul Suediei*, C-270/11, 30 mai 2013
[Amendă pentru nepunerea în aplicare a unei directive]

Cauza *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06, 29 ianuarie 2008
[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]

Cauza *Comisia Europeană/Ungaria*, C-288/12, 8 aprilie 2014
[Legitimitatea încetării mandatului autorității naționale pentru protecția datelor]

Cauza *Michael Schwarz/Stadt Bochum*, C-291/12, Avizul avocatului general, 13 iunie 2013
[Încălcarea dreptului primar al UE prin Regulamentul (CE) 2252/2004 care prevede stocarea elementelor biometrice în pașapoarte]

Cauze comune *Drepturile Digitale Irlanda și Seitlinger și alții*, C-293/12 şi C-594/12, 8 aprilie 2014
[Încălcarea legislației primare a UE prin Directiva privind păstrarea datelor]

Cauza *SABAM/Netlog NV*, C-360/10, 16 februarie 2012
[Obligația furnizorilor de rețele sociale de a împiedica utilizarea ilicită a operelor muzicale şi audiovizuale de către utilizatorii rețelei]

Cauzele conexate *Rechnungshof/Österreichischer Rundfunk și alții și Neukomm și Lauermann/Österreichischer Rundfunk*, C-465/00, C-138/01 şi C-139/01, 20 mai 2003
[Proporționalitatea obligației legale de a publica date cu caracter personal privind salariile angajaților anumitor categorii de instituții asociate sectorului public]

Cauzele conexate *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) și Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, C-468/10 şi C-469/10, 24 noiembrie 201
[Punerea în aplicare corectă a articolului 7 litera (f) din Directiva privind protecția datelor – „interesele legitime ale altor persoane" – în legislația națională]

Cauza *Comisia Europeană/Republica Federală Germania*, C-518/07, 9 martie 2010
[Independența unei autorități naționale de supraveghere]

Cauza *Huber/Bundesrepublik Deutschland*, C-524/06, 16 decembrie 2008
[Legitimitatea deținerii de date privind cetățenii străini într-un registru statistic]

Cauza *Deutsche Telekom AG/Bundesrepublik Deutschland*, C-543/09, 5 mai 2011
[Necesitatea reînnoirii consimțământului]

Cauza *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, C-553/07, 7 mai 2009
[Dreptul de acces al persoanei vizate]

Cauza *Comisia Europeană/Republica Austria*, C-614/10, 16 octombrie 2012
[Independența unei autorități naționale de supraveghere]

Jurisprudență pentru Regulamentul privind protecția datelor de către instituțiile UE

Cauza *Comisia Europeană/The Bavarian Lager Co. Ltd.*, C-28/08 P, 29 iunie 2010
[Accesul la documente]

Cauza *Interporc Im- und Export GmbH/Comisia Comunităților Europene*, C-41/00 P, 6 martie 2003
[Accesul la documente]

Cauza *Dimitrios Pachtitis/Comisiei Europene*, F-35/08, 15 iunie 2010
[Utilizarea datelor cu caracter personal în contextul angajării în cadrul instituțiilor UE]

Cauza *V/Parlamentul European*, F-46/09, 5 iulie 2011
[Utilizarea datelor cu caracter personal în contextul angajării în cadrul instituțiilor UE]

Lista cauzelor

Jurisprudența Curții Europene de Justiție

Jurisprudența Curții Europene a Drepturilor Omului

Jurisprudența instanțelor naționale

Agenția pentru Drepturi Fundamentale a Uniunii Europene
Consiliul Europei – Curtea Europeană a Drepturilor Omului

Manual de legislație europeană privind protecția datelor

2014 — 209 p. — 14,8 × 21 cm

ISBN 978-92-871-9938-6 (CoE)
ISBN 978-92-9239-339-7 (FRA)
doi:10.2811/55294

Mai multe informații privind Agenția pentru Drepturi Fundamentale a Uniunii Europene sunt disponibile pe internet. Puteți accesa pagina de internet a FRA la următoarea adresă fra.europa.eu.

Mai multe informații cu privire la Consiliul Europei sunt disponibile pe internet la adresa: hub.coe.int.

Mai multe informații cu privire la jurisprudența Curții Europene a Drepturilor Omului sunt disponibile pe pagina de internet a Curții: echr.coe.int. Baza de date HUDOC asigura accesul la hotărâri și decizii în engleză și/sau franceză, traduceri în alte limbi, note informative lunare legate de jurisprudență, comunicate de presă și alte informații despre activitatea Curții.

Cum se obțin publicațiile UE

Publicații gratis:
- o copie:
  via EU Bookshop (http://bookshop.europa.eu);
- mai mult de o copie sau afișe/hărți:
  de la reprezentanțele Uniunii Europene (http://ec.europa.eu/represent_en.htm);
  de la delegațiile statelor non-UE (http://eeas.europa.eu/delegations/index_en.htm);
  prin contactarea serviciului Direct Europa (http://europa.eu/europedirect/index_ro.htm)
  sau prin apelarea numărului 00 800 6 7 8 9 10 11 (apel gratuit de oriunde din UE) (*).

Publicații cu plată:
- via UE Bookshop (http://bookshop.europa.eu);

Abonări cu plată:
- via agenților de vânzări ai Oficiului de Publicații al Uniunii Europene (http://publications.europa.eu/others/agents/index_en.htm).

(*) Informațiile oferite sunt gratis, precum și majoritatea apelurilor (prin intermediul anumitor operatori, există posibilitatea de taxare din partea hotelurilor sau prin utilizarea cutiilor de telefon).

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 (http://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, precum și textul integral al convențiilor Consiliului Europei sunt disponibile pe site-ul internet al Biroului Tratate: http://conventions.coe.int/.

10.2811/55294
TK-01-13-772-RO-C

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

Dezvoltarea rapidă a tehnologiilor informației și comunicațiilor subliniază nevoia tot mai mare de o protecție solidă a datelor cu caracter personal – un drept garantat atât de instrumentele Uniunii Europene (UE), cât și de instrumentele Consiliului Europei (CE). Progresele tehnologice extind limitele supravegherii, interceptării comunicărilor și stocării datelor, acestea reprezentând provocări importante pentru dreptul de protecție a datelor. Prezentul manual este conceput pentru a familiariza practicienii în domeniul dreptului, nespecializați în domeniul protecției datelor, cu acest domeniu de drept. Acesta oferă o imagine de ansamblu asupra cadrelor juridice ale UE și CoE în vigoare. Ghidul explică jurisprudența-cheie, rezumând hotărâri majore atât ale Curții Europene a Drepturilor Omului (CEDO), cât și ale Curții de Justiție a Uniunii Europene (CJUE). În cazul în care nu există o astfel de jurisprudență, se prezintă ilustrații practice cu scenarii ipotetice. Într-un cuvânt, prezentul manual are scopul de a asigura susținerea cu vigoare și determinare a dreptului de protecție a datelor.

AGENȚIA PENTRU DREPTURI FUNDAMENTALE A UNIUNII EUROPENE
Schwarzenbergplatz 11 - 1040 Viena - Austria
Tel. +43 (1) 580 30-60 - Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

CONSILIUL EUROPEI
CURTEA EUROPEANĂ A DREPTURILOR OMULUI
67075 Strasbourg Cedex - Franța
Tel. +33 (0) 3 88 41 20 00 - Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Oficiul pentru Publicații
ISBN 978-92-871-9938-6 (CoE)
ISBN 978-92-9239-339-7 (FRA)