

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

CURTEA EUROPEANĂ A DREPTURILOR OMULUI

Ghid privind jurisprudența Convenției europene a drepturilor omului

Protecția datelor

Actualizat la 28 februarie 2025

Întocmit de Grefă. Nu obligă Curtea.





Invităm editorii sau organizațiile care doresc să traducă și/sau să reproducă integral sau parțial acest ghid, în format tipărit sau electronic (web), să completeze formularul de contact: *cererea pentru reproducerea sau republicarea unei traduceri* pentru a se informa cu privire la procedura de autorizare.

Pentru informații referitoare la traducerea ghidurilor privind jurisprudența, vă rugăm consultați lista *Traduceri în curs*.

Textul original al acestui ghid este în limba franceză. Acesta este actualizat periodic. Prezenta actualizare a fost finalizată la 28 februarie 2025. Textul poate suferi modificări de formă.

Ghidul poate fi descărcat de la adresa *https://ks.echr.coe.int*. Pentru informații actualizate despre publicații, vă rugăm să accesați contul X al Curții: *https://x.com/ECHR_CEDH*.

Prezenta traducere este publicată cu acordul Consiliului Europei și al Curții Europene a Drepturilor Omului și reprezintă responsabilitatea exclusivă a Institutului European din România.

© Consiliul Europei/Curtea Europeană a Drepturilor Omului, 2025

Cuprins

În atenția cititorilor 6

Introducere 7

I. Definiții și principii de bază privind protecția datelor 7

A. Terminologia protecției datelor 7
1. Conceptul de date cu caracter personal și domeniul său de aplicare 7
2. Categorii de date specifice 12
a. Categorii așa-zise „sensibile” 12
i. Date care dezvăluie originea rasială sau etnică 12
ii. Date care dezvăluie opiniile politice, convingerile religioase sau de altă natură, inclusiv filozofice 13
iii. Date care dezvăluie apartenența sindicală 13
iv. Date genetice și biometrice 13
v. Date privind sănătatea, viața sexuală sau orientarea sexuală 15
vi. Date privind condamnări penale și infracțiuni 16
b. Alte categorii de date 17
i. Date privind munca prestată 17
ii. Date financiare 18
iii. Date de transfer 18
iv. Eșantioane de voce 20
v. Date de localizare GPS 20
vi. Fotografii 21

B. Cele două aspecte (negativ și pozitiv) ale protecției datelor cu caracter personal 24

C. Cele trei „criterii” în materie de protecția datelor 27
1. Legalitatea ingerinței 27
2. Legitimitatea ingerinței 31
3. „Necesitatea într-o societate democratică” a ingerinței 32
a. Cerința de a reduce la minimum datele colectate sau înregistrate 33
b. Cerința privind exactitatea și actualizarea datelor înregistrate 33
c. Cu privire la cerința de a limita perioada de păstrare a datelor pentru o perioadă care să nu depășească perioada necesară îndeplinirii scopurilor pentru care au fost înregistrate 34
d. Cerința de a limita utilizarea datelor la scopul pentru care au fost înregistrate 35
e. Cerința de transparență a procesului de prelucrare a datelor 36

II. Protecția datelor cu caracter personal și dreptul la viață privată (art. 8 din Convenție) 36

A. Operațiuni în privința datelor care pot aduce atingere dreptului la viață privată 37
1. Colectarea de date cu caracter personal 37
a. Colectarea de date de către autorități prin intermediul supravegherii secrete 37
i. Interceptarea țintită a convorbirilor telefonice și contorizarea apelurilor telefonice 37
ii. Interceptarea mesajelor primite prin pager 39
iii. Supravegherea audiovizuală și supravegherea video 39
iv. Geolocalizarea unui vehicul prin GPS 40
v. Supravegherea de către detectivi particulari 40

vi. Monitorizarea corespondenței 41
vii. Operațiuni secrete de supraveghere, spionaj, supraveghere în masă 41
b. Colectarea de date de către angajatori la locul de muncă 43
c. Colectarea de date pentru a fi utilizate ca probe în cauze 46
i. Confiscări și percheziții 46
ii. Acte medicale obligatorii cu scopul de a colecta mostre de celule 49
d. Colectarea de date cu caracter personal în contextul sănătății 50
e. Transmiterea obligatorie de date cu caracter personal 51
2. Păstrarea datelor cu caracter personal 52
a. Culegerea de date în scopul combaterii criminalității 53
i. Caracterul nediscriminatoriu și nediferențiat al datelor stocate 54
ii. Perioada de stocare a datelor 55
iii. Garanții care privesc distrugerea sau ștergerea datelor stocate 57
iv. Garanții cu scopul de a reglementa accesul terților și de a păstra integritatea și confidențialitatea datelor 59
b. Păstrarea datelor cu caracter personal în contextul sănătății 60
c. Păstrarea on-line, în scopuri jurnalistice, a datelor cu caracter personal 60
3. Divulgarea datelor cu caracter personal 61
a. Impactul consimțământului prealabil 62
b. Divulgarea de date în contextul procedurilor judiciare 64
c. Divulgarea de date pentru protejarea sănătății publice 66
d. Divulgarea de date pentru protejarea securității naționale 67
e. Divulgarea de date pentru protejarea bunăstării economice a țării 68
f. Divulgarea în masă de date cu caracter personal 69
B. Drepturile persoanelor vizate 69
1. Dreptul de acces la datele proprii 69
2. Dreptul de rectificare 72
3. Dreptul la ștergere 74
a. „Dreptul de a fi uitat” 74
b. Alte contexte 77
4. Dreptul la garanții procedurale speciale și la un cadru procedural eficient pentru exercitarea drepturilor 79

III. Interacțiunea cu alte dispoziții din Convenție sau protocoalele sale 83

A. Protecția datelor și drepturile materiale 84
1. Protecția datelor și libertatea de gândire, de conștiință și de religie (art. 9 din Convenție) 85
2. Protecția datelor și libertatea de exprimare (art. 10 din Convenție) 86
3. Protecția datelor și interzicerea discriminării (art. 14 din Convenție) 90
4. Protecția datelor și dreptul la respectarea bunurilor (art. 1 din Protocolul nr. 1) 91
5. Protecția datelor și libertatea de circulație (art. 2 din Protocolul nr. 4) 91
B. Protecția datelor și drepturile procedurale 93
1. Dreptul la un proces echitabil (art. 6 din Convenție) 93
a. Garanții generale (art. 6 § 1 din Convenție) 93
i. Egalitatea armelor și respectarea procedurii contradictorii în contextul procedurilor care implică date sensibile sau confidențiale 94
ii. Motivarea hotărârilor și protecția datelor 94
iii. Administrarea de date cu caracter personal de probe colectate în mod ilegal sau contrar art. 8 95
iv. Publicarea dezbaterilor și a pronunțării hotărârii și confidențialitatea datelor 95

v. Durata procedurilor judiciare care se pronunță cu privire la chestiunea protecției datelor 96
b. Garanții speciale (art. 6 §§ 2 și 3 din Convenție) 96
i. Protecția datelor și respectarea prezumției de nevinovăție (art. 6 § 2 din Convenție) 96
ii. Protecția datelor și dreptul la apărare [art. 6 § 3 b) din Convenție] 97
2. Dreptul la un recurs efectiv (art. 13 din Convenție) 98
3. Dreptul la libertate și la siguranță (art. 5 din Convenție) 101

IV. Provocări moderne în materie de protecție a datelor 101

B. Progrese tehnologice, algoritmi și inteligență artificială 101
B. Internet și motoare de căutare 103
C. Transferuri de date și fluxuri de date 104

Lista cauzelor citate 106

În atenția cititorilor

Prezentul ghid face parte din seria *Ghiduri privind jurisprudența*, publicată de Curtea Europeană a Drepturilor Omului (denumită în continuare „Curtea”, „Curtea Europeană” sau „Curtea de la Strasbourg”), cu scopul de a informa practicienii din domeniul dreptului cu privire la hotărârile fundamentale pronunțate de aceasta. În situația de față, prezentul ghid analizează și rezumă jurisprudența referitoare la dispozițiile Convenției europene a drepturilor omului („Convenția” sau „Convenția europeană”) aplicabile în materie de protecția datelor. Acesta trebuie să fie citit împreună cu ghidurile privind jurisprudența elaborate pe articole, la care face trimitere în mod sistematic.

Jurisprudența citată a fost aleasă dintre hotărârile și deciziile de principiu, importante și/sau recente*.

Hotărârile Curții soluționează nu numai cauzele cu judecarea cărora aceasta a fost învestită, ci servesc, de asemenea, în mai mare măsură, la a clarifica, a proteja și a dezvolta normele Convenției; astfel, acestea contribuie la respectarea, de către state, a angajamentelor pe care și le-au asumat în calitate de părți contractante [*Irlanda împotriva Regatului Unit*, 18 ianuarie 1978, pct. 154, seria A nr. 25, și, recent, *Jeronovičs împotriva Letoniei* (MC),nr. 44898/10, pct. 109, 5 iulie 2016].

Sistemul instituit de Convenție are ca finalitate să soluționeze, în interes public, probleme care țin de ordinea publică, ridicând normele de protecție a drepturilor omului și extinzând jurisprudența din acest domeniu la întreaga comunitate a statelor care sunt părți la Convenție [*Konstantin Markin împotriva Rusiei* (MC), nr. 30078/06, pct. 89, CEDO 2012]. Astfel, Curtea a subliniat rolul Convenției ca „instrument constituțional al ordinii publice europene” în domeniul drepturilor omului [*Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi împotriva Irlandei* (MC), nr. 45036/98, pct. 156, CEDO 2005-VI și, recent, *N.D. și N.T. împotriva Spaniei* (MC), nr. 8675/15 și 8697/15, pct. 110, 13 februarie 2020].

Protocolul Nr. 15 la Convenție a introdus recent principiul subsidiarității în preambulul Convenției. Acest principiu impune „o responsabilitate comună a statelor părți și a Curții” în ceea ce privește protecția drepturilor omului, iar autoritățile și instanțele naționale trebuie să interpreteze și să aplice dreptul intern într-un mod care să asigure efectul deplin al drepturilor și libertăților definite în Convenție și în protocoalele la aceasta [*Grzęda împotriva Poloniei* (MC), pct. 324].

* Jurisprudența citată poate poate fi în una sau în ambele limbi oficiale (franceză și engleză) ale Curții și ale Comisiei Europene a Drepturilor Omului. Dacă nu se specifică altfel după denumirea cauzei, referința citată este cea a unei hotărâri pe fond, pronunțate de o Cameră a Curții. Abrevierea „(dec.)” arată că este vorba despre o decizie a Curții, iar „(MC)” că respectiva cauză a fost examinată de Marea Cameră. Hotărârile pronunțate de o Cameră, care nu sunt definitive la data prezentei actualizări, sunt marcate cu un asterisc (*).

Introducere

1. Progresele tehnologice împing granițele în ceea ce privește supravegherea, interceptarea comunicațiilor și păstrarea datelor, punând în permanență datele cu caracter personal în fața unor provocări majore. Odată cu pronunțarea hotărârii *Leander împotriva Suediei*, 1987, în care fosta Curte a examinat, pentru prima dată, problema stocării de către o autoritate publică a datelor cu caracter personal ale unei persoane, jurisprudența organelor Convenției în materie a cunoscut o anumită evoluție.

2. De-a lungul anilor, Curtea a examinat numeroase situații care ridică întrebări legate de această chestiune. O gamă largă de operațiuni efectuate cu privire la datele cu caracter personal, cum ar fi colectarea, stocarea, exploatarea și diseminarea unor astfel de date face în prezent obiectul unei jurisprudențe a organelor Convenției care este descrisă în prezentul ghid. Această jurisprudență se extinde pe măsura evoluției rapide a tehnologiilor informației și comunicațiilor.

I. Definiții și principii de bază privind protecția datelor

3. Dreptul la protecția datelor cu caracter personal nu face parte, ca drept autonom, din drepturile și libertățile garantate de Convenție. Cu toate acestea, Curtea a recunoscut că protecția datelor cu caracter personal joacă un rol fundamental în exercitarea dreptului la respectarea vieții private și de familie, a domiciliului și a corespondenței, garantat de art. 8 din Convenție [*Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei* (MC), 2017, pct. 137; *Z împotriva Finlandei*, 1997, pct. 95; *L.B. împotriva Ungariei* [MC], 2023, pct. 103]. Această dispoziție permite, în sistemul Convenției, să se asigure, în primul rând, protecția datelor cu caracter personal, deși considerații legate de această protecție pot apărea și în temeiul altor dispoziții ale Convenției și ale protocoalelor sale adiționale.

A. Terminologia protecției datelor

4. Odată cu dezvoltarea tehnologiilor, operațiunile efectuate asupra datelor cu caracter personal care pot constitui „prelucrare automată” iau forme foarte diferite. În pofida abordării generoase a Curții cu privire la definiția noțiunii „viață privată”, care i-a permis să dezvolte o jurisprudență ca răspuns la evoluția societății, orice operațiune efectuată asupra datelor cu caracter personal nu intră în mod necesar în domeniul de aplicare al art. 8 sau nu constituie în mod necesar atingere asupra unuia dintre interesele pe care le protejează.

1. Conceptul de date cu caracter personal și domeniul său de aplicare

5. În hotărârile sale, Curtea explică noțiunea „date cu caracter personal” făcând trimitere la Convenția 108 a Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal din 28 ianuarie 1981, intrată în vigoare în 1985 și modernizată în 2018 („Convenția 108”), al cărei scop este acela de a „garanta pe teritoriul fiecărui stat parte, fiecărei persoane fizice [...] respectarea drepturilor și libertăților sale fundamentale și, în special, dreptul la viața privată, față de prelucrarea automatizată a datelor cu caracter personal care îl privesc (art. 1)” [*Amann împotriva Elveției* (MC), 2000, pct. 65; *Haralambie împotriva României*, 2009, pct. 77]. Curtea precizează în mod clar că, în temeiul art. 2 din Convenția 108, datele cu caracter personal sunt definite ca „orice informație privind persoana fizică identificată sau identificabilă” [*Amann împotriva Elveției* (MC), 2000, pct. 65; *Haralambie împotriva României,* 2009, pct. 77].

6. Prin urmare, astfel de date nu includ numai elemente care pot conduce la stabilirea directă a identității civile a unei persoane („persoana vizată”), cum ar fi numele sau prenumele acesteia [*Guillot împotriva Franței*, 1996, pct. 21-22; *Mentzen împotriva Letoniei* (dec.), 2004; *Güzel Erdagöz împotriva*

Turciei, 2008, pct. 43; *Garnaga împotriva Ucrainei*, 2013, pct. 36; *Henry Kismoun împotriva Franței*, 2013, pct. 25; *Hájovský împotriva Slovaciei*, 2021, pct. 11-12 și 41], ci și orice element care ar putea conduce indirect la identificarea unei persoane, cum ar fi adresele IP (Internet Protocol) dinamice (*Benedik împotriva Sloveniei*, 2018, pct. 107-108; a se vedea, de asemenea, referitor la adresele IP mascate de un VPN, *Le Marrec împotriva Franței* (dec.), 2024, pct. 51-54).

7. Deși problema protecției datelor cu caracter personal pare să privească, la prima vedere, persoanele fizice, din perspectiva dreptului lor la respectarea „vieții private", garantat de art. 8, persoanele juridice pot, de asemenea, să îl invoce în fața Curții în cazul în care sunt afectate în mod direct de o măsură care aduce atingere dreptului lor la respectarea „corespondenței" sau a „domiciliului" lor. Aceasta este situația, de exemplu, a unei decizii prin care se dispunea ca o societate să transmită o copie a tuturor datelor de pe serverul informatic pe care îl partaja cu alte societăți ((*Bernh Larsen Holding AS și alții împotriva Norvegiei*, 2013, pct.106)) sau a interceptării de către Ministerul Apărării, pe baza unui mandat, a comunicațiilor către exterior ale unor organizații care activau în domeniul libertăților civile (*Liberty și alții împotriva Regatului Unit*, 2008, pct. 56-57). În schimb, în ceea ce privește măsurile care puneau în discuție protecția datelor cu caracter personal ale membrilor unei organizații religioase și respectarea „vieții private" a acestora, organizația nu era afectată în mod direct și nu era o „victimă", în sensul art. 34 din Convenție (*Avilkina și alții împotriva Rusiei*, 2013, pct. 59).

8. Datele cu caracter personal iau forme foarte diferite. Pot fi, de exemplu:

- informații cu privire la abonatul la un furnizor de servicii de Internet, asociate unei adrese IP dinamice specifice, atribuită la un anumit moment (*Benedik împotriva Sloveniei*, 2018, pct. 107-108), inclusiv adrese IP mascate de un VPN, dacă reclamantul poate fi identificat și localizat, [*Le Marrec împotriva Franței* (dec.), 2024, pct. 54];
- eșantioane de voce înregistrate pe un suport permanent și supuse unui proces de analiză destinat în mod direct identificării persoanei respective în lumina altor date cu caracter personal (*P.G. și J.H. împotriva Regatului Unit*, 2001, pct. 59);
- mostre de celule și profiluri ADN [S. și Marper împotriva Regatului Unit (MC), 2008, pct. 70-77] sau amprente digitale (*ibidem*, pct. 84) care, în pofida caracterului lor obiectiv și irefutabil, conțineau informații unice cu privire la persoana vizată și permiteau identificarea precisă într-un număr mare de circumstanțe (*ibidem*, pct. 85);
- informații referitoare la o anumită persoană, obținute fie din documente bancare, indiferent dacă aceste documente se referă sau nu la date sensibile sau la activități profesionale (*M.N. și alții împotriva Republicii San Marino*, 2015, pct. 51 și următoarele), fie din baza de date a Serviciului de informare privind contribuabili, inclusiv, în special, informații privind veniturile și activele nete ale unei persoane, precum și privind cauzele pendinte în fața autorităților fiscale [*Casarini împotriva Italiei* (dec.), 2024, pct. 56-57];
- date referitoare la profesia unei persoane identificate sau identificabile, colectate și stocate de poliție (*Khelili împotriva Elveției*, 2011, pct. 56);
- date privind utilizarea Internetului și a mesageriei instantanee (Yahoo) de către un angajat la locul său de muncă obținute prin instituirea unui sistem de supraveghere [*Bărbulescu împotriva României* (MC), 2017, pct. 18, 74-81];
- o copie a datelor electronice confiscate dintr-un cabinet de avocatură, chiar dacă acestea nu fuseseră decriptate, transcrise și atribuite în mod oficial persoanelor vizate (*Kırdök și alții împotriva Turciei*, 2019, pct. 36);
- date colectate în contextul supravegherii video nesecrete în amfiteatre universitare (*Antović și Mirković împotriva Muntenegrului*, 2017, pct. 44-45);
- informații privind veniturile și bunurile impozabile ale unui număr mare de persoane, în pofida faptului că publicul avea posibilitatea de a accesa aceste date în temeiul anumitor

reguli [*Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei* (MC), 2017, pct. 138];

- date referitoare la circumstanțele nașterii și abandonării unei persoane, care includeau informații necesare pentru descoperirea adevărului cu privire la un aspect important al identității personale [*Gaskin împotriva Regatului Unit*, 1989, pct. 39; *Mikulić împotriva Croației*, 2002, pct. 54-64 ; *Odièvre împotriva Franței* [MC], 2003, pct. 28-29; *Gauvin-Fournis și Silliau împotriva Franței*, 2023, pct. 106 și 112 ; *Cherrier împotriva Franței*, 2024, pct. 50];
- date care figurau într-un act de divorț prin acordul părților, inclusiv detalii privind distribuirea bunurilor matrimoniale, custodia și reședința copiilor minori, plata pensiei alimentare și o prezentare generală a bunurilor/veniturilor reclamantului (*Liebscher împotriva Austriei*, 2021, pct. 31 și 68).
- înregistrări video ale conversațiilor care au fost realizate de o persoană într-un cadru profesional utilizând o cameră ascunsă și care au fost utilizate în cele din urmă în procedurile penale împotriva reclamantului (*Sârbu împotriva României*, 2023 pct. 39-41).

9. În temeiul art. 2 din Convenția 108, o „prelucrare de date" include: „orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal, cum ar fi colectarea, stocarea, păstrarea, modificarea, recuperarea, dezvăluirea, punerea la dispoziție, ștergerea sau distrugerea sau efectuarea unor operațiuni logice și/sau aritmetice în legătură cu astfel de date". Odată cu dezvoltarea tehnologiilor, operațiunile care pot constitui „prelucrare de date" iau forme foarte diferite. Potrivit jurisprudenței Curții, constituie exemple tipice de astfel de prelucrări:

- colectarea de către poliție, de la un furnizor de servicii de internet, a informațiilor asociate adresei IP dinamice a unei persoane (*Benedik împotriva Sloveniei*, 2018, pct. 108-109);
- fapta de a colecta și stoca sistematic informații cu caracter public cu privire la o persoană, de exemplu, informații referitoare la activitatea sa politică [*Rotaru împotriva României* (MC), 2000, pct. 43-44; *Asociația „21 decembrie 1989" și alții împotriva României*, 2011, pct. 167-168; *Amann împotriva Elveției* (MC), 2000, pct. 65-67; *Catt împotriva Regatului Unit*, 2019, pct. 93];
- înregistrarea numelui unei persoane într-o bază de date judiciară internă a unui minister competent [*L.F. împotriva Franței* (dec.), 2024, pct. 30], într-un dosar judiciar național al autorilor infracțiunilor sexuale (*Gardel împotriva Franței*, 2009, pct. 58) sau într-o bază de date națională a tuturor procedurilor penale împotriva persoanelor fizice (*N.F. și alții împotriva Rusiei*, 2023, pct. 34 și 49), precum și colectarea și stocarea amprentelor digitale ale persoanelor suspectate de săvârșirea unor infracțiuni (*M.K. împotriva Franței*, 2013, pct. 29);
- înregistrarea în secret, într-o secție de poliție, pe un suport permanent, a vocilor persoanelor pentru a fi supuse unui proces de analiză destinat în mod direct identificării acestor persoane în lumina altor date (*P.G. și J.H. împotriva Regatului Unit*, 2001, pct. 59-60);
- fapta de a filma o persoană în camera de interogatoriu a poliției cu camere instalate din motive de securitate și perfect vizibile, înregistrarea secvenței în litigiu pe un suport permanent și introducerea acesteia într-un montaj în vederea unei utilizări ulterioare (*Perry împotriva Regatului Unit*, 2003, pct. 41);
- fapta de a colecta sistematic și de a păstra datele de monitorizare GPS care indicau locul în care se afla persoana vizată și deplasările sale în public (*Uzun împotriva Germaniei*, 2010, pct. 49-53);
- publicarea într-o revistă a unui articol ilustrat cu fotografii ale unor celebrități, realizate fără știrea acestora [*Von Hannover împotriva Germaniei (nr. 2)* (MC), 2012, pct. 95-99];

- înregistrarea și transmiterea către mass-media a unei filmări provenite de la o cameră de televiziune cu circuit închis care filma o persoană care încerca să se sinucidă într-un loc public (*Peck împotriva Regatului Unit*, 2003, pct. 59-63);
- fapta prin care organele de poliție stocau și păstrau date referitoare la presupusa profesie a unei persoane (*Khelili împotriva Elveției*, 2011, pct. 56);
- divulgarea de către un spital de psihiatrie, către jurnaliști, a unor informații confidențiale extrem de sensibile cu privire la viața privată a unei paciente (*Mockutė împotriva Lituaniei*, 2018, pct. 99);
- colectarea de către stat, în contextul luptei împotriva dopajului în sport, a locațiilor și a activităților zilnice detaliate, inclusiv la sfârșit de săptămână, ale unor sportivi de top [*Fédération nationale des associations et syndicats de sportifs (FNASS) și alții împotriva Franței*, 2018, pct. 155-159).
- practica scanării și înregistrării sistematice a corespondenței private a deținuților – atât a celei pe care doreau să o trimită, cât și a celei care le-a fost trimisă – în sistemul informatic al Rețelei Judiciare Naționale (*Nuh Uzun și alții împotriva Turciei*, 2022, pct. 80-82).
- utilizarea tehnologiei de recunoaștere facială cu scopul, pe de o parte, de a identifica reclamantul, care a participat singur la un eveniment fără declarație prealabilă, pe baza fotografiilor și a înregistrărilor video publicate pe un canal Telegram și, pe de altă parte, de a identifica și de a aresta reclamantul în timp ce acesta călătorea cu metroul (*Glukhin împotriva Rusiei*, 2023, pct. 73).

10. Astfel de măsuri sunt considerate aproape întotdeauna de Curte drept ingerințe, cu grade diferite de gravitate, în dreptul la respectarea vieții private, a domiciliului sau a corespondenței persoanelor vizate.

11. Cu toate acestea, nu orice operațiune efectuată cu privire la date cu caracter personal intră în mod necesar în domeniul de aplicare al art. 8 sau nu aduce automat atingere unuia dintre interesele pe care le protejează. Astfel, în cauza *Mehmedovic împotriva Elveției* (dec.), 2018 (pct. 18), Curtea a considerat că informațiile fragmentate, colectate întâmplător și lipsite de relevanță pentru anchetă, departe de a constitui o colectare sistematică sau permanentă, nu implicau o ingerință în dreptul la respectarea vieții private al persoanei vizate. În plus, în cauza *Cakicisoy și alții împotriva Ciprului* (dec.), 2014 (pct. 50-52), prelevarea de probe de sânge de la reclamanți, de către autorități, pentru a le extrage profilul ADN spre a fi utilizate în contextul unui program de exhumare care viza identificarea rămășițelor rudelor lor dispărute, sau distrugerea acestor probe atunci când nu mai erau supuse unor formulare de consimțământ valide, nu a fost considerată ca reprezentând o ingerință în dreptul reclamanților la respectarea vieții lor private.

12. Din jurisprudența Curții rezultă că operațiunile efectuate cu privire la datele cu caracter personal intră în domeniul de aplicare al art. 8 în cazul în care au fost colectate informații cu privire la o anumită persoană [*Amann împotriva Elveției*, (MC), 2000, pct. 66-67; *Rotaru împotriva României* (MC), 2000, pct. 43-44], în cazul în care datele în cauză au făcut obiectul unei înregistrări sistematice sau permanente (*Uzun împotriva Germaniei*, 2010, pct. 51), în cazul în care au fost supuse unui proces de analiză destinat în mod direct identificării unei persoane în lumina altor date cu caracter personal (*P.G. și J.H. împotriva Regatului Unit*, 2001, pct. 57) sau în cazul în care au fost făcute publice într-un mod sau într-o măsură care a depășit așteptările rezonabile ale persoanelor vizate (*Peck împotriva Regatului Unit,* 2003, pct. 58-59; *Perry împotriva Regatului Unit*, 2003, pct. 38). Contextul special în care au fost colectate și păstrate informațiile referitoare la o persoană, natura datelor înregistrate, modul în care acestea sunt utilizate și prelucrate și rezultatele care pot fi obținute din acestea joacă, de asemenea, un rol important [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 67].

13. Un element semnificativ, deși nu în mod necesar decisiv, este acela de a ști dacă o persoană are dreptul să aibă așteptări rezonabile privind protecția vieții sale private [*Perry împotriva Regatului Unit*, 2003, pct. 37; *Bărbulescu împotriva României* (MC), 2017, pct. 80;*Glukhin împotriva Rusiei*, 2023, pct.

66]. În ceea ce privește activitățile on-line, anonimatul informațiilor cu caracter personal on-line constituie un element important în această apreciere, iar faptul că un abonat al unui furnizor de servicii de Internet nu și-a ascuns adresa IP dinamică nu poate fi considerat determinant pentru a aprecia dacă așteptările sale în materie de protecție a vieții private erau rezonabile din punct de vedere obiectiv (*Benedik împotriva Sloveniei*, 2018, pct. 116). În caz contrar, la un loc de muncă, instrucțiunile angajatorului nu pot anula exercitarea vieții sociale private a angajaților, respectarea vieții lor private și, prin urmare, confidențialitatea comunicațiilor lor continuând să prevaleze, chiar dacă aceste comunicări pot fi limitate în măsura în care este necesar [*Bărbulescu împotriva României* (MC), 2017, pct. 80-81; a se vedea, de asemenea, pentru cadrul profesional, cauza *Sârbu împotriva României*, 2023, pct. 37-38; a se vedea, de asemenea, în contextul controlului de către un partid politic al corespondenței electronice a membrilor săi, *Tena Arregui împotriva Spaniei*, 2024, punctul 38).

Monitorizarea actelor sau gesturilor unei persoane într-un loc public prin intermediul unor mecanisme de monitorizare poate intra sub incidența articolului 8 dacă datele cu caracter personal astfel colectate sunt înregistrate în mod sistematic sau permanent (*Glukhin împotriva Rusiei*, 2023, pct. 66) sau dacă divulgarea acestor date, prin metodele sau amploarea sa, depășește ceea ce persoanele vizate ar fi putut aștepta în mod rezonabil (*Peck împotriva Regatului Unit*, 2003, pct. 62; *Perry împotriva Regatului Unit*, 2003, pct. 41-43). În ceea ce privește articolele de presă care ofereau informații privind arestarea unui actor de televiziune ilustrate cu fotografii, Curtea a considerat că „speranța legitimă" a unui actor de i se proteja efectiv viața sa privată era limitată de faptul că acesta se plasase el însuși într-un fel în centrul atenției, dezvăluind chiar el detalii din viața sa privată într-un anumit număr de interviuri [*Axel Springer AG împotriva Germaniei* (MC), 2012, pct. 101].

14. În ceea ce privește natura datelor colectate, anumite date cu caracter personal sau anumite metode de prelucrare a acestor date sunt mai problematice, întrucât dezvăluie informații mai sensibile cu privire la comportamentul, opiniile sau sentimentele persoanelor (*Uzun împotriva Germaniei*, 2010, pct. 52, în care au fost comparate datele colectate prin GPS cu datele colectate prin mijloace vizuale sau acustice de supraveghere). Stocarea sau divulgarea fără consimțământul persoanei vizate a unor date foarte intime sau sensibile referitoare, de exemplu, la starea de sănătate a persoanei intră în mod necesar în domeniul de aplicare a art. 8 (*Z împotriva Finlandei*, 1997, pct. 71; *Radu împotriva Republicii Moldova*, 2014, pct. 27; *Mockutė împotriva Lituaniei*, 2018, pct. 93-95). Păstrarea mostrelor de celule și a profilurilor ADN ale unei persoane trebuie considerată în sine ca fiind o atingere adusă dreptului acesteia la respectarea vieții private, având în vedere natura și cantitatea de informații cu caracter personal pe care le conțin, chiar dacă numai o mică parte a informațiilor sunt în realitate extrase sau utilizate de autorități și nu a fost cauzat niciun prejudiciu imediat [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 70-77].

15. Faptul că datele cu caracter personal se aflau deja în domeniul public sau că publicul avea posibilitatea de a le accesa nu le sustrage în mod necesar de la protecția oferită de articolul 8 [*Satakunnan Markkinapörssi oy și Satamedia oy împotriva Finlandei* (MC), 2017, pct. 134; *L.B. împotriva Ungariei* (MC), 2023; pct. 104]. Datele cu caracter public pot intra sub incidența „vieții private" a unei persoane atunci când au fost colectate și stocate în mod sistematic [*P.G. și J.H. împotriva Regatului Unit*, 2001, pct. 57; *Peck împotriva Regatului Unit*, 2003, pct. 58-59; *Perry împotriva Regatului Unit*, 2003, pct. 38), chiar și fără recurgerea la metode de supraveghere secrete [*Rotaru împotriva României* (MC), 2000, pct. 43-44; *Antović și Mirković împotriva Muntenegrului*, 2017, pct. 44-45]. Articolul 8 consacră dreptul la o formă de autodeterminare informațională, care permite persoanelor să invoce dreptul la viață privată în ceea ce privește date care, deși sunt neutre și aflate deja în domeniul public, sunt colectate, prelucrate și difuzate comunității, în asemenea forme sau în asemenea modalități astfel încât drepturile lor în temeiul articolului 8 pot fi puse în discuție [*Satakunnan Markkinapörssi oy și Satamedia oy împotriva Finlandei* (MC), 2017, pct. 137; *L.B. împotriva Ungariei* (MC), 2023; pct. 103].

16. În majoritatea cazurilor în care prelucrarea datelor cu caracter personal avea ca scop să permită autorităților să desfășoare o anchetă împotriva titularului acestora sau să colecteze probe în contextul unei proceduri judiciare în fața instanțelor naționale, Curtea a considerat că o astfel de prelucrare intra în domeniul de aplicare a art. 8 și dădea naștere unei ingerințe în viața privată a persoanelor vizate [*Perry împotriva Regatului Unit,* 2003, pct. 39-43; *Uzun împotriva Germaniei,* 2010, pct. 51-52; *Vukota-Bojić împotriva Elveției*, 2016, pct. 57-59; *López Ribalda și alții împotriva Spaniei* (MC), 2019, pct. 94; *Sârbu împotriva României*, 2023, pct. 38 și 41; a se vedea, a contrario, *Lupker și alții împotriva Țărilor de Jos*, 1992, care privea utilizarea de către poliție, în scopul identificării reclamanților, a unor fotografii care fuseseră predate voluntar autorităților sau care fuseseră făcute de poliție cu ocazia unor arestări anterioare; *Friedl împotriva Austriei*, 1994, pct. 50-51, care privea fotografiile făcute de autorități în timpul unei demonstrații în scopul unei eventuale anchetări ulterioare a demonstranților pentru încălcări ale codului rutier).

17. În sfârșit, pentru ca art. 8 să intre în discuție, rezultatele care pot rezulta din prelucrarea datelor cu caracter personal trebuie să atingă un anumit nivel de gravitate, astfel încât să se aducă atingere exercitării dreptului la respectarea vieții private (*M.L. și W.W. împotriva Germaniei*, 2018, pct. 88). În cauza *Vučina împotriva Croației* (dec.) 2019 (pct. 50), Curtea a respins ca fiind incompatibil *ratione materiae* un capăt de cerere întemeiat pe publicarea unei fotografii într-o revistă pentru femei cu un titlu greșit, care o prezenta pe reclamantă cu numele unei alte persoane. În opinia Curții, gradul scăzut de gravitate a acestei erori și inconvenientul foarte limitat care rezultase din această faptă nu erau suficient de grave pentru ca art. 8 să intre în joc.

2. Categorii de date specifice

18. Anumite informații foarte intime sau sensibile justifică în mod clar, în opinia Curții, o protecție sporită. Altor categorii de date trebuie, de asemenea, să li se acorde atenție, având în vedere dezvoltarea tehnologiilor care sporesc posibilitățile de acces la astfel de date și interconectarea acestora.

a. Categorii așa-zise „sensibile”

19. În temeiul art. 6 din Convenția 108, datele cu caracter personal care dezvăluie originea rasială, opiniile politice, convingerile religioase sau de altă natură, precum și datele cu caracter personal privind sănătatea sau viața sexuală a unei persoane sau eventualele condamnări penale nu pot fi prelucrate automat, cu excepția cazului în care dreptul intern prevede garanții adecvate. Informațiile care se încadrează în aceste categorii, pe care Curtea le califică drept „sensibile”, justifică, în opinia sa, o protecție sporită.

i. Date care dezvăluie originea rasială sau etnică

20. Identitatea etnică a unei persoane trebuie considerată un element important al vieții sale private [*S. și Marper împotriva Regatului Unit*, (MC), 2008, pct. 66; *Ciubotaru împotriva Moldova*, 2010, pct. 49]. Trebuie acordată importanță datelor care ar putea, având în vedere în special ritmul ridicat de inovare în domeniul geneticii și tehnologiei informației, să dezvăluie originea sau etnia unei persoane [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 71]. Probele de ADN și profilurile ADN conțin numeroase informații sensibile și oferă un mijloc de a descoperi relațiile genetice care pot exista între persoane și de a trage concluzii cu privire la originea etnică (*ibidem*, pct. 72-77; *Aycaguer împotriva Franței,* 2017, pct. 33). Într-o cauză care privea înscrierea originii etnice a unei persoane în registrele oficiale, Curtea, subliniind caracterul deosebit de sensibil al înregistrării unor astfel de date, a recunoscut existența unei obligații pozitive a statului de a garanta, în ceea ce privește datele respective, dreptul de a obține rectificarea înscrierii în cauză pe baza unor elemente obiective (*Ciubotaru împotriva Moldovei*, 2010, pct. 52-59).

ii. Date care dezvăluie opiniile politice, convingerile religioase sau de altă natură, inclusiv filozofice

21. Datele care dezvăluie opiniile politice sunt considerate o categorie „sensibilă” de date cu caracter personal și, în opinia Curții, este inacceptabil ca autoritățile naționale să neglijeze acest aspect și să prelucreze aceste date urmând doar normele generale la nivel intern, fără a ține seama de faptul că trebuie să beneficieze de un nivel sporit de protecție (*Catt împotriva Regatului Unit*, 2019, pct. 112). În cauza *Catt împotriva Regatului Unit*, care privea păstrarea într-o bază de date a poliției a datelor referitoare la un demonstrant pașnic, instanțele naționale făcuseră o simplă trimitere doar la legea privind protecția datelor, în general, în cursul examinării legalității ingerinței. Curtea a concluzionat o încălcare a art. 8, subliniind că natura sensibilă a datelor în cauză ar fi trebuit să constituie un element central al cauzei aflate pe rolul instanțelor interne, astfel cum s-a întâmplat în fața Curții (*ibidem*, pct. 112). Curtea a constatat, de asemenea, o încălcare a acestui articol în cauza *M. D. și alții împotriva Spaniei*, 2022, (pct. 63-64), care privea un raport întocmit de poliție cu privire la judecătorii și magistrații care profesau în Catalonia și care semnaseră un manifest în care declaraseră, din punct de vedere juridic, că erau în favoarea posibilității ca poporul catalan să își exercite „dreptul de a decide”, raport care dezvăluia în special opiniile politice ale unora dintre reclamanți. Curtea a clarificat, de asemenea, că datele cu caracter personal care dezvăluie o opinie politică necesită un nivel sporit de protecție [*Glukhin împotriva Rusiei*, 2023 (pct. 76 și 86), în cazul în care datele cu caracter personal referitoare la solicitant care au fost prelucrate conțineau informații privind participarea persoanei vizate la o demonstrație pașnică].

22. Dreptul la protecția datelor cu caracter personal care dezvăluie convingerile religioase sau alte convingeri ale unei persoane, inclusiv filozofice, a fost examinat de Curte în cauzele *Sinan Işık împotriva Turciei*, 2010 (pct. 37), și *Mockutė împotriva Lituaniei*, 2018 (pct. 117). În ceea ce privește menționarea religiei pe cărțile de identitate ale reclamanților, Curtea a subliniat importanța dreptului la protecția datelor referitoare la convingerile religioase, care se numără printre elementele cele mai importante ale identității credincioșilor și ale concepției lor de viață, protejate de art. 9 din Convenție (*Sinan Işık împotriva Turciei,* 2010, pct. 37).

iii. Date care dezvăluie apartenența sindicală

23. Datele cu caracter personal care dezvăluie apartenența sindicală a unei persoane sunt, de asemenea, date sensibile, care beneficiază de o protecție sporită. În cauza *Catt împotriva Regatului Unit*, 2019 (pct. 112), autoritățile polițienești colectaseră informații privind participarea reclamantului la diferite demonstrații organizate de o serie de sindicate, în special numele, prezența, data nașterii și adresa acestuia. În unele cazuri, aspectul său fusese de asemenea descris, însoțit de fotografii făcute în cursul manifestațiilor în cauză (*ibidem*, pct. 10). Curtea subliniază că faptul că o persoană participă la demonstrații pașnice beneficiază de o protecție specifică în temeiul art. 11 din Convenție, care conține, de asemenea, o protecție specială pentru sindicate (*ibidem*, pct. 123). În speță, deși colectarea de către poliție a datelor cu caracter personal referitoare la reclamant putea fi considerată o măsură justificată, păstrarea datelor sale nu răspundea, în opinia sa, unei nevoi imperioase, în lipsa unei norme care să stabilească termenul de păstrare a unor astfel de date (*ibidem*, pct. 117-119).

iv. Date genetice și biometrice

24. Curtea a soluționat mai multe cauze privind colectarea sau conservarea de:

- mostre de celule [*Van der Velden împotriva Țărilor de Jos* (dec.), 2005; *Schmidt împotriva Germaniei* (dec.), 2006; *S. și Marper împotriva Regatului Unit* (MC), 2008; *Canonne împotriva Franței* (dec.), 2015; *Caruana împotriva Maltei* (dec.), 2018; *Trajkovski și Chipovski împotriva Macedoniei de Nord*, 2020; *Boljević împotriva Serbiei*, 2020];
- profiluri ADN [*Van der Velden împotriva Țărilor de Jos* (dec.), 2005; *Schmidt împotriva Germaniei* (dec.), 2006; *S. și Marper împotriva Regatului Unit* (MC), 2008; *W. împotriva*

Țărilor de Jos (dec.), 2009; *Peruzzo și Martens împotriva Germaniei* (dec.), 2013; *Canonne împotriva Franței* (dec.), 2015; *Aycaguer împotriva Franței*, 2017; *Mifsud împotriva Maltei*, 2019; *Gaughran împotriva Regatului Unit*, 2020; *Trajkovski și Chipovski împotriva Macedoniei de Nord*, 2020; *Dragan Petrović împotriva Serbiei*, 2020];

- amprente digitale [*McVeigh, O'Neill și Evans împotriva Regatului Unit*, 1981; *Kinnunen împotriva Finlandei*, 1993; *S. și Marper împotriva Regatului Unit* (MC), 2008; *Dimitrov-Kazakov împotriva Bulgariei*, 2011; *M.K. împotriva Franței*, 2013; *Suprunenko împotriva Rusiei* (dec.), 2018; *Gaughran împotriva Regatului Unit*, 2020; *P.N. împotriva Germaniei*, 2020; *Willems împotriva Țărilor de Jos* (dec.), 2021];
- amprente palmare (*P.N. împotriva Germaniei*, 2020);
- eșantioane de voce (*P.G. și J.H. împotriva Regatului Unit*, 2001; *Allan împotriva Regatului Unit*, 2002; *Doerga împotriva Țărilor de Jos*, 2004; *Vetter împotriva Franței*, 2005; *Wisse împotriva Franței*, 2005).

25. Având în vedere ritmul ridicat cu care se succed inovațiile în domeniul geneticii și tehnologiilor informației, posibilitatea ca aspectele vieții private legate de informațiile genetice să facă în viitor obiectul unor noi atingeri prin noi mijloace, care nu pot fi prevăzute cu precizie în prezent, nu poate fi exclusă [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 71].

26. În cazul mostrelor de celule, păstrarea lor constituie în sine o atingere adusă dreptului la viață privată al persoanelor vizate, având în vedere natura și cantitatea informațiilor cu caracter personal pe care le conțin, în pofida faptului că doar o mică parte a acestor informații este efectiv extrasă sau utilizată de autorități în scopul creării de profiluri ADN și că nu este provocat niciun prejudiciu imediat într-un caz particular [*ibidem*, pct. 73; *Amann împotriva Elveției* (MC), 2000, pct. 69].

27. În ceea ce privește profilurile ADN, posibilitatea pe care o oferă de a trage concluzii cu privire la originea etnică face ca păstrarea lor să fie cu atât mai sensibilă și mai susceptibilă să aducă atingere dreptului la viață privată, impunând o protecție sporită [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 76]. Chiar dacă informațiile conținute în profilurile ADN pot fi considerate obiective și irefutabile, simplul fapt că profilurile ADN oferă un mijloc de descoperire a relațiilor genetice care pot exista între persoane este suficient în sine pentru a concluziona că păstrarea lor constituie o încălcare a dreptului la viață privată al acestor persoane, în pofida garanțiilor care le însoțesc și a probabilității producerii unui prejudiciu într-o anumit caz [*ibidem*, pct. 75; *Amann împotriva Elveției* (MC), 2000, pct. 69]. Faptul că informațiile nu erau inteligibile decât cu ajutorul calculatoarelor ca urmare a faptului că erau codificate și nu puteau fi interpretate decât de către un număr limitat de persoane nu schimba cu nimic lucrurile [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 74-75].

28. În ceea ce privește amprentele digitale, păstrarea lor fără consimțământul persoanei vizate nu poate fi considerată o măsură neutră sau banală ca urmare a faptului că acestea conțin în mod obiectiv informații unice cu privire la persoana vizată și permit identificarea precisă într-un număr mare de circumstanțe (*ibidem*, pct. 84). Chiar dacă păstrarea, într-o evidență a autorităților naționale, a amprentelor digitale ale unei persoane identificate sau identificabile are un impact mai redus asupra vieții sale private decât cea a mostrelor de celule și a profilurilor ADN (*ibidem*, pct. 69), poate da naștere unor preocupări importante în ceea ce privește viața privată, în pofida caracterului obiectiv și irefutabil al acestor date (*ibidem*, pct. 85, care a condus la o inversare a jurisprudenței în raport cu decizia Comisiei în cauza *Kinnunen împotriva Finlandei,* 1996). În cauza *Willems împotriva Țărilor de Jos* (dec.), 2021, capetele de cerere întemeiate pe obligația în temeiul legii pașapoartelor de a preleva amprentele digitale atunci când se solicita un pașaport, precum și păstrarea amprentelor digitale pe un cip electronic în urma încorporării în dreptul intern (fără nicio marjă de manevră din partea autorităților naționale) a Regulamentului UE privind securitatea și datele biometrice în documentele de călătorie au fost respinse ca vădit nefondate, având în vedere „prezumția unei protecții echivalente" în temeiul dreptului UE (*ibidem*, pct. 26-36).

29. Păstrarea mostrelor de celule și a profilurilor ADN are un impact mai mare asupra vieții private decât cea a amprentelor digitale [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 86]. Deși poate fi necesar să se facă distincție între amprentele digitale, pe de o parte, și mostre și profiluri, pe de altă parte, în ceea ce privește prelevarea, utilizarea și stocarea lor pentru a decide cu privire la justificarea ingerinței, nu este mai puțin adevărat că păstrarea amprentelor digitale constituie în sine o atingere adusă dreptului la respectarea vieții private.

30. În anumite circumstanțe, în special în contextul procedurilor care pun în discuție paternitatea unei persoane, autoritățile pot constrânge o persoană să furnizeze o probă biologică, cu condiția ca dreptul la apărare să fie respectat și să se asigure un echilibru just între interesele aflate în joc (*Mifsud împotriva Maltei*, 2019, pct. 77-78). Art. 8 nu interzice ca atare recurgerea la o intervenție medicală împotriva voinței unui suspect sau împotriva voinței unui martor în vederea obținerii de probe, întrucât astfel de metode, inclusiv în materie civilă, nu sunt, în sine, contrare statului de drept și justiției naturale (*ibidem*, pct. 71). Cu toate acestea, un sistem care nu prevede mijloace de constrângere a unui presupus tată să efectueze un test ADN nu este în sine incompatibil cu obligațiile care decurg din art. 8, în special dacă sistemul în cauză oferă alte mijloace prin care o autoritate independentă se poate pronunța rapid cu privire la acțiunea în stabilirea paternității (*Mikulić împotriva Croației*, 2002, pct. 55, 64).

v. Date privind sănătatea, viața sexuală sau orientarea sexuală

31. Informațiile privind sănătatea unei persoane reprezintă un element important al vieții sale private (*Yvonne Chave, născută Jullien, împotriva Franței,* 1991, pct. 75; *L.L. împotriva Franței*, 2006; *Radu împotriva Moldovei*, 2014; *L.H. împotriva Letoniei*, 2014, pct. 56; *Konovalova împotriva Rusiei*, 2014, pct. 27, 41; *Y.Y. împotriva Rusiei*, 2016, pct. 38; *Surikov împotriva Ucrainei*, 2017; *Frâncu împotriva României*, 2020, pct. 52). Respectarea confidențialității acestor informații este esențială nu numai pentru protejarea vieții private a pacienților, ci și pentru menținerea încrederii acestora în corpul medical și în serviciile de sănătate, în general. Aceste considerații sunt deosebit de relevante în ceea ce privește protecția confidențialității informațiilor referitoare la seropozitivitatea unei persoane [*Z împotriva Finlandei*, 1997, pct. 96; *Kiyutin împotriva Rusiei*, 2011, pct. 64; *Armonienė împotriva Lituaniei*, 2008, pct. 40; *Biriuk împotriva Lituaniei*, 2008, pct. 39; *I. împotriva Finlandei*, 2008, pct. 38; *C.C. împotriva Spaniei*, 2009, pct. 33; *Y. împotriva Turciei* (dec.), 2015, pct. 65; *P.T. împotriva Republicii Moldova*, 2020, pct. 5-6, 26; *Y.G. împotriva Rusiei*, 2022, pct. 45]. Divulgarea unor astfel de informații poate avea consecințe devastatoare asupra vieții private și de familie a persoanei vizate și asupra situației sale sociale și profesionale, expunând-o oprobriului și riscului de excluziune [*Z împotriva Finlandei*, 1997, pct. 96; *C.C. împotriva Spaniei*, 2009, pct. 33; *P. și S. împotriva Poloniei*, 2012, pct. 128; *Avilkina și alții împotriva Rusiei,* 2013, pct. 45; *Y. împotriva Turciei* (dec.), 2015, pct. 65; *Y.G. împotriva Rusiei*, 2022, pct. 45].

32. Interesul de a proteja confidențialitatea unor astfel de informații va avea așadar o pondere considerabilă atunci când se stabilește dacă ingerința era proporțională cu obiectivul legitim urmărit, ținând seama de faptul că o astfel de ingerință nu poate fi reconciliată cu art. 8 decât în cazul în care urmărește să protejeze un aspect primordial de interes public (*Z împotriva Finlandei*, 1997, pct. 96). Luând în considerare caracterul extrem de intim și sensibil al informațiilor referitoare la seropozitivitate, orice măsură luată de un stat pentru a constrânge comunicarea sau divulgarea acestora, fără consimțământul persoanei vizate, impune o examinare cât mai riguroasă de către Curte (*ibidem*, pct. 96).

33. Astfel, Curtea a constatat o încălcare a art. 8, de exemplu, în cauzele *Z împotriva Finlandei*, 1997 (pct. 113-114), pe motiv de publicare a identității și seropozitivității unei femei într-o hotărâre pronunțată în contextul procedurii penale intentate împotriva soțului său, transmisă presei; *L.L. împotriva Franței*, 2006 (pct. 32-48), pe motiv de reproducere, într-o hotărâre de divorț, a unui extras dintr-un document medical personal; *I. împotriva Finlandei*, 2008 pct. 35-49), pe motiv de protecție insuficientă împotriva accesului neautorizat la dosarul medical al unei asistente medicale seropozitive;

C.C. împotriva Spaniei, 2009 (pct. 26-41), pe motiv de publicare a identității reclamantului în hotărârea pronunțată cu privire la seropozitivitatea sa; *P. și S. împotriva Poloniei*, 2012 (pct. 128-137), pe motiv de divulgare de informații de către un spital public cu privire la o minoră gravidă care voia să avorteze în urma unui viol; *Konovalova împotriva Rusiei*, 2014 (pct. 39-50), pe motiv că pacienta a născut în prezența studenților la medicină fără consimțământul acesteia; *P.T. împotriva Republicii Moldova*, 2020 (pct. 24-33), pentru prezența inutilă a unor date medicale sensibile pe un certificat care avea scopul de a fi prezentat în diferite situații; *Frâncu împotriva României*, 2020 (pct. 52), pentru refuzul examinării, cu ușile închise, într-un caz de corupție care viza un primar, a unei cereri de eliberare din motive de sănătate, *Y.G. împotriva Rusiei*, 2022, (pct. 46-53), cauză în care reclamantul a pretins că o bază de date care deținea, în special, datele sale de sănătate fusese scoasă la vânzare pe piață; și *A.P. împotriva Armeniei*, 2024, pct. 150-159, cauză în care reclamanta s-a plâns că numele său complet, adresa și textul integral al hotărârilor judecătorești de respingere a cererii sale de despăgubire pentru abuz sexual fuseseră publicate în baza de date judiciare oficială online accesibilă publicului, deși aceasta solicitase în mod expres ca informațiile respective să nu fie publicate.

34. Informațiile despre sănătatea mintală a unei persoane sunt foarte sensibile (*Mockutė împotriva Lituaniei,* 2018, pct. 94, care privea divulgarea datelor despre starea de sănătate mintală a unui pacient de către un spital de psihiatrie; *Malanicheva împotriva Rusiei* (dec.), 2016, pct. 13, 15-18, care privea stocarea în dosarul unui spital a datelor referitoare la internarea nevoluntară a reclamanților), precum și a datelor care pot conduce la identificarea sexuală și la orientarea sexuală (*Dudgeon împotriva Regatului Unit,* 1981, pct. 41; *J.L. împotriva Italiei*, 2021, pct. 136; și *Drelon împotriva Franței*, 2022, pct. 79) și viața sexuală a unei persoane, precum datele referitoare la un avort transmise de către o autoritate publică alteia fără consimțământul persoanei vizate (*M.S. împotriva Suediei*, 1997, pct. 41-42). Legislația națională trebuie să prevadă garanții adecvate pentru a împiedica orice comunicare sau divulgare a unor astfel de date care nu respectă garanțiile prevăzute la art. 8 (*Z împotriva Finlandei*, 1997, pct. 95).

vi. Date privind condamnări penale și infracțiuni

35. Datele privind infracțiuni, proceduri penale, condamnări sau măsuri de siguranță conexe constituie o categorie de date care pot beneficia de o protecție sporită în temeiul art. 6 din Convenția 108 (*M.M. împotriva Regatului Unit*, 2012, pct. 188; *Margari împotriva Greciei*, 2023, pct. 59). Prin urmare, este esențial ca, atunci când sunt publicate date sensibile în contextul unor proceduri penale în curs sau al unor anchete privind infracțiuni penale, datele să reflecte cu exactitate situația și faptele pentru care este urmărit penal inculpatul, ținând seama și de necesitatea respectării prezumției de nevinovăție (*ibidem*). Prelucrarea datelor cu caracter personal ale unei persoane care a făcut obiectul unei proceduri finalizate fără începerea urmăririi penale (*Brunet împotriva Franței,* 2014, pct. 38-40; *N.F. și alții împotriva Rusiei*, 2023, pct. 38), sancționată printr-un avertisment (*M.M. împotriva Regatului Unit*, 2012, pct. 188-190), condamnată penal [*Gardel împotriva Franței*, 2009, pct. 58; *Peruzzo și Martens împotriva Germaniei* (dec.), 2013, pct. 44; *Trajkovski și Chipovski împotriva Macedoniei de Nord*, 2020, pct. 46; *N.F. și alții împotriva Rusiei*, 2023, pct. 38] sau care face obiectul unei măsuri de siguranță conexe precum arestul preventiv [*Suprunenko împotriva Rusiei* (dec.) (comitet), 2018, pct. 61] implică o ingerință în dreptul la respectarea vieții private al persoanei vizate.

36. Potrivit Curții, deși datele din cazierul judiciar sunt, într-un anumit sens, informații publice, stocarea lor sistematică în dosare centrale înseamnă că pot fi divulgate cu mult timp după eveniment, atunci când oricine altcineva, cu excepția persoanei vizate, este probabil să fi uitat incidentul. În timp, condamnarea sau avertismentul devine parte integrantă a vieții private a unei persoane, care trebuie respectată (*M.M. împotriva Regatului Unit*, 2012, pct. 188). Acest fapt este cu atât mai mult valabil atunci când astfel de date privesc trecutul îndepărtat al unei persoane (*B.B. împotriva Franței*, 2009, pct. 57; *Catt împotriva Regatului Unit*, 2019, pct. 93; *M.L. și W.W. împotriva Germaniei*, 2018, pct. 98-100).

37. O măsură care implică păstrarea, în evidențele poliției, a datelor de identificare, a amprentelor digitale și a fotografiilor cu identitatea unei persoane poate avea consecințe grave pentru aceasta, ceea ce îi poate îngreuna viața de zi cu zi (*Dimitrov-Kazakov împotriva Bulgariei*, 2011, pct. 8, 10, 13, 30). Într-o cauză care privea înscrierea unei persoane ca „autor al infracțiunii" în evidențele poliției, după ce fusese interogată cu privire la un viol, și menținerea acestei mențiuni fără nicio punere sub acuzare ulterioară, Curtea a concluzionat că a fost încălcat art. 8 după ce a constatat că persoana vizată făcuse obiectul, tocmai ca urmare a înscrierii în cauză, mai multor verificări ale poliției cu privire la plângerile de viol sau de dispariții ale unor tinere fete (*ibidem*, pct. 8, 10, 13, 30).

38. În plus, Curtea a statuat că păstrarea continuă a datelor referitoare la o sancțiune administrativă alternativă (o formă de soluționare fără condamnare a unei cauze penale) impusă unui reclamant a reprezentat o ingerință în exercitarea de către persoana vizată a dreptului său la respectarea vieții sale private garantat de articolul 8 din Convenție (*Borislav Tonchev împotriva Bulgariei*, 2024, pct. 125). Potrivit jurisprudenței Curții, simpla păstrare de către o autoritate publică a unor astfel de date constituie o ingerință, indiferent dacă datele sunt sau nu sunt utilizate ulterior. Curtea a constatat o încălcare a articolului 8 din Convenție pentru motivul că legislația bulgară relevantă era suficient de vagă pentru a confunda autoritățile naționale responsabile cu interpretarea și cele cu aplicarea sa și că, prin urmare, legislația nu era suficient de previzibilă. În plus, discrepanțele constatate s-au extins la aplicarea legislației UE privind protecția datelor (principiul limitării păstrării; *ibidem*, pct. 137).

b. Alte categorii de date

39. Pe lângă categoriile de informații așa-zise „sensibile", și alte categorii de date cu caracter personal trebuie să facă obiectul atenției, în special având în vedere tehnicile din ce în ce mai sofisticate de supraveghere și capacitatea tehnologiilor informației și comunicațiilor de a face zilnic viața mai dificilă persoanelor vizate.

i. Date privind munca prestată

40. Stocarea datelor referitoare la o persoană fizică identificată sau identificabilă referitoare la profesia sa și păstrarea acestora constituie o ingerință în dreptul la respectarea vieții private a persoanei vizate, protejat de art. 8 (*Khelili împotriva Elveției*, 2011, pct. 56; *Sõro împotriva Estoniei*, 2015, pct. 49, 56; *Florindo de Almeida Vasconcelos Gramaxo împotriva Portugaliei*, 2022, pct. 95-96). Întrucât informațiile colectate de autorități și păstrarea în dosarele acestora fac în prezent obiectul unei prelucrări automate care facilitează în mare măsură accesul la astfel de informații și difuzarea acestora, astfel de măsuri pot avea consecințe grave, care pot afecta reputația persoanelor sau pot îngreuna viața de zi cu zi a acestora. Curtea a constatat o încălcare a art. 8 în cauzele *Khelili împotriva Elveției,* 2011 (pct. 64), în care reclamanta fusese înregistrată ca „prostituată" de poliție, mențiune corectată ulterior și înlocuită cu cea de „croitoreasă" în fișierele electronice, și *Sõro împotriva Estoniei*, 2015 (pct. 63), în care reclamantul fusese obligat să își dea demisia în urma divulgării datelor privind activitatea sa de șofer în cadrul fostelor servicii de securitate. În cauza *Florindo de Almeida Vasconcelos Gramaxo împotriva Portugaliei*, din 2022 (pct. 95-96), în care angajatorul reclamantului instalase un sistem GPS în vehiculul utilizat de persoana vizată pentru a monitoriza distanțele pe care aceasta le-a parcurs în cadrul activității sale profesionale și, eventual, în timpul deplasărilor sale private, Curtea a statuat că informațiile astfel colectate constituiau date cu caracter personal. Aceasta a arătat de asemenea că angajaților nu li se permitea să dezactiveze sistemul GPS, astfel încât acesta rămânea activ 24 de ore pe zi, 7 zile pe săptămână, și că monitorizarea era, așadar, permanentă și sistematică, aducând astfel în mod incontestabil atingere vieții private a reclamantului[1].

[1]A se vedea, de asemenea, secțiunea intitulată „Date de localizare GPS" de mai jos.

ii. Date financiare

41. Informațiile obținute plecând de la documentele bancare ale unei persoane constituie date cu caracter personal, atunci când este vorba fie despre informații sensibile de natură privată, fie despre informații privind activitățile profesionale ale persoanei vizate *(M.N. și alții împotriva San Marino,* 2015, pct. 51; *G.S.B. împotriva Elveției*, 2015, pct. 51). Fapta prin care autoritățile copiază și păstrează informații bancare constituie o ingerință în exercitarea de către persoana vizată a dreptului său la respectarea vieții private și a corespondenței (*M.N. și alții împotriva San Marino*, 2015, pct. 55).

42. Curtea a examinat problema colectării, prelucrării și divulgării datelor financiare în contextul următor: o anchetă penală (*M.N. și alții împotriva Republicii San Marino*, 2015, pct. 7-9, pct. 53-55); publicarea pe scară largă de către presă a unor date financiare pentru a permite o dezbatere cu privire la chestiuni de interes general [*Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei* (MC), 2017, pct. 172-173]; obligația impusă unui avocat de a divulga date care fac obiectul secretului profesional prin raportarea suspiciunilor sale referitoare la activitățile ilicite de spălare a banilor ale clienților săi (*Michaud împotriva Franței,* 2012, pct. 91-92); transmiterea datelor financiare către autoritățile unui alt stat care nu este parte la Convenție (*G.S.B. împotriva Elveției*, 2015, pct. 50); respingerea unei acțiuni privind divulgarea de informații referitoare la numărul de identificare fiscală al reclamantei și declarația fiscală într-un reportaj televizat privind o cauză penală împotriva soțului său (*Samoylova împotriva Rusiei*, 2021, pct. 83 și 90-93); consultarea ilegală și utilizarea abuzivă a datelor stocate în baza de date a Serviciului de informare privind contribuabilii [*Casarini împotriva Italiei* (dec.), 2024, pct. 56-57].

43. Existența unui interes general în ceea ce privește disponibilitatea unor cantități mari de date fiscale și autorizarea de a colecta astfel de date nu înseamnă în mod necesar sau automat că există și un interes general de a difuza în masă astfel de date brute, ca atare, fără niciun aport analitic [*Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei* (MC), 2017, pct. 172-178, 198].

44. Chiar dacă, în materie fiscală, marja de apreciere a statului este mai largă în ceea ce privește protecția datelor pur financiare care nu conțin date intime sau strâns legate de identitatea persoanei vizate (*G.S.B. împotriva Elveției*, 2015, pct. 93) considerațiile legate de viața privată intră în discuție situațiile în care datele de natură fiscale au fost colectate de la o anumită persoană, sau atunci când au fost făcute publice într-un mod sau într-o măsură care depășește așteptările rezonabile ale persoanelor vizate [*M.N. și alții împotriva San Marino*, 2015, pct. 52-53; *Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei* (MC), 2017, pct. 136].

iii. Date de transfer

45. Datele de transfer sunt informații colectate de la operatorii de telefonie care nu au legătură cu conținutul comunicațiilor și care includ data, ora, durata fiecărei comunicații, precum și destinatarul sau destinatarii comunicației (*Malone împotriva Regatului Unit,* 1984, pct. 83-84; *Copland împotriva Regatului Unit*, 2007, pct. 43). Procesul de „contorizare" (*metering*) a apelurilor de pe telefonul unei persoane în contextul unei anchete penale prin utilizarea unui mecanism (un contor combinat cu o imprimantă) care înregistrează numerele formate de pe un anumit telefon, precum și ora și durata fiecărui apel, fără a supraveghea și fără a intercepta comunicațiile, constituie o ingerință în viața privată a persoanei vizate (*Malone împotriva Regatului Unit*, 1984, pct. 83-84). Exploatarea elementelor astfel colectate, în special a numerelor formate, poate ridica o problemă în temeiul art. 8, întrucât aceste elemente fac parte integrantă din comunicațiile telefonice (*Malone împotriva Regatului Unit*, 1984, pct. 84; *Copland împotriva Regatului Unit*, 2007, pct. 43). În opinia Curții, divulgarea lor către poliție fără consimțământul abonatului poate aduce atingere unui drept garantat de art. 8 (*Malone împotriva Regatului Unit*, 1984, pct. 84).

46. „Contorizarea" comunicațiilor, care, în sine, nu aduce atingere art. 8 dacă este efectuată, de exemplu, de o companie de telefonie în scopul facturării, se distinge prin însăși natura sa de interceptarea comunicațiilor (*Malone împotriva Regatului Unit*, 1984, pct. 83-84; *P.G. și J.H. împotriva*

Regatului Unit, 2001, pct. 42). O hotărâre judecătorească adresată unui operator de telefonie pentru a obține apelurile primite și efectuate prin intermediul a diferite telefoane mobile ale unei persoane și de a realiza o „localizare prin antenele de telefonie mobilă" a impulsurilor de pe telefoanele sale mobile care să permită urmărirea *a posteriori* a mișcărilor acestuia nu era în mod necesar incompatibilă cu art. 8, în măsura în care era autorizată printr-o lege care prevedea garanții suficiente împotriva arbitrariului (*Ben Faiza împotriva Franței*, 2018, pct. 56, 59, 69). Curtea a concluzionat lipsa unei încălcări a art. 8 într-o cauză în care astfel de dispoziții erau supuse autorizării prealabile de către un magistrat al parchetului, sub sancțiunea nulității, puteau face obiectul unui control jurisdicțional, iar probele obținute puteau fi excluse în caz de nelegalitate (*ibidem*, pct. 79, 73).

47. Datele cu caracter personal ale utilizatorilor de cartele SIM preplătite, precum numele, adresele, numerele de telefon ale clienților colectate de operatorii de telefonie mobilă, nu trebuie considerate „nesemnificative" (*Breyer împotriva Germaniei*, 2020, pct. 92-95). Simpla păstrare, de către operatorii de comunicații, a unor astfel de date ale clienților constituie o ingerință în dreptul la respectarea vieții private a persoanei vizate, indiferent de eventuala lor utilizare ulterioară (*ibidem*, pct. 92). O astfel de ingerință are totuși un caracter relativ limitat (*ibidem*, pct. 95) și statele membre ale Consiliului Europei se bucură de o anumită marjă de apreciere în materie, având în vedere lipsa unui consens european (*ibidem*, pct. 90). Existența unui control din partea unei autorități independente, cu competența de a examina, atunci când percepe motive pentru a o face, dacă este acceptabil să transmită datele în cauză autorităților care le solicită, precum și disponibilitatea unei căi de atac în fața unei autorități administrative deschisă oricărei persoane care consideră că a făcut obiectul unei proceduri de accesare a datelor sau al unei cereri de informații, are drept consecință faptul că lipsa unei notificări privind procedura de accesare a datelor nu este incompatibilă cu art. 8 (*ibidem*, pct. 103-107).

48. În cazul unei conexiuni la Internet, datele de transfer sunt date care permit identificarea utilizatorului, ca de exemplu adresa IP, adresa de e-mail, destinatarul sau destinatarii comunicației, datele referitoare la echipamentul terminal utilizat, serviciile suplimentare solicitate sau utilizate și furnizorii acestora (*Benedik împotriva Sloveniei*, 2018, pct. 96). În opinia Curții, informațiile privind abonații asociate unei adrese IP dinamice specifice atribuite la un moment dat sunt date cu caracter personal. Acestea nu sunt accesibile publicului și nu pot fi așadar comparate cu informațiile care figurează într-o listă de abonați telefonici tradițională sau într-o bază de date publică care conține numerele de înmatriculare ale vehiculelor (*ibidem*, pct. 108).

49. Obținerea datelor asociate comunicațiilor în contextul interceptării în masă nu este în mod necesar mai puțin intruzivă decât obținerea conținutului comunicațiilor [*Centrum för rättvisa împotriva Suediei* (MC), 2021, 277, și *Big Brother Watch și alții împotriva Regatului Unit* (MC), 2021, pct. 363]. Interceptarea și păstrarea datelor de comunicații aferente, precum și căutările efectuate asupra acestora trebuie, așadar, analizate în lumina acelorași garanții ca cele aplicabile conținutului comunicațiilor. Cu toate acestea, având în vedere natura diferită a datelor de comunicații aferente și modurile diferite în care sunt acestea utilizate de serviciile de informații, nu este necesar ca dispozițiile legale care reglementează prelucrarea datelor de comunicații aferente să fie identice sub toate aspectele cu cele care reglementează prelucrarea conținutului comunicațiilor [*Centrum för rättvisa împotriva Suediei* (MC), 2021, pct. 278; și *Big Brother Watch și alții împotriva Regatului Unit* (MC), 2021, pct. 364].

50. Preponderența acordată cerinței de confidențialitate a datelor de transfer se poate dovedi, în anumite circumstanțe, contrară art. 8 dacă este de natură să afecteze eficacitatea unei anchete penale care să permită identificarea și sancționarea autorului unei infracțiuni săvârșite prin intermediul Internetului (*K.U. împotriva Finlandei,* 2008, pct. 49). Garantarea respectării intimității utilizatorilor serviciilor de telecomunicații și de Internet trebuie uneori anulată atunci când există alte cerințe legitime, precum apărarea ordinii și prevenirea infracțiunilor sau protejarea drepturilor și libertăților altora (*ibidem*, pct. 49).

iv. Eșantioane de voce

51. Operațiunea de „instalare de microfoane” implică interceptarea conversațiilor unei persoane prin intermediul unui dispozitiv de supraveghere audio ascuns într-o proprietate privată [*Vetter împotriva Franței*, 2005, pct. 10, 20) sau publică (*P.G. și J.H. împotriva Regatului Unit*, 2001, pct. 38, 63; *Allan împotriva Regatului Unit*, 2002, pct. 35; *Doerga împotriva Țărilor de Jos*, 2004, pct. 43; *Wisse împotriva Franței*, 2005, pct. 29).

52. Înregistrarea secretă a vocii unei persoane pe un suport permanent în scopul unui proces de analiză destinat în mod direct identificării acestei persoane în lumina altor date cu caracter personal constituie o prelucrare de date cu caracter personal care relevă o ingerință în dreptul persoanei vizate la respectarea vieții sale private (*P.G. și J.H. împotriva Regatului Unit*, 2001, pct. 59-60). În lipsa unui cadru legislativ care să reglementeze utilizarea dispozitivelor de ascultare ascunse de poliție în propriile sedii sau într-un loc privat, Curtea a constatat o încălcare a art. 8 (*ibidem*, pct. 38, 63).

53. Ascultarea conversațiilor prin instalarea de microfoane reprezintă, la fel precum interceptarea conversațiilor telefonice, o atingere gravă adusă dreptului la respectarea vieții private al persoanei vizate (*Vetter împotriva Franței*, 2005, pct. 26). Prin urmare, aceasta trebuie să se întemeieze pe o „lege” specifică: de asemenea, în acest domeniu pare a fi indispensabilă existența unor norme clare și detaliate, cu atât mai mult cu cât procesele tehnice care pot fi utilizate nu încetează să se perfecționeze (*ibidem*, pct. 26). Potrivit Curții, „legea” trebuie să ofere justițiabililor „garanții adecvate” împotriva abuzurilor de aceeași natură precum în cazul ascultării convorbirilor telefonice (*ibidem*, pct. 26). Astfel, trebuie definite în special categoriile de persoane care pot face obiectul unei astfel de măsuri, precum și natura infracțiunilor care pot conduce la aceasta; instanța trebuie să fie obligată să stabilească o limită a duratei de executare a măsurii; de asemenea, trebuie precizate condițiile de întocmire a proceselor-verbale de sinteză, care consemnează conversațiile „ascultate”, precauțiile care trebuie luate pentru a comunica în mod intact și complet înregistrările realizate, în vederea unui control eventual din partea instanței și a avocatului apărării, precum și circumstanțele în care trebuie efectuată sau distrugerea respectivelor înregistrări, în special după pronunțarea neînceperii urmăririi penale sau a achitării (*ibidem*, pct. 26, care face trimitere la criteriile în materie de interceptare a comunicațiilor indicate în hotărârea *Kruslin împotriva Franței*, 1990, pct. 35).

54. În cazul în care înregistrarea vocii unei persoane a fost efectuată fără a se respecta gradul minim de protecție impus de statul de drept într-o societate democratică, conduce la o încălcare a art. 8 (*Wisse împotriva Franței*, 2005, pct. 34, care privea înregistrarea și utilizarea ulterioară a convorbirilor purtate la vorbitorul unui penitenciar de către reclamanți cu rudele lor; *Allan împotriva Regatului Unit*, 2002, pct. 36, privind instalarea unui dispozitiv de supraveghere audio plasat în celula unui deținut aflat în penitenciar).

v. Date de localizare GPS

55. Datele colectate prin GPS pot indica locul în care se afla o persoană și deplasările acesteia în public și constituie date cu caracter personal (*Uzun împotriva Germaniei*, 2010, pct. 51-52; *Florindo de Almeida Vasconcelos Gramaxo împotriva Portugaliei*, 2022, pct. 95). Prelucrarea și utilizarea unor astfel de date constituie o ingerință în exercitarea dreptului la respectarea vieții private a persoanei vizate (*Uzun împotriva Germaniei*, 2010, pct. 51-52; *Florindo de Almeida Vasconcelos Gramaxo împotriva Portugaliei*, 2022, pct. 96). Trebuie să se facă distincție între supravegherea prin GPS și alte metode de supraveghere prin mijloace vizuale sau acustice, care, ca regulă generală, sunt mai susceptibile să aducă atingere dreptului la respectarea vieții private al unei persoane, întrucât relevă mai multe informații cu privire la comportamentul, opiniile sau sentimentele persoanei care face obiectul supravegherii (*Uzun împotriva Germaniei*, 2010, pct. 52).

56. Întrucât este vorba despre o ingerință mai puțin importantă în viața privată a persoanei vizate în comparație cu interceptarea conversațiilor telefonice, criteriile relativ stricte stabilite și urmate în contextul specific al supravegherii telecomunicațiilor nu sunt aplicabile ca atare supravegherii prin GPS

a deplasărilor unei persoane (*ibidem*, pct. 66). Pentru a examina dacă, într-o cauză dată, o persoană afectată de o măsură de geolocalizare prin GPS a beneficiat de o protecție adecvată împotriva ingerințelor arbitrare în exercitarea drepturilor sale protejate de art. 8, Curtea trebuie să urmeze principii mai generale atunci când examinează chestiunea previzibilității legii (*ibidem*, pct. 66 și trimiterile citate la pct. 63). Emiterea unui mandat de către un organ independent nu este întotdeauna necesară, iar controlul judiciar ulterior al supravegherii unei persoane prin GPS este de natură să ofere o protecție suficientă împotriva arbitrariului (*ibidem*, pct. 72).

57. Instalarea unui dispozitiv de geolocalizare pe vehiculul unei persoane în contextul unei anchete penale privind traficul de droguri a fost considerată de Curte ca fiind contrară art. 8 într-o cauză în care dreptul intern, scris și nescris, nu indica suficient de clar amploarea și modalitățile de exercitare a puterii de apreciere a autorităților în materie (*Ben Faiza împotriva Franței*, 2018, pct. 58-61).

58. Pe de altă parte, într-o altă cauză în care Curtea a trebuit să examineze problema datelor cu caracter personal ale unei persoane colectate prin geolocalizare și utilizarea datelor astfel obținute în contextul procedurii penale îndreptate împotriva sa, Curtea a concluzionat că nu a fost încălcat art. 8 (*Uzun împotriva Germaniei*, 2010, pct. 60-74). Existența unui control judiciar ulterior al supravegherii prin GPS și posibilitatea de a exclude probele obținute prin intermediul unei supravegheri ilegale au constituit garanții importante, de natură să descurajeze autoritățile de anchetă să colecteze probe prin mijloace ilegale (*ibidem*, pct. 72). Faptul că dreptul intern subordona autorizarea măsurii de supraveghere în litigiu unor condiții foarte stricte, că supravegherea prin GPS fusese dispusă numai după ce alte măsuri de investigare, mai puțin intruzive la adresa vieții private, se dovediseră ineficiente, și că această măsură fusese pusă în aplicare pentru o perioadă relativ scurtă, au fost, de asemenea, luate în considerare în contextul examinării proporționalității ingerinței (*ibidem*, pct. 77-81).

59. În cauza *Florindo de Almeida Vasconcelos Gramaxo împotriva Portugaliei*,, 2022 (pct. 95-96 și 105-125), angajatorul reclamantului instalase un sistem GPS în vehiculul utilizat de persoana vizată pentru a monitoriza distanțele pe care aceasta le-a parcurs în cadrul activității sale profesionale și, eventual, în timpul deplasărilor sale private. Curtea a observat că sistemul în cauză permitea monitorizarea circulației unui vehicul în timp real: astfel, era posibil să se localizeze din punct de vedere geografic persoana sau persoanele care ar fi trebuit să îl utilizeze la un moment dat sau în mod continuu. Curtea a considerat că aceste informații constituiau date cu caracter personal. Aceasta a arătat de asemenea că angajaților nu li se permitea să dezactiveze sistemul GPS, astfel încât acesta rămânea activ 24 de ore pe zi, 7 zile pe săptămână, și că monitorizarea era, așadar, permanentă și sistematică, aducând astfel în mod incontestabil atingere vieții private a persoanei vizate. În același timp, Curtea a considerat că instanțele naționale au evaluat în mod corect interesele concurente în cauză, și anume, pe de o parte, dreptul reclamantului la respectarea vieții sale private și, pe de altă parte, dreptul angajatorului la buna funcționare a întreprinderii sale, ținând seama de obiectivul legitim urmărit de întreprindere, și anume dreptul de a-și controla cheltuielile. Curtea a concluzionat că nu a fost încălcat art. 8 din Convenție.

vi. Fotografii

60. Dreptul unei persoane la protecția imaginii sale este unul dintre elementele esențiale ale dezvoltării sale personale și presupune în principal că persoana respectivă deține controlul asupra imaginii sale (*Reklos și Davourlis împotriva Greciei*, 2009, pct. 40-43; *Margari împotriva Greciei*, 2023, pct. 28; *Glukhin împotriva Rusiei*, 2023, pct. 66). În cazul în care o persoană nu s-a expus, cu bună știință sau accidental, obiectivului unui fotograf în contextul unei activități posibil să fie înregistrată sau raportată public, protecția efectivă a imaginii sale presupune, în principiu, consimțământul persoanei de îndată ce s-a realizat captura, nu doar în momentul posibilei sale difuzări către public (*Reklos și Davourlis împotriva Greciei*, 2009, pct. 37, 40). Acest drept nu este totuși absolut. Statutul de persoană publică sau de persoană care se bucură de o anumită reputație poate justifica, în anumite

circumstanțe, în scopuri care țin de interesul general, captarea imaginii unei persoane fără consimțământul acesteia și difuzarea fără știrea sa[2].

61. În cazul persoanelor arestate sau urmărite penal, utilitatea obiectivă a fotografiilor făcute de autorități în urma arestării unei persoane suspectate de săvârșirea unei infracțiuni poate face necesară, într-o societate democratică, păstrarea acestor date în scopul combaterii infracționalității [*Suprunenko împotriva Rusiei* (dec.) (comitet), 2018, pct. 63-65]. Faptul că i se face o fotografie unei persoane suspectate de săvârșirea unei infracțiuni și că este păstrată în baza de date nu conduce în mod necesar la un stigmat de suspiciune sau de vinovăție în privința sa (*ibidem*, pct. 64). În cauza *Murray împotriva Regatului Unit* (MC), 1994 (pct. 92-93), fotografierea și păstrarea fotografiei unei persoane suspectate de terorism fără consimțământul acesteia nu constituie o măsură disproporționată în raport cu scopul urmărit de a preveni terorismul, legitim într-o societate democratică. Prin înregistrarea și păstrarea unor astfel de date cu caracter personal de bază ale persoanei arestate sau chiar ale altor persoane prezente la momentul și la locul arestării, autoritățile competente nu își depășiseră limitele legitime ale procedurii de urmărire penală a infracțiunilor de terorism (*ibidem*, pct. 93). De asemenea, Curtea a declarat vădit nefondată o cerere referitoare la păstrarea în sistemul informatic al Ministerului Internelor a unei fotografii a reclamantului, suspectat de săvârșirea unei infracțiuni, făcută de autorități în momentul reținerii sale de către poliție [*Suprunenko împotriva Rusiei* (dec.) (comitet), 2018, pct. 65]. În opinia sa, deși informațiile astfel colectate și stocate în computerul poliției erau de natură personală, nu puteau fi considerate intime sau sensibile (*ibidem*, pct. 64).

62. Pe de altă parte, Curtea a constatat o încălcare a articolului 8 în cazurile în care autoritățile polițienești au dat presei fotografii ale persoanelor arestate sau urmărite penal fără consimțământul acestora (*Sciacca împotriva Italiei*, 2005, pct. 29-31; *Khuzhin și alții împotriva Rusiei*, 2008, pct. 115-118; *Margari împotriva Greciei*, 2023, pct.54-60) sau a invitat echipe de televiziune să filmeze ilegal reclamantul la secția de poliție și să difuzeze aceste imagini la televiziune (*Toma împotriva României*, 2009, pct. 90-93; *Khmel împotriva Rusiei*, 2013, pct. 41), într-o cauză în care Ministerul de Interne publicase pe site-ul său internet fotografii ale reclamanților care fuseseră luați în custodie de poliție și în care identitatea persoanelor vizate nu fusese ascunsă (*D.H. și alții împotriva Macedoniei de Nord*, 2023, pct. 63-65), într-o cauză în care afișarea unei fotografii a reclamantului pe panoul persoanelor căutate nu era prevăzută de lege (*Guiorgui Nikolaichvili împotriva Georgiei*, 2009, pct. 129-131) și într-o cauză în care normele și procedurile în vigoare nu respectau cerința privind „calitatea legii” (*Negru împotriva Republicii Moldova*, 2023, pct. 29-35).

63. În opinia Curții, păstrarea, pe durată nelimitată, a fotografiei unei persoane suspectate de săvârșirea de infracțiuni, dar care nu a fost găsită vinovată, implică un risc de stigmatizare mai ridicat decât păstrarea datelor care aparțin persoanelor condamnate pentru săvârșirea unei infracțiuni [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 122; *Gaughran împotriva Regatului Unit*, 2020, pct. 82-84]. Factorul decisiv pentru a stabili dacă un stat și-a depășit marja de apreciere atunci când a decis să păstreze astfel de date cu caracter personal nu este în mod necesar durata păstrării datelor, ci dacă au fost puse în aplicare garanții efective (*ibidem*, pct. 88).

64. Tehnologia recunoașterii faciale și a cartografierii faciale care poate fi aplicată în prezent fotografiei unei persoane este din ce în ce mai complexă, iar instanțele interne trebuie să țină seama de aceasta atunci când examinează necesitatea unei ingerințe în dreptul la respectarea vieții private al persoanei a cărei imagine a fost captată de autorități (*ibidem*, pct. 67-70; a se vedea, de asemenea, utilizarea de către poliție a tehnologiei de recunoaștere facială cu scopul de a identifica reclamantul pe baza fotografiilor publicate pe un canal Telegram public *Glukhin împotriva Rusiei*, 2023, pct. 64-91).

[2] A se vedea, de asemenea, *Ghidul privind art. 10 din Convenție – libertatea de exprimare* cu privire la publicarea de fotografii în scopuri jurnalistice.

65. În cauza *Gaughran împotriva Regatului Unit*, 2020 (pct. 97-98), în care autoritățile deciseseră să păstreze pentru o perioadă nelimitată fotografia unei persoane condamnate pentru conducerea în stare de ebrietate, în plus față de profilul ADN și amprentele sale digitale, Curtea a concluzionat că a fost încălcat art. 8, considerând că păstrarea datelor cu caracter personal ale reclamantului, măsură luată fără a se ține seama de gravitatea infracțiunii săvârșite și fără a-i oferi o posibilitate reală de reexaminare, nu reflecta un just echilibru între interesele publice și private concurente. Chiar dacă statul păstrează o marjă de apreciere ușor mai largă în ceea ce privește păstrarea fotografiilor persoanelor condamnate în legătură cu păstrarea profilurilor lor ADN (*ibidem*, pct. 84, 96), această marjă extinsă nu este suficientă pentru a face ca păstrarea unor astfel de date să fie proporțională în toate circumstanțele, în special în lipsa unor garanții pertinente, inclusiv în lipsa unei examinări adecvate din partea instanțelor naționale (*ibidem*, pct. 96).

66. În cauza *P.N. împotriva Germaniei*, 2020 (pct. 76-91), Curtea a concluzionat că nu a fost încălcat art. 8 în ceea ce privește colectarea dispusă de poliție, în urma deschiderii unei noi proceduri penale împotriva unei persoane condamnate anterior, a unor elemente menite să identifice persoana condamnată anterior, cum ar fi fotografii ale feței și ale corpului său, în special eventuale tatuaje, precum și amprente digitale și palmare. Având în vedere amploarea relativ limitată a intruziunii și durata colectării datelor de identificare în cauză, efectul limitat asupra vieții de zi cu zi a reclamantului al păstrării datelor, limitată la cinci ani, într-o bază de date internă a poliției subordonată unor garanții și unui control individualizat, măsura în litigiu constituia o ingerință proporțională în dreptul reclamantului la respectarea vieții sale private.

67. În diferite contexte, Curtea a constatat că art. 8 a fost încălcat în cauza *Reklos și Davourlis împotriva Greciei*, 2009 (pct. 41-43), pe motiv că fotografierea unui nou-născut într-o clinică și păstrarea fotografiilor de către fotograf sub o formă care permitea identificarea, cu posibilitatea de a fi exploatate ulterior, se produsese împotriva voinței părinților, precum și în cauzele *Hájovský împotriva Slovaciei*, 2021 (pct. 46-49), care privea publicarea în presă a imaginilor needitate ale reclamantului, făcute știrea sa și folosind o stratagemă, și *Volodina împotriva Rusiei (nr. 2)*, 2021, pct. 68, care privea faptul că autorităților nu protejaseră o femeie împotriva violenței cibernetice repetate din partea partenerului său, care crease profiluri false cu numele ei și publicase fotografii intime ale acesteia.

68. În cauza *Vučina împotriva Croației* (dec.), 2019 (pct. 34-51), simplul fapt că un alt nume decât cel al reclamantei, nume care nu avea nicio conotație negativă, fusese indicat în mod eronat în descrierea unei fotografii publicate într-o revistă de sex feminin nu putea fi considerat o ingerință deosebit de importantă în dreptul la respectarea vieții private al persoanei vizate.

69. În cauza *Von Hannover împotriva Germaniei (nr. 2)* (MC), 2012 (pct. 114-126), refuzul instanțelor interne de a interzice publicarea unei fotografii a unui cuplu celebru făcută fără consimțământul celor doi nu a constituit o încălcare a art. 8, întrucât instanțele naționale au efectuat o punere în balanță detaliată între dreptul editurii la libertatea de exprimare și dreptul reclamanților la respectarea vieții lor private. Procedând astfel, au acordat o importanță primordială întrebării dacă fotografiile, examinate în lumina articolelor care le însoțeau, și-au adus contribuția la o dezbatere de interes general. În plus, acestea au examinat circumstanțele în care fuseseră făcute fotografiile.

70. În cauza *Kahn împotriva Germaniei*, 2016 (pct. 63-76), Curtea a concluzionat că nu a fost încălcat art. 8 în ceea ce privește neobligarea unui editor la plata unei sume pentru încălcarea interdicției de a publica fotografiile a doi copii ai unui fost portar al echipei naționale de fotbal germane. Curtea a specificat faptul că nu se putea deduce din art. 8 principiul potrivit căruia, pentru a proteja în mod efectiv viața privată a unei persoane, obligarea unui editor la plata unei sume pentru încălcarea unei interdicții de a publica nu putea fi suficientă decât dacă respectiva sumă revenea victimei, în condițiile în care statul, în exercitarea marjei sale de apreciere, pune la dispoziția persoanelor vătămate alte mijloace care se pot dovedi efective și care nu pot fi considerate ca limitând în mod disproporționat posibilitatea de a obține o reparație pentru încălcările invocate (*ibidem*, pct. 75).

B. Cele două aspecte (negativ și pozitiv) ale protecției datelor cu caracter personal

71. Art. 8, care asigură, în primul rând, protecția datelor cu caracter personal, impune în esență statelor obligația de a se abține de la orice ingerință arbitrară în exercitarea dreptului la respectarea „vieții private și de familie, a domiciliului și a corespondenței" unei persoane, indiferent dacă este vorba despre activitatea autorităților publice înseși sau a organelor private cărora statul le-a delegat în prealabil responsabilitățile sale. Această cerință mai degrabă negativă poate fi completată de obligații pozitive inerente respectării efective a drepturilor garantate de Convenție [*Bărbulescu împotriva României* (MC), 2017, pct. 108].

72. Atunci când o măsură care aduce atingere protecției datelor cu caracter personal ale unei persoane este luată de o persoană sau o entitate care aparține strict sectorului privat, Curtea examinează cauza din perspectiva obligațiilor pozitive ale statului [*Craxi împotriva Italiei (nr. 2)*, 2003, pct. 68-76; *Köpke împotriva Germaniei* (dec.), 2010; *Alkaya împotriva Turciei*, 2012, pct. 32; *Söderman împotriva Suediei* (MC), 2013, pct. 89; Bărbulescu împotriva României (MC), 2017, pct. 111; *López Ribalda și alții împotriva Spaniei* (MC), 2019, pct. 111; *Buturugă împotriva României*, 2020, pct. 60-63; *Volodina împotriva Rusiei (nr.2)*, 2021, pct. 58-68; *Florindo de Almeida Vasconcelos Gramaxo împotriva Portugaliei*, 2022, pct. 111; *Tena Arregui împotriva Spaniei*, 2024, pct. 35]. Atunci când o astfel de măsură este luată, în schimb, de o entitate care aparține strict sectorului public (*Copland împotriva Regatului Unit*, 2007, pct. 39; *Libert împotriva Franței,* 2018, pct. 41, *Drelon împotriva Franței*, 2022, pct. 85; *Cherrier împotriva Franței*, 2024, pct. 57), un organism privat căruia un organism public îi delegase anterior obligațiile sale (*Vukota-Bojić împotriva Elveției*2016, pct. 47) sau un organism privat care acționează potrivit unei obligații legale (*Podchasov împotriva Rusiei*, 2024, pct. 52), Curtea examinează cauza din perspectiva obligației negative a statului. În continuare, Curtea trebuie să verifice dacă ingerința era conformă cu cerințele art. 8 § 2, și anume dacă era prevăzută de lege, dacă urmărea un scop legitim și dacă era necesară într-o societate democratică. Acest aspect va fi analizat mai în detaliu în secțiunea de mai jos a prezentului ghid referitoare la Cele trei „criterii" în materie de protecția datelor.

73. În cauza *Vukota-Bojić împotriva Elveției*, 2016 (pct. 47), Curtea a subliniat că un stat nu se poate sustrage de la răspunderea care îi revine în temeiul Convenției delegând obligațiile sale unor organisme private sau unor persoane de drept privat. Întrucât societatea de asigurări privată, care colectase și stocase date cu caracter personal, punea în aplicare sistemul public de asigurări și era considerată autoritate publică în temeiul dreptului intern, trebuia să fie considerată ca atare, iar acțiunile sale să fie imputabile statului pârât (*ibidem,* pct. 47).

74. În cauza *Libert împotriva Franței,* 2018 (pct. 37-41), Curtea a respins obiecția guvernului potrivit căreia Societatea Națională a Căilor Ferate (SNCF), angajator al reclamantului, care fusese acuzată de deschiderea fișierelor personale stocate pe un calculator profesional, nu putea fi considerată o „autoritate publică" în sensul art. 8. Chiar dacă angajații săi se află într-un raport de drept privat, o astfel de societate este o persoană juridică de drept public, plasată sub controlul statului și a cărei conducere este desemnată de acesta, beneficiind de o garanție implicită din partea statului.

75. În ceea ce privește supravegherea apelurilor telefonice, a e-mail-urilor și a conexiunilor la Internet ale unui angajat al unui colegiu, Curtea a considerat că problema ridicată privea obligația negativă a statului de a nu aduce atingere vieții private și corespondenței persoanei vizate, din moment ce colegiul era un organism public de învățământ superior, ale cărui acte angajau răspunderea statului în temeiul Convenției (*Copland împotriva Regatului Unit*, 2007, pct. 39).

76. În cauza *Liebscher împotriva Austriei*, 2021, reclamantul se plângea că fusese obligat să prezinte în integralitate acordul său de divorț (și nu doar un extras) pentru a obține transferul către fosta soție a părții sale din bunurile imobiliare ale cuplului. Divorțul prin acordul părților menționa numele și locul de reședință al copiilor minori ai cuplului și ai fostei soții a reclamantului, cuantumul pensiei de

întreținere și modalitățile de îngrijire a copiilor, repartizarea bunurilor (mobile) ale cuplului și o listă a veniturilor și a bunurilor reclamantului. Transferul dreptului de proprietate asupra bunurilor imobile și, prin urmare, toate documentele aferente, inclusiv divorțul prin acordul părților, trebuiau să fie înscrise într-un registru cadastral public și, prin urmare, consultabile fără restricții de către orice persoană. Curtea a abordat cauza din punctul de vedere al obligației pozitive a statului de a adopta măsuri menite să asigure respectarea vieții private, în special prin stabilirea unui cadru de reglementare și prin aplicarea, după caz, a unor măsuri specifice (*ibidem*, pct. 60-61).

77. Deși granița dintre obligațiile pozitive și obligațiile negative ale statului în temeiul Convenției nu se pretează unei definiții precise, principiile aplicabile sunt totuși comparabile. În cele două cazuri, trebuie păstrat un just echilibru între interesul general și interesele individuale, statul beneficiind în orice situație de o marjă de apreciere [*Bărbulescu împotriva României* (MC), 2017, pct. 112; *Tena Arregui împotriva Spaniei*, 2024, pct. 32].

78. În cauzele care ridică problema protecției datelor cu caracter personal, Curtea a reținut că marja de apreciere a autorităților era mai largă: atunci când nu există un consens în cadrul statelor membre ale Consiliului Europei cu privire la importanța relativă a interesului în cauză sau cu privire la cele mai bune mijloace de protecție a acestuia [*Odièvre împotriva Franței* (MC), 2003, pct. 47; *Breyer împotriva Germaniei*, 2020, pct. 108; *Gauvin-Fournis și Silliau împotriva Franței*, 2023, pct. 111); atunci când datele cu caracter personal în discuție, strict financiare, nu sunt strâns legate de identitatea unui reclamant (*G.S.B. împotriva Elveției*, 2015, pct. 93); și, în sfârșit, în materie de securitate națională (*Leander împotriva Suediei*, 1987, pct. 59]. În schimb, marja de apreciere rezervată autorităților naționale a fost considerată mai restrânsă atunci când era vorba, de exemplu, de date cu caracter personal supuse unei prelucrări automate care facilita în mare măsură accesul și difuzarea acestora și care puteau afecta reputația unei persoane și să facă mult mai dificilă viața de zi cu zi a acesteia (*Khelili împotriva Elveției*, 2011, pct. 64, 70). Situația a fost valabilă și în cazul protecției categoriilor sensibile de date cu caracter personal, în special a datelor ADN care reflectau patrimoniul genetic al unei persoane și care aveau o importanță considerabilă atât pentru aceasta, cât și pentru familia sa [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 102-103].

79. Obligațiile pozitive inerente asigurării protecției efective a drepturilor și libertăților garantate de Convenție pot implica, de exemplu, obligația de a oferi unei persoane: accesul, într-un termen rezonabil, la informațiile stocate în mod sistematic despre acesta de fostele servicii secrete de stat, referitoare la trecutul îndepărtat al acestuia (*Haralambie împotriva României*, 2009, pct. 79; *Jarnea împotriva României*, 2011, pct. 50; *Joanna Szulc împotriva Poloniei*, 2012, pct. 87); o „procedură efectivă și accesibilă" care să îi permită să aibă acces la „toate informațiile relevante și adecvate" colectate și stocate de autoritățile publice pentru a afla și a-și înțelege copilăria și anii perioadei de formare (*Gaskin împotriva Regatului Unit*, 1989, pct. 49), pentru a-și descoperi identitatea personală [*Odièvre împotriva Franței* (MC), 2003, pct. 42; *Gauvin-Fournis și Silliau împotriva Franței*, 2023, pct. 110], sau pentru a identifica riscurile pentru sănătate la care au fost expuse [*Guerra și alții împotriva Italiei*, 1998, pct. 60; *McGinley și Egan împotriva Regatului Unit*, 1998, pct. 101; *Roche împotriva Regatului Unit* (MC), 2005, pct. 162].

80. Curtea a considerat, în schimb, că astfel de obligații pozitive nu le reveneau autoritățile naționale în contextul informațiilor sensibile pentru securitatea națională colectate despre o persoană de către autorități (*Leander împotriva Suediei*, 1987, pct. 51).

81. Astfel, în cauza *Kotilainen și alții împotriva Finlandei*, 2020 (pct. 83), care privea un atac armat produs într-o instituție de învățământ, Curtea a considerat că obligația pozitivă a autorităților de a proteja viața rudelor reclamanților nu se extindea, sub aspectul material al art. 2, la o obligație, din partea poliției, de a obține, înainte de atacul armat, dosarele medicale și militare ale autorului atacului pentru a verifica datele referitoare la sănătatea sa mintală. În opinia Curții, accesul poliției la datele medicale cu caracter personal ale unei persoane nu poate fi o chestiune de rutină și trebuie să facă în continuare obiectul unor cerințe specifice de necesitate și justificare.

82. În anumite circumstanțe în care se pune în discuție problema datelor cu caracter personal, în special în ceea ce privește acte interpersonale deosebit de grave, exercitarea efectivă a drepturilor garantate de Convenție impune statului să adopte un cadru legislativ capabil să protejeze dreptul în cauză. Astfel, în cauza *Söderman împotriva Suediei* (MC), 2013 (pct. 86-117), Curtea a concluzionat că a fost încălcat art. 8, având în vedere lipsa unor dispoziții legale clare care să incrimineze actul izolat constând în filmarea sau fotografierea unui copil dezbrăcat fără știrea acestuia, lacune care nu erau acoperite de alte dispoziții penale la momentul faptelor, precum și având în vedere ineficacitatea căilor de atac cu caracter civil (*ibidem*, pct. 108-114). În mod similar, în cauza *K.U. împotriva Finlandei*, 2008 (pct. 49-50), lipsa unei baze legale care să permită autorităților să oblige furnizorul de acces la Internet să dezvăluie identitatea unei persoane căutate pentru că postase un mesaj indecent cu privire la un minor pe un site de întâlniri și, prin urmare, să concilieze diferitele interese care trebuiau protejate în acest context a condus la constatarea unei încălcări a art. 8. Cauza *Khadija Ismayilova împotriva Azerbaidjanului*, 2019 (pct. 105-132), privea înregistrarea video în secret a unei jurnaliste la domiciliul său și difuzarea acestor materiale video către public. În speță, faptele în litigiu erau pasibile de sancțiuni penale și a fost deschisă efectiv o anchetă penală. Cu toate acestea, Curtea a reținut că autoritățile nu își îndepliniseră obligația pozitivă de a asigura protecția adecvată a vieții private a reclamantei prin efectuarea unei anchete penale eficiente cu privire la atingerea gravă adusă vieții sale private (*ibidem*, pct. 119-131). Cauza *Volodina împotriva Rusiei (nr. 2)*, 2021, pct. 68, privea lipsa protecției invocată de reclamantă față de violența cibernetică repetată din partea partenerului său, care crease profiluri false în numele său, publicase fotografii intime, îi urmărise deplasările și ii trimisese amenințări cu moartea prin intermediul mijloacelor de comunicare socială. Curtea constată, în special, că, deși autoritățile dispuneau de instrumente juridice pentru urmărirea penală a partenerului reclamantei, nu au desfășurat o anchetă eficientă și nu au analizat în niciun moment ce ar fi putut și ar fi trebuit să fie făcut pentru a o proteja. Prin urmare, autoritățile nu și-au îndeplinit obligația de a o proteja împotriva unor abuzuri grave.

83. În ceea ce privește acte interpersonale mai puțin grave, precum supravegherea angajaților la locul de muncă, statele pot alege să adopte, sau nu, o legislație specifică în ceea ce privește supravegherea video [*López Ribalda și alții împotriva Spaniei* (MC), 2019, pct. 113; *Köpke împotriva Germaniei* (dec.), 2010] sau supravegherea corespondenței angajaților și a comunicațiilor neprofesionale (*Bărbulescu împotriva României* (MC), 2017, pct. 119). Cu toate acestea, este de competența instanțelor interne să se asigure că punerea în aplicare de către un angajator a unor măsuri de supraveghere care încalcă dreptul la respectarea vieții private sau la corespondență al angajaților este proporțională și însoțită de garanții adecvate și suficiente împotriva abuzurilor [*Köpke împotriva Germaniei* (dec.), 2010; *Bărbulescu împotriva României* (MC), 2017, pct. 120; *López Ribalda și alții împotriva Spaniei* (MC), 2019, pct. 116; a se vedea, de asemenea, în contextul controlului de către un partid politic al corespondenței electronice a membrilor săi, *Tena Arregui împotriva Spaniei*, 2024, pct. 38).

84. În alte cauze care priveau problema divulgării datelor cu caracter personal, Curtea a reținut obligația pozitivă care îi revine statului de a ancheta încălcările invocate ale art. 8, indiferent dacă au fost efectuate de persoane de drept privat sau de autorități. De exemplu, în cauza *Craxi împotriva Italiei (nr. 2)*, 2003 (pct. 68-76), care privea citirea în ședința de judecată și divulgarea ulterioară în presă a conversațiilor telefonice ale unui politician, interceptate în contextul unei proceduri penale pentru corupție, Curtea a considerat că autoritățile aveau obligația pozitivă de a împiedica divulgarea în domeniul public a unor astfel de conversații private. Întrucât divulgarea nu a fost consecința directă a unui act al procurorului, ci mai degrabă rezultatul unei funcționări defectuoase a grefei instanței, Curtea a concluzionat că a fost încălcat art. 8, întrucât autoritățile nu luaseră măsurile care se impuneau pentru a asigura protecția efectivă a drepturilor reclamantului prin instituirea unor garanții adecvate și prin desfășurarea unei anchete eficiente.

85. În cauza *Alkaya împotriva Turciei*, 2012 (pct. 30-40), Curtea a pus sub semnul întrebării gradul de protecție, considerat insuficient, acordat de instanțele interne pentru protecția informațiilor cu caracter personal ale unei actrițe celebre, a cărui adresă completă fusese distribuită de un organ de

presă. Întrucât nu a identificat niciun element de natură să clarifice motivele de interes general pentru care ziarul a decis să divulge adresa de domiciliu a reclamantei, Curtea a observat că instanțele naționale nu luaseră în considerare impactul asupra vieții reclamantei al difuzării adresei sale personale în presă. În opinia sa, această neevaluarea intereselor în cauză de către instanțele interne nu putea fi considerată conformă cu obligațiile pozitive ale statului în temeiul art. 8.

86. În contextul violenței domestice, Curtea a considerat, în cauza *Buturugă împotriva României*, 2020 (pct. 73-78), în care fostul soț al reclamantei consultase în mod abuziv conturile electronice ale acesteia, inclusiv contul de Facebook, și făcuse copii ale conversațiilor private, documentelor și fotografiilor acesteia, că autoritățile aveau obligația să ancheteze violarea secretului corespondenței reclamantei. Recunoscând violența cibernetică ca aspect al violenței împotriva femeilor și fetelor, care se poate prezenta sub diverse forme, inclusiv intruziunea în computerul victimei și luarea, partajarea și manipularea datelor și imaginilor, inclusiv a datelor intime, Curtea a acceptat că acte precum supravegherea, accesarea sau păstrarea fără drept a corespondenței partenerului pot fi luate în considerare atunci când autoritățile naționale anchetează acte de violență domestică. Astfel de acuzații de violare a corespondenței necesită o examinare pe fond din partea autorităților pentru a putea avea o imagine globală a fenomenul violenței conjugale sub toate formele sale (*ibidem*, pct. 76-77). O astfel de examinare nu fusese efectuată în speță, iar Curtea a concluzionat că a fost încălcat art. 8 (a se vedea, într-un context similar, *Volodina împotriva Rusiei (nr. 2)*, 2021, pct. 48-68).

C. Cele trei „criterii” în materie de protecția datelor

87. Paragraful al doilea al art. 8 precizează condițiile în care poate exista o ingerință în exercitarea unui drept protejat; o astfel de ingerință trebuie să fie „prevăzută de lege”, să urmărească un „scop legitim” și să fie „necesară într-o societate democratică”.

1. Legalitatea ingerinței

88. Curtea a examinat în mai multe cauze dacă cerința enunțată la art. 5 din Convenția 108, potrivit căreia datele cu caracter personal care fac obiectul prelucrării automate trebuie să fi fost obținute și prelucrate în mod corect și legal, a fost sau nu respectată. Într-o serie de cauze, Curtea a concluzionat că a fost încălcat art. 8 numai în temeiul lipsei unei baze legale la nivel național care să autorizeze măsuri susceptibile să aducă atingere unui drept (*Taylor-Sabori împotriva Regatului Unit*, 2002, pct. 17-19; *Radu împotriva Moldovei*, 2014, pct. 31; *Mockutė împotriva Lituaniei*, 2018, pct. 103-104; *M.D. și alții împotriva Spaniei*, 2022, pct. 61-64 ; *Kaczmarek împotriva Poloniei*, 2024, pct. 74-80).

89. În special, în cauza *Mockutė împotriva Lituaniei*, 2018 (pct. 103-104), Curtea a observat că nici guvernul, nici instanțele naționale nu indicaseră vreo dispoziție juridică pe care s-ar fi bazat, după caz, comunicarea, de către spitalul de psihiatrie, mamei și jurnaliștilor, informații privind starea de sănătate a reclamantei, care era adultă. În cauza *Taylor-Sabori împotriva Regatului Unit*, 2002 (pct. 17-19), în care reclamantul făcuse obiectul supravegherii poliției prin intermediul unei „clone” a pagerului acestuia, dreptul intern nu conținea dispoziții care să reglementeze interceptarea comunicațiilor transmise de un sistem privat de telecomunicații. În cauza *Radu împotriva Republicii Moldova*, 2014 (pct. 31), difuzarea, de către un spital public, a informațiilor medicale privind sarcina reclamantei, starea de sănătate și tratamentul pe care aceasta îl primise angajatorului său nu era „prevăzută de lege”. În cauza *M.D. și alții împotriva Spaniei*, 2022 (pct. 61-64), poliția întocmise un raport privind judecătorii și magistrații care își desfășurau activitatea în Catalonia și care semnaseră un manifest în care își exprimaseră sprijinul, din punct de vedere juridic, pentru posibilitatea ca poporul catalan să își exercite „dreptul de a decide”. Raportul în cauză conținea date cu caracter personal, fotografii, informații profesionale și opiniile politice ale unora dintre persoanele vizate. Curtea a arătat că redactarea de către poliție a unui astfel de raport nu era prevăzută de lege și că, întrucât autoritățile publice utilizaseră date cu caracter personal în alte scopuri decât cele pentru care fuseseră colectate, simpla existență a acestui raport, care privea persoane care nu săvârșiseră nicio infracțiune, constituia

o încălcare a articolului 8 din Convenție. În cauza *Kaczmarek împotriva Poloniei*, 2024 (pct. 74-80), în care înregistrarea convorbirii telefonice a reclamantului a fost divulgată în cadrul unei conferințe de presă, Curtea a statuat că dispoziția relevantă din Codul de procedură penală, care privea în principal examinarea dosarului și realizarea de copii în cursul anchetei, nu putea fi considerată un temei juridic pentru o astfel de divulgare.

90. Într-o serie de alte cauze, Curtea a constatat o încălcare a articolului 8 pe motiv că legislația națională, care ar fi trebuit să protejeze datele cu caracter personal, era inaccesibilă sau confidențială (*Vasil Vasilev împotriva Bulgariei*, , 2021, pct. 169-170, *Nuh Uzun și alții împotriva Turciei*, 2022, pct. 80-99) sau nu era suficient de clară și previzibilă [*Vukota-Bojić împotriva Elveției*, 2016; *Ben Faiza împotriva Franței*, 2018, pct. 58-61; *Benedik împotriva Sloveniei*, 2018 *;* *Rotaru împotriva României* (MC), 2000; *Zoltán Varga împotriva Slovaciei*, 2021, pct. 162; *Haščák împotriva Slovaciei*, 2022, pct. 94-95; *Kaczmarek împotriva Poloniei*, 2024, pct. 93-96]. Astfel, în cauza *Nuh Uzun și alții împotriva Turciei*, 2022, pct. 80-99, corespondența deținuților a fost scanată și înregistrată în sistemul informatic al Rețelei Judiciare Naționale în conformitate cu instrucțiuni care fuseseră comunicate direct și specific parchetului și autorităților penitenciare de către Ministerul Justiției, dar care nu fuseseră puse la dispoziția publicului, în general, sau a reclamanților, în special. În cauza *Vukota-Bojić împotriva Elveției*, 2016 (pct. 71-77), dispozițiile pe care se întemeia supravegherea în secret a reclamantei de către societatea de asigurări în urma unui accident rutier nu indicau în mod suficient de clar amploarea și modalitățile de exercitare a puterii discreționare conferite societăților de asigurări, care acționau în calitate de autorități publice, de a supraveghea în secret un asigurat. În cauza *Rotaru împotriva României* (MC), 2000 (pct. 57-62), care privea informațiile cu caracter personal păstrate în dosarele deținute de serviciul de informații român, dreptul național nu definea tipul de informații care puteau fi prelucrate, categoriile de persoane în privința cărora puteau fi luate măsuri de supraveghere, circumstanțele în care puteau fi luate astfel de măsuri sau procedura care trebuia urmată. În cauza *Benedik împotriva Sloveniei*, 2018 (pct. 132), anumite dispoziții legale utilizate de poliție pentru a obține date privind abonații asociate adresei IP dinamice nu erau clare și nu erau ofereau nicio protecție împotriva unei ingerințe arbitrare, neprevăzând garanții împotriva unor eventuale abuzuri sau o supraveghere independentă a puterilor polițienești implicate. În mod similar, în cauza *Kaczmarek împotriva Poloniei*, 2024 (pct. 93-96), păstrarea de către autorități a unor elemente referitoare la reclamantă, care au fost colectate în cursul supravegherii în cadrul unei operațiuni de securitate al cărei obiect nu era ea însăși se întemeia pe dispoziții legale lipsite de claritate și care nu ofereau nicio garanție procedurală, astfel încât reclamanta nu a fost în măsură să obțină distrugerea materialului în cauză.

91. În schimb, în alte cauze, Curtea a concluzionat neîncălcarea art. 8 după ce a constatat că legislația națională era clară și previzibilă și oferea suficiente garanții împotriva eventualelor abuzuri [*Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei* (MC), 2017, pct. 154; *Ben Faiza împotriva Franței*, 2018, pct. 75]. În cauza *Ben Faiza împotriva Franței*, 2018 (pct. 70-76), hotărârea judecătorească utilizată pentru a obține de la un operator de telefonie mobilă date cu caracter personal ale reclamantului care nu priveau conținutul comunicațiilor sale era „prevăzută de lege”. O dispoziție legislativă internă autoriza și încadra o astfel de măsură, și conținea garanții împotriva arbitrariului, întrucât astfel de măsuri erau supuse autorizării prealabile de către un magistrat al parchetului, sub sancțiunea nulității, puteau face obiectul unui control jurisdicțional, iar probele obținute puteau fi excluse în caz de nelegalitate (*ibidem*, pct. 73).

92. Curtea a ajuns la o concluzie similară în cauza *Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei* (MC), 2017 (pct. 154), care privea o decizie a comisiei pentru protecția datelor cu caracter personal, confirmată de instanțe, care interzicea publicarea pe scară largă a informațiilor fiscale. Formularea legislației relevante în materie de protecția datelor, precum și modul în care aceste dispoziții au fost aplicate în urma orientărilor interpretative comunicate instanțelor finlandeze de către Curtea de Justiție a Uniunii Europene (CJUE) erau suficient de previzibile. Faptul că respectiva cauză era prima de acest tip în temeiul legii privind datele cu caracter personal iar Curtea

Administrativă Supremă a solicitat CJUE orientări interpretative cu privire la interpretarea unei derogări prevăzute de dreptul Uniunii Europene nu făceau ca interpretarea și aplicarea derogării respective, de către instanțele interne, să fie arbitrare sau imprevizibile (*ibidem*, pct. 150). Întrucât societățile reclamante erau societăți media, acestea ar fi trebuit, în această calitate, să aibă cunoștință de faptul că colectarea și difuzarea pe scară largă a datelor nu puteau fi considerate drept prelucrare de date efectuată „exclusiv" în scopuri jurnalistice în temeiul dreptului finlandez sau al dreptului Uniunii Europene (*ibidem*, pct. 151).

93. În cauza *Le Marrec împotriva Franței* (dec.), 2024, pct. 72-75, Curtea a concluzionat că un act normativ care conținea dispoziții precise, în special în ceea ce privește prelucrarea adreselor IP, și care fusese publicat pe site-ul internet al Casei de alocații familiale, era suficient de accesibil publicului și, prin urmare, îndeplinea cerința de „legalitate" prevăzută la articolul 8 din Convenție.

94. În sfârșit, în alte cauze, Curtea a constatat despre condiția ca ingerința să fie „prevăzută de lege" că era atât de strâns legată de cea de a fi „necesară într-o societate democratică" încât trebuia ca aceste condiții să fie discutate împreună [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 99; *Kvasnica împotriva Slovaciei*, 2009, pct. 84; *Kennedy împotriva Regatului Unit*, 2010, pct. 155; *Glukhin împotriva Rusiei*, 2023, pct. 78).

95. În contextul special al măsurilor de supraveghere secretă, precum interceptarea comunicațiilor, Curtea a hotărât că „previzibilitatea" nu poate fi înțeleasă în același mod ca în multe alte domenii. În opinia sa, previzibilitatea nu putea însemna că o persoană trebuie să fie în măsură să prevadă momentul în care autoritățile pot recurge la astfel de măsuri astfel încât să își poată adapta comportamentul în consecință (*Adomaitis împotriva Lituaniei*, 2022, pct. 83; a se vedea, de asemenea, *Sârbu împotriva României*, 2023, punctul 51, în care aceleași principii au fost aplicate în contextul înregistrărilor efectuate de o persoană care utiliza o cameră ascunsă). Cu toate acestea, întrucât riscul de arbitrar apare cu claritate atunci când puterile executivului sunt exercitate în secret, este esențial ca măsurile de supraveghere secretă să fie reglementate de norme clare și detaliate, în special cu atât mai mult cu cât procesele tehnice care pot fi utilizate nu încetează să se îmbunătățească. Dreptul intern trebuie să fie suficient de clar pentru a indica tuturor, în mod adecvat, în ce circumstanțe și în ce condiții este abilitată autoritatea publică să recurgă la astfel de măsuri [*Malone împotriva Regatului Unit,* 1984, pct. 67; *Leander împotriva Suediei*, 1987, pct. 51; *Valenzuela Contreras împotriva Spaniei,* 1998, pct. 46; *Weber și Saravia împotriva Germaniei* (dec.), 2006, pct. 93; *Asociația pentru integrarea europeană și drepturile omului și Ekimdjiev împotriva Bulgariei*, 2007, pct. 75; *Roman Zakharov împotriva Rusiei* (MC), 2015, pct. 229; *Denisiuk și alții împotriva Ucrainei*, 2025, pct. 88]. În plus, dreptul trebuie să definească domeniul de aplicare și modalitățile de exercitare a puterii discreționare acordate autorităților competente cu suficientă claritate pentru a oferi persoanei o protecție adecvată împotriva arbitrariului [*Roman Zakharov împotriva Rusiei* (MC), 2015, pct. 230].

96. De-a lungul evoluției jurisprudenței sale privind interceptarea comunicațiilor în contextul anchetelor penale, Curtea a stabilit că, pentru a preveni abuzul de putere, dreptul trebuie să prevadă cel puțin următoarele șase elemente: natura infracțiunilor care pot da naștere unui mandat de interceptare; definiția categoriilor de persoane ale căror comunicații pot fi interceptate; limita duratei de executare a măsurii; procedura care trebuie urmată pentru examinarea, utilizarea și stocarea datelor colectate; precauțiile care trebuie luate la comunicarea datelor către alte părți; și circumstanțele în care datele interceptate pot sau trebuie să fie șterse sau distruse [*Huvig împotriva Franței* , 1990, pct. 34; *Valenzuela Contreras împotriva Spaniei,* 1998, pct. 46; *Weber și Saravia împotriva Germaniei* (dec.), 2006, pct. 95; *Asociația pentru integrarea europeană și drepturile omului și Ekimdjiev împotriva Bulgariei*, 2007, pct. 76; *Denisiuk și alții împotriva Ucrainei*, 2025, pct. 88]. În hotărârea *Roman Zakharov împotriva Rusiei* (MC), 2015 (pct. 238), a confirmat că aceleași garanții minime se aplică și în cazurile în care interceptarea a fost efectuată din motive de securitate națională; cu toate acestea, pentru a stabili dacă legea în litigiu era contrară art. 8, Curtea a luat în considerare,

de asemenea, următoarele elemente: modalitățile de control al aplicării măsurilor de supraveghere secretă, posibila existență a unui mecanism de notificare și căile de atac prevăzute în dreptul intern[3].

97. În contextul datelor cu caracter personal colectate de autorități și păstrate în baze de date în scopul prevenirii sau al combaterii criminalității, Curtea a indicat că este esențial să se stabilească norme clare și detaliate care să reglementeze domeniul de aplicare și aplicarea unor astfel de măsuri și să impună un minim de cerințe privind, printre altele, durata, stocarea, utilizarea, accesul terților, procedurile menite să păstreze integritatea și confidențialitatea datelor cu caracter personal și procedurile de distrugere a acestora, astfel încât justițiabilii să dispună de garanții suficiente împotriva riscurilor de abuz și arbitrar [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 99, 103; *Nuh Uzun și alții împotriva Turciei*, 2022, pct. 86]. Curtea a concluzionat că a fost încălcat art. 8 în cauzele în care dreptul intern nu definea cu suficientă claritate domeniul de aplicare și modul de exercitare a puterii de apreciere conferite autorităților interne [*Shimovolos împotriva Rusiei* (dec.), 2011, pct. 69; *Dimitrov-Kazakov împotriva Bulgariei*, 2011, pct. 33; *Negru împotriva Republicii Moldova*, 2023, pct. 34]. În cauza *Shimovolos împotriva Rusiei* (dec.), 2011 (pct. 70), crearea și actualizarea unei baze de date referitoare la supravegherea secretă, care înregistra datele cu caracter personal și mișcările unui activist pentru drepturile omului, precum și modul în care își desfășura activitatea, erau reglementate printr-un ordin ministerial care nu fusese niciodată publicat sau pus altfel la dispoziția publicului. În cauza *Dimitrov-Kazakov împotriva Bulgariei*, 2011 (pct. 33), înregistrarea unei persoane ca „infractor" în evidențele poliției era întemeiată pe o instrucțiune fără caracter public la momentul faptelor, care era confidențială și era rezervată, până la declasarea ulterioară, pentru uz intern, de către Ministerul Afacerilor Interne. În cauza *Negru împotriva Republicii Moldova*, 2023 (pct. 24), reclamanta figura pe lista persoanelor căutate, ceea ce a însemnat că datele sale cu caracter personal fuseseră prelucrate în sistemul informatic automatizat și integrat care înregistra infracțiunile, cauzele penale și infractorii la nivel național, iar fotografia sa a fost plasată pe panoul public al unei secții de poliție în urma unei decizii care fusese emisă în contextul unei proceduri opace de către un procuror care a beneficiat de o latitudine pe care Curtea a considerat-o a fi o competență nelimitată.

98. În cauza *Catt împotriva Regatului Unit*, 2019 (pct. 97 și 106), Curtea a subliniat pericolul unei abordări ambigue din partea autorităților în ceea ce privește colectarea și păstrarea datelor cu caracter personal care favoriza noțiuni definite într-un mod mult prea vag în dreptul intern.

99. În contextul punerii în aplicare a tehnologiei de recunoaștere facială, Curtea a afirmat că, pentru a respecta cerința privind „calitatea legii", este esențial să existe norme detaliate care să reglementeze domeniul de aplicare și aplicarea măsurilor, precum și garanții solide împotriva riscului de abuz și de decizii arbitrare și că necesitatea unor garanții este cu atât mai mare atunci când tehnologia de recunoaștere facială este utilizată în timp real (*Glukhin împotriva Rusiei*, 2023, pct. 82). În cauza în discuție, în care a examinat pentru prima dată problema utilizării acestei tehnologii, Curtea a exprimat îndoieli serioase cu privire la respectarea cerinței privind „calitatea legii" în virtutea dispozițiilor legale în cauză care autorizau prelucrarea datelor biometrice cu caracter personal, inclusiv utilizarea tehnologiei de recunoaștere facială, „în cadrul administrării justiției", aceste dispoziții fiind formulate într-un sens foarte larg și părând să permită prelucrarea datelor în cauză în cadrul oricărui tip de procedură judiciară. Aceasta a arătat că dreptul național nu conținea nicio limită în ceea ce privește natura situațiilor în care putea fi utilizată tehnologia de recunoaștere facială, scopurile în care putea fi utilizată, categoriile de persoane care puteau fi vizate sau prelucrarea datelor sensibile cu caracter personal. Curtea a remarcat, de asemenea, că utilizarea tehnologiei de recunoaștere facială nu părea să dispună de nicio garanție procedurală – proceduri de autorizare, proceduri care trebuie urmate pentru examinarea, utilizarea și păstrarea datelor obținute, mecanisme de monitorizare sau căi de atac disponibile (*ibidem*, pct. 83).

[3] A se vedea, de asemenea, *Ghid privind art. 8 din Convenție – dreptul la respectarea vieții private și de familie* privind cerința de previzibilitate a legii în materie de interceptare a comunicațiilor, ascultare a conversațiilor telefonice și operațiuni de supraveghere secretă.

2. Legitimitatea ingerinței

100. Curtea a examinat în mai multe cazuri dacă cerința prevăzută la art. 5 din Convenția 108, potrivit căreia datele cu caracter personal care fac obiectul prelucrării automate trebuie să fi fost colectate sau înregistrate în scopuri determinate și legitime, a fost, sau nu, respectată. În aceste cauze, examinarea scopurilor legitime care pot justifica o ingerință în exercitarea drepturilor pe care le protejează, enumerate la art. 8 § 2, este mai degrabă succintă. Aceste scopuri sunt: protejarea securității naționale, a siguranței publice și a bunăstării economice a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei, ori protejarea drepturilor și libertăților altora. Curtea confirmă în general existența unuia sau a mai multora dintre aceste scopuri legitime invocate de guvern.

101. Curtea a considerat, de exemplu, că stocarea, într-o registru secret al poliției, a datelor referitoare la viața privată a persoanelor și utilizarea lor ulterioară în contextul evaluării aptitudinilor candidaților la posturi importante din punctul de vedere al securității naționale urmăreau un scop legitim în temeiul art. 8, și anume protejarea securității naționale (*Leander împotriva Suediei*, 1987, pct. 49). Supravegherea unui reclamant prin GPS, dispusă de procuror pentru a investiga mai multe acuzații de tentative de omor revendicate de o mișcare teroristă și pentru a preveni alte atentate cu bombă, a fost efectuată, în opinia Curții, în interesul securității naționale, al siguranței publice, al prevenirii infracțiunilor penale și al protecției drepturilor victimelor (*Uzun împotriva Germaniei,* 2010, pct. 77).

102. Curtea a hotărât, de asemenea, că apărarea bunăstării economice a țării constituia un scop legitim în ceea ce privește transmiterea datelor bancare către autoritățile unui alt stat în temeiul unui acord bilateral (*G.S.B. împotriva Elveției*, 2015, pct. 83). Întrucât sectorul bancar reprezenta o ramură economică importantă pentru statul pârât, măsura incriminată, care făcea parte dintr-un efort global al guvernului elvețian de a soluționa conflictul dintre o instituție bancară, descrisă ca „actor important pentru economia elvețiană și angajator al unui număr considerabil de persoane", și autoritățile fiscale americane, putea fi în mod valid considerată ca fiind de natură să contribuie la protejarea bunăstării economice a țării (*ibidem*, pct. 83).

103. Făcând trimitere la texte internaționale care fac din fairplay și egalitatea de șanse unul dintre fundamentele luptei împotriva dopajului, Curtea a considerat că protejarea sănătății și a moralei justifica obligația de a localiza sportivii, ținând seama de imperativul combaterii dopajului în domeniul sportului [*Fédération nationale des associations et syndicats de sportifs (FNASS) și alții împotriva Franței*, 2018, pct. 164-166]. În opinia Curții, ceea ce guvernul califica drept „moral", în ceea ce privește efortul de a avea un sport egalitar și autentic, avea, de asemenea, legătură cu scopul legitim de a asigura „protejarea drepturilor și a libertății altora", întrucât utilizarea substanțelor dopante pentru a obține rezultate dincolo de cele ale altor sportivi încurajează în mod periculos practicanții amatori, în special tinerii, să utilizeze astfel de procedee pentru a obține succese valorizante și să priveze spectatorii de o competiție loială, la care se așteaptă în mod legitim (*ibidem*, pct. 166).

104. În cauza *Ben Faiza împotriva Franței*, 2018 (pct. 77), Curtea a considerat că solicitarea, adresată de autoritățile de anchetă unui operator de telefonie mobilă și utilizată pentru a solicita date cu caracter personal care nu aveau legătură cu conținutul comunicațiilor, urmărea să permită stabilirea adevărului în contextul unei proceduri penale privind importul de droguri în bandă organizată, constituirea unui grup infracțional organizat și spălare de bani. Prin urmare, această măsură urmărea scopurile legitim de apărare a ordinii, prevenirea faptelor penale și protejarea sănătății publice.

105. În cauza *Adomaitis împotriva Lituaniei* din 2022 (pct. 84), Curtea a concluzionat că interceptarea comunicațiilor telefonice ale reclamantului – un director de penitenciar suspectat de corupție –, păstrarea acestor informații și divulgarea lor în cursul procedurii disciplinare care a condus la concedierea sa au avut ca scop prevenirea actelor de corupție și asigurarea transparenței și a deschiderii în cadrul serviciului public și că aceste măsuri au urmărit, prin urmare, obiectivele legitime

de apărare a ordinii publice și de prevenire a infracțiunilor, precum și de protecție a drepturilor și libertăților celorlalți.

Curtea a emis constatări similare în ceea ce privește înregistrarea conversațiilor cu ajutorul unei camere ascunse de către o persoană într-un cadru profesional, pe care autoritățile le-au utilizat ulterior pentru a dovedi că reclamantul se făcea vinovat de corupție (*Sârbu împotriva României*, 2023, pct. 54).

106. În cauza *López Ribalda și alții împotriva Spaniei* (MC), 2019 (pct. 118 și 123), interesul legitim al unui angajator de a adopta măsuri pentru a descoperi persoanele responsabile pentru pierderile constatate și pentru a le sancționa, cu scopul de a asigura protecția bunurilor sale și buna funcționare a societății, putea justifica măsurile de supraveghere a angajaților săi la locul lor de muncă.

107. Curtea a precizat că publicarea pe portalul internet al serviciilor fiscale a unor informații care permit identificarea reclamantului, inclusiv numele său complet și adresa domiciliului său, ca urmare a nerespectării de către reclamant a obligațiilor sale fiscale, urmărea să protejeze „bunăstarea economică a țării" și „protecția drepturilor și libertăților celorlalți" [*L.B. împotriva Ungariei* (MC), 2023, pct. 111-13]. În aceeași ordine de idei, aceasta a considerat că prelucrarea adresei IP a reclamantului și a altor date de conectare, care a permis Casei de alocații familiale să localizeze persoana vizată în scopul prevenirii fraudei sociale, a fost în interesul bunăstării economice a țării și a vizat prevenirea infracțiunilor [*Le Marrec împotriva Franței* (dec.), 2024, pct. 76].

3. „Necesitatea într-o societate democratică" a ingerinței

108. Pentru a fi „necesară într-o societate democratică", orice măsură care aduce atingere protecției datelor cu caracter personal care intră în domeniul de aplicare al art. 8 trebuie să răspundă unei „nevoi sociale imperioase" și să nu fie disproporționată în raport cu scopurile legitime urmărite (*Z împotriva Finlandei*, 1997, pct. 94; *Khelili împotriva Elveției*, 2011, pct. 62; *Vicent Del Campo împotriva Spaniei*, 2018, pct. 46). Motivele invocate de guvern trebuie să fie relevante și suficiente (*Z împotriva Finlandei*, 1997, pct. 94). Deși este de competența autorităților naționale să se pronunțe asupra îndeplinirii tuturor acestor condiții, responsabilitatea Curții este de a soluționa în final problema necesității ingerinței în raport cu exigențele Convenției [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 101].

109. În cauzele care privesc acte interpersonale de o anumită gravitate care pot aduce atingere art. 8, controlul Curții cu privire la cerința a ceea ce este „necesar într-o societate democratică" privește modul în care statul a asigurat, prin intermediul cadrului legislativ, o protecție adecvată și suficientă a persoanei [*K.U. împotriva Finlandei*, 2008, pct. 43-50; *Söderman împotriva Suediei* (MC), 2013, pct. 80-83). În ceea ce privește actele interpersonale mai puțin grave, cum ar fi, de exemplu, supravegherea lucrătorilor la locul lor de muncă, controlul exercitat de Curte cu privire la cerința a ceea ce este „necesar într-o societate democratică" privește modul în care instanțele naționale au luat în considerare criteriile pe care Curtea le-a stabilit în propria jurisprudență și care permit să se verifice dacă interesele aflate în joc au fost corect puse în balanță [*López Ribalda și alții împotriva Spaniei* (MC), 2019, pct. 116-117, pct. 122]. În contextul controlului criteriilor stabilite, în cazul în care unul dintre elemente lipsește, garanțiile care decurg din alte criterii se vor dovedi cu atât mai importante, și pot compensa elementul deficient (*ibidem*, pct. 131).

110. La un nivel mai general, pentru a verifica dacă o măsură care aduce atingere protecției datelor cu caracter personal care intră în domeniul de aplicare al art. 8 îndeplinește sau nu îndeplinește condiția a ceea ce este „necesar într-o societate democratică", Curtea trebuia să examineze dacă aceasta respecta una dintre cerințele enumerate la art. 5 din Convenția 108, și anume, în special, cerința reducerii la minim a datelor stocate, exactitatea, caracterul adecvat și relevanța acestora în raport cu scopurile pentru care sunt înregistrate, limitarea duratei de păstrare, utilizarea în scopul pentru care au fost colectate și transparența procesului de prelucrare.

a. Cerința de a reduce la minimum datele colectate sau înregistrate

111. Curtea a examinat într-o serie de cauze dacă datele cu caracter personal care făcuseră obiectul unei prelucrări automate au fost adecvate, pertinente și neexcesive în raport cu scopurile pentru care fuseseră înregistrate [*L.L. împotriva Franței*, 2006, pct. 45-46; *Vicent Del Campo împotriva Spaniei*, 2018, pct. 51; *Khadija Ismayilova împotriva Azerbaidjanului*, 2019, pct. 147, *Kruglov și alții împotriva Rusiei*, 2020, pct. 132 *in fine; L.F. împotriva Franței (dec.), 2024, pct. 34]*.

112. Curtea a concluzionat că nu a fost încălcat art. 8: după ce a observat că nicio procedură de filtrare a dispozitivelor de stocare ale reclamanților care ar fi putut reduce la minimum datele confiscate de anchetatori nu fusese urmată în cursul percheziților (*Kruglov și alții împotriva Rusiei*, 2020, pct. 132 *in fine*); în ceea ce privește desemnarea unei persoane, într-o hotărâre judecătorească internă, drept hărțuitor al unei coleg de muncă, în măsura în care judecătorul nu putea să îi indice numele sau să îi menționeze doar inițialele pentru a-i evita stigmatizarea (*Vicent Del Campo împotriva Spaniei*, 2018, pct. 51); în ceea ce privește divulgarea considerată excesivă și inutilă, în contextul unui raport privind stadiul anchetei, a datelor cu caracter personal ale unei jurnaliste care fusese filmată fără știrea sa în intimitatea propriei locuințe (*Khadija Ismayilova împotriva Azerbaidjanului*, 2019, pct. 147).

113. În opinia Curții, dosarele pe care autoritățile naționale trebuie să le constituie pentru a contribui la urmărirea penală și la prevenirea anumitor infracțiuni nu pot fi utilizate în mod excesiv pentru a crește la maxim numărul informațiilor pe care le introduc în dosar (*B.B. împotriva Franței*, 2009, pct. 62; *Gardel împotriva Franței*, 2009, pct. 63; *M.B. împotriva Franței,* 2009, pct. 54). Fără respectarea unei necesare proporționalități în raport cu scopurile legitime care le sunt atribuite, avantajele pe care le aduc ar fi compromise de atingeri grave pe care le-ar cauza drepturilor și libertăților pe care statele trebuie să le asigure persoanelor aflate sub jurisdicția lor (*M. K. împotriva Franței*, 2013, pct. 35; *Aycaguer împotriva Franței*, 2017, pct. 34). În contextul unui sistem de păstrare nediferențiată și nelimitată a datelor cu caracter personal, acceptarea argumentului potrivit căruia cu cât sunt păstrate mai multe date, cu atât ar fi mai mult evitată infracționalitatea, în practică, ar însemna să se justifice stocarea de informații despre întreaga populație și rudele decedate, ceea ce ar fi cu siguranță un fapt excesiv și irelevant (*Gaughran împotriva Regatului Unit*, 2020, pct. 89).

114. În cauza *Catt împotriva Regatul Unit*, 2019 (pct. 122), Curtea a statuat că lipsa unor garanții efective care să permită ștergerea, dintr-o bază de date a poliției, a datelor cu caracter personal care dezvăluiau opiniile politice ale unui protestatar pașnic de îndată ce păstrarea acestor date a devenit disproporționată se consideră o încălcare a art. 8.

115. În schimb, Curtea a statuat că prelucrarea datelor cu caracter personal care nu sunt „sensibile” în sensul articolului 6 din *Convenția 108* respectă cerințele articolului 8, întrucât se limitează la păstrarea într-o bază de date internă a Ministerului Justiției a unor informații factuale și obiective referitoare la procedurile judiciare la care o persoană este parte [*L. F. împotriva Franței* (dec.), 2024, pct. 34 și 40]. În mod similar, în cauza *Le Marrec împotriva Franței* (dec.), 2024, pct. 78-79, Curtea a observat că adresa IP a reclamantului și alte „date de conectare”, a căror prelucrare de către Casa de alocații familiale a permis să se stabilească faptul că acesta locuia într-o „altă țară”, nu erau „sensibile” în sensul prezentat mai sus și nici nu se refereau la aspectele cele mai intime sau la aspecte deosebit de importante ale existenței sau identității persoanei vizate: de fapt, acestea erau informații aproximative privind reclamantul și, prin urmare, marja de apreciere acordată autorităților în această privință era extinsă.

b. Cerința privind exactitatea și actualizarea datelor înregistrate

116. Curtea a trebuit să examineze o serie de cauze care priveau păstrarea, de către autorități, a unor date care s-au dovedit inexacte sau a căror exactitate a fost contestată de partea interesată [*Cemalettin Canlı împotriva Turciei*, 2008, pct. 34-37, care privea prezența unor dosare inexacte ale poliției într-o procedură penală; *Rotaru împotriva României* (MC), 2000, pct. 36, care privea

imposibilitatea de a dezminți datele referitoare la o presupusă participare a unei persoane la o mișcare legionară în trecutul său îndepărtat, colectate de serviciile de informații].

117. Informații cu caracter personal, false sau incomplete, colectate și stocate de autorități pot îngreuna viața de zi cu zi a persoanei vizate (*Khelili împotriva Elveției*, 2011, pct. 64), se pot dovedi defăimătoare [*Rotaru împotriva României* (MC), 2000, pct. 44] sau pot anula o serie de garanții procedurale importante prevăzute de lege pentru a proteja drepturile persoanelor vizate atunci când astfel de date pot fi transmise între diferite autorități (*Cemalettin Canlı împotriva Turciei*, 2008, pct. 42-43). Curtea a subliniat, de asemenea, că este inadecvat să se colecteze date cu caracter personal în absența unei baze factuale dovedite, exclusiv pe baza speculațiilor sau a prezumțiilor (*Drelon împotriva Franței*, 2022, pct. 97).

118. Potrivit Curții, le revine autorităților sarcina de a proba exactitatea datelor care au făcut obiectul unei astfel de stocări. În cauza *Khelili împotriva Elveției*, 2011 (pct. 66-70), în care existau incertitudini cu privire la acuzația vagă și generală de prostituție la adresa reclamantei formulată de autorități, menținerea termenului „prostituată" în dosarul poliției timp de mai mulți ani a fost considerată ca nefiind „necesară într-o societate democratică", având în vedere comportamentul contradictoriu al autorităților, principiul potrivit căruia revenea acestora sarcina de a proba exactitatea unei anumite informații, marja de apreciere redusă de care beneficiau și gravitatea ingerinței în dreptul la respectarea vieții private garantat de art. 8. În mod similar, în cauza *Drelon împotriva Franței,* din 2022 (pct. 95-97), care privea refuzul centrului de transfuzie sanguină francez de a accepta donarea de sânge a reclamantului din cauza pretinsei sale homosexualități, Curtea a observat că colectarea datelor cu caracter personal trebuia să se bazeze pe o bază factuală precisă și exactă, dar că centrul de transfuzie sanguină francez ajunsese la o concluzie cu privire la practicile sexuale ale reclamantului numai pe baza faptului că persoana vizată refuzase să răspundă la întrebări privind sexualitatea sa în timpul interviului medical prealabil donării.

119. În cauza *Anchev împotriva Bulgariei* (dec.), 2017 (pct. 112-115), în care reclamantul făcuse obiectul a trei anchete și fusese denunțat, pe baza arhivelor, drept colaborator al fostelor servicii de securitate în temeiul unei legi privind divulgarea numelor persoanelor titulare de funcții publice despre care se considera că au colaborat cu regimul comunist, Curtea a respins capătul de cerere al reclamantului ca fiind vădit lipsit de temei, după ce a constatat că acesta avusese posibilitatea să consulte arhivele, și ulterior să le conteste în mod public credibilitatea pe baza unor elemente concrete.

120. În cauza *Margari împotriva Greciei* din 2023, pct. 59, în care informațiile publicate în presă cu privire la infracțiunile de care este acuzată reclamanta nu reflectau cu exactitate acuzațiile aduse împotriva sa, Curtea a subliniat că este esențial ca datele publicate în contextul procedurilor penale sau al anchetelor în curs privind infracțiunile să reflecte cu exactitate situația și acuzațiile împotriva inculpatei, respectând în același timp prezumția de nevinovăție.

c. Cu privire la cerința de a limita perioada de păstrare a datelor pentru o perioadă care să nu depășească perioada necesară îndeplinirii scopurilor pentru care au fost înregistrate[4]

121. Problema necesității de a limita durata păstrării datelor cu caracter personal a fost examinată de Curte în mai multe cauze [*S. și Marper împotriva Regatului Unit* (MC), 2008; *B.B. împotriva Franței*, 2009; *Gardel împotriva Franței*, 2009; *M.B. împotriva Franței,* 2009; *M.K. împotriva Franței*, 2013; *J.P.D. împotriva Franței* (dec.), 2014; *Peruzzo și Martens împotriva Germaniei* (dec.), 2013; *W. împotriva Țărilor de Jos* (dec.), 2009; *Brunet împotriva Franței*, 2014; *Drelon împotriva Franței*, 2022,

[4] A se vedea, de asemenea, infra, secțiunea din prezentul ghid privind „Perioada de stocare a datelor".

pct. 98]. O perioadă de păstrare de maximum treizeci de ani în dosarul judiciar automat național al autorilor de infracțiuni sexuale de la expirarea pedepsei cu închisoarea de la cinci la cincisprezece ani pentru viol asupra minorilor nu a fost considerată disproporționată în raport cu scopurile legitime urmărite, prin stocarea de informații, de apărare a ordinii și de prevenire a infracțiunilor (*B.B. împotriva Franței*, 2009, pct. 67-68; *Gardel împotriva Franței*, 2009, pct. 68-69; *M.B. împotriva Franței*, 2009, pct. 59-60).

122. În schimb, păstrarea permanentă, într-o bază de date națională, a amprentelor digitale, a mostrelor biologice și a profilurilor ADN ale persoanelor suspectate de săvârșirea unei infracțiuni, dar necondamnate, indiferent de natura sau gravitatea infracțiunii de care fusese suspectată persoana și indiferent de vârstă, a fost considerată contrară art. 8 [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 125-126]. În cazul unor minori suspectați de săvârșirea unei infracțiuni, dar necondamnați, păstrarea permanentă a datelor lor poate fi deosebit de dăunătoare, având în vedere situația lor specială și importanța dezvoltării și integrării lor în societate (*ibidem*, pct. 124).

123. Acestea fiind spuse, distrugerea imediată a datelor colectate, de îndată ce acestea sunt considerate irelevante pentru colectarea în cauză, în special în cadrul unei măsuri secrete, nu este, în sine, contrară Convenției (*Denisiuk și alții împotriva Ucrainei*, 2025, pct. 108).

124. Lipsa unei perioade maxime de păstrare a datelor cu caracter personal nu este în mod necesar incompatibilă cu art. 8 [*Gaughran împotriva Regatului Unit*, 2020, pct. 88; *Peruzzo și Martens împotriva Germaniei* (dec.), 2013, pct. 46], garanțiile procedurale sunt cu atât mai necesare atunci când stocarea datelor depinde în totalitate de diligența cu care autoritățile se asigură că durata lor de păstrare este proporțională (*ibidem*, pct. 46; *Aycaguer împotriva Franței*, 2017, pct. 44-46). În cauza *Grande Oriente d'Italia împotriva Italiei* din 2024, pct. 144-46, un număr mare de documente, care conțineau în special date cu caracter personal referitoare la membrii asociației reclamante, au fost confiscate în cursul unei percheziții a incintelor acestei asociații, dispusă în cadrul unei anchete parlamentare privind criminalitatea organizată. Curtea a observat că o copie a documentelor confiscate era încă păstrată în arhivele comisiei parlamentare de anchetă, chiar dacă aceasta își încheiase misiunea și fusese dizolvată și că, în conformitate cu dreptul intern, documentele confiscate ar fi trebuit returnate sau copiile lor distruse la sfârșitul anchetei. Curtea a amintit în această privință că lipsa unor norme care să impună distrugerea copiilor documentelor obținute în cursul unei percheziții ar putea fi incompatibilă cu articolul 8 din Convenție.

d. Cerința de a limita utilizarea datelor la scopul pentru care au fost înregistrate

125. Curtea a considerat că este important să se limiteze utilizarea datelor la scopul pentru care au fost înregistrate. Astfel, în cauza *Karabeyoğlu împotriva Turciei*, 2016 (pct. 112-121), utilizarea în contextul unei anchete disciplinare a datelor provenite din interceptarea convorbirilor telefonice în contextul unei anchete penale și, prin urmare, în alt scop decât cel pentru care au fost colectate datele, a fost considerată contrară art. 8.

126. În cauza *Surikov împotriva Ucrainei*, 2017 (pct. 83-95), păstrarea datelor referitoare la sănătatea unei persoane pentru o perioadă foarte lungă și difuzarea și utilizarea acestora în scopuri lipsite de legătură cu motivele pentru care fuseseră colectate inițial au fost considerate o ingerință disproporționată în dreptul la viață privată al persoanei vizate.

127. Problema riscului de utilizare abuzivă a informațiilor cu caracter personal s-a ridicat, de asemenea, în cauza *K.H. și altele împotriva Slovaciei*, 2009 (pct. 45-57), în care reclamantele, opt femei de origine romă care suspectau că ar fi fost sterilizate în timpul ședерii lor în spitale se plângeau că nu au putut obține fotocopii ale dosarelor lor medicale. Curtea a concluzionat că a fost încălcat art. 8, subliniind că, pentru a evita riscul de utilizare abuzivă a informațiilor medicale invocat de guvern, ar fi fost suficient să se pună în aplicare un mecanism legislativ care să vizeze limitarea strictă a cazurilor în care acestea puteau fi utilizate și a numărului persoanelor care puteau avea acces la dosare (*ibidem*, pct. 56).

128. Pentru a stabili limita intimității vieții private garantată de art. 8, Curtea a făcut distincție între supravegherea actelor unei persoane într-un loc public în scopuri de securitate și înregistrările acestor acte utilizate în alte scopuri, care depășiseră ceea ce persoana vizată ar fi putut să prevadă (*Peck împotriva Regatului Unit*, 2003, pct. 59-62, care privea înregistrarea unui reclamant pe un drum public în scopuri de securitate, comunicată către mass-media; *Perry împotriva Regatului Unit*, 2003, pct. 41-42, care privea un subterfugiu utilizat de poliție în scopul identificării video a reclamantului care depășise limitele utilizării normale sau previzibile a camerelor de supraveghere în secțiile de poliție; *Glukhin împotriva Rusiei*, 2023, pct. 65-73, privind utilizarea tehnologiei de recunoaștere facială în contextul supravegherii spațiului public prin intermediul camerelor de supraveghere cu circuit închis).

e. Cerința de transparență a procesului de prelucrare a datelor[5]

129. Într-o serie de cauze care priveau date cu caracter personal colectate și stocate de autoritățile publice, Curtea a considerat că autorităților le revenea obligația pozitivă de a pune la dispoziție persoanelor vizate o „procedură efectivă și accesibilă" care să le permită să aibă acces la „toate informațiile relevante și adecvate" pentru a afla și a-și înțelege copilăria și anii perioadei de formare (*Gaskin împotriva Regatului Unit*, 1989, pct. 49), pentru a-și descoperi identitatea personală (*Odièvre împotriva Franței* (MC), 2003, pct. 41-49], pentru a identifica riscurile pentru sănătate la care au fost expuse [*Roche împotriva Regatului Unit* (MC), 2005, pct. 162; *Guerra și alții împotriva Italiei,* 1998, pct. 60*; McGinley și Egan împotriva Regatului Unit*, 1998, pct. 101), sau pentru a-și rememora parcursul personal în perioada unui fost regim totalitar (*Haralambie împotriva României*, 2009, pct. 93).

130. O astfel de cerință de transparență este mai redusă în contextul informațiilor sensibile pentru securitatea națională [*Leander împotriva Suediei*, 1987, pct. 51; *Segerstedt-Wiberg și alții împotriva Suediei*, 2006, pct. 102; *Dalea împotriva Franței* (dec.), 2010].

II. Protecția datelor cu caracter personal și dreptul la viață privată (art. 8 din Convenție)

Articolul 8 din Convenție

„1. Orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului său și a corespondenței sale.

2. Nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acest amestec este prevăzut de lege și dacă constituie o măsură care, într-o societate democratică, este necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei, ori protejarea drepturilor și libertăților altora. ”

131. Până în prezent, Curtea a examinat un număr mare de operațiuni efectuate în privința datelor cu caracter personal de către autorități sau entități private pentru a examina dacă „viața privată", „domiciliul" și/sau „corespondența" persoanei vizate au fost afectate într-un mod incompatibil cu art. 8. În diferite contexte, a clarificat domeniul de aplicare al mai multor drepturi de care persoanele fizice sau juridice în cauză se puteau prevala pentru a-și proteja datele cu caracter personal.

[5] A se vedea, de asemenea, infra, secțiunea din prezentul ghid privind „Dreptul de acces la datele proprii".

A. Operațiuni în privința datelor care pot aduce atingere dreptului la viață privată

132. Odată cu dezvoltarea tehnologiilor, colectarea, păstrarea sau divulgarea datelor iau forme foarte diferite. Într-o serie de cauze, Curtea a examinat dacă una sau toate aceste operațiuni au condus la o ingerință nejustificată în dreptul la viață privată al persoanei vizate.

1. Colectarea de date cu caracter personal

133. Operațiunea de colectare a datelor cu caracter personal a fost examinată de Curte în diferite contexte: în ceea ce privește lupta împotriva crimei organizate și a terorismului, prin intermediul diferitelor sisteme secrete de supraveghere puse în aplicare de autorități; în contextul judiciar, în ceea ce privește datele cu caracter personal colectate de autorități pentru a fi exploatate ca probe; în contextul sănătății; în contextul datelor colectate la locul de muncă, fie că este vorba de angajatori publici sau privați; și, sfârșit, în contextul obligațiilor legale care le revin entităților publice sau private de a transmite autorităților date cu caracter personal aflate în posesia lor pentru a proteja un interes public general.

a. Colectarea de date de către autorități prin intermediul supravegherii secrete[6]

134. Curtea a trebuit să examineze un număr considerabil de cauze care priveau problema colectării de date cu caracter personal prin intermediul unor diferite metode de supraveghere secretă. Indiferent de sistemul de supraveghere utilizat de autorități, existența unor garanții adecvate și suficiente împotriva abuzurilor este esențială. În opinia Curții, puterea de a supraveghea în secret cetățenii nu este tolerabilă decât în măsura considerată absolut necesară pentru protejarea instituțiilor democratice (*Klass și alții împotriva Germaniei*, 1978, pct. 42; *Szabó și Vissy împotriva Ungariei*, 2016, pct. 72-73). O astfel de ingerință trebuie să se întemeieze pe motive relevante și suficiente și trebuie să fie proporțională cu scopurile legitime urmărite (*Segerstedt-Wiberg și alții împotriva Suediei*, pct. 88). Legislația internă trebuie să fie însoțită de garanții suficient de precise, efective și cuprinzătoare în ceea ce privește dispunerea și executarea de măsurilor de supraveghere și eventualele căi de atac față de acestea (*Szabó și Vissy împotriva Ungariei*, 2016, pct. 89).

i. Interceptarea țintită a convorbirilor telefonice și contorizarea apelurilor telefonice

135. În contextul judiciar, Curtea a constatat o încălcare a art. 8 în ceea ce privește: interceptarea comunicațiilor și transmiterea către poliție a înregistrărilor contorizării apelurilor telefonice (numerele de telefon apelate) (*Malone împotriva Regatului Unit*, 1984, pct. 63-89); ascultarea și transcrierea tuturor apelurilor telefonice comerciale și private ale părților interesate (*Huvig împotriva Franței*, 1990, pct. 24-35); interceptarea și înregistrarea mai multor conversații ale reclamantului prin ascultarea liniei telefonice a unei terțe părți (*Kruslin împotriva Franței*, 1990, pct. 25-36); interceptarea conversațiilor telefonice ale unei persoane prin intermediul liniei telefonice a unei terțe părți (*Lambert împotriva Franței* , 1998, pct. 21-41); interceptarea și înregistrarea de către Ministerul Public a unui apel telefonic primit de o persoană aflată în biroul său de la o altă persoană de la ambasada, la momentul faptelor, sovietică de la Berna [*Amann împotriva Elveției (MC)*, 2000, pct. 45-62]; interceptarea convorbirilor telefonice efectuată în contextul unei anchete preliminare (*Prado Bugallo împotriva Spaniei,*, 2003, pct. 28-33); conversații telefonice interceptate în contextul unei proceduri penale și difuzate ulterior în presă [*Craxi împotriva Italiei (nr. 2)*, 2003, pct. 57-84]; depunerea la dosarul penal al reclamantului a transcrierii convorbirilor telefonice efectuate în contextul unei proceduri în care acesta nu fusese implicat (*Matheron împotriva Franței*, 2005, pct. 27-44); interceptarea comunicațiilor telefonice de către autorități în lipsa unei autorizații din partea procurorului emise pe numele suspectului și în lipsa unei legi care să ofere garanții suficiente împotriva

[6] A se vedea, de asemenea, *Ghidul privind art. 8 din Convenție – dreptul la respectarea vieții private și de familie*.

arbitrarului [*Dumitru Popescu împotriva României (nr. 2)* , 2007, pct. 61-86]; ascultarea comunicărilor telefonice ale unui avocat în contextul unor anchete penale (*Kvasnica împotriva Slovaciei*, 2009, pct. 80-89); garanții insuficiente împotriva caracterului arbitrar în dispozițiile interne privind interceptarea convorbirilor telefonice (*Dragojević împotriva Croației*, 2015, pct. 85-102; *Liblik și alții împotriva Estoniei* , 2019, pct. 132-143; *Denisiuk și alții împotriva Ucrainei*, 2025, pct. 93-135)); lipsa unor garanții judiciare adecvate (*Moskalev împotriva Rusiei*, 2017, pct. 35-45); lipsa unei control eficient al înregistrării comunicațiilor telefonice în contextul unei proceduri penale (*Pruteanu împotriva României*, 2015, pct. 41-58); interceptarea conversațiilor de pe telefonul mobil (*Šantare și Labazņikovs împotriva Letoniei*, 2016, pct. 56-63); lipsa nejustificată a unei notificări *a posteriori* a interceptării temporare a telefonului mobil (*Cevat Özel împotriva Turciei,*, 2016, pct. 29-37); interceptarea preventivă a comunicațiilor telefonice (*Mustafa Sezgin Tanrıkulu împotriva Turciei,* 2017, pct. 45-66); puterea practic nelimitată a serviciilor de informații de a desfășura o operațiune de supraveghere a unei persoane și a întâlnirilor care erau organizate într-un apartament al cărui proprietar era în lipsa unor garanții juridice suficiente (*Zoltán Varga împotriva Slovaciei*, 2021, pct. 170-171), care a afectat în mod aleatoriu și o altă persoană care nu beneficia de nicio protecție în temeiul dreptului intern (*Haščák împotriva Slovaciei*, 2022, pct. 95); și interceptarea, înregistrarea și transcrierea unei conversații telefonice între un avocat și unul dintre clienții săi, fost ministru al apărării, care era supravegheat în secret în contextul unei anchete penale (*Vasil Vasilev împotriva Bulgariei*,, 2021, pct. 167-181).

136. Curtea a constatat că nu a existat o încălcare a art. 8 în ceea ce privea interceptarea convorbirilor telefonice care fusese autorizată prin hotărâre judecătorească și având în vedere faptul că necesitatea măsurii fusese evaluată de instanțe (*İrfan Güzel împotriva Turciei*, 2017, pct. 78-89).

137. Curtea a constatat, de asemenea, că nu a existat o încălcare a art. 8 în ceea ce privește: colectarea de către poliție a numerelor de telefon apelate de o persoană prin plasarea sub contorizare a telefonului său privat (*P.G. și J.H. împotriva Regatului Unit* , 2001, pct. 42-51); și ascultarea liniilor telefonice ale unui magistrat în contextul unei anchete penale privind o organizație ilegală la care acesta era suspectat de apartenență sau de ajutor și susținere (*Karabeyoğlu împotriva Turciei*, 2016, pct. 74-111); și interceptarea convorbirilor telefonice ale unui director de închisoare în cadrul unei anchete privind acte de corupție pe care persoana vizată era suspectată că le-a comis în scopul îmbogățirii personale în cadrul funcției sale, chiar dacă ancheta a fost în cele din urmă întreruptă din lipsă de dovezi suficiente (*Adomaitis împotriva Lituaniei*, 2022, pct. 81-90).

138. O serie de cereri au fost declarate inadmisibile pe motiv de lipsă vădită de temei în ceea ce privește: interceptarea convorbirilor telefonice în contextul unor anchete preventive ale poliției [*Deveci împotriva Turciei* (dec.), 2022]; interceptarea convorbirilor telefonice în contextul unei anchete preliminare [*Greuter împotriva Țărilor de Jos* (dec.), 2002]; interceptarea liniilor telefonice în contextul unei anchete penale, întrucât constituise unul dintre principalele mijloace de investigare care contribuiseră la demonstrarea implicării unor persoane într-un caz important de trafic de droguri [*Coban împotriva Spaniei* (dec.), 2006]; și interceptarea comunicațiilor telefonice unui membru al Parlamentului European acuzat de abuz de bunuri sociale și inaplicabilitatea în această speță a tratamentului special rezervat membrilor Parlamentului [*Marchiani împotriva Franței* (dec.), 2008].

139. În contextul detenției în penitenciar, înregistrarea și păstrarea convorbirilor telefonice ale unui deținut de către autoritățile penitenciare, care nu erau prevăzute de lege, și utilizate ulterior ca probe pentru condamnarea deținutului pentru o altă infracțiune au condus la o încălcare a art. 8 în cauza *Doerga împotriva Țărilor de Jos*, 2004 (pct. 43-54).

140. În diverse alte domenii, Curtea a constatat o încălcare a art. 8 în ceea ce privește: un regim de supraveghere generală și nediferențiată a corespondenței și a convorbirilor telefonice ale minorilor plasați într-o școală internat cu regim închis, excluzând orice tip de confidențialitate, fără nicio distincție în ceea ce privește tipul de schimburi interceptate (*D.L. împotriva Bulgariei*, 2006, pct. 100-116); interceptarea de către Ministerul Apărării, pe baza unui mandat, a comunicărilor către exterior

ale unor organizații care își desfășurau activitatea în domeniul libertăților civile (*Liberty și alții împotriva Regatului Unit*, 2008, pct. 56-70); simpla existență a unei legislații care permitea interceptarea telecomunicațiilor unei organizații neguvernamentale moldovenești, specializată în reprezentarea reclamanților în fața Curții (*Iordachi și alții împotriva Moldovei*, 2009, pct. 29-54); scurgerile de informații în mass-media și difuzarea unei conversații private înregistrate, cu aprobarea autorităților, de la o linie telefonică a unui om politic, care era anchetat de organele de urmărire penală (, 2012, pct. 62); deficiențele cadrului juridic care reglementa supravegherea secretă a comunicațiilor mobile pusă în aplicare de operatorii de telefonie mobilă, care permiteau Serviciului Federal de Securitate să intercepteze orice comunicații telefonice fără autorizație judiciară prealabilă [*Roman Zakharov împotriva Rusiei* (MC), 2015, pct. 163-305]; și utilizarea în contextul unei anchete disciplinare a datelor provenite din interceptarea convorbirilor telefonice obținute în contextul unei anchete penale (*Karabeyoğlu împotriva Turciei*, 2016, pct. 112-121); utilizarea transcrierii unei conversații cu un client prin intermediul interceptării telefonică, în contextul unei proceduri disciplinare împotriva unei avocate (*Versini-Campinchi și Crasnianski împotriva Franței*, 2016, pct. 49-84). În schimb, Curtea a constatat că utilizarea, în cadrul unei proceduri disciplinare împotriva unui director de penitenciar, a informațiilor care au fost colectate prin intermediul unei interceptări dispuse în cadrul unei anchete penale privind fapte de corupție pe care persoana vizată era suspectată că le-a săvârșit era proporțională (*Adomaitis împotriva Lituaniei*, 2022, pct. 87).

ii. Interceptarea mesajelor primite prin pager

141. În contextul procedurilor judiciare, interceptarea de către poliție a mesajelor reclamantului primite prin pager și trimiterea ulterioară la aceste mesaje pentru a constitui temeiul unei condamnări au fost considerate, în cauza *Taylor-Sabori împotriva Regatului Unit,* 2002, pct. 18-19, contrare art. 8, în lipsa unui cadru juridic care să reglementeze această formă de interceptare.

iii. Supravegherea audiovizuală și supravegherea video

142. Curtea a concluzionat că a fost încălcat art. 8 în cazul în care înregistrarea unei conversații prin intermediul unui dispozitiv de transmisie radio ca parte a unei operațiuni secrete a poliției nu fusese însoțită de garanții procedurale [*Bykov împotriva Rusiei* (MC), 2009, pct. 81, 83; *Oleynik împotriva Rusiei*, 2016, pct. 75-79].

143. Curtea a făcut distincție între supravegherea actelor unei persoane într-un loc public în scopuri de securitate și înregistrările acelor acte utilizate în alte scopuri, depășind ceea ce persoana vizată ar fi putut să prevadă (*Peck împotriva Regatului Unit*, 2003, pct. 59-62; *Perry împotriva Regatului Unit*, 2003, pct. 41-42) pentru a stabili, în domeniul măsurilor de supraveghere secretă sau al interceptării comunicațiilor de către autoritățile publice, limita vieții private garantate de art. 8. Aceasta a subliniat, de asemenea, caracterul foarte intruziv al tehnologiei de recunoaștere facială, în special tehnologia de recunoaștere facială în timp real utilizată pentru supravegherea locurilor publice prin intermediul camerelor de supraveghere cu circuit închis, care a permis poliției să identifice și să aresteze reclamantul, în timp ce acesta călătorea cu metroul, pentru că fusese implicat într-o demonstrație individuală fără o declarație prealabilă. Curtea a subliniat că este necesar un nivel ridicat de justificare pentru ca aceste măsuri să fie considerate „necesare, într-o societate democratică", cel mai înalt nivel de justificare fiind necesar pentru utilizarea tehnologiilor de recunoaștere facială în timp real (*Glukhin împotriva Rusiei*, 2023, pct. 86).

144. În contextul judiciar, Curtea a concluzionat că a fost încălcat art. 8 în ceea ce privește: înregistrarea vocilor reclamanților în momentul punerii sub acuzare și în interiorul celulei acestora din secția de poliție (*P.G. și J.H. împotriva Regatului Unit*, 2001, pct. 56-63); înregistrarea video cu ajutorul unei camere de televiziune cu circuit închis ascunse, în scopul identificării, a unui suspect într-o secție de poliție (*Perry împotriva Regatului Unit*, 2003, pct. 36-49); înregistrarea de către poliție, prin instalarea unui dispozitiv de ascultare în locuința unui terț pe care îl vizitase reclamantul, a unei conversații spontane și neprovocate în cursul căreia reclamantul recunoscuse că era complice într-o

rețea de import de droguri (*Khan împotriva Regatului Unit*, 2000, pct. 25-28); montarea de microfoane de către poliție într-o locuință privată în contextul unei anchete judiciare (*Vetter împotriva Franței*, 2005, pct. 20-27); înregistrarea unei conversații cu ajutorul unui dispozitiv de ascultare instalat pe corp de către autoritățile polițienești și utilizarea acesteia ulterioară ca probă esențială în contextul procesului penal, fără a fi singura probă incriminatoare (*Heglas împotriva Republicii Cehe*, 2007, pct. 71-76); înregistrarea comunicațiilor de către o persoană particulară în contextul și în beneficiul unei anchete oficiale, penală sau de altă natură, cu complicitatea și asistența tehnică a autorităților publice de anchetă (*Van Vondel împotriva Țărilor de Jos*, 2007, pct. 47-55). În schimb, aceasta nu a constatat nicio încălcare într-o cauză privind utilizarea în cadrul procedurilor penale a înregistrărilor video ale conversațiilor dintre reclamant și o persoană într-un context profesional, înregistrări pe care persoana vizată le-a realizat din proprie inițiativă cu ajutorul unei camere video ascunse și pe care autoritățile le-au descoperit cu ocazia examinării computerului unui terț pe care au fost salvate (*Sârbu împotriva României*, 2023, pct. 48-59).

145. În contextul detenției în penitenciar, Curtea a concluzionat că a fost încălcat art. 8 în ceea ce privește: utilizarea de către autorități a unor dispozitive de înregistrare video și audio plasate fără știrea reclamantului în celula acestuia și în zona de vizitare a penitenciarului, precum și în persoana unui codetinut care a făcut posibilă înregistrarea declarațiilor nespontane și neprovocate ale reclamantului (*Allan împotriva Regatului Unit*, 2002, pct. 35-36); înregistrarea discuțiilor deținuților cu rudele lor la vorbitor în penitenciare (*Wisse împotriva Franței*, 2005, pct. 28-34); supravegherea secretă a consultărilor unui deținut cu avocatul său (*R.E. împotriva Regatului Unit*, 2015, pct. 115-143); și supravegherea video continuă a deținuților din celulele lor cu ajutorul unei camere de televiziune cu circuit închis ascunse (*Gorlov și alții împotriva Rusiei*, 2019, pct. 83-100).

146. Curtea a concluzionat că art. 8 nu a fost încălcat în ceea ce privește supravegherea secretă a consultărilor deținutului cu persoana desemnată să îl asiste, în calitate de persoană vulnerabilă, după arestarea sa (*R.E. împotriva Regatului Unit*, 2015, pct. 154-168). Dispozițiile care prevedeau posibilitatea de a supraveghea consultările dintre un deținut vulnerabil și un adult calificat fuseseră însoțite de garanții suficiente împotriva abuzurilor.

147. În diferite contexte în care colectarea datelor fusese realizată prin intermediul unor camere ascunse, Curtea a concluzionat că a fost încălcat art. 8 în ceea ce privește: transmiterea către mass-media a unui material video provenit de la o cameră de televiziune cu circuit închis ascunsă, filmând o persoană care încerca să se sinucidă într-un loc public (*Peck împotriva Regatului Unit*, 2003, pct. 57-87); difuzarea la televiziune a imaginii fără a fi obturată sau acoperită a unei persoane private obținute prin intermediul unei camere video ascunse (*Bremner împotriva Turciei*, 2015, pct. 71-85); înregistrarea video secretă a unei jurnaliste în locuința sa și difuzarea acestor înregistrări video către public (*Khadija Ismayilova împotriva Azerbaidjanului*, 2019, pct. 108-132).

iv. Geolocalizarea unui vehicul prin GPS[7]

148. Supravegherea prin GPS a unei persoane suspectate de terorism nu a constituit o încălcare a art. 8 în cauza *Uzun împotriva Germaniei*, 2010 (pct. 49-81). În schimb, în cauza *Ben Faiza împotriva Franței*, 2018 (pct. 53-61), plasarea unui dispozitiv de geolocalizare într-un vehicul și exploatarea datelor rezultate din această măsură, care au permis anchetatorilor să cunoască, în timp real, mișcările reclamantului și apoi să procedeze la arestarea acestuia, au fost considerate contrare art. 8.

v. Supravegherea de către detectivi particulari

149. Supravegherea ilegală de către detectivi particulari a activităților unui beneficiar de prestații sociale în litigiu a condus la constatarea unei încălcări a art. 8 în cauza *Vukota-Bojić împotriva Elveției*, 2016 (pct. 52-78). Dreptul intern nu indica suficient de clar amploarea și modalitățile de exercitare a

[7] A se vedea, de asemenea, supra, partea din prezentul ghid privind „Date de localizare GPS”.

puterii discreționare conferite societăților de asigurare, acționând în calitate de autorități publice în litigiile în materie de asigurări, pentru a efectua supravegherea în secret a asiguraților.

vi. Monitorizarea corespondenței

150. În contextul detenției în penitenciar, Curtea a concluzionat că a fost încălcat art. 8 în ceea ce privește: confiscarea și reținerea corespondenței unui deținut (*Lavents împotriva Letoniei*, 2002, pct. 136-137); deschiderea corespondenței deținutului, inclusiv în cazul unei funcționări defectuoase a serviciului poștal din unitatea penitenciară (*Demirtepe împotriva Franței*, 1999, pct. 26-28; *Valašinas împotriva Lituaniei*, 2001, pct. 128-130); interceptarea și cenzurarea corespondenței unui deținut [*Silver și alții împotriva Regatului Unit*, 1983, pct. 84-105; *Labita împotriva Italiei* (MC), 2000, pct. 176-184; *Niedbała împotriva Poloniei*, 2000, pct. 78-84; *Messina împotriva Italiei (nr. 2)*, 2000, pct. 78-83]; interceptarea scrisorilor deținuților către avocații lor (*Ekinci și Akalın împotriva Turciei*, 2007, pct. 37-48); interceptarea corespondenței deținuților cu avocatul și cu Comisia Europeană a Drepturilor Omului (*Campbell împotriva Regatului Unit*, 1992, pct. 32-54; *A.B. împotriva Țărilor de Jos*, 2002, pct. 81-94); deschiderea corespondenței adresate unui deținut de către Comisie (, 2001, pct. 81-84); supravegherea corespondenței unui deținut cu medicul specialist care îi urmărea starea de sănătate (*Szuluk împotriva Regatului Unit*, 2009, pct. 47-55); practica scanării și înregistrării în sistemul informatic al Rețelei Judiciare Naționale a corespondenței deținuților – atât a celei pe care doreau să o trimită, cât și a celei care le-a fost trimisă (*Nuh Uzun împotriva Turciei*, 2022, pct. 80-99). În schimb, în cauza *Erdem împotriva Germaniei*, 2001 (pct. 53-70), monitorizarea corespondenței dintre o persoană suspectată de terorism și avocatul său nu a condus la constatarea unei încălcări a art. 8.

151. Într-un alt context, corespondența unei persoane care dăduse faliment și care fusese copiată de mandatarul-lichidator a condus la o încălcare a art. 8 (*Foxley împotriva Regatului Unit*, 2000, pct. 27-47).

vii. Operațiuni secrete de supraveghere, spionaj, supraveghere în masă

152. În cauza *Roman Zakharov împotriva Rusiei* (MC), 2015 (pct. 171-172), Curtea a admis că un reclamant ar putea pretinde că este victima unei încălcări care rezultă din simpla existență a unor măsuri de supraveghere secretă sau a unei legislații care permite astfel de măsuri dacă sunt îndeplinite anumite condiții. Curtea a considerat, de asemenea, că abordarea urmată în cauza *Kennedy împotriva Regatului Unit*, 2010 (pct. 124) era cel mai bine adaptată necesității de a veghea că caracterul secret al măsurilor de supraveghere nu determină ca acestea să fie în practică inatacabile și să scape de sub controlul autorităților judiciare naționale și al Curții. În cauza *Ekimdzhiev și alții împotriva Bulgariei*, 2022 (pct. 262-277 și 371-384), aceasta a admis, pe baza principiilor pe care le-a dezvoltat în cauza *Roman Zakharov împotriva Rusiei* (MC), 2015 (pct. 171), că reclamanții, doi avocați și două organizații neguvernamentale asociate acestora ar putea pretinde că sunt victime ale unei ingerințe în exercitarea de către aceștia a drepturilor lor consacrate la articolul 8 pentru simplul motiv că există o legislație sau practici interne care autorizează supravegherea secretă, precum și legi care reglementează accesul autorităților la datele privind comunicațiile păstrate (a se vedea de asemenea *Podchasov împotriva Rusiei*, 2024, pct. 54-55, pentru o abordare similară în ceea ce privește obligația legală a furnizorilor de servicii de comunicații prin internet de a stoca conținutul comunicațiilor pe internet și datele privind comunicațiile asociate, de a acorda, la cerere, acces la astfel de date forțelor de ordine și serviciilor de securitate și, dacă este cazul, de a decripta mesajele electronice criptate).

153. Curtea a concluzionat că a fost încălcat art. 8 în ceea ce privește: posibilitatea asociației reclamante de a face obiectul unor măsuri de supraveghere în orice moment, fără avertisment, în temeiul legii privind mijloacele de supraveghere speciale (*Asociația pentru integrarea europeană și drepturile omului și Ekimdjiev împotriva Bulgariei*, 2007, pct. 69-94); interceptarea și înregistrarea unei conversații prin intermediul unui aparat de radiotransmisie în contextul unei operațiuni secrete a poliției fără garanții procedurale [*Bykov împotriva Rusiei* (MC), 2009, pct. 72-83]; înregistrarea conversațiilor desfășurate în contextul unui test operativ la inițiativa Serviciului Federal de Securitate,

care nu era „prevăzută de lege” (*Oleynik împotriva Rusiei*, 2016, pct. 74-79); interceptarea de către Ministerul Apărării, pe baza unui mandat, a comunicațiilor către exterior ale unor organizații care își desfășurau activitatea în domeniul libertăților civile (*Liberty și alții împotriva Regatului Unit*, 2008, pct. 55-70); înregistrarea și supravegherea de către poliție a unui reclamant ca urmare a apartenenței sale la o organizație pentru apărarea drepturilor omului (*Shimovolos împotriva Rusiei*, 2011, pct. 64-71); legislația în materie de supraveghere secretă prin care era înființat un grup operativ special în materie de combatere a terorismului, în lipsa unor garanții suficiente împotriva abuzurilor (*Szabó și Vissy împotriva Ungariei*, 2016, pct. 52-89); păstrarea informațiilor colectate prin supraveghere secretă [*Rotaru împotriva României* (MC), 2000, pct. 45-63; *Asociația „21 decembrie 1989” și alții împotriva României*, 2011, pct. 169-177); diferitele deficiențe ale cadrului juridic național care reglementa supravegherea secretă a comunicațiilor de telefonie mobilă [*Roman Zakharov împotriva Rusiei* (MC), 2015, pct. 163-305]; și regimuri de interceptare în masă a comunicațiilor care nu conțineau suficiente garanții „de la un capăt la altul” pentru a oferi o protecție adecvată și efectivă împotriva arbitrarului și a riscului de abuzuri, în pofida anumitor garanții solide pe care le conțineau [*Centrum för rättvisa împotriva Suediei* (MC), 2021, pct. 365-374, și *Big Brother Watch și alții împotriva Regatului Unit* (MC), 2021, pct. 424-427]. În cauza *Ekimdzhiev și alții împotriva Bulgariei*, 2022 (pct. 356-359 și 419-421), aceasta a constatat, de asemenea, o încălcare a articolului 8: Curtea a observat, în special, că, în pofida îmbunătățirilor semnificative de la examinarea sa în cauza *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdjiev împotriva Bulgariei*, 2007, legislația privind supravegherea secretă, astfel cum a fost aplicată în practică, încă nu oferea, în mai multe privințe, garanțiile minime împotriva arbitrariului și a abuzurilor pe care ar fi trebuit să le ofere. La aceeași concluzie s-a ajuns și în ceea ce privește legile privind păstrarea datelor privind comunicațiile și accesul autorităților la astfel de date. În aceeași ordine de idei, Curtea a statuat în cauza *Pietrzak și Bychawska-Siniarska și alții împotriva Poloniei*, 2024 (pct. 195-278) că două legi poloneze care permit măsuri de supraveghere secretă și păstrarea și prelucrarea datelor privind comunicațiile nu oferă garanții suficiente împotriva arbitrariului.

154. În cauza *Denisiuk și alții împotriva Ucrainei*, 2025 (pct. 93-135 și pct. 148-50), trei reclamanți au făcut obiectul unor măsuri de supraveghere secretă în contextul operațiunilor polițienești desfășurate în contextul procedurilor penale care îi priveau. Aceste măsuri de supraveghere secretă ar fi putut conduce la interceptarea comunicărilor lor cu al patrulea reclamant, un avocat, ceea ce ar fi adus atingere confidențialității relațiilor dintre avocat și client. Având în vedere, pe de o parte, faptul că reclamanților li s-a refuzat accesul, fără nicio evaluare comparativă a intereselor concurente în cauză, la deciziile judiciare prin care a fost autorizată punerea în aplicare a măsurilor de supraveghere, pentru simplul motiv că aceste decizii erau „clasificate”, pe de altă parte, lipsa unor norme sau directive interne precise care să prevadă procedura care trebuie urmată pentru identificarea și prelucrarea comunicărilor confidențiale dintre un avocat și clientul său care au fost interceptate accidental sau instituirea unei autorități independente responsabile cu monitorizarea interceptării comunicațiilor private; și (iii) în lipsa unor garanții procedurale suficiente pentru a controla *a posteriori* legalitatea și necesitatea ingerinței în cauză și pentru a oferi o cale de atac adecvată în cazul unei pretinse încălcări a drepturilor garantate de articolul 8, Curtea a concluzionat că ingerința în cauză nu era „prevăzut[ă] de lege” și că, prin urmare, a existat o încălcare a articolului 8 din Convenție

155. Curtea a concluzionat că nu a fost încălcat art. 8 în ceea ce privește: utilizarea unui agent infiltrat, împreună cu ascultarea conversațiilor telefonice ale reclamantului, acuzat de trafic de droguri (*Lüdi împotriva Elveției*, 1992, pct. 38-41); un regim care autoriza supravegherea secretă a corespondenței, a trimiterilor poștale și a comunicațiilor telefonice ale populației (*Klass și alții împotriva Germaniei*, 1978, pct. 39-60); un cadru legislativ care permitea interceptarea comunicațiilor interne pentru a combate terorismul și infracțiunile grave (*Kennedy împotriva Regatului Unit*, 2010, pct. 151-170).

156. Curtea a declarat vădit nefondată cauza *Weber și Saravia împotriva Germaniei* (dec.), 2006 (pct. 143-153), care privea supravegherea în scopuri strategice a telecomunicațiilor, cauză care a urmat cauzei *Klass și alții împotriva Germaniei*, 1978.

b. Colectarea de date de către angajatori la locul de muncă

157. Curtea a examinat, din perspectiva art. 8, problema colectării de date cu caracter personal la locul de muncă de către angajatori din sectorul public (*Halford împotriva Regatului Unit*, 1997, pct. 49, 45; *Antović și Mirković împotriva Muntenegrului*, 2017, pct. 58; *Libert împotriva Franței*, 2018, pct. 41) sau privat [*Köpke împotriva Germaniei*(dec.), 2010; *Bărbulescu împotriva României* (MC), 2017, pct. 109; *López Ribalda și alții împotriva Spaniei* (MC), 2019, pct. 109]. Într-o serie de cauze, operațiunea de colectare avusese loc fără cunoștință persoanei vizate subiectul datelor, în cursul supravegherii secrete, în totalitate [*Halford împotriva Regatului Unit*, 1997, pct. 49; *Copland împotriva Regatului Unit*, 2007, pct. 45; *Bărbulescu împotriva României* (MC), 2017, pct. 78) sau în parte (*López Ribalda și alții împotriva Spaniei* (MC) ,2019, pct. 93], în timp ce, în alte cauze, colectarea fusese făcută la vedere și cu cunoștința angajaților vizați (*Antović și Mirković împotriva Muntenegrului*, 2017, pct. 44).

158. Datele cu caracter personal vizate de colectare provin din: monitorizarea convorbirilor telefonice neprofesionale din spații profesionale (*Halford împotriva Regatului Unit*, 1997, pct. 44); monitorizarea telefonului, a mesageriei electronice și a Internetului la locul de muncă (*Copland împotriva Regatului Unit*, 2007, pct. 44-49); monitorizarea utilizării Internetului și a mesageriei instantanee (Yahoo) (*Bărbulescu împotriva României*[MC], 2017, pct. 74); deschiderea fișierelor stocate de un angajat pe un calculator pus la dispoziția acestuia de angajatorul său pentru a-și exercita atribuțiile (*Libert împotriva Franței*, 2018, pct. 25); imagini captate prin intermediul unei înregistrări video care arată comportamentul unui angajat identificat sau identificabil la locul său de muncă [*Köpke împotriva Germaniei* (dec.), 2010; *Antović și Mirković împotriva Muntenegrului*, 2017, pct. 44; *López Ribalda și alții împotriva Spaniei* (MC), 2019, pct. 92]; sau monitorizarea, prin intermediul unui sistem GPS, a distanțelor parcurse de vehiculul de serviciu al unui angajat în cursul activităților sale profesionale și, după caz, în timpul călătoriilor private (*Florindo de Almeida Vasconcelos Gramaxo împotriva Portugaliei*, 2022, pct. 94-96).

159. În primele două hotărâri în acest domeniu (*Halford împotriva Regatului Unit*, 1997, pct. 44, *Copland împotriva Regatului Unit*, 2007, pct. 41), Curtea a considerat că apelurile telefonice în scopuri neprofesionale de la sediile societăților puteau fi incluse în noțiunile „viață privată” și „corespondență” în sensul art. 8. A considerat, de asemenea, că mesajele electronice trimise de la locul de muncă trebuie să beneficieze de aceeași protecție în temeiul art. 8, la fel ca în cazul probelor colectate prin monitorizarea utilizării Internetului de către o persoană (*Copland împotriva Regatului Unit*, 2007, pct. 41). Ulterior, Curtea a precizat, de asemenea, că datele identificate în mod clar ca fiind private și stocate de un angajat pe un calculator pus la dispoziția acestuia de angajatorul său în scopul exercitării atribuțiilor sale pot intra în sfera „vieții private” a acestuia (*Libert împotriva Franței*, 2018, pct. 25). În plus, o înregistrare video efectuată în secret care prezintă comportamentul angajatului la locul de muncă fără a-l avertiza aduce atingere, de asemenea, „vieții private” [*Köpke împotriva Germaniei* (dec.), 2010]. Ulterior, Curtea nu a identificat niciun motiv pentru a se abate de la această constatare, și anume dacă privește supravegherea video secretă sau nesecretă a angajaților la locul lor de muncă [*Antović și Mirković împotriva Muntenegrului*, 2017, pct. 44; *López Ribalda și alții împotriva Spaniei* (MC), 2019, pct. 93].

160. În cauzele *Halford împotriva Regatului Unit*, 1997 (pct. 50-51) și *Copland împotriva Regatului Unit,* 2007 (pct. 48), Curtea a hotărât că, în lipsa, la momentul faptelor, unei dispoziții de drept intern care să autorizeze colectarea de date cu caracter personal provenite din apelurile telefonice cu caracter neprofesional ale angajaților și, respectiv, din mesajele electronice trimise de la locul de muncă, atingerea adusă dreptului lor la respectarea vieții private nu era „prevăzută de lege”. În cauza *Köpke împotriva Germaniei* (dec.), 2010, Curtea a declarat vădit nefondat capătul de cerere întemeiat pe colectarea de date de către un angajator cu ajutorul unei agenții de detectivi particulari, prin supravegherea video în secret a unui casiere a unui supermarket, suspectată de furt. Chiar dacă, la momentul faptelor, condițiile în care un angajator putea recurge la supravegherea video a unui angajat nu erau încă prevăzute în legislație, jurisprudența Curții federale pentru litigii de muncă

dezvoltase garanții importante împotriva ingerințelor arbitrare la adresa dreptului unui angajat la respectarea vieții sale private

161. Existența unor motive verosimile de a bănui că au fost comise nereguli grave și amploarea deficiențelor constatate ar putea să pară justificări serioase pentru măsurile de colectare de date cu caracter personal luate de angajatori la locul de muncă [*López Ribalda și alții împotriva Spaniei* (MC), 2019, pct. 134]. În schimb, simpla suspiciune că angajații au comis furturi sau alte delicte nu poate justifica recurgerea la supraveghere secretă de către angajator (*ibidem*, pct. 134).

162. În cauza *Bărbulescu împotriva României* (MC), 2017 (pct. 121), Curtea a definit o serie de criterii pe care trebuie să le respecte măsurile de control al corespondenței și al comunicărilor angajaților la locul de muncă pentru a nu fi încălcat art. 8. În acest context, autoritățile naționale trebuie să țină seama de următorii factori: A fost informat angajatul asupra posibilității angajatorului de a adopta măsuri de monitorizare corespondența și a celorlalte comunicări ale sale, precum și cu privire la punerea în aplicare a unor astfel de măsurii? Care au fost amploarea monitorizării efectuate de angajator și gradul de intruziune în viața privată a angajatului? A invocat angajatorul motive pentru a justifica monitorizarea comunicărilor angajatului? Ar fi fost posibilă instituirea unui sistem de monitorizare bazat pe mijloace și măsuri mai puțin intruzive decât accesul direct la conținutul comunicărilor angajatului? Care au fost consecințele monitorizării pentru angajatul care a fost supus la aceasta? I s-au oferit angajatului garanții corespunzătoare, în special atunci când măsurile de monitorizare ale angajatorului au avut un caracter intruziv? În cele din urmă, pentru a asigura aplicarea efectivă a acestor cerințe, angajații în cauză trebuie să beneficieze de o cale de atac în fața unui organ judiciar independent care să aibă competența de a se pronunța, cel puțin pe fond, cu privire la respectarea acestor criterii, precum și asupra legalității măsurilor contestate (*ibidem*, pct. 122).

163. Ulterior, în cauza *López Ribalda și alții împotriva Spaniei* (MC), 2019 (pct. 116), Curtea a precizat că aceste criterii puteau fi transpuse măsurilor de supraveghere video pe care un angajator le pune în aplicare la locul de muncă. În cauza *Florindo de Almeida Vasconcelos Gramaxoîmpotriva Portugaliei* din 2022 (pct. 115), Curtea a aplicat aceste criterii și în contextul monitorizării GPS pe care un angajator a instituit-o pentru a monitoriza distanțele parcurse de un angajat cu vehiculul de serviciu.

164. Curtea a concluzionat că a fost încălcat art. 8 în cauzele în care a constatat că instanțele naționale nu se asiguraseră că punerea în aplicare de către angajator a unor măsuri de supraveghere era proporțională și însoțită de garanții adecvate și suficiente. În cauza *Bărbulescu împotriva României* (MC), 2017 (pct. 108-141), instanțele judecătorești naționale nu stabiliseră motivele specifice care să justifice punerea în aplicare a unor măsuri de supraveghere, sau dacă angajatorul ar fi putut să utilizeze măsuri mai puțin intruzive pentru viața privată și corespondența angajatului sau dacă acesta din urmă fusese informat în prealabil de către angajator cu privire la posibilitatea ca comunicările sale să fie monitorizate. În schimb, în cauza *Libert împotriva Franței*, 2018 (pct. 37-53), Curtea a concluzionat că nu a fost încălcat art. 8 în ceea ce privește deschiderea fișierelor personale stocate pe un calculator profesional, al cărui conținut pornografic descoperit a fost considerat ca fiind temeiul concedierii angajatului, după ce a observat că dreptul intern, astfel cum era interpretat și aplicat de instanțele judecătorești naționale, conținea suficiente garanții împotriva arbitrariului, în special faptul că angajatorul nu putea deschide fișiere identificate ca fiind personale decât în prezența angajatului.

165. În opinia Curții, doar un imperativ predominant legat de protecția unor interese publice sau private importante ar putea justifica nefurnizarea de către angajator a unor informații prealabile cu privire la măsurile care pot afecta protecția datelor angajaților [*López Ribalda și alții împotriva Spaniei* (MC), 2019, pct. 133]. Înainte de a pune în aplicare măsuri de colectare a datelor lor, angajatorii trebuie să informeze în mod clar angajații cu privire la existența și la modalitățile unei astfel de colectări, chiar dacă doar la modul general (*ibidem*, pct. 131). Cerința de transparență și dreptul la informare care rezultă din aceasta sunt fundamentale, în special în contextul raporturilor de muncă, unde angajatorul dispune de prerogative importante față de angajați a căror utilizare abuzivă ar trebui evitată. Cu toate acestea, informațiile furnizate persoanei care face obiectul monitorizării și amploarea

acestora nu reprezintă decât unul dintre criteriile care trebuie luate în considerare la evaluarea proporționalității unei astfel de măsuri într-o situație particulară. În cazul în care aceste informații nu sunt furnizate, garanțiile care decurg din alte criterii vor avea mai multă importanță (*ibidem*, pct. 131).

166. În cazul lipsei unei informări prealabile, este important să se știe dacă angajații care fac obiectul unei măsuri de supraveghere dispuneau de căi de atac la nivel național special concepute pentru a asigura protecția efectivă a dreptului la viață privată. În contextul măsurilor impuse salariaților la locul de muncă, o astfel de protecție poate fi asigurată prin diferite mijloace, care pot fi reglementate de dreptul muncii, dar și de dreptul civil (*ibidem*, pct. 136).

167. În ceea ce privește, mai precis, supravegherea video a angajaților, Curtea a precizat în cauza *López Ribalda și alții împotriva Spaniei* (MC), 2019 (pct. 125), că era necesar să se facă distincția, în analiza proporționalității, între diferitele locuri în care s-a realizat monitorizarea în raport cu așteptarea în materie de protecție a vieții private pe care angajatul o poate avea în mod rezonabil. Această așteptare este foarte importantă în spațiile care țin de intimitate, cum ar fi toaletele sau vestiarele, unde se justifică o protecție sporită sau chiar o interdicție a supravegherii video (*ibidem*, pct. 125, 61, 65, care citează instrumentele internaționale relevante). Rămâne însă ridicată în spații de muncă închise, cum ar fi birourile. Este vădit mai redusă în locuri vizibile sau accesibile colegilor sau unui public larg (*ibidem*, pct. 125).

168. În această privință, în cauza *Köpke împotriva Germaniei* (dec.), 2010, Curtea a declarat inadmisibilă, pe motiv de lipsă vădită de temei, capătul de cerere al reclamantei, casieră într-un supermarket, privind o măsură de supraveghere video secretă pusă în aplicare de angajatorul său cu ajutorul unei agenții de detectivi particulari. Curtea a observat în special că măsura în litigiu fusese limitată în timp (două săptămâni) și nu privise decât spațiul accesibil publicului și din apropierea casei de marcat, că probele video obținute fuseseră prelucrate de un număr limitat de persoane care lucrau pentru agenția de detectivi și de personalul angajatorului, și că nu fuseseră utilizate decât în contextul concedierii reclamantei și al procedurii în fața instanțelor pentru litigii de muncă.

169. În schimb, în *Antović și Mirković împotriva Muntenegrului*, 2017 (pct. 55-60), Curtea a concluzionat că a fost încălcat art. 8, considerând că pretinsa încălcare a vieții private a reclamanților, doi profesori universitari, rezultată din instalarea unui sistem de supraveghere video în spațiile de predare, nu era prevăzută de lege.

170. În cauza *López Ribalda și alții împotriva Spaniei* (MC), 2019 (pct. 137), Curtea a concluzionat că nu a fost încălcat art. 8 în ceea ce privește o supraveghere video parțial vizibilă și parțial ascunsă a casierelor și a vânzătoarelor dintr-un supermarket, ținând seama, printre altele, de garanțiile importante oferite de cadrul legislativ spaniol, inclusiv căile de atac pe care reclamantele nu le utilizaseră.

171. În mod similar, cauza *Florindo de Almeida Vasconcelos Gramaxo împotriva Portugaliei* din 2022 (pct. 105-125) privea concedierea reclamantului pe baza datelor de kilometraj colectate prin intermediul unui sistem GPS instalat de angajatorul reclamantului pe vehiculul său de serviciu. Curtea a concluzionat că articolul 8 nu a fost încălcat pentru motivul că instanțele naționale evaluaseră în mod corect interesele concurente în cauză, și anume, pe de o parte, dreptul reclamantului la respectarea vieții sale private și, pe de altă parte, dreptul angajatorului la buna funcționare a întreprinderii sale, ținând seama de obiectivul legitim urmărit de întreprindere, și anume dreptul de a-și controla cheltuielile.

172. Principii similare se aplică și în alte contexte, în special în ceea ce privește controlul de către un partid politic al comunicațiilor electronice ale membrilor săi, chiar dacă structurile organizaționale interne ale partidelor politice diferă de cele ale întreprinderilor private, iar legăturile juridice dintre un angajator și un angajat și dintre un partid politic și membrii săi sunt fundamental diferite (*Tena Arregui împotriva Spaniei*, 2024, pct. 38 și 41).

c. Colectarea de date pentru a fi utilizate ca probe în cauze

173. Colectarea de probe materiale în cauze ridică probleme legate de protecția datelor cu caracter personal ale persoanelor, indiferent de poziția acestora în cadrul procedurilor în cauză, indiferent dacă sunt părți, martori sau simple părți terțe.

i. Confiscări și percheziții

174. Într-o serie de cauze, Curtea a subliniat că statele contractante pot considera necesar să recurgă la măsuri precum percheziții și confiscări pentru a obține probe materiale ale anumitor infracțiuni (*Vasylchuk împotriva Ucrainei*, 2013, pct. 79; *K.S. și M.S. împotriva Germaniei*, 2016, pct. 43). Controlul privește așadar relevanța și caracterul suficient al motivelor invocate pentru a justifica astfel de măsuri, precum și respectarea principiului proporționalității în raport cu scopul urmărit (*Smirnov împotriva Rusiei*, 2007, pct. 44). Gravitatea infracțiunii care a motivat percheziția și sechestrul, circumstanțele în care a fost emis mandatul, în special celelalte probe disponibile la momentul faptelor, conținutul și întinderea mandatului, având în vedere, în special, natura spațiilor percheziționate și garanțiile luate pentru ca măsura să nu aibă efecte nerezonabile, modul în care s-a desfășurat percheziția, și întinderea posibilelor repercusiuni asupra vieții private a persoanei vizate sunt elemente importante care trebuie luate în considerare în momentul punerii în balanță a diferitelor interese aflate în joc (*ibidem*, pct. 44; *Modestou împotriva Greciei*, 2017, pct. 42 și trimiterile citate). Curtea solicită, de asemenea, ca dreptul intern să ofere garanții adecvate și suficiente împotriva arbitrariului (*Vinci Construction și GTM Génie Civil et Services împotriva Franței*, 2015, pct. 66; *Modestou împotriva Greciei*, 2017, pct. 43; *Reznik împotriva Ucrainei*, 2025, pct. 58). Existența unui „control eficient” al măsurilor care încalcă art. 8 figurează printre aceste garanții (*Modestou împotriva Greciei*, 2017, pct. 42).

175. În cauza *Trabajo Rueda împotriva Spaniei*, 2017 (pct. 44-47), o măsură de confiscare a calculatorului personal al reclamantului care permisese accesul poliției la toate arhivele personale stocate pe calculator pe motiv că conținea materiale pornografice cu minori a fost considerată contrară art. 8. Curtea nu a fost convinsă de urgența care ar fi constrâns poliția să confiște arhivele computerului personal al reclamantului și să acceseze toate datele stocate fără a obține în prealabil autorizația judiciară necesară în mod normal, chiar dacă această autorizație ar fi putut fi obținută relativ rapid.

176. În cauza *K.S. și M.S. împotriva Germaniei*, 2016 (pct. 32-58), Curtea a considerat ca nefiind contrară art. 8 percheziția efectuată la domiciliul reclamanților în temeiul unui mandat emis pe baza unor informații care conțineau date cu caracter personal, copiate în mod ilegal de un angajat al unei bănci și apoi vândute serviciilor secrete, referitoare la activele acestora într-o bancă din străinătate. Legislația și practica germane ofereau garanții adecvate și efective împotriva abuzurilor. Iar instanțele naționale nu își depășiseră marja de apreciere atunci când și-au întemeiat mandatul de percheziție pe date provenite din străinătate. Printre altele, Curtea a acordat o importanță deosebită faptului că, la momentul emiterii mandatului de percheziție, setul de date în cauză era unul dintre puținele seturi care fusese achiziționat de autoritățile germane (*ibidem*, pct. 51). De asemenea, simplul fapt că nu exista nicio normă absolută care să interzică utilizarea într-o procedură penală a unor probe obținute cu încălcarea normelor de procedură nu însemna că autoritățile colectaseră în mod deliberat datele cu încălcarea dreptului internațional și a dreptului intern (*ibidem*, pct. 51). În plus, suportul de date nu conținea nicio informație strâns legată de identitatea reclamanților, ci doar informații referitoare la situația lor financiară, pe care erau obligați să le transmită autorităților fiscale naționale (*ibidem*, pct. 53; a se compara cu cauza *G.S.B. împotriva Elveției*, 2015, pct. 93, care privea transmiterea de date bancare către autoritățile fiscale ale unui alt stat, în temeiul unui acord bilateral).

177. Perchezițiile efectuate la sediile societăților pentru a colecta probe materiale ridică probleme legate de protecția datelor, din perspectiva dreptului la respectarea „corespondenței” și a „domiciliului” acestora, garantat de art. 8. De exemplu, în cauza *Bernh Larsen Holding AS și alții*

împotriva Norvegiei, 2013 (pct. 104-175), Curtea a concluzionat că nu a fost încălcat art. 8 în ceea ce privește o decizie prin care o societate era obligată să prezinte o copie a datelor complete de pe serverul informatic pe care îl partaja cu alte societăți. Chiar dacă legea aplicabilă nu impunea autorizarea prealabilă din partea unei autorități judiciare, Curtea a luat în considerare existența unor garanții efective și adecvate împotriva abuzurilor, interesele atât ale societăților, cât și ale angajaților acestora, și interesul public legat de realizarea de controale fiscale eficiente (*ibidem*, pct. 172-175). În schimb, Curtea a concluzionat că a fost încălcat art. 8 în cauza *DELTA PEKÁRNY a.s. împotriva Republicii Cehe*, 2014 (pct.92-93), care privea inspecția unor spații comerciale pentru a căuta indicii și probe privind existența unei înțelegeri ilicite privind prețurile, contrară regulilor de concurență. Curtea a făcut trimitere la lipsa unei autorizări prealabile din partea unei instanțe, a unui control *a posteriori* efectiv al necesității măsurii și a unei reglementări privind posibila distrugere a datelor obținute.

178. În cauza *Buck împotriva Germaniei*, 2005 (pct. 30-53), perchezițiile la domiciliu și la sediile profesionale în legătură cu o infracțiune rutieră comisă de un terț au constituit o încălcare a art. 8. Ținând seama de circumstanțele speciale ale cauzei, în special faptul că percheziția și sechestrul în cauză fuseseră dispuse în legătură cu o simplă contravenție, considerată a fi fost comisă de un terț, și că acestea vizaseră deopotrivă și domiciliul privat al reclamantului, Curtea a concluzionat că ingerința nu putea fi considerată proporțională cu scopurile legitime urmărite (*ibidem*, pct. 52).

179. În ceea ce privește perchezițiile spațiilor profesionale ale jurnaliștilor, ale locuințelor și ale vehiculelor acestora și confiscările în masă în scopul identificării surselor acestora, Curtea a concluzionat că a fost încălcat art. 8 în cauza *Ernst și alții împotriva Belgiei*, 2003 (pct. 110-117). În materie de luptă împotriva încălcării secretului urmăririi penale, legislația statelor contractante și practica acestora, care pot să prevadă percheziții la domiciliu și confiscări, trebuie să ofere garanții adecvate și suficiente împotriva abuzurilor. Or, nu aceasta ar fi situația în speță, întrucât reclamanții nu fuseseră acuzați de nicio infracțiune, iar diferitele mandate de percheziție fuseseră redactate în termeni generali, fără a oferi nicio informație cu privire la urmărirea penală în cauză, locațiile exacte care trebuiau să fie percheziționate și obiectele care trebuiau să fie confiscate, conferind astfel puteri extinse anchetatorilor. În plus, reclamanții nu fuseseră informați despre motivele concrete ale percheziților (a se vedea, de asemenea, infra, pct. 355 din prezentul ghid referitor la încălcarea art. 10 în această cauză).

180. În ceea ce privește confiscările operate în cabinetul de avocatură al unui avocat, acestea trebuiau să fie însoțite de garanții procedurale speciale, capabile să păstreze confidențialitatea datelor, care stă la baza relației de încredere care există între avocat și clientul său[8]. În cauza *Kırdök și alții împotriva Turciei*, 2019 (pct. 52-58), confiscarea datelor electronice ale mai multor avocați de către autoritățile judiciare în contextul unei proceduri penale îndreptate împotriva unui alt avocat care împărțea același birou cu aceștia și refuzul de a le restitui sau de a le distruge au condus la o încălcare a art. 8. Curtea a acordat importanță faptului că, în timpul percheziției, nu fusese respectată nicio procedură de filtrare a documentelor sau a datelor electronice protejate de secretul profesional. Iar refuzul de a restitui datele confiscate pe motiv că, întrucât nu fuseseră încă transcrise, nu se putea stabili cui îi aparțineau, nu era prevăzut în mod clar de lege și era contrar esenței însești a secretului profesional, care impunea confidențialitatea acestor date.

181. În cauza *Kruglov și alții împotriva Rusiei*, 2020 (pct. 123-138), Curtea a considerat că confiscările de calculatoare și de hard diskuri care conțineau informații cu caracter personal și documente care intrau sub incidența secretului profesional al reclamanților, avocaților sau clienților acestora în cursul percheziților efectuate de poliție la domiciliile și birourile lor, fără să fi filtrat datele astfel confiscate, erau contrare art. 8. Printre altele, existența unei autorizații judiciare prealabile a avut un efect limitat, întrucât instanțele judecătorești naționale nu au încercat niciodată să pună în balanță obligația de a

[8] A se vedea, de asemenea, *Ghid privind art. 8 din Convenție – dreptul la respectare a vieții private și de familie* pentru detalii suplimentare privind garanțiile procedurale aplicabile confiscărilor operate în cabinetele de avocatură.

proteja confidențialitatea datelor cu nevoile anchetei penale, de exemplu, prin examinarea posibilității de a obține informații din alte surse (*ibidem*, pct. 126-129). La un nivel mai general, Curtea consideră drept o ingerință disproporționată în drepturile protejate de art. 8 din Convenție inclusiv faptul că dispozitivele electronice ale unui avocat, care pot conține elemente acoperite de secretul profesional, sunt confiscate, retrase și consultate de reprezentanți ai autorităților fără a fi necesar niciun control extern sau nicio altă garanție (*Reznik împotriva Ucrainei*, 2025, pct. 76 și trimiterile citate în aceasta).

182. De asemenea, Curtea a concluzionat că a fost încălcat art. 8 în cauza *Smirnov împotriva Rusiei*, 2007 (pct. 36-49), care privea perchezițiile și confiscările a numeroase documente și unitatea centrală a computerului unui avocat, efectuate la domiciliul acestuia, fără nicio justificare sau garanție; în cauza *Wieser și Bicos Beteiligungen GmbH împotriva Austriei*, 2007 (pct. 42-68), care privea perchezițiile și confiscarea datelor electronice ale unui avocat cu încălcarea garanțiilor procedurale prevăzute de lege; în cauza *Robathin împotriva Austriei*, 2012 (pct. 52), care privea autorizarea insuficient motivată pentru percheziția și confiscarea tuturor datelor electronice dintr-un cabinet de avocatură; în cauza *Särgava împotriva Estoniei*, 2021 (pct. 107-108), care privea garanțiile procedurale considerate insuficiente pentru a proteja datele acoperite de secretul profesional în momentul confiscării, apoi al examinării calculatorului și telefonului mobil al unui avocat; și în cauza *Reznik împotriva Ucrainei*, 2025 (pct. 73-77), privind garanțiile procedurale insuficiente pentru a asigura protecția drepturilor garantate de art. 8 reclamantului, un avocat al cărui domiciliu a fost percheziționat în contextul unei proceduri penale îndreptate împotriva clientului său și ale cărui dispozitive de stocare a datelor au fost confiscate, apoi examinate de experți.

183. În cauza *Vinci Construction et GTM Génie Civil et Services împotriva Franței*, 2015 (pct. 69-81), Curtea a concluzionat că a fost încălcat art. 8 ca urmare a percheziției și confiscării datelor informatice ale societăților, inclusiv a mesajelor electronice confidențiale referitoare la relațiile dintre un avocat și clientul său. Instanța sesizată, deși avea cunoștință despre prezența corespondenței unui avocat printre documentele reținute de anchetatori, se limitase la a evalua legalitatea cadrului formal al confiscărilor în litigiu, fără a efectua examinarea concretă care se impunea.

184. În cauza *André și alții împotriva Franței*, 2008 (pct. 37-49), percheziția la domiciliu și confiscarea documentelor dintr-un cabinet de avocatură de către agenții administrației fiscale în vederea descoperirii unor probe incriminatoare împotriva unei societăți cliente a acestui cabinet constituise o încălcare a art. 8. Scopul vizitei la domiciliu în litigiu era acela de a descoperi la sediul reclamanților, în singura lor calitate de avocați ai societății suspectate de fraudă, documente de natură să probeze pretinsa fraudă și să le utilizeze împotriva acesteia. Reclamanții nu au fost niciodată acuzați sau suspectați de comiterea unei infracțiuni sau de participarea la o fraudă comisă de clientul lor (*ibidem*, pct. 46).

185. Un nou sechestru, efectuat la cinci minute după restituirea materialelor confiscate ilegal, a constituit o încălcare a art. 8 în cauza *Visy împotriva Slovaciei*, 2018 (pct. 33-47). Reclamantul nu a putut beneficia de garanții efective împotriva arbitrariului și a abuzurilor în ceea ce privește cel de-al doilea sechestru.

186. În materie de terorism, în cauza *Sher și alții împotriva Regatului Unit*, 2015 (pct. 171-176), Curtea a fost sesizată cu privire la problema unui mandat de percheziție extins în cazul unor suspiciuni de activități teroriste. În opinia sa, complexitatea unor astfel de cauze era de natură să justifice o percheziție întemeiată pe termeni mai largi decât cei admisibili în mod normal. În cazul în care s-ar impune, în temeiul art. 8, obligația de a descrie în detaliu într-un mandat de percheziție natura exactă a probelor care trebuie căutate și confiscate, ar exista riscul de a compromite în mod grav eficacitatea anchetei, în cazurile în care numeroase vieți sunt potențial în pericol. În astfel de cauze, este necesar să i se acorde poliției o anumită flexibilitate să evalueze, pe baza probelor descoperite în cursul percheziției, pe cele care pot fi legate de activități teroriste și să le confișteze pentru o examinare mai amplă (*ibidem*, pct. 74).

187. În ceea ce privește puterea autorităților vamale de a consulta și de a copia datele electronice ale persoanelor de drept privat, în cauza *Ivashchenko împotriva Rusiei*, 2018 (pct. 59-95), a fost încălcat art. 8, în lipsa unor motive verosimile de a bănui fapte ilicite. Percheziționarea laptopului reclamantului, copierea datelor sale personale și profesionale și comunicarea lor ulterioară în scopul expertizării, precum și păstrarea acestor date pe o perioadă aproximativ doi ani au depășit ceea ce ar putea fi considerat ca fiind proceduri „de rutină" care să nu fie intruzive, pentru care se dă în general consimțământul. Reclamantul nu a fost în măsură să aleagă dacă dorea să se prezinte la vamă împreună cu bunurile sale și să fie expus unui eventual control al acestora. (A se vedea, de asemenea, cauza *Gillan și Quinton împotriva Regatului Unit,* 2010, pct. 61-67, care privea puterea conferită de a aresta și de a percheziționa persoane fără a exista o bănuială întemeiată că au săvârșit o infracțiune, constituind încălcare a art. 8. Curtea a precizat în cauza respectivă că natura publică a percheziției, care implică disconfortul cauzat de faptul că informațiile cu caracter personal sunt expuse altora, poate chiar să agraveze, în anumite cazuri, ingerința în viața privată a persoanei vizate prin adăugarea unui element de umilire și rușine. Puterea discreționară de care se bucură orice polițist constituie un motiv de îngrijorare: polițistul nu numai că nu este obligat să demonstreze existența unei bănuieli întemeiate pentru a suspecta o infracțiune, dar nici măcar nu este obligat să aibă vreo suspiciune subiectivă cu privire la persoana care face obiectul opririi în vederea efectuării unui control și al percheziționării).

ii. Acte medicale obligatorii cu scopul de a colecta mostre de celule

188. În general, recursul la diverse acte medicale obligatorii cu scopul de a preleva mostre de celule, precum mostre de sânge sau de salivă, nu este interzisă ca atare, în contextul administrării de probe în contextul procedurilor civile sau penale [*Jalloh împotriva Germaniei* (MC), 2006, pct. 70; *Caruana împotriva Maltei* (dec.), 2018, pct. 41; *D.H. și alții împotriva Macedoniei de Nord*, 2023, pct. 52].

189. În cauza *D.H. și alții împotriva Macedoniei de Nord d* din 2023 (pct. 52-53), în special, Curtea a considerat că decizia de a preleva probe de sânge de la reclamante, lucrătoare sexuale, pentru motivul că erau suspectate de răspândirea bolilor cu transmitere sexuală, respecta cerințele articolului 8, întrucât actul medical a fost dispus de un judecător și efectuat de un medic într-o clinică, iar reclamanta nu a susținut în niciun moment că a fost supusă în acest context unei utilizări excesive a forței sau că actul în cauză a avut efecte dăunătoare asupra sănătății sale. Prin urmare, aceasta a respins capătul de cerere în cauză pentru motivul că era vădit nefondat.

190. În cauza *Mikulić împotriva Croației*, 2002 (pct. 64), Curtea a considerat că lipsa unor mijloace de natură să forțeze presupusul tată să efectueze un test ADN nu era compatibilă cu principiul proporționalității decât dacă ar fi fost oferite alte mijloace prin care să poată fi asigurate interesele reclamantului în acțiunea în stabilirea paternității. Curtea a constatat o încălcare a art. 8 ca urmare a lipsei unor astfel de motive în dreptul intern, privând persoana vizată de incertitudinea privind identitatea sa personală, fără întârzieri inutile, în fața refuzului presupusului său tată de a efectua teste ADN (*ibidem*, pct. 65-66).

191. În cauza *Mifsud împotriva Maltei*, 2019 (pct. 61-78), ordinul impus reclamantului, de către instanțele naționale, de a se supune unui test genetic împotriva voinței sale, în cadrul unei proceduri de recunoaștere de paternitate în temeiul dreptului maltez, nu era contrară art. 8. Înainte de a dispune ca persoana vizată să se supună unui test ADN, instanțele interne au efectuat necesara punere în balanță a intereselor în cauză, în cadrul unei proceduri judiciare la care reclamantul a participat, reprezentat de avocatul ales de acesta, și în care drepturile sale procedurale au fost respectate în aceeași măsură ca și cele ale părții adverse. Instanțele naționale au păstrat astfel un just echilibru între interesul presupusei fiice a reclamantului de a stabili o legătură de paternitate și cel al reclamantului de a nu fi supus unui test ADN (*ibidem*, pct. 77). În ansamblu, procesul decizional a fost echitabil și a protejat în mod corespunzător interesele reclamantului protejate de art. 8.

192. În cauza *Boljević împotriva Serbiei*, 2020 (pct. 50-56), respingerea pe motiv de prescripție, de către instanțele judecătorești naționale, a unei cereri de reexaminare a unei decizii definitive pronunțate cu patruzeci de ani în urmă, care admisese acțiunea în tăgada paternității a unei persoane de sex masculin și în care nu existau teste ADN, a fost considerată de Curte contrară art. 8. În viziunea acesteia, faptul că termenele prevăzute în procedura recunoașterii de paternitate erau menite să protejeze securitatea juridică nu constituia un motiv suficient pentru a priva reclamantul de dreptul de a cunoaște adevărul cu privire la un aspect important al identității sale personale, fără a pune în balanță interesele aflate în joc în cazul său. Dreptul intern referitor la termenele de redeschidere a procedurii nu permitea autorităților să efectueze o astfel de punere în balanță, ținând seama de circumstanțele foarte specifice ale cauzei reclamantului, și anume faptul că acesta nu luase la cunoștință de procedura recunoașterii de paternitate decât atunci când persoana despre care credea că este tatăl său biologic decedase. Potrivit Curții, viața privată a unei persoane decedate nu putea, în orice caz, să fie afectată de o cerere de prelevare de ADN. Curtea ajunsese în prealabil la aceeași decizie în cauzele *Succession Kresten Filtenborg Mortensen împotriva Danemarcei* (dec.), 2006, care privea exhumarea unei persoane decedate în vederea efectuării unor teste genetice, și *Jäggi împotriva Elveției*, 2006 (pct. 42), în care refuzul instanțelor de a autoriza o expertiză ADN asupra unui defunct, solicitată de presupusul său fiu care dorea să stabilească cu certitudine filiația, constituise o încălcare a art. 8 (*ibidem*, pct. 34-44).

193. În cauza *Caruana împotriva Maltei* (dec.), 2018 (pct. 28-42), Curtea a declarat vădit nefondat un capăt de cerere întemeiat pe obligația potrivit căreia soția presupusului autorului al unui omor a fost supusă unei prelevări de mostre de celule din cavitatea bucală. În viziunea sa, prelevarea de mostre de celule din cavitatea bucală constituie un act de importanță minoră care, în general, nu cauzează nici vătămări fizice, nici suferințe fizice sau morale. Întrucât omorul reprezintă o infracțiune gravă, fusese atât rezonabil, cât și necesar să fie colectate cât mai multe probe posibil (*ibidem*, pct. 41). În plus, Curtea a făcut distincție între situația unui martor și cea a unui inculpat, al cărui refuz de a se supune unei astfel de măsuri în contextul unei proceduri penale poate avea impact asupra unei eventuale constatări a vinovăției și asupra sancțiunilor aferente refuzului (*ibidem*, pct. 40).

194. În cauza *Dragan Petrović împotriva Serbiei*, 2020 (pct. 79-84), prelevarea de mostre de celule din cavitatea bucală în contextul unei anchete asupra unui omor a constituit o încălcare a art. 8, în lipsa unor dispoziții legale previzibile. Astfel, faptul că reclamantul acceptase să dea agenților de poliție o mostre de salivă nu era relevant pentru a se stabili dacă existase sau nu o ingerință în viața sa privată, întrucât nu făcuse acest lucru decât sub amenințarea, în caz de refuz, a unei prelevări a unei mostre de sânge prin coerciție (*ibidem*, pct. 79).

195. Curtea a concluzionat, de asemenea, că a fost încălcat art. 8 în ceea ce privește colectarea datelor medicale ale unor membri ai organizației Martorii lui Iehova care refuzaseră să facă transfuzii de sânge (*Avilkina și alții împotriva Rusiei*, 2013); a se vedea, de asemenea, infra, pct. 188 din prezentul ghid.

196. Prelevarea de organe pentru transplant fără cunoștința și fără consimțământul rudelor apropiate ale persoanei decedate (*Petrova împotriva Letoniei*, 2014, pct. 87-98) și lipsa de precizie din dreptul național cu privire la consimțământul rudelor apropiate pentru prelevarea de probe de țesut din corpul unei persoane decedate (*Elberte împotriva Letoniei*, 2015, pct. 105-117) au constituit încălcări ale art. 8.

d. Colectarea de date cu caracter personal în contextul sănătății

197. Curtea a trebuit să abordeze problema colectării de date sensibile în domeniul sănătății. În cauza *L.H. împotriva Letoniei*, 2014 (pct. 47-60), colectarea de date medicale privind o pacientă dintr-un spital public de către o agenție de stat („agenția”) responsabilă cu monitorizarea calității asistenței medicale a fost considerată ca nefiind conformă cu art. 8, în lipsa unei legi formulate cu precizie care să protejeze împotriva arbitrariului. Agenția colectase datele în cauză pentru o perioadă de șapte ani, fără deosebire și fără a face o evaluare prealabilă pentru a stabili dacă acestea ar fi decisive, relevante

sau importante pentru atingerea scopului urmărit de anchetă. Agenția nu era obligată să solicite și să obțină consimțământul pentru colectarea datelor din partea persoanei vizate (*ibidem*, pct. 53). Întinderea datelor private care puteau fi colectate nu era limitată (*ibidem,* pct. 57). În plus, relevanța și caracterul suficient al motivelor colectării nu par să fi fost examinate de instanțele judecătorești naționale (*ibidem*, pct. 57). În aceste circumstanțe, obligația legală a agenției de a păstra confidențialitatea datelor cu caracter personal devenea, în opinia Curții, mai puțin relevantă (*ibidem*, pct. 58).

198. În cauza *Surikov împotriva Ucrainei*, 2017 (pct. 75-95), colectarea și păstrarea datelor cu caracter personal referitoare la sănătatea mintală a unei persoane pentru o perioadă extrem de îndelungată, precum și difuzarea și utilizarea acestora în scopuri lipsite de legătură cu motivele colectării lor inițiale au constituit o ingerință disproporționată în dreptul la viața privată al persoanei vizate, cu încălcarea art. 8. Deși angajatorii pot avea interesul legitim de a obține informații despre sănătatea angajaților lor, în special în contextul atribuirii anumitor funcții legate de aptitudini, responsabilități sau competențe specifice, colectarea și prelucrarea informațiilor relevante trebuie să fie licite și de natură să asigure un just echilibru între interesele angajatorului și preocupările candidatului în ceea ce privește viața sa privată (*ibidem*, pct. 91).

199. În cauza *Z împotriva Finlandei*, 1997 (pct. 106-110), Curtea a concluzionat că nu a fost încălcat art. 8 în ceea ce privește confiscarea dosarelor medicale și adăugarea acestora la dosarul anchetei fără consimțământul prealabil al pacientei în cursul procedurii penale inițiate împotriva soțului acesteia. Procesul decizional nu generase nicio neregulă și se pare că existau căi de atac disponibile pentru a contesta confiscarea și pentru a anula perioada indicată în ordin în ceea ce privește confidențialitatea.

200. În cauza *Drelon împotriva Franței*, 2022 (pct. 79-100), reclamantul a încercat să doneze sânge unui centru de colectare a sângelui din Franța, care i-a respins cererea din cauza pretinsei sale homosexualități. Chiar dacă reclamantul ar fi refuzat să răspundă la întrebările referitoare la sexualitatea sa care i-au fost adresate în timpul interviului medical prealabil donării, datele ar fi inclus o contraindicație specifică bărbaților care au întreținut relații sexuale cu un bărbat. După ce a luat act de caracterul lor sensibil, Curtea a admis că colectarea și stocarea datelor în cauză se întemeiau pe motive pertinente și suficiente, și anume protecția sănătății și necesitatea de a asigura siguranța transfuziilor. În același timp, Comisia a observat că datele colectate s-au bazat pe simple speculații și nu pe o bază factuală dovedită. Aceasta a subliniat, de asemenea, caracterul excesiv al perioadei de păstrare a datelor, care a permis utilizarea repetată a acestora împotriva reclamantului, ceea ce a condus la excluderea sa automată de la donarea de sânge. Având în vedere aceste elemente, Curtea a constatat încălcarea art. 8 din Convenție

e. Transmiterea obligatorie de date cu caracter personal

201. Obligația care le revine operatorilor de telefonie mobilă, furnizorilor de servicii de Internet, instituțiilor bancare, sportivilor de top și spitalelor, de a transmite autorităților datele cu caracter personal de care dispun în temeiul unei legi sau al unui ordin al autorităților, a fost examinată de Curte într-o serie de cauze.

202. În ceea ce privește lupta împotriva criminalității organizate și a terorismului, Curtea a acceptat că metodele de anchetă trebuie adaptate la mijloacele de comunicare moderne. În cauza *Breyer împotriva Germaniei*, 2020 (pct. 81-110), obligația legală a operatorilor de telefonie mobilă de a colecta date cu caracter personal de la utilizatorii cartelelor SIM preplătite și de a le pune la dispoziția autorităților, în temeiul unei legi privind telecomunicațiile care autoriza diferite autorități publice să solicite extragerea și transmiterea unor astfel de date fără a fi necesară o hotărâre judecătorească sau notificarea persoanelor vizate, nu a fost considerată contrară art. 8. Păstrarea datelor nu viza decât un set limitat de date și nu era păstrată nicio dată referitoare la anumite comunicații; astfel, ingerința fusese relativ limitată (*ibidem*, pct. 92-95). În plus, existaseră anumite garanții: asigurarea securității tehnice, o perioadă de păstrare limitată, date limitate la informațiile necesare pentru identificarea

clară a abonatului vizat; posibilitățile de consultare și utilizare ulterioară a datelor păstrate reglementate; supravegherea de către o autoritate independentă; și posibilitatea oferită oricărei persoane care considera că i-au fost încălcate drepturile de a face recurs, chiar dacă nivelul examinării și al controlului nu era un element decisiv în aprecierea proporționalității colectării și păstrării setului limitat de date în discuție în speță (*ibidem*, pct. 96-107).

203. În schimb, Curtea a considerat că punerea în aplicare a unei obligații legale care impunea furnizorilor de servicii de Internet să extragă datele de conectare păstrate de la unul dintre abonații lor și să le transmită poliției a constituit o încălcare a art. 8, întrucât dispozițiile legale utilizate de poliție nu erau clare și nu ofereau nicio protecție împotriva unei ingerințe arbitrare, în special în lipsa unei supravegheri independente a puterilor poliției în speță (*Benedik împotriva Sloveniei*, 2018, pct. 132-134).

204. În cauza *Sommer împotriva Germaniei*, 2017 (pct. 63), inspectarea contului bancar al unui avocat a constituit o încălcare a art. 8, având în vedere pragul redus al acestei inspecții, întinderea cererilor de informații, divulgarea ulterioară, stocarea continuă a informațiilor cu caracter personal și insuficiența garanțiilor procedurale.

205. În ceea ce privește colectarea datelor medicale ale unor membri ai organizației Martorii lui Iehova care refuzaseră să facă transfuzii de sânge, Curtea a considerat, în cauza *Avilkina și alții împotriva Rusiei*, 2013 (pct. 54), că colectarea de către parchet a datelor referitoare la reclamanți de la unitățile medicale care îi îngrijiseră, fără a informa persoanele vizate cu privire la aceste date și fără a le da posibilitatea de a se opune, fusese contrară art. 8. Pentru a da curs plângerilor pe care le primise împotriva organizației religioase în cauză, parchetul dispunea de alte mijloace, cum ar fi să interogheze persoanele vizate sau să le solicite consimțământul (*ibidem*, pct. 48).

206. În cauza *Fédération nationale des associations et syndicats de sportifs (FNASS) și alții împotriva Franței*, 2018 (pct. 155-191), obligația legală impusă sportivilor de top, înscriși într-un „grup țintă", de a transmite în prealabil informații privind localizarea lor în vederea efectuării de controale inopinate pentru a combate dopajul, sub sancțiunea aplicării unor sancțiuni în cazul a trei încălcări pe parcursul unei perioade de optsprezece luni consecutive, nu a fost considerată contrară art. 8. Fără a subestima impactul pe care îl au obligațiile de localizare asupra vieții private a reclamanților, Curtea a considerat că reducerea sau suprimarea obligațiilor impuse sportivilor de top ar crește pericolele dopajului pentru sănătatea lor și pentru sănătatea întregii comunități sportive și ar fi contrară comunității europene și internaționale de viziuni cu privire la necesitatea efectuării de controale inopinate (*ibidem*, pct. 191).

207. În cauza *Aycaguer împotriva Franței*, 2017 (pct. 45-47), Curtea a concluzionat că a fost încălcat art. 8, întrucât condamnarea penală a reclamantului pe motiv că a refuzat să se supună prelevării de probe biologice obligatorii în vederea înregistrării profilului său ADN în registrul național automatizat al persoanelor condamnate nu putea fi considerată o măsură necesară într-o societate democratică. Acțiunile reclamantului care dăduseră naștere obligației de a se supune prelevării de probe biologice obligatorii se înscriau într-un context politic și sindical și priveau simple lovituri de umbrelă aplicate unor jandarmi neidentificați, pentru care fusese condamnat la două luni de închisoare cu suspendare. Or, nu era prevăzută nicio diferențiere în sistemul național computerizat de date genetice în funcție de natura și de gravitatea infracțiunii săvârșite, în pofida decalajelor semnificative între situațiilor care pot apărea, precum cea a reclamantului (*ibidem*, pct. 43). În sfârșit, reclamantul nu avusese acces la o procedură pentru ștergerea datelor stocate (procedură prevăzută numai pentru persoanele suspectate, nu și pentru cele condamnate) (*ibidem*, pct. 43).

2. Păstrarea datelor cu caracter personal

208. Stocarea de către o autoritate publică a datelor referitoare la viața privată a unei persoane, indiferent de modul în care au fost obținute, constituie o ingerință în dreptul la respectarea vieții private al persoanei vizate, în sensul art. 8, indiferent dacă aceste date au fost sau nu au fost utilizate

ulterior [*Amman împotriva Elveției* (MC), 2000, pct. 69; *Rotaru împotriva României* (MC), 2000, pct. 46; *S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 67; *M.K. împotriva Franței,* 2013, pct. 29; *Aycaguer împotriva Franței,* 2017, pct. 33]. Având în vedere caracterul intrinsec privat al acestor informații, Curtea trebuie să efectueze o examinare riguroasă a oricărei măsuri luate de un stat pentru a autoriza păstrarea lor de către autorități fără consimțământul persoanei vizate [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 104].

a. Culegerea de date în scopul combaterii criminalității

209. Interesul persoanelor vizate și al comunității în ansamblu în protejarea datelor cu caracter personal nu poate prevala în fața interesului legitim pe care în constituie prevenirea infracțiunilor [*S. și Marper împotriva Regatului Unit*(MC), 2008, pct. 104]. Pentru a proteja populația astfel cum au obligația de a o face, autoritățile naționale pot să creeze fișiere de date care să contribuie în mod eficient la reprimarea și prevenirea anumitor infracțiuni, în special a celor mai grave, cum ar fi cele de natură sexuală (*B.B. împotriva Franței*, 2009, pct. 62; *Gardel împotriva Franței*, 2009, pct. 63; *M.B. împotriva Franței,* 2009, pct. 54; *N.F. și alții împotriva Rusiei*, 2023, pct. 44).). Deși colectarea inițială a datelor cu caracter personal are ca scop să lege o anumită persoană de infracțiunea de care este suspectată că a comis-o, păstrarea acestor date în fișiere și baze de date tinde să aibă un obiectiv mai larg, și anume acela de a contribui la identificarea viitorilor delincvenți [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 100]. Curtea nu poate pune la îndoială obiectivele de prevenție a unor astfel de fișiere (*Gardel împotriva Franței*, 2009, pct. 63; *B.B. împotriva Franței*, 2009, pct. 62; *M.B. împotriva Franței,* 2009, pct. 54). Combaterea criminalității, în special a criminalității organizate și a terorismului, care reprezintă în prezent una dintre provocările cu care se confruntă societățile europene, depinde în mare măsură de utilizarea de tehnici moderne de cercetare științifică și de identificare [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 105]. În același timp, întrucât protecția datelor cu caracter personal joacă un rol fundamental în exercitarea dreptului la respectarea vieții private și de familie, consacrat de art. 8, este esențial ca dreptul intern să prevadă garanții adecvate pentru a preveni orice utilizare a datelor cu caracter personal care nu ar fi conformă cu garanțiile prevăzute la acest articol (*ibidem*, pct. 103; *Glukhin împotriva Rusiei*, 2023, pct. 75).

210. Curtea a examinat o serie de cauze care priveau păstrarea în fișiere de date destinate combaterii și prevenirii criminalității a datelor cu caracter personal ale persoanelor care fuseseră condamnate pentru infracțiuni minore (*M.K. împotriva Franței*, 2013, pct. 6, 8, 41; *Aycaguer împotriva Franței*, 2017, pct. 8, 43), grave [*B.B. împotriva Franței*, 2009, pct. 6, 62; *Gardel împotriva Franței*, 2009, pct. 8, 9, 63; *M.B. împotriva Franței,* 2009, pct. 6, 54; *Peruzzo și Martens împotriva Germaniei* (dec.), 2013, pct. 6, 12, 37-38; *Trajkovski și Chipovski împotriva Macedoniei de Nord*, 2020, pct. 6, 12), sau pentru o serie de infracțiuni care nu erau nici minore, nici deosebit de grave (*P.N. împotriva Germaniei*, 2020, pct. 6, 81). Alte cauze priveau păstrarea în fișiere de date destinate reprimării și prevenirii criminalității a datelor cu caracter personal ale persoanelor suspectate de săvârșirea unei infracțiuni, dar care fuseseră în cele din urmă achitate [*S. și Marper împotriva Regatului Unit* (MC), 2007, pct. 10, 11, 113; *M.K. împotriva Franței*, 2013, pct. 7, 9, 42; *Brunet împotriva Franței*, 2014, pct. 6, 7, 40], achitate [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 10, 113], sau care au primit doar un avertisment la finalul procedurii, fără să fi fost pronunțată vreo condamnare împotriva acestora (*M.M. împotriva Regatului Unit*, 2012, pct. 7-9). Într-un caz, datele cu caracter personal referitoare la reclamanți au fost colectate și stocate într-o bază de date a Ministerului de Interne pentru simplul motiv că persoanele vizate au făcut în mai multe rânduri obiectul unor proceduri penale. Sistemul de înregistrare în cauză a înregistrat nu numai condamnări penale – indiferent de natura și de gravitatea infracțiunilor în cauză și chiar în cazul în care condamnările au fost anulate sau șterse –, ci și cazuri în care o persoană a făcut obiectul unei proceduri penale și în care procedura penală a fost ulterior abandonată din „motive nedezincriminatoare” (*N.F. și alții împotriva Rusiei*, 2023, pct. 49). Alte cauze priveau la măsuri de natură preventivă de stocare a datelor cu caracter personal în registrele poliției, pe baza unor simple suspiciuni (*Shimovolos împotriva Rusiei*, 2011, pct. 16; *Khelili împotriva Elveției*, 2011, pct. 8, 9, 59; *Catt împotriva Regatului Unit*, 2019, pct. 6, 14, 119).

211. Următoarele elemente sunt importante atunci când se analizează necesitatea unei măsuri de stocare a datelor cu caracter personal în scopuri polițienești.

i. Caracterul nediscriminatoriu și nediferențiat al datelor stocate

212. Într-o serie de cauze, Curtea a pus în discuție domeniul de aplicare larg al modalităților de culegere a datelor instituite de autorități, care nu făceau o distincție în funcție de natura sau de nivelul de gravitate al infracțiunii care condusese la o condamnare (*M.K. împotriva Franței*, 2013, pct. 41; *Aycaguer împotriva Franței,* 2017, pct. 43; *Gaughran împotriva Regatului Unit*, 2020, pct. 94; *N.F. și alții împotriva Rusiei*, 2023, pct. 49), sau în funcție de faptul că persoana vizată fusese condamnată, achitată, pusă în libertate sau supusă unui simplu avertisment, după ce a fost suspectată de săvârșirea unei infracțiuni [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 119; *M.M. împotriva Regatului Unit*, 2012, pct. 198; *M.K. împotriva Franței*, 2013, pct. 42*; Brunet împotriva Franței*, 2014, pct. 41; *N.F. și alții împotriva Rusiei*, 2023, pct. 49]. În opinia Curții, măsurile instituite de autorități pentru a contribui la combaterea și prevenirea anumitor infracțiuni nu pot fi puse în aplicare în mod excesiv pentru a maximiza informațiile referitoare la acestea. Fără respectarea unei necesare proporționalități în raport cu obiectivele legitime care le sunt atribuite, avantajele pe care le aduc ar fi afectate de atingerile grave pe care le-ar cauza drepturilor și libertăților pe care statele trebuie să le asigure persoanelor aflate sub jurisdicția lor (*M. K. împotriva Franței*, 2013, pct. 35; *Aycaguer împotriva Franței*, 2017, pct. 34).

213. În cauza *S. și Marper împotriva Regatului Unit* (MC), 2008 (pct. 119 și 125), un sistem de culegere de date prin care amprentele digitale, mostrele de celule și profiluri ADN puteau fi prelevate și stocate de la orice persoană suspectată de comiterea unor infracțiuni, dar care nu fusese condamnată, indiferent de vârstă, de natura și de gravitatea infracțiunilor, fără limitarea perioadei și fără un control independent al justificării păstrării datelor pe baza unor criterii precise, a condus la constatarea unei încălcări a art. 8. Caracterul general și nediferențiat al unui astfel de sistem nu reflecta un just echilibru între interesele publice și cele private concurente aflate în joc.

214. Există un risc de stigmatizare atunci când persoanele condamnate pentru orice infracțiune și care au dreptul să beneficieze de prezumția de nevinovăție sunt tratate în același mod precum cele condamnate [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 122]. Chiar dacă păstrarea datelor cu caracter personal referitoare la persoane suspectate de comiterea unei infracțiuni, dar achitate sau puse în libertate nu echivalează cu exprimarea de suspiciuni, impresia că acestea nu trebuie considerate nevinovate poate fi întărită dacă datele care le privesc sunt păstrate pe o perioadă nedeterminată precum datele referitoare la persoanele condamnate, în timp ce cele referitoare la persoane care nu au fost niciodată suspectate de săvârșirea unei infracțiuni trebuie distruse (*ibidem*, pct. 122). Astfel, faptul că o persoană a fost achitată după ce a fost suspectată de săvârșirea unei infracțiuni justifică primirea unui tratament diferit față de cel al unei persoane condamnate (*ibidem*, pct. 122; a se vedea, de asemenea, în același sens, *M.K. împotriva Franței*, 2013, pct. 42; *Brunet împotriva Franței*, 2014, pct. 40). Astfel, în cauza *Brunet împotriva Franței*, 2014 (pct. 40), în care reclamantul beneficiase de neînceperea urmăririi penale după recurgerea la mediere, Curtea a pus în discuție caracterul nediferențiat al datelor cu caracter personal colectate în fișierele de date ale autorităților, fără a face distincție între persoanele condamnate și cele pentru care se dispusese neînceperea urmăririi penale. În cauza *Aycaguer împotriva Franței,* 2017 (pct. 42-43), în care datele cu caracter personal fuseseră colectate și păstrate în urma unei condamnări pentru fapte care nu prezentau nicio gravitate deosebită, Curtea a pus în discuție domeniul de aplicare larg al dispozitivului de culegere de date instituit de autorități, care nu făcea distincție în funcție de gradul de gravitate a infracțiunii care condusese la o condamnare, în pofida disparității semnificative a situațiilor care pot apărea în domeniul de aplicare a legii. În opinia Curții, faptele reproșate reclamantului, simple lovituri cu umbrela date jandarmilor într-un context politic și sindical, nu era comparabil cu fapte susceptibile să constituie infracțiuni deosebit de grave precum infracțiunile sexuale, terorismul sau, mai mult, crimele împotriva umanității sau traficul de persoane.

215. În cauza *M.M. împotriva Regatului Unit*, 2012 (pct. 187-207), înscrierea pe viață a unui avertisment în cazierul judiciar al unei persoane după ce aceasta a dispărut timp de o zi cu nepotul său, un copil, în încercarea de a preveni plecarea acestuia în Australia în urma eșecului mariajului fiului său, a condus la constatarea unei încălcări a art. 8. Curtea a pus sub semnul întrebării domeniul de aplicare deosebit de larg al sistemului de păstrare a datelor, care acoperea nu numai condamnările, ci și deciziile neurmate de o condamnare precum reținerile, avertismentele, mustrările, precum și un volum important de date suplimentare înregistrate de forțele de poliție pe baza unei prezumții generale în favoarea păstrării datelor până când persoana vizată împlinește vârsta de o sută de ani (*ibidem*, pct. 202). În opinia sa, cu cât este mai mare domeniul de aplicare al sistemului de colectare și stocare a datelor cu caracter personal și, prin urmare, cu cât este mai mare volumul și caracterul sensibil al datelor deținute și disponibile spre divulgare, cu atât este mai important conținutul garanțiilor care trebuie aplicate în diferitele etape cruciale ale prelucrării ulterioare a datelor (*ibidem*, pct. 200). Situația a fost una similară în cauza *Gaughran împotriva Regatului Unit,* 2020 (pct. 94-97), care privea păstrarea pe o perioadă nelimitată a datelor biometrice și a fotografiilor reclamantului condamnat pentru conducere în stare de ebrietate, ceea ce a condus la o încălcare a art. 8.

216. Cauza *N.F. și alții împotriva Rusiei*, 2023 (pct. 49-55), vizează un sistem de stocare a datelor în care informațiile referitoare la procedurile penale erau colectate și stocate în mod automat după ce o persoană a făcut obiectul unei proceduri penale. Această bază de date conținea informații cu privire la toate condamnările penale, stinse sau nu, indiferent de natura și de gravitatea infracțiunii săvârșite, precum și informații cu privire la procedurile penale care au fost întrerupte din „motive nedezincriminatoare". Curtea a constatat că domeniul de aplicare și aplicarea acestui sistem erau excesive. De asemenea, aceasta a considerat că prelucrarea continuă a datelor era deosebit de intruzivă pentru persoanele care nu fuseseră condamnate pentru nicio infracțiune. Aceasta a constatat, de asemenea, că ingerința în viața privată a persoanelor condamnate atingea un nivel ridicat din momentul în care condamnarea lor era ștearsă sau anulată de o instanță. Curtea a constatat că, în lipsa unor garanții suficiente împotriva abuzurilor și a unei posibilități de control, un astfel de tratament era disproporționat.

217. Păstrarea datelor referitoare la persoanele necondamnate poate fi deosebit de prejudiciabilă în cazul minorilor, având în vedere situația lor specială și importanța dezvoltării și integrării lor în societate. Trebuie să se acorde o atenție deosebită protejării lor față de orice prejudiciu de acest tip [*S. împotriva Regatului Unit* (MC), 2008, pct. 124].

ii. Perioada de stocare a datelor

218. Perioada pentru care autoritățile aleg să păstreze datele cu caracter personal ale unei persoane este un element important, deși nu decisiv, care trebuie luată în considerare atunci când se analizează dacă o măsură de păstrare a datelor cu caracter personal într-un dosar sau într-o bază de date în scopuri polițienești este proporțională, sau nu, cu scopul legitim urmărit. Curtea a constatat o încălcare a art. 8 în următoarele contexte:

- păstrarea nelimitată a amprentelor digitale și a datelor ADN ale persoanelor suspectate de săvârșirea unei infracțiuni, dar pentru care procedurile s-au încheiat cu o rezoluție de neîncepere a urmăririi penale sau cu o achitare [*S. împotriva Regatului Unit* (MC), 2008];
- păstrarea nelimitată a profilurilor ADN, a amprentelor digitale și a fotografiei unei persoane găsite condamnate pentru săvârșirea unei infracțiuni, chiar și după ce condamnarea sa fusese ștearsă din cazierul său judiciar la expirarea termenului prevăzut de lege (*Gaughran împotriva Regatului Unit*, 2020);
- păstrarea într-un cazier judiciar a tuturor condamnărilor, achitărilor, avertismentelor, reținerilor sau mustrărilor dispuse împotriva unei persoane (*M.M. împotriva Regatului Unit*, 2012);

- păstrarea pentru o perioadă nelimitată a profilurilor ADN ale persoanelor condamnate pentru furt calificat (*Trajkovski și Chipovski împotriva Macedoniei de Nord*, 2020).
- păstrarea pentru o perioadă maximă de patruzeci de ani a datelor cu caracter personal ale unei persoane condamnate pentru o infracțiune minoră (*Ayçaguer împotriva Franței*, 2017);
- păstrarea pentru o perioadă maximă de douăzeci și cinci de ani a amprentelor digitale ale unei persoane suspectate de săvârșirea unui furt de cărți, dar care nu a fost condamnată (*M. K. împotriva Franței*, 2013);
- păstrarea pentru o perioadă maximă de douăzeci de ani a datelor cu caracter personal ale unei persoane în urma unei plângeri de violență față de partenera sa, finalizată cu neînceperea urmăririi penale, în urma unei medieri (*Brunet împotriva Franței*, 2014).
- păstrarea, fără limită de timp, a datelor referitoare la sancțiunea administrativă alternativă aplicată reclamantului (*Borislav Tonchev împotriva Bulgariei*, 2024).

219. Pe de altă parte, Curtea a constatat că nu a existat nicio încălcare a art. 8 într-o serie de cauze care priveau păstrarea datelor cu caracter personal ale persoanelor condamnate pentru agresiuni sexuale, pentru o perioadă maximă de treizeci de ani, la sfârșitul căreia ștergerea datelor intervenea automat, întrucât fuseseră instituite proceduri care să permită ștergerea datelor de îndată ce acestea nu mai erau relevante (*B.B. împotriva Franței*, 2009, pct. 67; *Gardel împotriva Franței*, 2009, pct. 69; *M.B. împotriva Franței,* 2009, pct. 59). De asemenea, Curtea a declarat vădit nefondată o cauză referitoare la păstrarea, pentru o perioadă nelimitată, a datelor cu caracter personal ale persoanelor condamnate pentru infracțiuni grave, însoțită de controale la intervale regulate care nu ar fi trebuit să depășească zece ani, de natură să stabilească dacă stocarea continuă a datelor era încă necesară [*Peruzzo și Martens împotriva Germaniei* (dec.), 2013, pct. 44-49]. Și în cauza *P.N. împotriva Germaniei*, 2020 (pct. 87-90), Curtea a constatat că nu a existat nicio încălcare a art. 8 în ceea ce privea păstrarea pentru o perioadă de cinci ani, sub rezerva garanțiilor și a unui control individual, a datelor unui recidivist cu scopul de a-l identifica în urma deschiderii unei noi proceduri penale împotriva sa.

220. Elementul determinant pentru a stabili dacă un stat și-a depășit marja de apreciere atunci când a decis să păstreze pentru o perioadă nelimitată date cu caracter personal ale unor persoane condamnate nu este în mod necesar durata păstrării datelor, ci dacă au fost puse în aplicare garanții efective (*Gaughran împotriva Regatului Unit*, 2020, pct. 88). Atunci când decide să își acorde sieși puterea cea mai extinsă în materie de păstrare a datelor, și anume păstrarea datelor pentru o perioadă nelimitată, statul se plasează la limita marjei sale de apreciere și trebuie să asigure existența anumitor garanții efective (*ibidem*, pct. 88). Existența sau lipsa unui control independent al justificării păstrării datelor în sistemul de evidență, efectuat pe baza unor criterii specifice, cum ar fi gravitatea infracțiunii, forța suspiciunilor asupra persoanei, antecedentele acesteia, sau orice altă circumstanță specială, constituie o garanție importantă pentru a garanta că perioada de păstrare a datelor este proporțională [*ibidem*, pct. 94; *S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 119; *B.B. împotriva Franței*, 2009, pct. 68; *Gardel împotriva Franței*, 2009, pct. 69; *M.B. împotriva Franței,* 2009, pct. 60].

221. Lipsa unei perioade maxime de păstrare a datelor cu caracter personal nu este în mod necesar incompatibilă cu art. 8 [*Peruzzo și Martens împotriva Germaniei* (dec.), 2013, pct. 46; *Gaughran împotriva Regatului Unit*, 2020, pct. 88], însă garanțiile procedurale sunt cu atât mai necesare atunci când stocarea datelor depinde în totalitate de diligența cu care autoritățile se asigură în privința caracterului proporțional al perioadei lor de păstrare [*Peruzzo și Martens împotriva Germaniei* (dec.), 2013, pct. 46; *Ayçaguer împotriva Franței*, 2017, pct. 38].

222. În cauza *Peruzzo și Martens împotriva Germaniei* (dec.), 2013 (pct. 44), care privea păstrarea pentru o perioadă nelimitată a datelor biometrice ale persoanelor condamnate pentru infracțiuni grave și cu riscul de recidivă, Curtea a constatat cu satisfacție că dreptul intern obliga Oficiul Federal pentru Investigații Criminale să verifice la intervale regulate, care nu depășeau zece ani, dacă păstrarea datelor era încă necesară sau dacă datele puteau fi șterse, ținând seama, în fiecare caz, de scopul pentru care fuseseră păstrate datele, precum și de natura și de gravitatea circumstanțelor fiecărei

cauze care condusese la o măsură de culegere de date (*ibidem*, pct. 46). În opinia Curții, durata unor astfel de intervale nu fusese nerezonabilă, având în vedere faptul că profilurile ADN puteau fi obținute numai pentru persoanele condamnate care săvârșiseră infracțiuni care atinseseră un anumit nivel de gravitate (*ibidem*, pct. 48-49).

223. În cauza *Gaughran împotriva Regatului Unit*, 2020 (pct. 96), păstrarea pentru o perioadă nelimitată a amprentelor digitale, a profilului ADN și a fotografiei unei persoane condamnate pentru conducere în stare de ebrietate a condus la constatarea unei încălcări a art. 8. Autoritățile nu luaseră în considerare gravitatea infracțiunii săvârșite sau necesitatea de a păstra aceste date pentru o perioadă nelimitată și nu oferiseră o posibilitate reală de reexaminare (*ibidem*, pct. 96).

224. O perioadă maximă de stocare a datelor cu caracter personal prevăzută de dreptul intern poate fi asimilată, în practică, mai degrabă unei norme decât unui maxim în cazul în care șansele de succes ale unei cereri de ștergere înainte de expirarea termenului prevăzut de lege sunt ipotetice (*M. K. împotriva Franței*, 2013, pct. 44-47; *Brunet împotriva Franței*, 2014, pct. 41-45; *Ayçaguer împotriva Franței*, 2017, pct. 44-46). Curtea a concluzionat că a fost încălcat art. 8 într-o serie de cauze în care sistemul național prevedea perioade maxime de stocare de douăzeci sau douăzeci și cinci de ani pentru fapte pentru care se pronunțase neînceperea urmăririi penale (*M. K. împotriva Franței*, 2013, pct. 44-47; *Brunet împotriva Franței*, 2014, pct. 41-45), sau chiar o perioadă maximă de stocare de patruzeci de ani pentru fapte fără o gravitate deosebită pentru care fusese pronunțată o decizie de condamnare (*Ayçaguer împotriva Franței*, 2017, pct. 42).

225. În cauza *Catt împotriva Regatului Unit*, 2019 (pct. 120), păstrarea într-o bază de date a poliției privind extremismul național pentru o perioadă de cel puțin șase ani, data la care acestea făceau obiectul unei revizuiri planificate, a datelor cu caracter personal ale reclamantului a condus la constatarea unei încălcări a art. 8. Reclamantul depindea în totalitate de diligența cu care autoritățile aplicau garanțiile prevăzute de Codul de bune practici aplicabil, care aveau un caracter foarte flexibil, pentru a asigura caracterul proporțional al perioadei de păstrare a datelor sale. Lipsa unor garanții care să permită ștergerea datelor de îndată ce păstrarea continuă a datelor devine disproporționată este deosebit de îngrijorătoare în ceea ce privește păstrarea pentru o perioadă nelimitată a datelor care dezvăluie opinii politice, care beneficiază de un nivel de protecție sporit (*ibidem*, pct. 122-123).

226. Consecințele schimbărilor politicii în ceea ce privește perioada de păstrare a datelor cu caracter personal într-un cazier judiciar asupra perspectivelor de angajare ale persoanei vizate au fost examinate în cauza *M.M. împotriva Regatului Unit*, 2012 (pct. 204). În opinia Curții, era puțin probabil ca păstrarea nediferențiată și necondiționată a tuturor condamnărilor, achitărilor, avertismentelor, reținerilor și mustrărilor împotriva unei persoane să respecte cerințele prevăzute la art. 8, în lipsa unor dispoziții legale clare și detaliate care să precizeze garanțiile aplicabile și care să stabilească normele care reglementau, printre altele, durata păstrării acestora (*ibidem*, pct. 199).

227. A se vedea, de asemenea, într-un context diferit, problema limitării la zece ani, dispusă de o instanță, a perioadei de confidențialitate a probelor prezentate în cadrul procesului care conținea date medicale de natură să dezvăluie identitatea și seropozitivitatea unei persoane în cauza *Z împotriva Finlandei*, 1997 (pct. 111-113). În speță, perioada de confidențialitate de zece ani nu corespundea dorințelor sau intereselor părților la procedură, iar prezentarea, fără consimțământul reclamantei, a informațiilor în cauză condusese deja la o atingere gravă adusă vieții sale private și de familie. Ingerința suplimentară pe care ar fi suferit-o în cazul în care informațiile și materialele în cauză ar fi intrat în domeniul public după 10 ani nu se bazase pe motive imperioase.

iii. Garanții care privesc distrugerea sau ștergerea datelor stocate[9]

228. În opinia Curții, eliminarea datelor dintr-o bază de date în care au fost colectate în scopuri polițienești nu este o sarcină excesiv de complexă (*Catt împotriva Regatului Unit*, 2019, pct. 127). Ar

[9] A se vedea, de asemenea, infra, secțiunea din prezentul ghid privind „Dreptul la ștergere”.

fi total contrar necesității de a proteja dreptul la viață privată consacrat la art. 8 ca un stat să poată crea o bază de date în care ar fi dificil să se examineze sau să se modifice datele și să se invoce ulterior pe modul în care a fost concepută respectiva bază de date pentru a-și justifica refuzul de a elimina informații din aceasta (*ibidem*, pct. 127).

229. Existența la nivel național a unei proceduri judiciare de ștergere a datelor care să poată asigura un control independent al justificării păstrării lor pe baza unor criterii precise și care să ofere garanții suficiente și adecvate în ceea ce privește respectarea vieții private a persoanei vizate constituie un element important pentru evaluarea comparativă a diferitelor interese aflate în joc [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 119; *Gardel împotriva Franței*, 2009, pct. 69].

230. Curtea a constatat lipsa unei încălcări a art. 8 în cauze în care, deși era vorba despre date stocate pentru perioade „îndelungate", de până la treizeci de ani (*B.B. împotriva Franței*, 2009, pct. 66, 68; *Gardel împotriva Franței*, 2009, pct. 67, 69; *M.B. împotriva Franței,* 2009, pct. 58, 60) sau chiar pentru o perioadă nelimitată [*Peruzzo și Martens împotriva Germaniei* (dec.), 2013, pct. 46], persoana vizată beneficiase de o procedură judiciară care asigurase un control independent al justificării păstrării datelor sale pe baza unor criterii precise, care să îi permită să obțină ștergerea datelor în termenul maxim prevăzut de lege sau, în cazul păstrării nelimitate, de îndată ce acestea nu mai erau relevante [a se vedea, *a contrario*, *S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 119].

231. Astfel, în cauzele *B.B. împotriva Franței*, 2009 (pct. 68), *Gardel împotriva Franței*, 2009 (pct. 69), și *M.B. împotriva Franței,* 2009 (pct. 60), Curtea a hotărât că procedura judiciară de ștergere a datelor, deschisă la simpla cerere a persoanei vizate în fața procurorului Republicii, a cărui decizie era supusă unor căi de atac jurisdicționale, asigura un control independent al justificării păstrării informațiilor pe baza unor criterii precise și oferea garanții suficiente și adecvate. A se vedea, de asemenea, supra, pct. 204 din prezentul ghid, în ceea ce privește cauza *Peruzzo și Martens împotriva Germaniei* (dec.), 2013 (pct. 44).

232. În cauza *P.N. împotriva Germaniei*, 2020 (pct. 81 și 88), care privea păstrarea datelor cu caracter personal ale unui delincvent adult ale cărui infracțiuni nu erau nici minore, nici deosebit de grave, regula care stabilea ștergerea acestor date după cinci ani, în lipsa unei noi anchete penale asupra persoanei vizate în termenul respectiv, nu a fost considerată contrară art. 8. Necesitatea de a păstra datele în cauză în dosarele poliției putea face obiectul unei revizuiri de către poliție, sub control jurisdicțional, iar reclamantul putea obține astfel ștergerea datelor sale în cazul în care comportamentul său demonstra că datele nu mai erau necesare pentru activitatea poliției (*ibidem*, pct. 88).

233. Lipsa unor garanții eficiente pentru a obține ștergerea datelor cu caracter personal atunci când acestea nu păreau a mai fi relevante pentru scopul dosarului este deosebit de îngrijorătoare în ceea ce privește categoriile sensibile de date cu caracter personal păstrate, care impun o protecție sporită (*Catt împotriva Regatului Unit*, 2019, pct. 123).

234. Posibilitatea prevăzută în dreptul intern de a obține ștergerea datelor se dovedește a fi o garanție „teoretică și iluzorie", iar nu una „concretă și efectivă" atunci când dreptul de a depune o cerere de ștergere a acestor date în fața instanței în orice moment riscă să fie contrar interesului serviciilor de anchetă de a dispune de un dosar cu cât mai multe referințe posibil și în cazul în care interesele implicate sunt, fie și parțial, contradictorii (*M.K. împotriva Franței,* 2013, pct. 44). Garanția de a obține ștergerea datelor are, de asemenea, un efect limitat atunci când autoritățile refuză, ca răspuns la o cerere adresată de persoana vizată, să șteargă datele în cauză sau să își motiveze decizia de a le păstra (*Catt împotriva Regatului Unit*, 2019, pct. 122). Situația este una similară și atunci când cererile de ștergere nu sunt admise decât în circumstanțe excepționale sau sunt respinse atunci când persoana vizată a recunoscut infracțiunea și faptul că datele sunt exacte (*M.M. împotriva Regatului Unit*, 2012, pct. 202).

235. În opinia Curții, persoanele care fac obiectul unei hotărâri de condamnare ar trebui, de asemenea, precum cele achitate sau puse în libertate, să aibă, de asemenea, posibilitatea concretă de a depune o cerere de ștergere a datelor lor stocate în dosarele autorităților (*B.B. împotriva Franței*, 2009*,* pct. 68*; Brunet împotriva Franței*, 2014, pct. 41-43; *Ayçaguer împotriva Franței*, 2017, pct. 44). În cauza *Ayçaguer împotriva Franței*, 2017 (pct. 44), în care nu era pusă în aplicare o procedură de ștergere decât pentru persoanele suspectate de săvârșirea unei infracțiuni, nu și pentru cele condamnate, Curtea a constatat o încălcare a art. 8. În opinia sa, regimul de păstrare a profilurilor ADN în sistemul național privind infracțiunile nu oferea, atât din cauza duratei sale, cât și a lipsei posibilității de ștergere, un just echilibru între interesele publice și private concurente aflate în joc (*ibidem*, pct. 45).

236. În cauza *Khelili împotriva Elveției*, 2011 (pct. 68-70), Curtea a concluzionat că a fost încălcat art. 8, după ce a subliniat incertitudinile și dificultățile întâmpinate de persoana vizată în încercarea de a obține ștergerea termenului „prostituată” din dosarele poliției ca fiind profesia sa, deși aceasta nu fusese niciodată condamnată pentru practicarea ilegală a prostituției. Curtea a observat că nu s-a susținut că eliminarea termenului în litigiu din dosarele poliției ar fi fost imposibilă sau dificilă din motive tehnice (*ibidem*, pct. 68).

iv. Garanții cu scopul de a reglementa accesul terților și de a păstra integritatea și confidențialitatea datelor

237. Curtea a examinat în mai multe cauze dacă dreptul intern conține sau nu garanții de natură să protejeze în mod eficace datele cu caracter personal stocate în dosarele autorităților împotriva utilizărilor improprii și abuzive [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 103; *B.B. împotriva Franței*, 2009, pct. 61; *Gardel împotriva Franței*, 2009 pct. 62; *M.M. împotriva Regatului Unit*, 2012, pct. 195; *M.K. împotriva Franței,* 2013, pct. 35; *Brunet împotriva Franței*, 2014, pct. 35; *Ayçaguer împotriva Franței*, 2017, pct. 38]. Curtea a constatat că astfel de garanții există atunci când, de exemplu,

- consultarea datelor colectate în dosar era accesibilă exclusiv autorităților supuse obligației de confidențialitate [*B.B. împotriva Franței*, 2009, pct. 69; *Peruzzo și Martens împotriva Germaniei* (dec.), 2013, pct. 47];
- datele stocate făceau obiectul unor proceduri de consultare suficient delimitate, care reglementau persoanele abilitate să consulte dosarul (*M.K. împotriva Franței,* 2013, pct. 37; a se vedea, *a contrario*, *Khelili împotriva Elveției*, 2011, pct. 64);
- identitatea persoanei de la care era prelevat materialul ADN nu era dezvăluită experților în crearea de profiluri ADN, care erau, de asemenea, obligați să ia măsurile corespunzătoare pentru a preveni utilizarea neautorizată a mostrelor de celule examinate [*Peruzzo și Martens împotriva Germaniei* (dec.), 2013, pct. 45]; mostrele de celule urmau să fie distruse fără întârziere de îndată ce nu mai era necesar să se stabilească profilul ADN și doar profilurile ADN extrase din mostrele de celule respective puteau fi stocate în baza de date a Oficiului Federal pentru Investigații Criminale (*ibidem*, pct. 45); iar profilurile ADN păstrate nu puteau fi comunicate autorităților competente decât în scopuri clar delimitate, care vizau prevenirea pericolelor și asistența judiciară internațională (*ibidem*, pct. 47).

238. În cauza *Gardel împotriva Franței*, 2009 (pct. 70), în care cadrul autorităților publice care aveau acces la datele stocate într-un dosar fusese extins în mai multe rânduri pentru a nu se limita doar la autoritățile judiciare și polițienești, ci și pentru a include organe administrative, Curtea a constatat cu satisfacție că consultarea era accesibilă exclusiv autorităților supuse unei obligații de confidențialitate și în circumstanțe precis stabilite.

239. În cauza *P.N. împotriva Germaniei*, 2020 (pct. 89), nu exista niciun indiciu că datele de identificare ale unui delincvent adult păstrate de autorități pentru o perioadă maximă de cinci ani nu erau suficient protejate împotriva unor abuzuri precum accesul sau dezvăluirea fără autorizație.

240. În schimb, în cauza *M.M. împotriva Regatului Unit*, 2012 (pct. 204), care privea păstrarea pe viață a unui avertisment în cazierul judiciar al unei persoane și dezvăluirea acestor date unui viitor angajator în contextul căutării unui loc de muncă, Curtea a pus în discuție deficiențele procedurii prin care se urmărea reglementarea accesului terților la cazierul judiciar al persoanelor aflate în căutarea unui loc de muncă, care nu permiteau să se aprecieze, în niciun stadiu, relevanța datelor pentru locul de muncă căutat sau dacă persoana vizată putea fi percepută drept continuând să prezinte un risc. De asemenea, în cauza *N. F. și alții împotriva Rusiei*, 2023 (pct. 51), care privea o bază de date care conținea informații privind proceduri penale care fie fuseseră abandonate din „motive nedezincriminatoare", fie care avuseseră ca rezultat condamnări, Curtea a arătat că reglementarea în vigoare nu făcea nicio distincție în ceea ce privește scopurile și alte metode importante de prelucrare a datelor în cauză și că, prin urmare, nu oferea nicio posibilitate reală de a efectua, în conformitate cu cerințele articolului 8 din Convenție, o analiză a proporționalității privind un eventual acces al terților la datele în cauză.

b. Păstrarea datelor cu caracter personal în contextul sănătății

241. Curtea a trebuit să examineze problema păstrării datelor sensibile în domeniul sănătății. În cauza *Malanicheva împotriva Rusiei* (dec.), 2016 (pct. 13, 15-18), Curtea a considerat că funcționarea eficientă a instituțiilor sanitare naționale și procesul decizional al instanțelor făceau necesare stocarea și schimbul de informații relevante. A respins ca vădit nefondate capetele de cerere întemeiate pe înscrierea numelui reclamantei în registrul spitalului cu persoanele care sufereau de tulburări psihiatrice și pe pretinsele trimiteri false la diferite aspecte ale sănătății sale mintale în comunicările interne ulterioare dintre instituțiile sanitare, precum și în observațiile lor în fața instanțelor. Nu exista niciun indiciu că informațiile în cauză păstrate de autorități fuseseră puse la dispoziția publicului sau fuseseră utilizate în alte scopuri decât luarea deciziei cu privire la asistența medicală cea mai adecvată pentru persoana vizată.

242. În cauza *Drelon împotriva Franței*, 2022 (punctul 98), care viza păstrarea până în 2278 a datelor cu caracter personal referitoare la presupusa homosexualitate a reclamantului care fuseseră colectate în 2004, Curtea a statuat că durata perioadei în cauză era excesivă.

243. Anterior, Comisia a declarat vădit nefondată și a respins o cauză care privea păstrarea în dosarul unui spital de psihiatrie a datelor referitoare la internarea obligatorie a unei paciente a cărei nelegalitate fusese recunoscută de instanțele judecătorești naționale (*Yvonne Chave, născută Jullien, împotriva Franței*, 1991). Potrivit Comisiei, păstrarea informațiilor privind pacienții cu tulburări psihice servește nu doar interesului legitim de a asigura funcționarea eficientă a serviciilor din spitalele publice, ci și interesului de a proteja drepturile pacienților înșiși, întrucât contribuie la prevenirea riscului de internare arbitrară și constituie un mijloc de investigație aflat la dispoziția autorităților administrative sau judiciare însărcinate cu supravegherea instituțiilor psihiatrice. În speță, datele cu caracter personal ale persoanei vizate înscrise în registrul spitalului de psihiatrie erau protejate de reguli de confidențialitate adecvate.

244. A se vedea, de asemenea, supra, pct. 182 din prezentul ghid în ceea ce privește încălcarea art. 8 în cauza *Surikov împotriva Ucrainei*, 2017 (pct. 75-95).

c. Păstrarea on-line, în scopuri jurnalistice, a datelor cu caracter personal

245. Curtea a subliniat funcția auxiliară, totuși importantă, a presei, care constă în constituirea de arhive plecând de la informații deja publicate și în punerea acestora la dispoziția publicului. În această privință, punerea la dispoziție a arhivelor pe Internet contribuie în mod semnificativ la conservarea și accesibilitatea știrilor și a informațiilor, întrucât arhivele digitale constituie o sursă prețioasă de educare și de cercetare istorică, în special prin faptul că sunt imediat accesibile publicului și, în general, gratuite [*Times Newspapers Ltd împotriva Regatului Unit (nr. 1 și 2)*, 2009, pct. 27, 45; *Węgrzynr.wski și Smolczewski împotriva Poloniei*, 2013, pct. 59; *M.L. și W.W. împotriva Germaniei*, 2018, pct. 90; a se

vedea, de asemenea, *Hurbain împotriva Belgiei* (MC), 2023, pct. 180, unde Curtea a efectuat o examinare din perspectiva articolului 10].

3. Divulgarea datelor cu caracter personal

246. Într-o serie de cauze, Curtea a avut ocazia să examineze diferite măsuri care au condus la divulgarea datelor cu caracter personal ale unei persoane de către operatorul de date, către:

- o altă persoană fizică sau o persoană juridică (*Mockutė împotriva Lituaniei*, 2018, pct. 99-100, care privea transmiterea de către un spital a informațiilor referitoare la sănătatea unei paciente către un membru al familiei sale și către jurnaliști; *Y. împotriva Turciei* (dec.), 2015, pct. 70-72, care privea divulgarea informațiilor referitoare la seropozitivitatea unui pacient de către personalul ambulanței către personalul spitalului; *Radu împotriva Republicii Moldova*, 2014, pct. 27, care privea divulgarea, de către un spital, a informațiilor medicale referitoare la starea de sănătate a unui pacient către angajatorul acestuia; *M.C. împotriva Regatului Unit*, 2021, pct. 46, care privea divulgarea de către autorități către un angajator potențial a informațiilor referitoare la antecedentele penale ale reclamantei];
- o autoritate publică (*M.S. împotriva Suediei*, 1997, pct. 35, care privea divulgarea informațiilor medicale ale unei paciente de către un serviciu de ginecologie către casa de asigurări sociale; *P.T. împotriva Republicii Moldova*, 2020, pct. 5-6, 29-31, care privea prezența inutilă a unor date medicale sensibile pe un certificat care urma să fie prezentat în diferite situații);
- public [*Hájovský împotriva Slovaciei*, 2021 pct. 46-49, care privea publicarea într-un jurnal al unui canal de televiziune a unor informații care dezvăluiau identitatea și imaginea neobturată a unei persoane, fără știrea sa și folosind o stratagemă; *Peck împotriva Regatului Unit*, 2003, pct. 63, care privea i transmiterea către mass-media a unei filmări provenite de la o cameră de televiziune cu circuit închis care filma o persoană care încerca să se sinucidă într-un loc public; *Bremner împotriva Turciei*, 2015, pct. 71-85, care privea difuzarea la televiziune a imaginii fără a fi obturată sau acoperită a unei persoane private obținute prin intermediul unei camere video ascunse; *Khadija Ismayilova împotriva Azerbaidjanului*, 2019, pct. 108-132, care privea înregistrarea video secretă a unei jurnaliste în locuința sa și difuzarea acestor înregistrări video către public; *Z împotriva Finlandei*, 1997, pct. 70-71, care privea divulgarea printr-o hotărâre judecătorească transmisă presei a identității și stării de sănătate a unei persoane; *Apostu împotriva României*, 2015, pct. 121-132, care privea divulgarea către presă a unor probe din dosarul cauzei; *Montera împotriva Italiei* (dec.), 2002, care privea divulgarea către a unui raport al unei comisii parlamentare referitor la viața privată și deontologia profesională a unui magistrat; *Von Hannover împotriva Germaniei*, 2004, pct. 61-81, care privea publicarea în presa tabloidă a unor fotografii referitoare la viața privată a unei prințese; *Polanco Torres și Movilla Polanco împotriva Spaniei*, 2010, pct. 44-54, care privea un articol de presă, bazat pe declarațiile unui fost contabil, care acuza soția unui judecător de rang înalt de implicare în operațiuni ilegale cu o societate; *Alkaya împotriva Turciei*, 2012, pct. 30-31, care privea divulgarea de către un cotidian național de mare tiraj a adresei complete de domiciliu a unei actrițe celebre; *Mityanin și Leonov împotriva Rusiei*, 2018, pct. 111-121, care privea difuzarea în presă a fotografiei unui suspect, însoțită de declarații care îl acuzau de delicte minore și infracțiuni; *Bogomolova împotriva Rusiei*, 2017, pct. 54-58, care privea divulgarea fotografiei unui copil pe pagina de gardă a unei broșuri intitulate „Copiii au nevoie de o familie”, publicată de un centru de asistență psihologică, medicală și socială; *L.B. împotriva Ungariei* (MC), 2023, privind publicarea obligatorie, pe lista principalilor debitori disponibilă pe site-ul internet al autorității fiscale, a datelor cu caracter personal referitoare la reclamant, inclusiv numele și adresa sa de domiciliu].

a. Impactul consimțământului prealabil

247. Consimțământul prealabil al persoanei vizate cu privire la transmiterea, divulgarea sau publicarea datelor sale se dovedește a fi un factor important, chiar dacă nu decisiv, pentru a stabili, într-o cauză, dacă astfel de operațiuni constituie o atingere adusă dreptului său la viață privată (*M.S. împotriva Suediei*, 1997, pct. 31, 35; *M.M. împotriva Regatului Unit*, 2012, pct. 186, 189) sau dacă pot fi considerate ca fiind „prevăzute de lege" în sensul art. 8 § 2 (*Radu împotriva Republicii Moldova*, 2014, pct. 27; *Mockutė împotriva Lituaniei*, 2018, pct. 101). Curtea a concluzionat că a fost încălcat art. 8 într-o serie de cauze în care divulgarea datelor cu caracter personal de către operatorul de date avusese loc fără consimțământul persoanei vizate (*Radu împotriva Republicii Moldova*, 2014, pct. 30, 32; *Mockutė împotriva Lituaniei*, 2018, pct. 103, 106; *Peck împotriva Regatului Unit*, 2003, pct. 85-87; *Sõro împotriva Estoniei*, 2015, pct. 17-19, pct. 64).

248. Pentru a fi valabil, consimțământul persoanei vizate trebuie să fie informat și fără echivoc (*M.S. împotriva Suediei*, 1997, pct. 32; *Konovalova împotriva Rusiei*, 2014, pct. 47-48). Într-o cauză care privea transmiterea dosarului medical al unei persoane de către un organ public (serviciul de ginecologie al unui spital) către un altul (casa de asigurări sociale), fără consimțământul persoanei vizate, se punea întrebarea dacă, prin inițierea unei proceduri pentru obținerea de despăgubiri, persoana vizată renunțase la dreptul său la confidențialitatea datelor (*M.S. împotriva Suediei*, 1997, pct. 31-32). Curtea a hotărât că, întrucât această transmitere depindea nu doar de prezentarea de către persoana vizată a unei cereri de despăgubire, ci și de o serie de elemente independente de voința sa, nu putea deduce din cererea de despăgubiri că renunțase în mod neechivoc la confidențialitatea dosarului său medical. Astfel, art. 8 era aplicabil în speță.

249. Faptul că divulgarea datelor cu caracter personal ale unei persoane a avut loc la cererea sau cu consimțământul acesteia nu o privează de protecția conferită de art. 8 atunci când persoana vizată nu a avut în mod real opțiunea de a le da sau nu, de exemplu atunci când un angajator a solicitat divulgarea datelor cu caracter personal înscrise în cazierul judiciar al unei persoane aflate în căutarea unui loc de muncă (*M.M. împotriva Regatului Unit*, 2012, pct. 189). În cauza *M.M. împotriva Regatului Unit* (2012, pct. 187-207), în care reclamanta solicitase divulgarea către un potențial angajator informații referitoare la un avertisment înscris în cazierul său judiciar, Curtea a constatat o încălcare a art. 8 în lipsa unor garanții suficiente în sistemul național pentru divulgarea de date referitoare la cazierul judiciar al unei persoane, ceea ce nu permitea să se aprecieze, în niciun stadiu, relevanța datelor pentru ocuparea locului de muncă dorit sau dacă persoana vizată putea fi percepută ca prezentând în continuare un risc (*ibidem*, pct. 204). În cauza *M.C. împotriva Regatului Unit*, 2021, pct. 47-57, Curtea a luat act de modificările legislative intervenite ca urmare a hotărârii *M.M. împotriva Regatului Unit* și a constatat că noul regim care reglementa divulgarea informațiilor referitoare la cazierul judiciar al unei persoane era compatibil cu cerințele art. 8: acesta făcea distincție între diferitele tipuri de infracțiuni, permitea să se stabilească cu certitudine în orice moment condamnările care puteau fi divulgate și stabilea o durată limitată a divulgării, care varia în funcție de vârsta autorului infracțiunii și de gravitatea estimată a infracțiunii.

250. Obținerea consimțământului persoanei vizate nu este întotdeauna posibilă atunci când, de exemplu, secvențele provenite de la înregistrări cu camere de televiziune cu circuit închis instalate de autorități pe domeniul public, menite să contribuie la identificarea delincvenților și la prevenirea infracțiunilor, indică un număr mare de persoane (*Peck împotriva Regatului Unit*, 2003, pct. 81). În opinia Curții, un sistem de camere de televiziune cu circuit închis, a cărui divulgare de imagini astfel surprinse ar fi condiționată de consimțământul persoanei vizate, riscă în practică să compromită orice acțiune menită să promoveze eficacitatea unui astfel de sistem de supraveghere în detecția și prevenirea infracțiunilor, rol care devine și mai eficient prin publicitatea făcută rezultatelor (*ibidem*, pct. 81). În astfel de circumstanțe, sau în cazul în care persoanele ale căror imagini au fost surprinse în acest mod refuză să își dea consimțământul pentru difuzarea imaginilor lor, operatorului de date îi revine sarcina de a lua în considerare soluții alternative, care pot consta în mascarea identității înainte

de a le divulga (*ibidem*, pct. 82) sau în asigurarea faptului că destinatarul datelor le maschează el însuși în mod adecvat și suficient (*ibidem*, pct. 83).

251. În cauza *Peck împotriva Regatului Unit*, 2003 (pct. 87), comunicarea de către un consiliu municipal, în comunicatul său de presă și către mass-media, a imaginilor surprinse de o cameră de televiziune cu circuit închis filmând o persoană care încerca să se sinucidă într-un loc public a condus la o încălcare a art. 8. Curtea a hotărât că, întrucât secvența în cauză privea și atrăgea atenția asupra unei singure persoane, operatorul camerei de televiziune cu circuit închis care alertase poliția și îi observase intervenția ar fi putut să solicite identificarea reclamantului și, prin urmare, consimțământul acestuia pentru divulgarea imaginilor (*ibidem*, pct. 81).

252. Difuzarea, într-un reportaj de televiziune filmat cu camera ascunsă, a imaginii fără a fi obturată sau acoperită a unei persoane private a fost considerată contrară art. 8 în cauza *Bremner împotriva Turciei*, 2015 (pct. 71-85). Având în vedere, în special, lipsa de notorietate a reclamantului, nimic nu permitea să se considere că o astfel de difuzare de imagini ar fi avut valoare informativă sau că ar fi fost utilizată în mod corespunzător.

253. În plus, având în vedere potențialul efect disuasiv al unei obligații de notificare prealabilă, îndoielile cu privire la eficacitatea unei astfel de obligații și marja largă de apreciere lăsată autorităților naționale în acest domeniu, Curtea a concluzionat că art. 8 nu impunea o obligație legală, în cazul unui ziar, să notifice o persoană înainte de publicarea informațiilor cu privire la viața sa privată, în cauza *Mosley împotriva Regatului Unit*, 2011 (pct. 132).

254. În anumite circumstanțe, divulgarea datelor privind sănătatea mintală a unei persoane, fără consimțământul acesteia, către un membru de familie apropiat poate conduce la o încălcare a dreptului la respectarea vieții sale private. În cauza *Mockutė împotriva Lituaniei*, 2018 (pct. 100), Curtea a hotărât că, având în vedere divulgarea către mama unei paciente de informații privind starea de sănătate a fiicei sale adulte fără consimțământul acesteia, având în vedere relația tensionată dintre aceste două persoane adulte, nu a fost conformă cu dreptul garantat de art. 8.

255. În ceea ce privește persoanele arestate sau urmărite penal, Curtea a constatat o încălcare a articolului 8 în cazurile în care autoritățile polițienești au dat presei fotografii ale reclamanților fără consimțământul acestora (*Sciacca împotriva Italiei*, 2005, pct. 29-31; *Khuzhin și alții împotriva Rusiei*, 2008, pct. 115-118; *Margari împotriva Greciei*, 2023, pct.54-60) sau a invitat echipe de televiziune să filmeze reclamantul la secția de poliție fără consimțământul său și să difuzeze aceste imagini la televiziune (*Toma împotriva României*, 2009, pct. 90-93; *Khmel împotriva Rusiei*, 2013, pct. 41), într-o cauză în care Ministerul de Interne publicase pe site-ul său internet fotografii ale reclamanților care fuseseră luați în custodie de poliție și în care identitatea persoanelor vizate nu fusese ascunsă (*D.H. și alții împotriva Macedoniei de Nord*, 2023, pct. 63-65), într-o cauză în care afișarea unei fotografii a reclamantului pe panoul persoanelor căutate nu era prevăzută de lege (*Guiorgui Nikolaichvili împotriva Georgiei*, 2009, pct. 129-131) și într-o cauză în care normele și procedurile în vigoare nu respectau cerința privind „calitatea legii” (*Negru împotriva Republicii Moldova*, 2023, pct. 29-35).

256. Lipsa consimțământului prealabil al persoanei vizate pentru transmiterea, divulgarea sau publicarea datelor sale nu antrenează în mod necesar constatarea unei încălcări a art. 8, atunci când alte cerințe legitime, precum necesitatea de a cerceta infracțiunile și de a asigura publicitatea procedurilor judiciare (*Avilkina și alții împotriva Rusiei,* 2013, pct. 45; *Z împotriva Finlandei*, 1997, pct. 97), necesitatea de a proteja sănătatea publică [(*Y. împotriva Turciei* (dec.), 2015, pct. 74], securitatea națională [*Anchev împotriva Bulgariei* (dec.), 2017, pct. 100] sau bunăstarea economică a unei țări (*M.S. împotriva Suediei*, 1997, pct. 38) intră în joc.

b. Divulgarea de date în contextul procedurilor judiciare

257. Într-o serie de cauze, Curtea a examinat diferite măsuri luate de autorități în contextul procedurilor judiciare care au condus la divulgarea datelor cu caracter personal ale părților sau ale terților, de exemplu:

- faptul că o instanță a reprodus, într-o hotărâre de divorț, un extras dintr-un dosar medical personal (*L.L. împotriva Franței*, 2006, pct. 46) și a dispus ca perioada de confidențialitate a probelor prezentate care conțineau date medicale să fie limitată la zece ani (*Z împotriva Finlandei*, 1997, pct. 112-113),
- divulgarea datelor psihiatrice confidențiale în cadrul unei audieri publice (*Panteleienko împotriva Ucrainei*, 2006, pct. 57); și verificarea unui certificat medical prezentat ca dovadă în sprijinul unei cereri de amânare [*Stokłosa împotriva Poloniei* (dec.) 2021, pct. 43-44],
- divulgarea identității și a seropozitivității unei persoane, într-o hotărâre transmisă presei (*Z împotriva Finlandei*, 1997, pct. 113),
- divulgarea identității complete a unei terțe părți într-o hotărâre, fără ca aceasta să fi fost informată în prealabil (*Vicent Del Campo împotriva Spaniei*, 2018, pct. 47-51), sau
- utilizarea unui limbaj și a unor argumente care dezvăluiau, în hotărârea pronunțată, date cu caracter personal ale victimei care aduceau atingere rolului femeilor și care puteau afecta protecția efectivă a drepturilor victimelor violenței de gen, în pofida unui cadru legislativ satisfăcător (*J.L. împotriva Italiei*, 2021, pct. 136-142).
- publicarea în presă (*Margari împotriva Greciei*, 2023, pct. 54) sau pe o listă publică a persoanelor căutate afișată în secțiunea publică a unei secții de poliție (*Negru împotriva Republicii Moldova*, 2023, pct. 24) a fotografiilor și a datelor cu caracter personal privind inculpații în cadrul procedurilor penale;
- publicarea într-o bază de date judiciară oficială online accesibilă publicului a numelui și adresei complete ale reclamantei, precum și a textului integral al hotărârilor judecătorești de respingere a cererii sale de despăgubiri pentru abuz sexual (*A.P. împotriva Armeniei*, 2024, pct. 159).

258. În opinia Curții, necesitatea de a păstra confidențialitatea datelor cu caracter personal ale părților sau ale terților în contextul procedurilor judiciare poate fi uneori eliminată în fața necesității de a ancheta infracțiunile și de a garanta publicitatea procedurilor judiciare (*Avilkina și alții împotriva Rusiei,* 2013, pct. 45; *Z împotriva Finlandei*, 1997, pct. 97). Autorităților naționale competente trebuie să li se acorde o anumită marjă de apreciere în a stabili un echilibru just între, pe de o parte, protecția publicității procedurilor judiciare, necesară pentru a păstra încrederea în instanțele judecătorești și, pe de altă parte, interesele unei părți sau ale unui terț în ceea ce privește confidențialitatea datelor sale (*C.C. împotriva Spaniei*, 2009, pct. 35). Orice măsură de natură să dezvăluie publicului datele cu caracter personal ale unei persoane, indiferent dacă este parte sau terță parte la o procedură judiciară, trebuie să răspundă unei nevoi sociale imperioase (*Vicent Del Campo împotriva Spaniei*, 2018, pct. 46) și să se limiteze, pe cât posibil, la cele care sunt strict necesare date fiind particularitățile procedurii (*L.L. împotriva Franței*, 2006, pct. 45; *Margari împotriva Greciei*, 2023, pct. 47).

259. Pentru a stabili, într-o cauză dată, dacă există motive suficiente pentru a dezvălui, în textul unei hotărâri judecătorești, identitatea unei persoane și alte date cu caracter personal care o privesc, un factor important constă în a cunoaște dacă alte măsuri, mai puțin intruzive, erau posibile în temeiul dreptului și al practicii naționale. Poate fi vorba, în special, de posibilitatea ca o instanță națională să nu menționeze în hotărârea sa nume care permit identificarea persoanei vizate (*Z împotriva Finlandei*, 1997, pct. 113; *Vicent Del Campo împotriva Spaniei*, 2018, pct. 50), să decidă ca expunerea de motive completă să rămână confidențială pentru o anumită perioadă și să publice, în schimb, o versiune prescurtată a expunerii de motive și a dispozitivului și o trimitere succintă la legislația aplicată (*Z împotriva Finlandei*, 1997, pct. 113), sau să limiteze accesul la textul unei hotărâri sau la anumite părți

ale acesteia (*Vicent Del Campo împotriva Spaniei*, 2018, pct. 50). În opinia Curții, se consideră, în general, că astfel de măsuri reduc impactul produs de o hotărâre asupra dreptului persoanei vizate la protecția vieții sale private.

260. În cauza *Panteleyenko împotriva Ucrainei,* 2006 (pct. 82), organizarea unei ședințe în camera de consiliu ar fi putut, de asemenea, să permită, în opinia Curții, să se evite divulgarea către public, în cadrul unei ședințe publice, de informații confidențiale privind sănătatea mintală a unei persoane, obținute de la un spital de psihiatrie și tratamentul psihiatric la care fusese supusă, chiar dacă acest fapt nu ar fi împiedicat în mod necesar să fie aduse la cunoștința părților și depuse la dosarul cauzei.

261. În cauza *Frâncu împotriva României*, 2020 (pct. 72-73), s-a constatat că nerespectarea de către o curte de apel a obligației de a asigura confidențialitatea informațiilor medicale referitoare la reclamant prin respingerea unei cereri de examinare în camera de consiliu într-o cauză de corupție care viza un primar a fost considerată contrară art. 8. În opinia Curții, limitându-se la a afirma, fără a furniza explicații suplimentare, că situația reclamantului nu corespundea „niciuneia dintre situațiile" prevăzute de dispoziția din Codul de procedură penală referitoare la examinarea în camera de consiliu, instanța în cauză nu păstrase un just echilibru între interesul general de a asigura transparența procedurilor judiciare și, pe de altă parte, interesul justițiabilului de a păstra confidențialitatea datelor privind starea sa de sănătate. Chiar dacă reputația unui acuzat poate constitui unul dintre elementele care trebuie luate în considerare în cadrul analizei proporționalității unei cereri de examinare în camera de consiliu a unei cauze, în speță, curtea de apel nu efectuase nicio examinare individuală a proporționalității unei astfel de măsuri.

262. În cauza *Khadija Ismayilova împotriva Azerbaidjanului*, 2019 (pct. 105-132), Curtea a hotărât că divulgarea de către organele de urmărire penală a unor informații cu caracter personal sensibile precum numele și adresa reclamantei, jurnalist de profesie, și numele prietenilor, membrilor familiei și ale colegilor săi într-un comunicat de presă care pretindea că furnizează un raport privind stadiul unei anchete penale, a condus la constatarea unei încălcări a art. 8 (*ibidem*, pct. 142-150).

263. În cauza *M.P. împotriva Portugaliei*, 2021, pct. 48-49, prezentarea de către fostul soț al reclamantei, fără consimțământul acesteia, în cadrul procedurii de divorț, a mesajelor electronice schimbate de soția sa pe un site de întâlniri la care se pare că aceasta i-ar fi dat acces nu a constitut o încălcare a art. 8, instanța specializată pe dreptul familiei neluând în final în considerare aceste mesaje, accesul publicului la dosarele acestui tip de proceduri fiind, de altfel, restrâns.

264. În cauza *J.S. împotriva Regatului Unit* (dec.), 2015 (pct. 71-73), Curtea a respins ca vădit nefondat un capăt de cerere întemeiat pe divulgarea, într-un comunicat publicat de parchet, a unor informații cu caracter personal care nu depășeau ceea ce era furnizat în general către mass-media ca răspuns la întrebările referitoare la procedurile judiciare și care nu dezvăluiau nici numele reclamantului (un minor acuzat de agresarea unui profesor), nici vârsta sau școala sa sau orice alte informații cu caracter personal.

265. În cauza *L.L. împotriva Franței*, 2006 (pct. 46), în care judecătorul se bazase, cu titlu subsidiar, în cadrul unei proceduri de divorț, pe corespondența privată dintre un medic specialist și medicul reclamantului, care conținea un document medical confidențial, faptul că judecătorul sau ofițerul care conducea procedura ar fi putut exclude divulgarea, în motivarea unei hotărâri, a datelor medicale în cauză, ajungând la aceeași concluzie, a constituit un element important de luat în considerare. Întrucât orice persoană putea obține o copie a motivării deciziei, fără a justifica existența unui interes, ingerința suferită de reclamant în dreptul său la respectarea vieții private nu era justificată, având în vedere rolul fundamental jucat de protecția datelor cu caracter personal, în pofida faptului că dezbaterile dintre părțile la divorț nu erau publice, iar decizia opozabilă terților nu conținea decât dispozitivul (*ibidem*, pct. 47, 33).

266. În cauza *Vicent Del Campo împotriva Spaniei*, 2018 (pct. 53, 56), faptul că reclamantul, parte terță în cadrul unei proceduri judiciare, fusese privat de orice posibilitate de a solicita instanței, înainte de

pronunțarea hotărârii, să se abțină de la comunicarea identității sale a constituit o încălcare a art. 8. Persoana vizată nu fusese informată, interogată, citată pentru a se înfățișa sau acuzată în vreun fel.

267. Într-o cauză în care instanțele naționale au stabilit ca perioada de confidențialitate a documentelor din dosar care dezvăluiau seropozitivitatea și identitatea reclamantei să fie de zece ani, Curtea a constatat încălcarea art. 8, considerând că autoritățile judiciare nu acordaseră suficientă pondere intereselor de a proteja datele cu caracter personal ale părților și cele ale terților care puteau fi afectați (*Z împotriva Finlandei*, 1997, pct. 111-112). În opinia sa, ingerința gravă în dreptul la respectarea vieții private al persoanei vizate care rezulta din prezentarea, în contextul unei proceduri judiciare, fără consimțământul său, a unor informații privind starea sa de sănătate ar fi fost amplificată dacă probele în cauză ar fi intrat în domeniul public după termenul de zece ani (*ibidem*, pct. 112). În schimb, în cauza *Y. împotriva Turciei* (dec.), 2015 (pct. 81-82), faptul că identitatea și seropozitivitatea reclamantului fuseseră dezvăluite într-o singură decizie privind lipsa de competență emisă de o instanță administrativă care fusese publicată sau făcută publică și care nu fusese pusă la dispoziția publicului, în măsura în care niciuna dintre celelalte decizii pronunțate în cadrul aceleiași proceduri cu care fusese sesizată nu a fost considerată ca aducând atingere dreptului la respectarea vieții private al persoanei vizate.

268. În cauza *Drakšas împotriva Lituaniei*, 2012 (pct. 60), divulgarea, în contextul procedurii de punere sub acuzare, a înregistrărilor convorbirilor telefonice interceptate de serviciile secrete dintre reclamant, un politician cunoscut, și președintele vizat de procedura de destituire, în cadrul unei ședințe publice în fața Curții Constituționale, difuzată în direct de posturile de televiziune naționale, nu a condus la constatarea unei încălcări a art. 8. În opinia Curții, în calitate de persoană publică, reclamantul era expus în mod inevitabil și conștient unui control atent al faptelor și gesturilor sale atât de către jurnaliști, cât și de către publicul larg. Prin urmare, divulgarea, prevăzută de lege, a convorbirilor telefonice fără caracter privat, dar de natură politică sau comercială, în cursul unei proceduri constituționale era necesară pentru protejarea drepturilor altora.

269. În cauza *A.P. împotriva Armeniei*, 2024 (pct. 150-162), Curtea a statuat că publicarea datelor cu caracter personal ale reclamantei, precum și textul integral al hotărârilor judecătorești de respingere a cererii sale de despăgubiri pentru abuz sexual constituie o încălcare a dreptului său la respectarea vieții private. Informațiile în cauză fuseseră publicate într-o bază de date judiciară oficială online accesibilă publicului, cu toate că reclamanta solicitase în mod expres ca aceste informații să nu fie publicate. Curtea a statuat că publicarea în cauză nu avea niciun temei juridic în dreptul național și a concluzionat că ingerința nu era „prevăzută de lege” în sensul articolului 8 din Convenție.

270. A se vedea, de asemenea, supra pct. 255 din prezentul ghid privind comunicarea către presă, de către serviciile polițienești, a fotografiilor persoanelor arestate sau urmărite penal fără consimțământul acestora, și supra, pct. 80 – 82 privind obligațiile pozitive ale statului în cauzele referitoare la divulgarea de date cu caracter personal de către persoane de drept privat.

c. Divulgarea de date pentru protejarea sănătății publice

271. Dreptul unei persoane la protecția confidențialității datelor sale medicale nu este absolut și trebuie conciliat cu alte drepturi și interese legitime, precum dreptul la o procedură contradictorie al angajatorului său [*Eternit împotriva Franței* (dec.), 2012, pct. 37]. Acesta poate fi anulat de necesitatea de a apăra un aspect primordial de interes public, cum ar fi siguranța personalului spitalicesc și protejarea sănătății publice [*Y. împotriva Turciei* (dec.), 2015, pct. 74].

272. În anumite circumstanțe, atunci când este în joc tratamentul pacienților în spitale și sistemul de sănătate, transmiterea de informații referitoare la starea unui pacient poate fi relevantă și necesară pentru a asigura nu doar tratamentul medical adecvat al pacientului, ci și protecția drepturilor și a intereselor personalului medical implicat în tratamentul său și al altor pacienți, permițând adoptarea măsurilor de precauție necesare [*Y. împotriva Turciei* (dec.), 2015, pct. 74]. În cazul în care lucrătorii din domeniul sănătății sunt ei înșiși expuși unui risc de infecție din cauza expunerii în cursul activității

lor, siguranța personalului spitalicesc și protejarea sănătății publice pot justifica transmiterea de informații privind starea de sănătate a unui pacient între diferiții operatori medicali implicați în îngrijirea sa, pentru a evita orice risc de transmitere intraspitalicească a bolii (*ibidem*, pct. 78).

273. Modalitățile de transmitere a unor date sensibile precum date privind sănătatea unui pacient trebuie să se facă cu preocuparea de a evita orice formă de stigmatizare a persoanei vizate și prin oferirea unor garanții suficiente pentru a exclude orice risc de abuz [*Y. împotriva Turciei* (dec.), 2015, pct. 79]. Destinatarul informațiilor trebuie să se supună normelor de confidențialitate specifice profesioniștilor din domeniul sănătății sau normelor de confidențialitate comparabile (*ibidem*, pct. 74).

274. În cauza *Y. împotriva Turciei* (dec.), 2015 (pct. 78-79), Curtea a respins ca vădit nefondată o cerere care privea divulgarea unor informații privind seropozitivitatea unui pacient între diferiții operatori medicali ai unui spital implicat în îngrijirea sa, considerând că siguranța personalului spitalicesc și protejarea sănătății publice puteau să o justifice în mod legitim, în pofida lipsei consimțământului persoanei vizate. A insistat asupra faptului că, în temeiul dreptului intern, fiecare operator medical era obligat să respecte confidențialitatea datelor care îi erau transmise ca urmare a situației sau a profesiei sale, sub sancțiunea expunerii la proceduri disciplinare sau penale.

d. Divulgarea de date pentru protejarea securității naționale

275. Într-o serie de cauze care priveau desființarea moștenirii fostelor regimuri comuniste, Curtea a examinat problema divulgării către public a datelor privind trecutul îndepărtat al unei persoane, colectate și stocate pentru a proteja securitatea națională [*Sõro împotriva Estoniei*, 2015, pct. 58; *Anchev împotriva Bulgariei* (dec.), 2017, pct. 100]. Aspectele legate de individualizarea măsurilor puse în aplicare pentru desființarea, încadrarea acestora și garanțiile oferite sunt importante.

276. Astfel, în cauza *Sõro împotriva Estoniei*, 2015 (pct. 56-64), divulgarea unor informații care indicau faptul că reclamantul fusese angajat ca șofer în cadrul fostelor servicii de securitate a condus la constatarea unei încălcări a art. 8. Deși reclamantul fusese informat în prealabil cu privire la faptul că publicarea urma să aibă loc și deși fusese în măsură să conteste comunicarea, nu exista nicio procedură care să permită evaluarea sarcinii specifice îndeplinite în mod individual de către angajații serviciilor de securitate și, prin urmare, diferențierea în funcție de pericolul pe care aceștia îl puteau reprezenta într-un sistem democratic, la mulți ani după încheierea carierei lor în cadrul respectivelor servicii (*ibidem*, pct. 61). În opinia Curții, trecerea unei mari perioade de timp între publicarea datelor cu caracter personal și restabilirea independenței Estoniei a redus în mod necesar pericolul pe care reclamantul îl putea reprezenta inițial pentru noul sistem democratic (*ibidem*, pct. 62). Chiar dacă legea privind divulgarea nu impunea, în sine, limitări asupra noului loc de muncă al reclamantului, reclamantul a fost constrâns să își părăsească postul din cauza atitudinii colegilor săi față de el, ceea ce demonstrează gravitatea ingerinței în dreptul reclamantului la respectarea vieții private (*ibidem*, pct. 63).

277. În schimb, în cauza *Anchev împotriva Bulgariei* (dec.), 2017 (pct. 92-116), în care procesul de divulgare era puternic încadrat și asociat cu o serie de garanții împotriva arbitrariului și abuzurilor, inclusiv faptul că fusese încredințat unei comisii independente speciale, ale cărei decizii puteau face obiectul unui control jurisdicțional public la două niveluri de jurisdicție, divulgarea publică a datelor referitoare la trecutul îndepărtat al reclamantului nu a fost considerată incompatibilă cu art. 8. Întrucât divulgarea nu a condus la sancțiuni sau incapacități juridice, ingerința nu a depășit marja largă de apreciere de care se bucurau autoritățile (*ibidem*, pct. 106-113). Curtea a declarat despre concluzia sa că ar fi putut fi una diferită în cazul în care statul ar fi recurs la măsuri care să implice un grad mai ridicat de intruziune în sfera personală a persoanei vizate, precum interzicerea exercitării unei profesii sau privarea parțială de dreptul de vot (*ibidem*, pct. 113).

e. Divulgarea de date pentru protejarea bunăstării economice a țării

278. Măsurile, considerate a asigura protejarea bunăstării economice a țării, care aduc atingere confidențialității datelor colectate sau stocate de autorități nu sunt în mod necesar contrare art. 8 dacă sunt însoțite de garanții efective și satisfăcătoare (*M.S. împotriva Suediei*, 1997, pct. 41). În punerea în balanță a intereselor aflate în joc, întrebarea dacă dreptul intern reglementează sau nu măsurile pe care le pot lua operatorii de date, dacă responsabilitatea lor este angajată în caz de nerespectare a cerințelor legale și dacă obligația de a respecta norme și garanții similare, în special obligația de confidențialitate, revine destinatarului datelor, sunt elemente importante de luat în considerare (*ibidem*, pct. 43).

279. În cauza *M.S. împotriva Suediei*, 1997 (pct. 31-44), transmiterea dosarului medical al unei persoane de către un organ public (serviciul de ginecologie al unui spital) către un alt organ (casa de asigurări Sociale), care avea responsabilitatea de a aprecia dacă persoana vizată îndeplinea condițiile legale pentru a obține o prestație pe care o solicitase nu a condus la o încălcare a art. 8. În opinia Curții, această comunicare era potențial decisivă pentru alocarea de fonduri publice solicitanților care îndeplineau anumite criterii și, prin urmare, putea fi considerată ca fiind destinată să protejeze bunăstarea economică a țării (*ibidem*, pct. 38). Divulgarea datelor confidențiale ale persoanei vizate era însoțită de garanții efective și satisfăcătoare împotriva abuzurilor: legislația națională impunea ca informațiile să fie relevante pentru aplicarea legii privind asigurarea în caz de invaliditate profesională (*ibidem*, pct. 18, 43); răspunderea civilă și/sau penală a personalului serviciului de ginecologie în cazul în care nu ar fi respectat aceste condiții (*ibidem*, pct. 22, 43); iar destinatarul datelor avea o obligație similară, de a le respecta confidențialitatea (*ibidem*, pct. 20, 22, 43).

280. Cauza *L.B. împotriva Ungariei* (MC), 2023 (pct. 20-29) se referea la publicarea pe lista principalilor contribuabili debitori, disponibilă pe site-ul web al autorității fiscale naționale, a datelor cu caracter personal referitoare la reclamant (inclusiv numele și adresa acestuia). Introdusă în legislația relevantă ca instrument de combatere a nerespectării legislației fiscale, publicarea sistematică și obligatorie a acestor date s-a aplicat tuturor contribuabililor care, la sfârșitul trimestrului, aveau de plătit impozite semnificative pentru o perioadă mai mare de 180 de zile consecutive. Curtea a subliniat că alegerea de către legiuitor a unui astfel de regim general nu era problematică în sine; același raționament fiind valabil și pentru publicarea datelor contribuabililor ca atare. Aceasta a precizat, de asemenea, că statele contractante dispuneau de o largă marjă de apreciere pentru a stabili, în special în scopul asigurării bunei funcționări a colectării impozitului în ansamblul său, necesitatea de a institui un regim de divulgare a datelor cu caracter personal referitoare la contribuabilii care nu-și îndeplineau obligațiile de plată. Ea a adăugat însă că marja de apreciere de care dispun statele contractante în această privință nu era nelimitată și a precizat că, în acest context, trebuia să se asigure că autoritățile naționale competente, la nivel legislativ, executiv sau judiciar, au evaluat în mod corect interesele concurente și, în acest context, au ținut seama în mod corespunzător nu numai de (i) interesul public de a divulga informațiile în cauză, ci și de (ii) natura informațiilor divulgate, de (iii) repercusiunile asupra exercitării de către persoanele vizate a dreptului la respectarea vieții lor private și de riscul de atingere a acestui drept, de (iv) amploarea potențială a suportului utilizat pentru difuzarea informațiilor, în special a internetului, și de (v) principiile fundamentale ale protecției datelor, în special cele referitoare la limitarea scopurilor, la limitarea păstrării, la reducerea la minimum a datelor și la exactitatea acestora.

Curtea a precizat de asemenea că existența unor garanții procedurale ar putea juca, de asemenea, un rol important în acest context (*ibidem*, pct. 128).

281. În ceea ce privește situația în fapt, Curtea a subliniat două caracteristici ale regimului de publicare în cauză: includerea în datele cu caracter personal care trebuie publicate a adresei domiciliului contribuabilului și faptul că autoritatea fiscală națională nu dispunea de nicio marjă de apreciere pentru a efectua o evaluare individuală a proporționalității măsurii. Luând în considerare aceste elemente, Curtea a analizat calitatea controlului efectuat de legiuitor și a identificat

următoarele deficiențe: (i) neevaluarea necesității și a complementarității măsurii generale în cauză (în special în ceea ce privește obligația de a publica adresa de domiciliu a contribuabilului debitor) în lumina instrumentelor existente care urmăresc același scop disuasiv, (ii) neluarea în considerare a impactului asupra dreptului la viață privată și, în special, a riscului de utilizare abuzivă a adresei de domiciliu a contribuabilului debitor de către alți membri ai publicului, (iii) neluarea în considerare a domeniului de aplicare potențial al suportului utilizat pentru difuzarea informațiilor în cauză (internet), care implica accesul nelimitat la informații destul de sensibile (numele și adresa persoanei vizate), cu riscul ca republicarea să fie o consecință naturală, probabilă și previzibilă a publicării inițiale și (iv) neluarea în considerare a cerințelor de protecție a datelor prevăzute de dreptul național și de dreptul Uniunii și posibilitatea de a lua măsuri pentru a concepe răspunsuri suficient de adecvate având în vedere principiul reducerii la minimum a datelor. În acest context, Curtea a concluzionat că, în pofida marjei largi de apreciere de care dispune statul pârât, ingerința în cauză nu era „necesară într-o societate democratică” (*ibidem*, pct. 129-140).

f. Divulgarea în masă de date cu caracter personal

282. Existența unui interes general ca astfel de cantități mari de date fiscale să fie accesibile și să poată fi colectate în scopuri jurnalistice nu înseamnă în mod necesar sau automat că există, de asemenea, și un interes general de a difuza în masă astfel de date brute, ca atare, fără niciun aport analitic. În cauza *Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei* (MC), 2017 (pct. 175), Curtea a subliniat că trebuie să se facă o distincție între prelucrarea datelor în scopuri jurnalistice și difuzarea de date brute la care jurnaliștii au acces în condiții privilegiate. Fapta de a împiedica ca date cu caracter personal de natură fiscală să fie difuzate în masă, potrivit unor modalități contrare reglementărilor naționale și normelor Uniunii Europene privind protecția datelor nu constituie, în sine, o sancțiune, chiar dacă limitările impuse cantităților de date de publicat ar putea, în practică, să facă să fie mai puțin profitabile activitățile comerciale ale societăților reclamante (*ibidem*, pct. 197).

B. Drepturile persoanelor vizate

283. Jurisprudența Curții recunoaște că persoanele vizate de date cu caracter personal au o serie de prerogative care le permit să beneficieze de dreptul garantat de art. 8 din Convenție.

1. Dreptul de acces la datele proprii

284. Persoanele ale căror date cu caracter personal au fost colectate și stocate de autorități au un interes, protejat de art. 8, să primească informațiile: colectate în privința lor de către fostele servicii secrete în timpul regimurilor totalitare și păstrate în arhivele statului (*Haralambie împotriva României*, 2009, pct. 79; *Jarnea împotriva României*, 2011, pct. 50; *Joanna Szulc împotriva Poloniei*, 2012, pct. 87); necesare în ceea ce privește sănătatea lor sau riscurile pentru sănătatea lor, la care au fost expuse [*Roche împotriva Regatului Unit* (MC), 2005, pct. 155; *K.H. și alții împotriva Slovaciei*, 2009, pct. 44; *Yonchev împotriva Bulgariei*, 2017, pct. 46]; pentru a afla și a-și înțelege copilăria și anii perioadei de formare (*Gaskin împotriva Regatului Unit*, 1989, pct. 41); sau pentru a-și identifica originile, în special identitatea părinților lor [*Odièvre împotriva Franței* (MC), 2003, pct. 43-44; *Godelli împotriva Italiei*, 2012, pct. 62-63; *M.G. împotriva Regatului Unit*, 2002, pct. 27].

285. În aceste diferite contexte, autoritățile au obligația pozitivă inerentă de a respecta efectiv dreptul la viață privată, garantat de art. 8, de a prevedea o procedură eficientă și accesibilă care să permită părților interesate să aibă acces la toate informațiile relevante și adecvate necesare unor scopuri specifice [*Roche împotriva Regatului Unit* (MC), 2005, pct. 162; *Haralambie împotriva României*, 2009, pct. 86; *Joanna Szulc împotriva Poloniei*, 2012, pct. 86, 94).

286. În schimb, atunci când statul se poate teme în mod legitim că accesul la informații care conțin date cu caracter personal riscă să compromită eficacitatea sistemului de supraveghere secretă destinat să protejeze securitatea națională sau să combată terorismul, poate refuza accesul la

informațiile colectate și stocate într-un registru secretizat, fără ca acest fapt să fie incompatibil cu obligația pozitivă care le revine autorităților în temeiul art. 8 (*Leander împotriva Suediei*, 1987, pct. 66; *Segerstedt-Wiberg și alții împotriva Suediei*, 2006, pct. 102). Pentru a stabili dacă statul este îndreptățit să considere că interesele legate de securitatea națională și combaterea terorismului prevalează asupra interesului unei persoane de a avea acces la toate informațiile care o privesc, stocate de serviciile de securitate, Curtea trebuie să se asigure că există suficiente garanții împotriva arbitrariului. Calitatea legii (*ibidem*, pct. 79-80) și garanțiile instituite, în special posibilitatea controlului măsurii în cauză și căile de atac de care dispune persoana vizată la nivel național (*ibidem*, pct. 52-68), sunt criterii importante care trebuie luate în considerare atunci când sunt puse în balanță interesele aflate în joc (*ibidem*, pct. 103). Principii similare se aplică în contextul expulzării străinilor. În cauza *Hassine împotriva României*, 2021, pct. 55-69, reclamantul, resortisant tunisian cu reședința legală în România, fusese expulzat din România din motive de securitate națională și i se interzisese dreptul de ședere în România pentru o perioadă de cinci ani, pe baza informațiilor furnizate de serviciile secrete române. Aceste informații, clasificate secrete, indicau, potrivit autorităților, că era implicat în activități de natură să aducă atingere securității naționale. Nici reclamantul, nici avocatul său nu au primit autorizația să ia cunoștință despre acestea. Curtea a hotărât că procedura administrativă de expulzare a reclamantului nu prezentase garanțiile procedurale necesare și a concluzionat că a fost încălcat art. 1 din Protocolul nr. 7.

287. Distrugerea imediată a datelor colectate, din momentul în care acestea sunt considerate irelevante pentru colectarea în cauză, nu este, în sine, contrară Convenției, chiar dacă o astfel de măsură a avut ca efect împiedicarea persoanelor vizate să consulte datele respective. Acestea fiind spuse, persoanele vizate pot avea un interes legitim să obțină o copie a deciziei emise de autoritatea competentă pentru a dispune distrugerea obiectelor interceptate, precum și „actul" distrugerii (*Denisiuk și alții împotriva Ucrainei*, 2025, pct. 108-109). În plus, este imperativ să se stabilească și să se facă publice norme și orientări clare care să definească procedura de control și distrugere a documentelor interceptate, inclusiv norme privind controlul procedurilor relevante de către un organism independent (*Denisiuk și alții împotriva Ucrainei*, 2025, pct. 110-113).

288. Într-o cauză care privea includerea pe termen lung a datelor cu caracter personal ale reclamantului în sistemul de informații Schengen, Curtea a hotărât că imposibilitatea părții interesate de a obține accesul personal la integralitatea informațiilor pe care le solicitase nu adusese atingere dreptului la respectarea vieții sale private, având în vedere necesitatea imperioasă de a proteja securitatea națională [*Dalea împotriva Franței* (dec.), 2010]. Chiar dacă partea interesată nu avusese posibilitatea de a se opune motivului specific al acestei includeri, avusese cunoștință despre toate celelalte date care o priveau din sistemul Schengen, iar semnalarea sa ca persoană inadmisibilă se întemeia pe considerații care țineau de siguranța statului, apărare și siguranța publică (*ibidem*, cu trimitere la *Leander împotriva Suediei*, 1987, pct. 66).

289. Atunci când doar o parte din documentele cuprinse într-un sistem de evidență a datelor păstrat de autorități cu privire la o persoană care conțin date cu caracter personal au fost clasificate secrete din motive de apărare, autoritățile ar putea permite părții interesate accesul parțial la acestea (*Yonchev împotriva Bulgariei*, 2017, pct. 55-59). Astfel, într-o cauză în care era în discuție refuzul autorităților de a permite reclamantului, fost polițist, să consulte anumite documente din dosarul său personal, în speță evaluările sale psihologice, Curtea a concluzionat că a fost încălcat art. 8 ca urmare a existenței, la nivel național, a unor reguli excesiv de formale, potrivit cărora, în cazul în care numai unul dintre documentele din dosar a fost clasificat secret, restul trebuiau, de asemenea, să fie considerat automat clasificate și, prin urmare, supuse regulilor de protecție a informațiilor clasificate (*ibidem*, pct. 60).

290. În cazul în care dreptul intern prevedea în mod expres un drept de acces la dosarul personal colectat și păstrat de fostele servicii de securitate în timpul regimurilor totalitare ale fostelor state comuniste, statul era obligat să ofere o procedură efectivă și accesibilă care să permită părții interesate să aibă acces, într-un termen rezonabil, la toate informațiile relevante (*Haralambie*

împotriva României, 2009, pct. 86; *Jarnea împotriva României*, 2011, pct. 50; *Antoneta Tudor împotriva României*, 2013, pct. 34; *Joanna Szulc împotriva Poloniei*, 2012, pct. 86, 94). Curtea a concluzionat că a fost încălcat art. 8 într-o cauză în care reclamantul nu a putut avut acces decât la o parte din dosarul pe numele său, colectat și păstrat de fostele servicii secrete (*Jarnea împotriva României*, 2011, pct. 54-60) și în alte două cauze în care accesul la documentele care îi priveau nu a fost permis decât la zece ani de la prima cerere a părților interesate (*Joanna Szulc împotriva Poloniei*, 2012, pct. 93-95; *Antoneta Tudor împotriva României*, 2013, pct. 34-40). Deficiențe ale sistemului de arhivare sau erori materiale precum o eroare în înscrierea datei de naștere a reclamantului în dosarul personal identificat pe numele său nu au putut justifica o perioadă de așteptare de șase ani înainte de a avea acces la datele sale cu caracter personal (*Haralambie împotriva României,* 2009, pct. 95). Vârsta înaintată a unei persoane care solicită accesul la acest tip de informații face să fie și mai urgent interesul său de a-și rememora parcursul personal în perioada regimului totalitar (*ibidem*, pct. 93 *in fine*).

291. În ceea ce privește informațiile referitoare la sănătate sau riscurile pentru sănătate, dreptul de acces la datele cu caracter personal se extinde la punerea la dispoziție, în favoarea persoanei vizate, a unor copii ale dosarelor care o privesc (*K.H. și alții împotriva Slovaciei*, 2009, pct. 47). Revine deținătorului unor astfel de dosare sarcina de a defini măsurile care trebuie luate pentru a permite persoanei vizate să copieze documentele și să stabilească cine trebuie să suporte costurile implicate (*ibidem*, pct. 48). Persoana vizată nu trebuie să fie constrânsă să își justifice cererea. Autorităților le revine sarcina de a demonstra existența unor motive imperioase pentru refuzul unui astfel de serviciu (*ibidem* pct. 48). În cauza *K.H. și alții împotriva Slovaciei*, 2009 (pct. 50-58), fostele paciente ale unui spital s-au regăsit în imposibilitatea de a fotocopia dosarele originale, colectate și păstrate de un spital public, care conțineau informații pe care le considerau importante din punctul de vedere al integrității lor morale și fizice. În opinia Curții, posibilitatea, care le fusese acordată de spital, de a lua note exclusiv olografe ale dosarelor originale nu le oferise un acces efectiv la documentele relevante privind sănătatea lor.

292. În cazul în care un stat se implică în activități periculoase care pot avea consecințe negative ascunse pentru sănătatea persoanelor care participă la acestea, autoritățile au obligația pozitivă de a oferi persoanelor vizate o „procedură efectivă și accesibilă” care să le permită să aibă acces la „toate informațiile relevante și adecvate” și, astfel, să evalueze orice risc pentru sănătatea lor la care ar fi putut fi expuse [*McGinley și Egan împotriva Regatului Unit*, 1998, pct. 101; *Roche împotriva Regatului Unit* (MC), 2005, pct. 161-162]. O perioadă de așteptare nerezonabilă, de exemplu atunci când serviciile de informare și studii de sănătate au inițiat procese de căutare și de divulgare a documentelor relevante la aproximativ zece ani de la momentul la care partea interesată a început să caute documentele relevante, a constitut o încălcare din partea statului, contrar art. 8, a obligației sale pozitive inerente în ceea ce privește viața privată a persoanei vizate, în pofida dificultăților legate de vechimea și caracterul dispersat al respectivelor documente (*ibidem*, pct. 166).

293. În ceea ce privește accesul la datele cu caracter personal ale unei persoane încredințate, în copilărie, serviciilor sociale în urma decesului părinților săi sau având în vedere incapacitatea acestora de a-i avea îngriji, un sistem care permite accesul la dosare cu condiția consimțământului din partea „informatorilor”, și anume a persoanelor aflate la originea documentelor relevante, poate fi, în principiu, compatibil cu art. 8, având în vedere marja de apreciere a statului. Cu toate acestea, sistemul trebuie să protejeze interesele oricărei persoane care dorește să consulte documente referitoare la viața sa privată și de familie și, în cazul în care informatorul nu răspunde sau nu își dă consimțământul, acest fapt nu este compatibil cu principiul proporționalității decât dacă un organ independent preia sarcina de a lua decizia finală cu privire la accesul la date (*Gaskin împotriva Regatului Unit*, 1989, pct. 49). În cauzele în care sistemul național nu prevedea recursul la un astfel de organ în cazul refuzului serviciilor sociale de a acorda acces la toate documentele din dosarul aflat în posesia lor, inclusiv în cazul în care o terță parte vizată sau aflată la originea informațiilor nu a consimțit ca datele

să fie divulgate, Curtea a constatat o încălcare a art. 8 (*ibidem,* pct. 49; *M.G. împotriva Regatului Unit*, 2002, pct. 30-32).

294. În opinia Curții, un copil născut în afara căsătoriei care încearcă să stabilească o legătură juridică cu tatăl său natural are un interes vital, protejat de Convenție, de a obține informațiile care îi sunt indispensabile pentru a descoperi adevărul despre un aspect important al identității sale personale (*Mikulić împotriva Croației*, 2002, pct. 64; *Boljević împotriva Serbiei*, 2020, pct. 50). Un sistem care nu prevede mijloace pentru a constrânge pretinsul tată să se conformeze unui ordin al unei instanțe prin care i se impune să efectueze teste ADN poate fi considerat, în principiu, compatibil cu obligațiile care decurg din art. 8, având în vedere marja de apreciere a statului (*Mikulić împotriva Croației*, 2002, pct. 64). Cu toate acestea, lipsa oricărei măsuri procedurale obligatorii în cauză nu este conformă cu principiul proporționalității decât dacă sistemul în cauză oferă alte mijloace prin care o autoritate independentă să poată să se pronunțe cu celeritate cu privire la acțiunea în stabilirea paternității (*ibidem*, pct. 64). Curtea a concluzionat că a fost încălcat art. 8 atunci când, în cazul refuzului pretinsului tată de a coopera la procedura medicală, sistemul național nu oferea nici măsuri pentru a-l obliga să participe la testele ADN, nici alte mijloace prin care o autoritate independentă să poată să se pronunțe cu celeritate cu privire la acțiunea în stabilirea paternității (*ibidem*, pct. 64). Interesul pe care îl poate avea o persoană de a-și cunoaște descendența nu încetează în niciun fel odată cu vârsta, ci dimpotrivă (*Jäggi împotriva Elveției*, 2006, pct. 40, care privea refuzul de a autoriza o expertiză ADN asupra unui defunct, solicitată de presupusul fiu care dorea să își stabilească cu certitudine filiația; *Boljević împotriva Serbiei*, 2020, pct. 54).

295. În ceea ce privește copiii născuți în urma unor nașteri anonime, chestiunea accesului la origini și la cunoașterea identității părinților biologici nu este aceeași cu cea a accesului la dosarul personal al unui copil luat în îngrijire sau cu cea a obținerii de probe privind o pretinsă paternitate [*Odièvre împotriva Franței* (MC), 2003, pct. 43; *Godelli împotriva Italiei,* 2012, pct. 62]. Având în vedere diversitatea sistemelor și tradițiilor juridice, statele trebuie să dispună de o anumită marjă de apreciere pentru a păstra confidențialitatea identității părinților biologici [*Odièvre împotriva Franței* (MC), 2003, pct. 46; *Godelli împotriva Italiei,* 2012, pct. 65]. S-a constatat că un sistem național care permitea părții interesate să aibă acces la informații fără date de identificare cu privire la mama sa și la familia sa biologică, care să permitea să își reconstituie istoria personală, respectând totodată protecția intereselor părților terțe, însoțit de posibilitatea, deschisă în temeiul unei legi recent adoptate, de a face apel la un organism independent însărcinat cu facilitarea căutării originilor biologice pentru a solicita dezvăluirea secretului identității mamei sale sub rezerva acordului acesteia, a fost considerat conform cu art. 8 [(*Odièvre împotriva Franței* (MC), 2003, pct. 49; a se vedea, de asemenea, în ceea ce privește accesul persoanelor născute prin reproducere medicală asistată cu donatori terți la informațiile referitoare la donator *Gauvin-Fournis și Silliau împotriva Franței*, 2023, pct. 113-33). În schimb, un sistem care acorda o preferință necondiționată mamei care dorea să își păstreze anonimatul și care nu oferea copilului adoptat și nerecunoscut la naștere nicio posibilitate de a solicita accesul la informații fără date de identificare cu privire la originea sa sau la caracterul reversibil al secretului a fost considerat ca nefiind conform cu cerințele art. 8 (*Godelli împotriva Italiei*, 2012, pct. 70-72).

2. Dreptul de rectificare

296. Curtea a examinat o serie de cauze care priveau stocarea de către autorități a unor date false sau a căror exactitate era contestată de partea interesată [*Rotaru împotriva României* (MC), 2000, pct. 42-44, 55-63, care privea imposibilitatea de a contesta datele referitoare la pretinsa participare a unei persoane la mișcarea legionară într-un dosar colectat de serviciile de securitate; *Cemalettin Canlı împotriva Turciei*, 2008, pct. 34-37, care privea prezența în cadrul procedurilor judiciare a unor date cu caracter personal incomplete, colectate de poliție; *Khelili împotriva Elveției*, 2011, pct. 56, care privea menținerea în evidențele poliției a termenului „prostituată” ca fiind activitatea unei persoane, activitate în care contestase în mod sistematic că ar fi fost implicată].

297. Lipsa posibilității ca o persoană să obțină rectificarea unei înscrieri despre aceasta în fișierele sistemului de informații Schengen [*Dalea împotriva Franței* (dec.), 2010] sau înscrierea originii etnice în registrele oficiale (*Ciubotaru împotriva Moldovei*, 2010, pct. 59) constituie o ingerință în dreptul la respectarea vieții private al acesteia. În anumite circumstanțe, în special atunci când intervin considerente care țin de siguranța statului, de apărare și de siguranța publică, o astfel de ingerință nu este în mod necesar incompatibilă cu art. 8 [*Dalea împotriva Franței* (dec.), 2010]. Existența unor garanții împotriva arbitrariului și posibilitatea ca măsura să fie controlată, prin procedură contradictorie, de un organ independent și imparțial, abilitat să examineze toate aspectele *de facto* și *de jure* relevante, pentru a se pronunța cu privire la legalitatea măsurii și pentru a sancționa orice abuz din partea autorităților, sunt esențiale (*ibidem*, cu trimitere la *Leander împotriva Suediei*, 1987, pct. 66).

298. Informațiile cu caracter personal false sau incomplete colectate și stocate de autorități pot îngreuna viața de zi cu zi a persoanei vizate (*Khelili împotriva Elveției*, 2011, pct. 64), se pot dovedi defăimătoare [*Rotaru împotriva României* (MC), 2000, pct. 44] sau pot ignora o serie de garanții procedurale importante prevăzute de lege pentru a proteja drepturile persoanelor vizate (*Cemalettin Canlı împotriva Turciei*, 2008, pct. 35, 40-42). Într-o cauză în care un dosar al poliției intitulat „notă de informare privind alte infracțiuni" a fost prezentat în fața unei instanțe naționale făcând trimitere la două acțiuni penale inițiate în trecut pentru apartenența la organizații ilegale împotriva persoanei anchetate, Curtea a constatat o încălcare a art. 8. În speță, nu numai că informațiile indicate în dosar erau false, dar nici nu fusese menționată nicăieri achitarea părții interesate în cursul primei proceduri penale și scoaterea de sub urmărire penală în cursul celei de-a doua acțiuni penale (*ibidem*, pct. 42). Omisiunea de a menționa rezultatul procedurilor menționate era contrară obligațiilor neechivoce prevăzute de normele de drept intern, înlăturând o serie de garanții procedurale importante prevăzute de lege pentru a proteja drepturile reclamantului (*ibidem*, 2008, pct. 42).

299. Impunerea în sarcina unei persoane care solicită rectificarea datelor sale cu caracter personal în registrele oficiale ale statului a unei cerințe care îi creează acesteia un obstacol insurmontabil se poate dovedi incompatibilă cu obligația statului de a garanta respectarea efectivă a vieții sale private (*Ciubotaru împotriva Moldovei*, 2010, pct. 51-59). Într-o cauză care privea imposibilitatea ca reclamantul să obțină modificarea înscrierii originii sale etnice în registrele oficiale, cerința de a dovedi că părinții săi aparțineau unei anumite etnii a creat pentru persoana vizată un obstacol insurmontabil în calea înscrierii unei identități etnice, alta decât cea atribuită părinților săi, de către autorități (*ibidem*, pct. 57).

300. În contextul cererilor de rectificare a registrelor de stare civilă pentru a ține seama de noua situație a unei persoane transsexuale care a fost supusă unei operații, existența unei necesare coerențe, în ordinea internă, a unor practici administrative și juridice constituie un element important care trebuie luat în considerare pentru a aprecia necesitatea, din perspectiva art. 8, a unor astfel de cereri [*Christine Goodwin împotriva Regatului Unit* (MC), 2002, pct. 78]. Într-o cauză care privea refuzul autorităților de a modifica registrul de nașteri, Curtea s-a declarat surprinsă de faptul că schimbarea de gen a părții interesate, care fusese efectuată în mod legal și fusese realizată de serviciul național de sănătate, nu a condus la o consacrare juridică în drept, ca etapa ultimă și finalizarea procesului de transformare lung și dificil suferit de partea interesată [*ibidem*, pct. 78, care a condus la o inversare a jurisprudenței pentru a ține seama de evoluția științei și a societății față de hotărârile mai vechi, în special față de cauzele *Rees împotriva Regatului Unit*, 1986, pct. 42-44, *Cossey împotriva Regatului Unit,* 1990, pct. 39-40, și *Sheffield și Horsham împotriva Regatului Unit* (MC), 1998, pct. 60-61]. Atunci când un stat autorizează un tratament și o intervenție chirurgicală pentru a ușura situația unei persoane transsexuale, finanțează în totalitate sau parțial o parte dintre operații și ajunge până la a consimți la inseminarea artificială a unei femei care era partenera unei persoane transsexuale, pare ilogic ca acesta să refuze recunoașterea consecințelor juridice ale rezultatului la care a condus tratamentul [*Christine Goodwin împotriva Regatului Unit* (MC), 2002, pct. 78], cu atât mai mult atunci

când dificultățile legate de rectificarea sexului înscris inițial în registrul de nașteri sunt departe de a fi insurmontabile (*ibidem*, pct. 91).

301. În cauza *S.V. împotriva Italiei*, 2018 (pct. 72), refuzul autorităților de a autoriza schimbarea de nume a unei persoane transsexuale în cursul procesului de tranziție sexuală și înainte de finalizarea operațiunii de schimbare de gen se întemeia pe o procedură judiciară rigidă care plasase reclamanta pentru o perioadă nerezonabilă de doi ani și jumătate într-o situație anormală, inspirându-i sentimente de vulnerabilitate, umilire și anxietate.

302. Curtea a considerat în cauza *Hämäläinen împotriva Finlandei* (MC), 2014 (pct. 87-89), că nu era disproporționat să se prevadă ca o condiție prealabilă pentru recunoașterea juridică a schimbării de sex că căsătoria dintre un bărbat devenit femeie cu o altă femeie trebuie să se transforme în parteneriat înregistrat, aceasta din urmă fiind o opțiune serioasă care oferea cuplurilor de același sex o protecție juridică practic identică cu căsătoria, întrucât dreptul finlandez interzicea căsătoria între persoane de același sex. În consecință, nu se putea afirma că, din cauza diferențelor minore care existau între aceste două forme juridice de uniune, sistemul în vigoare nu permitea statului finlandez să își îndeplinească obligațiile pozitive care îi reveneau. A se vedea, de asemenea, cauza *A.P., Garçon și Nicot împotriva Franței*, 2017, care privea condițiile juridice pentru schimbarea stării civile a persoanelor transgen, precum ireversibilitatea transformării înfățișării (pct. 116-135), realitatea sindromului transsexual (pct. 138-144) și obligația de a se supune unui examen medical (pct. 149-154).

3. Dreptul la ștergere

303. Chestiunea dreptului la ștergerea datelor cu caracter personal după expirarea unei anumite perioade de timp a fost abordată de Curte în contexte diferite și, în special legătură cu:

- „dreptul de a fi uitat” în ceea ce privește o decizie sau o practică a mass-mediei de a (re)publica sau de a pune la dispoziție pe site-urile lor internet informații sau arhive care conțin date cu caracter personal, inclusiv numele, prenumele și fotografiile persoanelor vizate, care au fost divulgate în trecut [*Węgrzynowski și Smolczewski împotriva Poloniei*, 2013; *M.L. și W.W. împotriva Germaniei*, 2018; *Biancardi împotriva Italiei*, 2021;*Mediengruppe Österreich GmbH împotriva Austriei*, 2022; *Hurbain împotriva Belgiei* [GC], 2023];
- posibilitatea ca persoanele acuzate sau doar suspectate de săvârșirea unei infracțiuni să obțină, după o anumită perioadă de timp, ștergerea datelor lor cu caracter personal (profil ADN, fotografii de identitate și amprente digitale), colectate de autorități, din bazele de date create cu scopul de a preveni și combate infracțiunile (*B.B. împotriva Franței*, 2009; *Gardel împotriva Franței*, 2009; *M.B. împotriva Franței*, 2009; *M. K. împotriva Franței*, 2013; *Brunet împotriva Franței*, 2014; *Ayçaguer împotriva Franței*, 2017; *Catt împotriva Regatului Unit*, 2019; *Gaughran împotriva Regatului Unit*, 2020);
- imposibilitatea ca o persoană să obțină ștergerea antecedentelor din cazierul său judiciar după o anumită perioadă de timp (*M.M. împotriva Regatului Unit*, 2012);
- păstrarea prelungită în arhivele Securității a datelor cu caracter personal ale reclamanților care nu mai îndeplineau cerința de a fi „necesare într-o societate democratică”, având în vedere natura și vechimea lor (*Segerstedt-Wiberg și alții împotriva Suediei*, 2006).

a. „Dreptul de a fi uitat”

304. Deși noțiunea de „drept de a fi uitat” s-a născut recent și este încă în construcție, aplicarea sa în practică este deja foarte specifică [*Hurban împotriva Belgiei* (MC), 2023, pct. 191 și 194]. Această noțiune a fost elaborată pentru prima dată în practica judiciară națională în contextul utilizării de către presă a unor informații de natură judiciară deja divulgate în trecut, persoana care invocă un „drept de a fi uitat” încercând în practică să obțină condamnarea persoanei care a preluat aceste informații

(*ibidem*, pct. 194). În continuare, o nouă formă a acestui „drept de a fi uitat” s-a dezvoltat în practica judiciară națională în contextul digitalizării articolelor de presă, ceea ce a condus la difuzarea lor pe scară largă pe site-urile internet ale ziarelor în cauză. Efectul acestei difuzări a fost amplificat simultan de referințele create de motoarele de căutare. Această dispoziție, consacrată la nivel terminologic ca „dreptul de a fi uitat”, vizează cereri de ștergere, de modificare sau de restricționare a accesului la datele disponibile pe internet adresate redactorului de presă sau operatorului unui motor de căutare. În acest caz, nu este vorba despre reapariția informațiilor, ci despre permanența informațiilor pe internet (*ibidem*, pct. 195). În general, „dreptul de a fi uitat” poate da naștere în practică unor diverse măsuri care pot fi luate de operatorii motoarelor de căutare sau de redactorii de presă. Aceste măsuri privesc fie conținutul propriu-zis al unui articol arhivat, cum ar fi, de exemplu, ștergerea, modificarea sau anonimizarea unui articol, fie limitarea accesibilității informațiilor. În acest din urmă caz, accesul poate fi restricționat atât de motoarele de căutare, cât și de redactorii de presă. (*ibidem*, pct. 175).

305. În practica sa, Curtea a soluționat mai multe cauze referitoare la cereri de ștergere, de modificare, de anonimizare sau de dezindexare a unor articole de presă care conțin date cu caracter personal. Curtea a examinat aceste cauze fie din punctul de vedere al articolului 8, în cazul în care persoanele care au sesizat-o au invocat dreptul lor la respectarea vieții private (*Węgrzynowski și Smolczewski împotriva Poloniei*, 2013; *M.L. și W.W. împotriva Germaniei*, 2018), fie din cel al articolului 10, atunci când a fost sesizată de jurnaliști, redactori sau proprietari de mass-media care și-au invocat dreptul la libertatea de exprimare [*Biancardi împotriva Italiei*, 2021; *Mediengruppe Österreich GmbH împotriva Austriei*, 2022; *Hurbain împotriva Belgiei* (MC), 2023].

306. Mai specific, cauza *Biancardi împotriva Italiei*, 2021, pct. 67-70, a dat Curții ocazia, pentru prima dată, să se pronunțe cu privire la compatibilitatea cu art. 10 a condamnării în civil a unui jurnalist pentru că nu a dezindexat informațiile publicate pe Internet. În centrul cauzei se afla faptul că reclamantul nu a dezindexat informațiile sensibile publicate, care priveau o procedură penală inițiată împotriva unor persoane de drept privat, și decizia sa de a păstra articolul să fie ușor accesabil. Anonimatul protagoniștilor din articolul online nu era în discuție în această cauză. Curtea a observat că articolul rămăsese online și rămăsese ușor accesabil timp de opt luni, în timp ce partea interesată solicitase oficial ștergerea acestuia. Severitatea sancțiunii – care implica răspunderea civilă și nepenală – și cuantumul despăgubirii acordate nu au fost considerate excesive de către Curte.

307. În contextul publicării inițiale a informațiilor referitoare la trecutul unei persoane, Curtea a trebuit să se pronunțe cu privire la cauza *Mediengruppe Österreich GmbH împotriva Austriei*, 2022, care privea interdicția impusă de instanțele naționale unui ziar de a publica informații referitoare la o persoană care avea o legătură indirectă cu campania electorală a unui candidat la președinție. Ziarul în cauză a publicat o fotografie a fratelui șefului de cabinet al candidatului, care era activ în „cercurile de dreapta”, și a arătat că persoana vizată era un „neonazist condamnat”. Totuși, mai mult de 20 de ani trecuseră între această condamnare și publicarea articolului în cauză și aproximativ 17 ani de la eliberarea persoanei vizate. În plus, condamnarea fusese deja ștearsă din cazierul judiciar al reclamantului la momentul publicării articolului în cauză. Instanța superioară națională a subliniat că nu există nicio legătură temporală și a interzis societății reclamante să publice fotografii ale fratelui șefului de cabinet fără consimțământul persoanei vizate în cazul în care se afirma în același articol că acesta era un neonazist care fusese condamnat. Concluzionând că articolul 10 nu a fost încălcat, Curtea a ținut seama în special de timpul scurs între condamnarea, eliberarea și publicarea articolului în cauză, pierderea reputației persoanei vizate, faptul că persoana vizată nu a făcut obiectul niciunei condamnări penale anterioare, importanța reintegrării sociale a persoanelor care și-au executat pedeapsa, precum și interesul legitim și foarte important al acestor persoane de a nu fi confruntate cu condamnarea lor după o anumită perioadă de timp.

308. În ceea ce privește arhivele web ale mass media care conțin date cu caracter personal referitoare la o persoană care a făcut obiectul unei știri în trecut, Curtea a subliniat că acest context era diferit în raport cu cel al cauzelor privind publicațiile inițiale (*Hurban împotriva Belgiei* (MC), 2023, pct. 205) și

că, prin urmare, s-a ridicat în primul rând problema permanenței unor astfel de informații pe internet, iar nu cea a publicării lor inițiale (*ibidem*, pct. 174).

309. În acest context, Curtea a statuat în cauza *Węgrzynowski și Smolczewski împotriva Poloniei* (2013, pct. 60-70) că refuzul instanțelor de a dispune retragerea unui articol care aduce atingere reputației unui avocat și care este disponibil în arhivele online ale unui ziar nu constituie o încălcare a articolului 8. Curtea a admis că nu era rolul autorităților judiciare să rescrie istoria dispunând ștergerea din domeniul public a oricăror urme de publicații din trecut care, prin hotărâri definitive, au fost considerate ca reprezentând o atingere nejustificată adusă reputației unor persoane (*ibidem*, pct. 65). Curtea a reamintit, printre altele, că interesul legitim al publicului de a avea acces la arhivele electronice publice ale presei este protejat de art. 10 (*ibidem*, pct. 65). Aceasta a adăugat că este important de observat faptul că instanțele poloneze au indicat că ar fi fost de dorit să se adauge la articolul care figura pe site-ul Internet al ziarului un comentariu care să informeze publicul despre rezultatul primului set de proceduri. Potrivit Curții, acest lucru a demonstrat că instanțele interne erau conștiente de impactul pe care îl puteau avea publicațiile de pe Internet asupra protecției efective a drepturilor persoanelor și de importanța pe care o avea difuzarea de informații complete despre hotărârile judecătorești referitoare la un articol în litigiu publicat online pe site-ul Internet al ziarului. Or, Curtea a indicat că avocatul nu a solicitat adăugarea la articolul în litigiu a unei trimiteri la hotărârile pronunțate în favoarea sa (*ibidem*, pct. 66-67).

310. În cauza *M.L. și W.W. împotriva Germaniei*, 2018, două persoane, care fuseseră condamnate pentru omor și liberate paisprezece ani mai târziu, după executarea pedepsei cu închisoarea, solicitaseră fără succes ca arhivele web ale ziarelor și posturilor de radio să înceteze să le afișeze fotografiile și să le menționeze identitățile complete (nume și prenume), astfel încât să își poată reface fără a mai fi expuse public. Curtea a concluzionat că nu a fost încălcat art. 8, considerând că interesul publicului de a avea acces la arhive cu un conținut veridic și obiectiv trebuie să prevaleze (*ibidem*, pct. 116). În special, Curtea a ținut seama de faptul că rapoartele în litigiu au contribuit întotdeauna, la momentul depunerii cererilor lor de anonimizare, la o dezbatere de interes general, de faptul că reclamanții nu erau simple persoane necunoscute publicului, de comportamentul reclamanților față de presa căreia i se adresaseră după condamnarea lor în vederea obținerii unei revizuiri a acesteia, de faptul că reportajele relatau faptele în mod obiectiv și fără intenția de a prezenta reclamanții în mod derogatoriu sau de a le afecta reputația, precum și de accesibilitatea limitată a informațiilor în litigiu (*ibidem*, pct. 98-115).

311. În cauza *Hurban împotriva Belgiei* (MC), 2023, Curtea și-a revizuit jurisprudența existentă și a adaptat criteriile care trebuie aplicate pentru evaluarea comparativă a drepturilor respective care decurg din articolele 8 și 10 privind disponibilitatea continuă a unei versiuni electronice arhivate a unui articol care divulga date cu caracter personal referitoare la o persoană fizică. Cauza a fost introdusă în fața Curții de un redactor de presă care a fost obligat de instanțele naționale să anonimizeze o versiune arhivată online a unui articol publicat cu aproximativ 20 de ani în urmă care conținea o versiune fidelă a unui accident mortal, în numele „dreptului de a fi uitat” al conducătorului auto care a cauzat accidentul respectiv.

312. În hotărârea sa, Curtea a recunoscut efectele negative ale menținerii anumitor informații disponibile pe internet și, în special, impactul considerabil asupra modului în care persoana vizată a fost percepută de opinia publică, precum și riscurile asociate creării unui profil al persoanei vizate și unei prezentări fragmentate și denaturate a realității. Cu toate acestea, Curtea a explicat că solicitarea de a fi uitat nu constituie un drept autonom protejat de Convenție și, în măsura în care intră sub incidența articolului 8, nu poate viza decât anumite situații și informații (*ibidem*, pct. 199).

313. Curtea a precizat în continuare că evaluarea comparativă a drepturilor relevante (de valoare egală) care trebuie efectuată cu ocazia examinării unei cereri de modificare a conținutului de presă arhivat online trebuie să ia în considerare următoarele criterii: (i) natura informațiilor arhivate; (ii) timpul scurs de la data faptelor, de la prima publicare și de la publicarea online; (iii) relevanța

contemporană a informațiilor; (iv) notorietatea persoanei care solicită să fie uitată și comportamentul său de la data faptelor; (v) repercusiunile negative cauzate de permanența informațiilor pe internet; (vi) gradul de accesibilitate a informațiilor în arhivele digitale și (vii) impactul măsurii asupra libertății de exprimare, în special asupra libertății presei (*ibidem*, pct. 205).

314. Curtea a subliniat de asemenea că, cel mai adesea, vor trebui luate în considerare mai multe criterii atât pentru a decide cu privire la protecția care trebuie acordată vieții private în raport cu celelalte interese implicate, cât și cu privire la mijloacele care au fost utilizate pentru a pune în aplicare această protecție într-un anumit caz. Aceasta a adăugat că protecția vieții private în cadrul unei cereri privind „dreptul de a fi uitat" nu poate fi, așadar, considerată ca nesocotind mijloacele cu care a fost pusă în aplicare în practică și că, din acest punct de vedere, va fi necesar să se efectueze o evaluare comparativă pentru a concluziona dacă, având în vedere ponderea intereselor concurente și intensitatea mijloacelor utilizate în speță, ponderea acordată „dreptului de a fi uitat", prin dreptul la respectarea vieții private, sau libertății de exprimare a fost sau nu excesivă. Aceasta a precizat de asemenea că criteriile care trebuie aplicate nu au toate aceeași pondere și că, prin urmare, ar trebui să se acorde o atenție deosebită unui echilibru adecvat între, pe de o parte, interesele persoanelor care formulează cererea și, pe de altă parte, impactul unor astfel de cereri asupra redactorilor. Curtea a considerat că principiul păstrării integrității arhivelor de presă presupune să se asigure că modificările și, *a fortiori*, ștergerile arhivelor sunt limitate la strictul necesar, astfel încât să se evite orice efect disuasiv al unor astfel de măsuri asupra exercitării de către presă a misiunii sale de informare și de arhivare (*ibidem*, pct. 206 și 211).

315. În cadrul aplicării criteriilor menționate mai sus în împrejurările cauzei cu care fusese sesizată, Curtea a arătat că instanțele naționale au ținut seama în mod constant de natura și de gravitatea faptelor de natură jurisdicțională vizate de articolul în litigiu, de lipsa pertinenței acestuia sau de interesul istoric sau științific, precum și de faptul că persoana vizată nu era foarte cunoscută. Aceasta a arătat de asemenea că instanțele în cauză au acordat importanță prejudiciului grav suferit de persoana vizată ca urmare a păstrării articolului respectiv online, cu acces liber, ceea ce era de natură să creeze un „cazier judiciar virtual", având în vedere în special timpul scurs de la publicarea articolului inițial. Curtea a adăugat că, după examinarea eventualelor măsuri de echilibrare a drepturilor în cauză, instanțele în cauză au concluzionat că anonimizarea respectivă nu constituia o sarcină exorbitantă și excesivă pentru reclamant, reprezentând în același timp, pentru persoana vizată, măsura cea mai eficientă pentru protecția vieții sale private (*ibidem*, pct. 255). Prin urmare, Curtea a constatat că instanțele naționale au evaluat în mod corespunzător interesele aflate în joc și a concluzionat că nu a existat nicio încălcare a articolului 10 (*ibidem*, pct. 256).

b. Alte contexte

316. În cauza *M.M. împotriva Regatului Unit*, 2012 (pct. 187-207), înscrierea pe viață a unui avertisment în cazierul judiciar al unei persoane a condus la constatarea unei încălcări a art. 8. În opinia Curții, condamnarea sau avertismentul impuse unei persoane în trecut devine, odată cu trecerea timpului, parte integrantă a vieții sale private, care trebuie respectată. Deși datele incluse în cazierul judiciar sunt, într-un anumit sens, informații publice, stocarea lor sistematică în evidențele centrale înseamnă că acestea pot fi divulgate la mult timp după eveniment, atunci când oricine altcineva, cu excepția persoanei vizate, este probabil să fi uitat incidentul. Curtea și-a exprimat îngrijorarea cu privire la faptul că criteriile de control care permiteau ștergerea unor astfel de date erau foarte restrictive și că cererile de ștergere a datelor nu erau admise decât în circumstanțe excepționale (*ibidem*, pct. 202).

317. În opinia Curții, atunci când un stat membru își extinde marja de apreciere atribuindu-și cea mai puterea cea mai extinsă în materie de păstrare a datelor, cea de păstrare a datelor pentru o perioadă nelimitată, existența anumitor garanții efective care să permită ștergerea datelor cu caracter personal de îndată ce păstrarea continuă a datelor cu caracter personal devine disproporționată este decisivă (*Catt împotriva Regatului Unit*, 2019, pct. 119; *Gaughran împotriva Regatului Unit*, 2020, pct. 94). Într-

o cauză în care datele biometrice și fotografiile reclamantului, condamnat pentru conducere în stare de ebrietate, fuseseră păstrate în conformitate cu politica de păstrare pentru o perioadă nelimitată a datelor cu caracter personal ale oricărei persoane condamnate pentru săvârșirea unei infracțiuni, Curtea a constatat o încălcare a art. 8 (*ibidem*, pct. 98). Nu exista nicio dispoziție care să permită reclamantului să depună o cerere de ștergere a datelor în cazul în care păstrarea datelor care îl priveau nu mai părea relevantă având în vedere scopul dosarului, având în vedere natura infracțiunii pe care o săvârșise, vârsta sa la momentul săvârșirii faptei, timpul scurs de la acea dată și personalitatea sa din prezent. Poliția nu avea puterea de a șterge datele biometrice și fotografiile persoanelor condamnate decât în cazuri excepționale. Posibilitățile de reexaminare erau atât de limitate încât deveniseră aproape ipotetice (*ibidem*, pct. 94).

318. Lipsa unor garanții eficiente privind ștergerea datelor cu caracter personal atunci când acestea nu par a mai fi relevante pentru scopul dosarului este deosebit de îngrijorătoare în ceea ce privește categoriile sensibile de date cu caracter personal păstrate, care impun o protecție sporită (*Catt împotriva Regatului Unit*, 2019, pct. 112). Într-o cauză care privea păstrarea într-o bază de date a poliției a unor date sensibile referitoare la un demonstrant pașnic, dezvăluindu-i opiniile sale politice, Curtea a concluzionat o încălcare a art. 8 (*ibidem*, pct. 128). În lipsa oricărei norme care să stabilească durata maximă de păstrare a unor astfel de date, reclamantul depindea în întregime de diligența cu care autoritățile aplicau garanțiile Codului de bune practici aplicabil, care erau foarte flexibile, pentru a asigura proporționalitatea perioadei de păstrare a datelor sale. În opinia Curții, garanția pentru a obține ștergerea datelor are un efect limitat atunci când autoritățile refuză, în urma unei cereri din partea persoanei vizate, să șteargă datele în cauză sau să își motiveze decizia de a le stoca (*ibidem*, pct. 118 și 122).

319. Într-o serie cauze care priveau păstrarea datelor cu caracter personal ale persoanelor condamnate pentru agresiuni sexuale, Curtea a concluzionat că nu a fost încălcat art. 8 după ce a constatat că persoanele vizate puteau formula o cerere de ștergere în cazul în care păstrarea datelor care le priveau nu mai părea a fi relevantă, având în vedere, printre altele, timpul scurs de la condamnarea lor (*B.B. împotriva Franței*, 2009, pct. 66-68; *Gardel împotriva Franței*, 2009, pct. 67-69; *M.B. împotriva Franței*, 2009, pct. 58-60). În același timp, lipsa oricărei posibilități de a solicita ștergerea datelor nu implică în mod necesar o încălcare a articolului 8 menționat și trebuie apreciată în raport cu scopul urmărit prin păstrarea acestor date, cu natura datelor și cu garanțiile oferite persoanelor vizate împotriva riscului de arbitrar și de abuz. În special, Curtea a statuat că, în cazul în care datele relevante stocate într-o bază de date internă a Ministerului Justiției nu sunt „sensibile” în sensul articolului 6 din *Convenția 108*, sunt limitate la informații factuale și la elemente obiective referitoare la procedurile judiciare la care o persoană este parte, iar prelucrarea lor vizează buna administrare a justiției și buna funcționare a serviciilor publice în cauză și este însoțită de garanții adecvate (posibilitatea de a asigura exactitatea datelor și limitarea în timp a păstrării acestora), lipsa unei proceduri pentru obținerea ștergerii timpurii a acestor date nu este disproporționată [*L.F. împotriva Franței* (dec.), 2024, pct. 44-47].

320. În cauza *Peruzzo și Martens împotriva Germaniei* (dec.), 2013 (pct. 46), care privea păstrarea datelor cu caracter personal într-un dosar în urma unei condamnări pentru fapte grave legate de traficul de droguri, Curtea s-a declarat satisfăcută de faptul că, deși nu existau termene maxime prevăzute de lege pentru stocarea profilurilor ADN, Oficiul Federal pentru Investigații Criminale avea obligația să verifice la intervale regulate, care nu trebuiau să depășească zece ani, dacă păstrarea datelor era încă necesară având în vedere scopul pentru care fuseseră păstrate datele, precum și natura și gravitatea circumstanțelor cauzei.

321. În cauza *Ayçaguer împotriva Franței*, 2017 (pct. 44), Curtea a concluzionat că a fost încălcat art. 8, considerând că sistemul de stocare a profilurilor ADN în sistemul național privind infracțiunile, pe care reclamantul l-a contestat refuzând prelevarea datelor sale cu caracter personal, nu oferea o protecție suficientă părții interesate, atât din cauza perioadei de păstrare, cât și din cauza lipsei posibilității de ștergere a datelor (*ibidem*, pct. 45). Curtea a subliniat că persoanele condamnate, similar persoanelor

suspectate de săvârșirea unei infracțiuni, achitate sau puse în libertate, trebuie să li se ofere o posibilitate concretă de a depune o cerere de ștergere a datelor stocate pentru a se asigura că perioada de păstrare este proporțională cu natura infracțiunilor și cu scopurile restricțiilor (*ibidem*, pct. 45; *B.B. împotriva Franței*, 2009, pct. 68; *Brunet împotriva Franței*, 2014, pct. 41-43).

322. Posibilitatea prevăzută în dreptul intern de a obține ștergerea datelor se dovedește a fi o garanție „teoretică și iluzorie", iar nu una „concretă și efectivă" atunci când dreptul de a depune o cerere de ștergere a acestor date în fața instanței în orice moment riscă să fie contrar interesului serviciilor de anchetă de a dispune de un dosar cu cât mai multe referințe posibil și în cazul în care interesele implicate sunt, fie și parțial, contradictorii (*M.K. împotriva Franței*, 2013, pct. 44).

323. În cauza *Segerstedt-Wiberg și alții împotriva Suediei*, 2006 (pct. 73-92), păstrarea în dosarele serviciilor de securitate a statului a datelor cu caracter personal foarte vechi ale reclamanților, care priveau participarea lor la o reuniune politică, faptul că avuseră o rezistență violentă în momentul controlului poliției în timpul demonstrațiilor sau apartenența lor la un anumit partid politic, a condus la o încălcare a art. 8. În opinia Curții, interesul statului de a proteja securitatea națională și de a combate terorismul, care justifica colectarea și păstrarea acestor informații, trebuia să fie pusă în balanță cu gravitatea ingerinței în exercitarea de către fiecare dintre reclamanți a dreptului la respectarea vieții private al acestora. Având în vedere natura acestor informații și vechimea lor, motivele care justificaseră păstrarea informațiilor referitoare la părțile interesate, chiar dacă erau relevante, nu puteau fi considerate suficiente la aproximativ treizeci de ani după ce fuseseră colectate (*ibidem*, pct. 90).

4. Dreptul la garanții procedurale speciale și la un cadru procedural eficient pentru exercitarea drepturilor

324. Chiar dacă art. 8 nu conține nicio cerință procedurală explicită, este important, pentru exercitarea efectivă a drepturilor garantate de acest articol, ca procesul decizional relevant să fie echitabil și de natură să respecte în mod corespunzător interesele pe care le protejează. Acesta trebuie să permită reclamantului să își susțină drepturile în mod echitabil, inclusiv în materie de probe (*I. împotriva Finlandei*, 2008, pct. 44; *Ciubotaru împotriva Moldovei*, 2010, pct. 51). Fapta de a impune o cerință care creează un obstacol insurmontabil pentru o persoană care solicită rectificarea datelor sale de identitate în registrele oficiale ale statului se poate dovedi incompatibilă cu obligația pozitivă a statului de a garanta respectarea efectivă a dreptului la respectarea vieții private a acesteia (*ibidem*, pct. 51-59). Într-o cauză care privea privind divulgarea seropozitivității reclamantei, Curtea, constatând o încălcare a art. 8, a insistat asupra faptului că statul impusese reclamantei o sarcină a probei mult prea excesivă în cadrul unei proceduri civile în care aceasta solicitase despăgubiri pentru difuzarea de informații privind starea sa de sănătate (*I. împotriva Finlandei*, 2008, pct. 44).

325. Restricțiile impuse prin lege puterii conferite instanțelor naționale de a repara prejudiciul suferit ca urmare a divulgării, prin intermediul presei, a unor informații confidențiale privind sănătatea unor persoane identificate și de a descuraja repetarea unor astfel de abuzuri sunt de natură să împiedice efectivitatea unui eventual recurs, privând părțile interesate de măsurile de protecție a vieții lor private la care aveau dreptul să se aștepte. Astfel, în cauzele *Armonienė împotriva Lituaniei*, 2008 (pct. 47-48) și *Biriuk împotriva Lituaniei*, 2008 (pct. 46-47), Curtea a constatat o încălcare a art. 8 ca urmare a plafonării, prin legea privind difuzarea de informații publicului, în vigoare la momentul faptelor, a despăgubirilor acordate reclamanților de către instanțele naționale ca urmare a divulgării seropozitivității lor în cel mai mare cotidian național, fără consimțământul acestora și dezvăluindu-le identitatea. În plus, Curtea a constatat că o acțiune pur compensatorie a fost inoperantă într-o cauză în care reclamantul s-a plâns de o situație continuă care decurge din protecția inadecvată a datelor cu caracter personal care îl privesc și care au fost stocate într-o bază de date deținută de stat (Serviciul de informare privind contribuabilii) și în cazul căreia, pentru o lungă perioadă de timp, autoritățile nu au împiedicat accesul abuziv la baza de date în cauză [*Casarini împotriva Italiei* (dec.), 2024, pct. 89].

326. Nerespectarea de către stat a obligației de a prevedea, la nivel național, exercitarea unui control independent al necesității de a păstra datele cu caracter personal colectate în cadrul unor proceduri penale sau ca urmare a unor proceduri penale finalizate prin achitare, neînceperea urmăririi penale sau condamnare constituie un element important care trebuie luat în considerare pentru a stabili dacă o astfel de păstrare a datelor este compatibilă sau nu cu art. 8 [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 119, 125]. Într-o cauză care privea păstrarea pe termen nelimitat a mostrelor de celule, a profilurilor ADN și a amprentelor digitale de la două persoane după finalizarea procedurilor penale declanșate împotriva acestora prin achitare și, respectiv, printr-o decizie de neîncepere a urmăririi penale, Curtea a concluzionat că a fost încălcat art. 8 după ce a constatat că nu existau decât puține posibilități pentru ca persoanele să obțină ștergerea datelor din baza de date națională sau distrugerea mostrelor.

327. În cauza *Vicent Del Campo împotriva Spaniei*, 2018 (pct. 39 și 53), faptul că reclamantul, terț în cadrul unei proceduri judiciare, fusese privat de posibilitatea de a solicita unei instanțe naționale să se abțină de la comunicarea identității sale sau a informațiilor sale cu caracter personal care îl priveau înainte de pronunțarea unei hotărâri, l-a privat de un cadru procedural eficient pentru a-și susține drepturile.

328. Neefectuarea de către autorități a unei analize a proporționalității prin punerea în balanță a intereselor concurente aflate în joc și neluarea în considerare a dreptului reclamantului la respectarea vieții sale private și a aspectelor legate de protecția datelor a condus la o nerespectare a cerințelor prevăzute la art. 8 din Convenție (*Liebscher împotriva Austriei*, 2021, pct. 64-69).

329. În cauza *M. D. și alții împotriva Spaniei* din 2022 (pct. 65-72), care privea scurgerea de date cu caracter personal referitoare la reclamanți către presă dintr-o bază de date a poliției la care numai autoritățile aveau acces, având în vedere amploarea acestei divulgări ilegale a datelor private păstrate de o autoritate publică, Curtea a considerat că obligația pozitivă prevăzută la articolul 8 implica o „obligație de a efectua o anchetă efectivă” pentru a stabili circumstanțele în care jurnaliștii au avut acces la date și, dacă este cazul, pentru a sancționa persoanele responsabile pentru deficiențele constatate. Aceasta a constatat că neefectuarea de către autorități a unei astfel de investigații încalcă articolul 8. În mod similar, în cauza *Y.G. împotriva Rusiei*, 2022 (pct. 46-53), în care reclamantul a susținut că a fost oferită spre vânzare o bază de date care conține date cu caracter personal care îl privesc, inclusiv informații privind starea sa de sănătate, aceasta a considerat că, în contextul unei atingeri de așa amploare a vieții private, reclamantul, dacă acționa din proprie inițiativă și fără a primi ajutorul din partea statului sub forma unei anchete oficiale, nu dispunea de mijloace eficace de identificare a autorilor unor astfel de acte. Aceasta a concluzionat că plângerea penală a reclamantului nu constituia o cale de atac inadecvată având în vedere aceste circumstanțe. Curtea a considerat că, prin neefectuarea unei anchete, autoritățile nu și-au îndeplinit obligația pozitivă de a asigura persoanei vizate o protecție adecvată a dreptului său la respectarea vieții sale private.

330. În cauza *Casarini împotriva Italiei* (dec.), 2024, pct. 92-105, în care un agent de la garda financiară a accesat în mod repetat și ilegal datele cu caracter personal ale reclamantului stocate în baza de date a Serviciului de informare privind contribuabilii și apoi le-a comunicat unui jurnalist spre publicare, Curtea a statuat că o plângere adresată autorității pentru protecția datelor ar fi constituit o cale de atac eficace și că, prin urmare, această cale de atac ar fi trebuit să fie epuizată. Deși autoritatea pentru protecția datelor nu este un organism judiciar, aceasta este un organism administrativ pe deplin autonom, lipsit de presiuni externe: procedura în fața acestui organ are caracter contradictoriu și dă naștere unor decizii obligatorii care puteau fi contestate în fața autorităților judiciare competente și, eventual, putea face obiectul unui recurs în fața Curții de Casație.

331. Caracterul efectiv al căilor de atac disponibile la nivel național pentru persoanele care doresc să aibă acces la datele lor cu caracter personal impune ca persoanele vizate să poată obține prelucrarea cererilor lor într-un termen rezonabil. În cauza *Roche împotriva Regatului Unit* (MC), 2005 (pct. 166-167, 169), Curtea a concluzionat că a fost încălcat art. 8 ca urmare a unei perioade de așteptare

considerată nerezonabilă înainte ca reclamantul să poată avea acces la documente care conțineau date cu caracter personal care i-ar fi permis să evalueze riscurile pentru sănătatea sa care ar fi putut rezulta din participarea sa la teste militare cu gaze.

332. Termenele stricte sau limitările procedurale necesită, de asemenea, un control. În cauza *Moldovan împotriva Ucrainei*, 2024, (pct. 52-53), reclamantul s-a plâns că instanțele naționale sesizate cu cererea sa de recunoaștere a tatălui său biologic au aplicat dispoziții legale vechi care făceau dovada coabitării indispensabilă pentru recunoașterea unei legături de filiație, în pofida testelor ADN disponibile. Curtea a considerat că efectele unei astfel de abordări a instanțelor naționale erau comparabile cu cele ale unor termene rigide sau ale altor limitări procedurale. Curtea a concluzionat că această abordare, combinată cu faptul că instanța națională nu a tratat suficient probele genetice care i-au fost prezentate, echivala cu o neîndeplinire a obligațiilor pozitive care revin instanțelor naționale în temeiul articolului 8 din Convenție.

333. O atenție prea mare acordată de autoritățile naționale cerinței de confidențialitate a datelor de transfer ale utilizatorilor de Internet se poate dovedi, în anumite circumstanțe, contrară art. 8 dacă este de natură să constituie un obstacol la adresa eficacității unei anchete penale care să permită identificarea și pedepsirea autorului unei infracțiuni (*K.U. împotriva Finlandei,* 2008, pct. 49). În cauza *K.U. împotriva Finlandei*, 2008 (pct. 49-50), Curtea a concluzionat că a fost încălcat art. 8 pe motiv că nu exista un cadru procedural care să permită identificarea și aducerea în fața justiției a unei persoane care a publicat pe Internet un anunț publicitar care a făcut dintr-un minor o țintă pentru pedofili, astfel încât victima să poată obține repararea pecuniară a prejudiciului din partea sa. Garantarea respectării intimității utilizatorilor serviciilor de telecomunicații și de Internet trebuie uneori anulată atunci când există alte cerințe legitime, precum apărarea ordinii și prevenirea infracțiunilor sau protejarea drepturilor și libertăților altora.

334. În materie de securitate națională, orice persoană care face obiectul unei măsuri întemeiate pe aceste motive trebuie să aibă posibilitatea de a solicita controlul măsurii în cauză de către un organ independent și imparțial, abilitat să examineze toate aspectele de fapt și de drept relevante și să sancționeze, dacă este cazul, orice eventual abuz din partea autorităților. În fața acestui organ de control, persoana vizată trebuie să beneficieze de o procedură contradictorie pentru a-și putea prezenta punctul său de vedere și a contesta argumentele autorităților. Astfel, în cauza *Dalea împotriva Franței* (dec.), 2010, Curtea a hotărât că includerea pe termen lung a datelor cu caracter personal ale reclamantului în sistemul de informații Schengen putea fi considerată „necesară într-o societate democratică", întrucât partea interesată beneficiase de un control al măsurii în litigiu. Chiar dacă nu i s-a oferit posibilitatea de a obiecta împotriva motivului specific al includerii sale în sistem, luase la cunoștință despre toate celelalte date care îl priveau incluse în baza de date Schengen.

335. Organul independent și imparțial în fața căruia orice persoană care face obiectul unei măsuri întemeiate pe motive de securitate națională trebuie să aibă posibilitatea de a solicita controlul măsurii în litigiu nu este în mod necesar o autoritate judiciară. În cauza *Leander împotriva Suediei*, 1987 (pct. 59), care privea utilizarea unui dosar secret al poliției pentru angajarea unui dulgher, Curtea a constatat neîncălcarea art. 8 în prezența unor garanții care constau în special în posibilitatea ca parlamentul și instituțiile independente să exercite un control asupra operațiunilor care autorizau autoritățile interne competente să colecteze și să stocheze în dosare secrete informații despre persoane, și apoi să le utilizeze (*ibidem*, pct. 65) chiar dacă reclamantul nu avea dreptul la o cale de atac jurisdicțională (*ibidem*, pct. 62, 67). Pentru a evalua eficacitatea unei căi de atac în fața unui organ solicitat, la nivel intern, să examineze o măsură întemeiată pe motive de securitate națională, sunt relevante puterile și garanțiile procedurale de care dispune organul în cauză (*ibidem*, pct. 77, 80, 83-84). Un recurs ierarhic în fața unui superior ierarhic direct al autorității ale cărei acte sunt contestate nu îndeplinește criteriile de independență necesare pentru a constitui o protecție suficientă împotriva abuzului de putere [*Roman Zakharov împotriva Rusiei* (MC), 2015, pct. 292].

336. În contextul măsurilor de supraveghere secretă, controlul și supravegherea acestor măsuri poate interveni în trei etape: atunci când este dispusă supravegherea, în timp ce este în curs de desfășurare sau după încetarea acesteia. În primele două etape, natura și însăși logica supravegherii secrete fac necesară efectuarea, fără cunoștința părții interesate, nu numai a supravegherii înseși, ci și a controlului care o însoțește. Întrucât partea interesată va fi așadar împiedicată să introducă un recurs efectiv din proprie inițiativă sau să participe direct la orice procedură de control, este esențial ca procedurile existente să ofere ele însele garanții adecvate și echivalente pentru a proteja drepturile persoanei. Într-un domeniu în care abuzurile sunt potențial ușor de produs în cazuri individuale și ar putea antrena consecințe negative pentru societatea democratică în ansamblu, este, în principiu, de dorit ca acest control să fie încredințat unui judecător, întrucât controlul jurisdicțional oferă cele mai bune garanții de independență, imparțialitate și procedură legală (*ibidem*, pct. 233; *Klass și alții împotriva Germaniei*, 1978, pct. 55-56; *Denisiuk și alții împotriva Ucrainei*, 2025, pct. 88).

337. În ceea ce privește a treia etapă, respectiv încetarea supravegherii, chestiunea notificării *a posteriori* a măsurilor de supraveghere este indisolubil legată de cea a eficacității căilor de atac și deci de existența unor garanții efective împotriva folosirii abuzive a competențelor de supraveghere [*Roman Zakharov Roman Zaharov împotriva Rusiei* (MC), 2015, pct. 234]. Persoana vizată nu poate, în principiu, să conteste retroactiv în justiție legalitatea măsurilor luate fără cunoștința sa, cu excepția cazului în care este informată cu privire la acestea [*Klass și alții împotriva Germaniei*, 1978, pct. 57-59; *Weber și Saravia împotriva Germaniei* (dec.), 2006, pct. 135-137) sau în cazul în care orice persoană care consideră că a făcut obiectul unei supravegheri are posibilitatea de a introduce o acțiune în fața instanțelor competente, chiar dacă subiectul supravegherii nu a fost informat cu privire la măsurile luate [*Kennedy împotriva Regatului Unit*, 2010, pct. 167, 169; *Roman Zakharov împotriva Rusiei* (MC), 2015, pct. 234].

338. În cauzele *Klass și alții împotriva Germaniei*, 1978 (pct. 57-59) și *Weber și Saravia împotriva Germaniei* (dec.), 2006 (pct. 135-137), Curtea a constatat că recursurile existente la nivel național erau suficiente. Persoanele ale căror comunicări fuseseră supravegheate erau notificate cât mai curând posibil, fără a compromite scopul supravegherii. Căile de atac erau, de asemenea, însoțite de garanții efective, cum ar fi, de exemplu, faptul că o autoritate independentă avea puterea de a decide dacă o persoană care făcea obiectul unei supravegheri trebuia să fie informată cu privire la măsura respectivă. Pornind de la această notificare, persoana beneficia de diferite căi de atac, de exemplu, introducerea unei acțiuni civile în despăgubire sau o cerere în fața Curții Constituționale Federale pentru a se pronunța cu privire la posibila încălcare a legii fundamentale (*Klass și alții împotriva Germaniei*, 1978, pct. 57, 24).

339. În cazul sistemelor care nu prevăd notificarea persoanei vizate despre măsurile luate împotriva sa, faptul că persoanele care se consideră lezate de dreptul lor la viață privată prin intermediul unei măsuri de supraveghere secretă se pot adresa unui organ independent și imparțial chiar fără să fi fost informată în prealabil despre interceptarea comunicațiilor lor a fost considerat de Curte o garanție importantă într-o cauză în care aceasta a concluzionat că nu a fost încălcat art. 8 (*Kennedy împotriva Regatului Unit*, 2010, pct. 167, 169). Pe de altă parte, în cazul în care căile de atac oferite de sistemul intern sunt deschise numai persoanelor care dispun de un minim de informații despre măsura incriminată, Curtea a considerat că părțile interesate nu dispuneau de un recurs efectiv împotriva măsurilor de supraveghere secretă, cu încălcarea art. 8 [*Roman Zakharov împotriva Rusiei* (MC), 2015, pct. 293-298, 305; *Denisiuk și alții împotriva Ucrainei*, 2025, pct. 116-132].

III. Interacțiunea cu alte dispoziții din Convenție sau protocoalele sale

340. Pe lângă dreptul la respectarea vieții private și de familie, a domiciliului și a corespondenței, garantat de art. 8 din Convenție, care asigură, în primul rând, protecția datelor cu caracter personal în sistemul Convenției, chestiunile legate de această protecție pot fi de asemenea puse în discuție în temeiul altor dispoziții ale Convenției și ale protocoalelor adiționale la aceasta. Sarcina principală a Curții este apoi de a o pune în balanță și de a o reconcilia cu alte drepturi și interese legitime. În anumite cauze, problema protecției datelor cu caracter personal a permis Curții să stabilească domeniul de aplicare al oricăruia dintre celelalte drepturi garantate de Convenție și de protocoalele adiționale la aceasta.

A. Protecția datelor și drepturile materiale[10]

Articolul 9 din Convenție

„1. Orice persoană are dreptul la libertatea de gândire, de conștiință și de religie; acest drept include libertatea de a-și schimba religia sau convingerea, precum și libertatea de a-și manifesta religia sau convingerea în mod individual sau în colectiv, în public sau în particular, prin cult, învățământ, practici și îndeplinirea ritualurilor.

2. Libertatea de a-și manifesta religia sau convingerile nu poate face obiectul altor restrângeri decât acelea care, prevăzute de lege, constituie măsuri necesare, într-o societate democratică, pentru siguranța publică, protecția ordinii, a sănătății sau a moralei publice ori pentru protejarea drepturilor și libertăților altora."

Articolul 10 din Convenție

„1. Orice persoană are dreptul la libertatea de exprimare. Acest drept cuprinde libertatea de opinie și libertatea de a primi sau de a comunica informații ori idei fără amestecul autorităților publice și fără a ține seama de frontiere. Prezentul articol nu împiedică statele să supună societățile de radiodifuziune, de cinematografie sau de televiziune unui regim de autorizare.

2. Exercitarea acestor libertăți, ce comportă îndatoriri și responsabilități, poate fi supusă unor formalități, condiții, restrângeri sau sancțiuni prevăzute de lege, care constituie măsuri necesare, într-o societate democratică, pentru securitatea națională, integritatea teritorială sau siguranța publică, apărarea ordinii și prevenirea infracțiunilor, protecția sănătății sau a moralei, protecția reputației sau a drepturilor altora, pentru a împiedica divulgarea de informații confidențiale sau pentru a garanta autoritatea și imparțialitatea puterii judecătorești."

Articolul 14 din Convenție

„Exercitarea drepturilor și libertăților recunoscute de prezenta Convenție trebuie sa fie asigurată fără nici o deosebire bazată, în special, pe sex, rasa, culoare, limba, religie, opinii politice sau orice alte opinii, origine națională sau socială, apartenența la o minoritate națională, avere, naștere sau orice altă situație."

Articolul 1 din Protocolul nr. 1

„Orice persoană fizică sau juridică are dreptul la respectarea bunurilor sale. Nimeni nu poate fi lipsit de proprietatea sa decât pentru cauza de utilitate publică și în condițiile prevăzute de lege și de principiile generale ale dreptului internațional.

Dispozițiile precedente nu aduc atingere dreptului statelor de a adopta legile pe care le consideră necesare pentru a reglementa folosința bunurilor conform interesului general sau pentru a asigura plata impozitelor ori a altor contribuții, sau a amenzilor."

[10] Prezentul capitol trebuie citit în lumina și coroborat cu *Ghidul privind art. 9*, *Ghidul privind art. 10*, *Ghidul privind art. 14 și art. 1 din Protocolul nr. 12* și *Ghidul privind art. 1 din Protocolul nr. 1*.

Articolul 2 din Protocolul nr. 4

„1. Oricine se găsește în mod legal pe teritoriul unui stat are dreptul să circule în mod liber și să-și aleagă în mod liber reședința sa.

2. Orice persoană este liberă să părăsească orice țară, inclusiv pe a sa.

3. Exercitarea acestor drepturi nu poate face obiectul altor restrângeri decât acelea care, prevăzute de lege, constituie măsuri necesare, într-o societate democratică, pentru securitatea națională, siguranța publică, menținerea ordinii publice, prevenirea faptelor penale, protecția sănătății sau a moralei, ori pentru protejarea drepturilor și libertăților altora.

4. Drepturile recunoscute în paragraful 1 pot, de asemenea, în anumite zone determinate, să facă obiectul unor restrângeri care, prevăzute de lege, sunt justificate de interesul public într-o societate democratică."

1. Protecția datelor și libertatea de gândire, de conștiință și de religie (art. 9 din Convenție)

341. Curtea s-a pronunțat cu privire la încălcarea sau lipsa unei încălcări a art. 9 într-o serie de cauze care ridicau, de asemenea, problema protecției datelor cu caracter personal.

342. În cauza *Sinan Işık împotriva Turciei*, 2010 (pct. 37-53), Curtea s-a confruntat cu problema menționării, fie ea obligatorie sau facultativă, a religiei reclamantului în cartea sa de identitate. În opinia sa, a solicita în scris autorităților să înlocuiască o religie cu alta în registrele de stare civilă și în cartea de identitate, precum și simpla deținere a unei cărți de identitate în care rubrica „religie" rămâne necompletată echivalează în cazul părții interesate cu divulgarea împotriva voinței sale unei informații referitoare la un aspect al religiei sau al convingerilor sale dintre cele mai profunde. Curtea a hotărât că a fost încălcat art. 9 după ce a reamintit că libertatea de a-și manifesta religia sau convingerile implică un aspect negativ, și anume dreptul persoanei de a nu fi obligată să își manifeste religia sau să acționeze astfel încât să se poată concluziona că persoana are, sau nu, astfel de convingeri. Chiar dacă rubrica rezervată menționării religiei putea fi lăsată necompletată, chiar faptul de a o lăsa necompletată avea, în sine, o conotație specifică, întrucât permitea în mod inevitabil să se facă o distincție între titularii unei cărți de identitate care conținea o astfel de informație și cei care ar fi ales să nu o indice (*ibidem,* pct. 51).

343. În cauza *Alexandridis împotriva Greciei*, 2008 (pct. 41), obligația avocatului de a declara, atunci când prestează jurământ, că nu este creștin ortodox și că nu dorește să presteze jurământul religios, pentru a putea face o declarație solemnă, a adus atingere dreptului său garantat de art. 9. Autoritățile statului nu au dreptul de a interveni în domeniul libertății de conștiință a persoanei și de a cunoaște convingerile religioase ale acesteia sau de a o obliga să își manifeste convingerile cu privire la divinitate. Acest lucru este cu atât mai adevărat atunci când o persoană este obligată să facă acest lucru cu scopul de a exercita anumite funcții, în special atunci când prestează un jurământ (*ibidem*, pct. 38). În cauza *Dimitras și alții împotriva Greciei*, 2010 pct. 88), obligația reclamanților de a-și divulga convingerile religioase pentru a nu presta jurământul religios în calitate de martori în cadrul unei proceduri penale a constituit, de asemenea, la o încălcare a art. 9. Curtea a considerat că dispozițiile Codului de procedură penală, care prevedeau, în vederea verificării identității unui martor și înainte de audierea acestuia, ca acesta să-și indice, printre alte elemente, religia, erau incompatibile cu dreptul său la libertatea de religie (*ibidem*, pct. 88).

344. În cauza *Mockutė împotriva Lituaniei*, 2018 (pct. 129), Curtea a afirmat că era pregătită să accepte că necesitatea unui tratament psihiatric putea implica necesitatea ca un psihiatru să discute diverse aspecte, inclusiv religia, cu un pacient. Însă astfel de discuții nu ar trebui să ia forma unor

imixtiuni, din partea psihiatrilor, în convingerile pacienților, pentru a le „corecta” în cazul în care nu există niciun risc clar și iminent ca astfel de convingeri să se manifeste în acțiuni periculoase pentru pacient sau pentru alte persoane. Un stat nu poate să dicteze ce crede o persoană sau ia măsuri coercitive pentru a-i schimba convingerile, iar marja de apreciere a statelor nu poate fi mai largă sau mai restrânsă în funcție de natura convingerilor religioase.

345. În cauza *Martorii lui Iehova împotriva Finlandei* din 2023 (pct. 80-99), Curtea a fost chemată să decidă dacă s-a găsit un echilibru just între dreptul comunității reclamante la libertatea religioasă și dreptul la respectarea vieții private a persoanelor (persoanele vizate) pe care membrii comunității reclamante le-au vizitat în cursul activităților lor de predicare din ușă în ușă. Pe plan intern, autoritățile competente au constatat că consimțământul explicit sau neechivoc al persoanelor vizate era necesar în timpul acestor activități atunci când au fost colectate și prelucrate date cu caracter personal și sensibile (numele și adresa persoanelor vizate). Curtea a admis că aplicarea obligației de a obține consimțământul persoanelor vizate în cadrul unei activități de predicare din ușă în ușă – o activitate religioasă care vizează manifestarea sau diseminarea credinței – desfășurată de comunitatea reclamantă a constituit o ingerință în drepturile acestei comunități garantate de articolul 9 (pct. 81). În același timp, aceasta a considerat că ingerința în cauză era „prevăzută de lege”, având în vedere în special faptul că Curtea Administrativă Supremă interpretase actul juridic intern relevant, care a servit drept temei pentru măsurile în cauză și care se baza pe directiva UE relevantă, în conformitate cu interpretarea dată de Curtea de Justiție a Uniunii Europene (pct. 84-88). Aceasta a adăugat că măsura în cauză urmărea, totodată, obiectivul legitim de a proteja „drepturile și libertățile celorlalți” (punctul 89) și era „necesară într-o societate democratică”. Cu privire la acest din urmă aspect, Curtea a arătat că, deși obligația de a obține consimțământul persoanei vizate constituia o garanție adecvată și necesară pentru a împiedica orice comunicare sau divulgare a unor date cu caracter personal și sensibile în cadrul activităților de predicare „din ușă în ușă” desfășurate de comunitatea reclamantă, aceasta din urmă nu demonstrase în ce mod obligația respectivă era de natură să aducă atingere substanței dreptului său la libertatea de religie (pct. 95). Ea a adăugat că această obligație se aplica tuturor comunităților și activităților religioase (pct. 96) și că comunitatea reclamantă, în pofida unei cereri în acest sens, nu a făcut obiectul niciunei sancțiuni (pct. 97).

2. Protecția datelor și libertatea de exprimare (art. 10 din Convenție)[11]

346. În general, în cauzele în care Curtea a fost solicitată să pună în balanță și să reconcilieze dreptul la protecția datelor cu caracter personal, astfel cum este garantat de art. 8, cu dreptul la libertatea de exprimare consacrat de art. 10, Curtea a considerat că, în principiu, rezultatul nu putea varia în funcție de faptul că fusese sesizată cu respectiva cauză din perspectiva art. 8 sau din perspectiva art. 10. În opinia Curții, aceste drepturi merită un egal respect [*Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei*(MC), 2017, pct. 163; *Alpha Doryforiki Tileorasi Anonymi Etairia împotriva Greciei*, 2018, pct. 46].

347. Refuzul autorităților de a acorda organizațiilor neguvernamentale acces la anumite informații care conțin date cu caracter personal deținute de stat a constituit o încălcare a art. 10 în cauzele:

- *Centrul pentru democrație și statul de drept împotriva Ucrainei*, 2020 (pct. 120-121), care privea refuzul comisiei electorale centrale de a furniza unui ONG o copie a *curriculum vitae*-urilor liderilor partidelor politice candidați la alegerile parlamentare, pe motiv că informațiile solicitate aveau caracter confidențial și puteau fi comunicate în întregime numai cu consimțământul persoanelor vizate;

[11] Prezentul capitol trebuie citit în lumina și coroborat cu *Ghid privind art. 10* din Convenție (a se vedea în special pag. 26-47; 58-60 și 62-65)

- *Magyar Helsinki Bizottság împotriva Ungariei* (MC), 2016 (pct. 195-197, 200), în care autoritățile refuzaseră să comunice unui ONG care realiza un studiu numele și numărul numirilor de avocați din oficiu;
- *Youth Initiative for Human Rights împotriva Serbiei*, 2013 (pct. 24-26), care privea refuzul unui serviciu de informații de a comunica informații unui ONG, în pofida unui ordin în acest sens.

348. În ceea ce privește divulgarea datelor cu caracter personal în presa scrisă sau în mijloacele de informare audiovizuale, Curtea a concluzionat că a fost încălcat art. 10 într-o serie de cauze, printre care:

- *N. Š. împotriva Croației*, 2020 (pct. 92-117), în care reclamanta a fost condamnată pentru divulgarea, în cadrul unei emisiuni de televiziune, a unor informații pretins confidențiale despre care luase cunoștință în cursul unei proceduri administrative privind încredințarea unui minor. Din cauza vulnerabilității acestora, protecția datelor cu caracter personal ale copiilor este esențială (*ibidem*, pct. 99). Cu toate acestea, o abordare excesiv de formalistă a instanțelor naționale, care nu ține seama de contextul divulgării, și în special de faptul că informațiile divulgate se aflau deja în domeniul public, nu este compatibilă cu art. 10 (*ibidem*, pct. 115-116);
- *Gîrleanu împotriva României*, 2018 (pct. 68-100), care privea condamnarea la plata unei amenzi administrative pentru divulgarea de informații militare confidențiale în contextul unei anchete jurnalistice.
- *Couderc și Hachette Filipacchi Associés împotriva Franței* (MC), 2015 (pct. 94-153), care privea condamnarea directoarei editurii și a societății editoare a unei reviste săptămânale pentru publicarea unui articol și a unor fotografii care dezvăluia existența copilului nelegitim al unui monarh;
- *Axel Springer AG împotriva Germaniei* (MC), 2012 (pct. 75-111), care privea interdicția de a relata arestarea și condamnarea unui actor cunoscut;
- *Dupuis și alții împotriva Franței*, 2007 (pct. 30-32, 39-49), care privea condamnarea unor jurnaliști pentru că utilizaseră și reproduseseră în cărțile lor elemente din dosarul unei anchete penale în curs, inclusiv date cu caracter personal ale inculpatului.

349. În schimb, a constatat inexistența unei încălcări a art. 10 sau inadmisibilitatea într-o serie de cauze, între care:

- *Hurban împotriva Belgiei* (MC), 2023 (pct. 167-257), în ceea ce privește condamnarea civilă a reclamantului, redactor de presă, pentru a anonimiza arhiva electronică online a unui articol care menționează numele complet al unui conducător auto care a fost responsabil de un accident rutier mortal care avusese loc cu mulți ani în urmă;
- *Biancardi împotriva Italiei*, 2021 (pct. 67-71), care privea condamnarea în urma unui proces civil a unui redactor de presă pentru că nu a dezindexat informații sensibile publicate pe Internet referitoare la o procedură penală inițiată împotriva unei persoane de drept privat și decizia sa de a le păstra ușor de accesat în pofida opoziției formulate de persoana vizată;
- *Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei* (MC), 2017 (pct. 139-199), care privea o hotărâre judecătorească prin care se interzicea publicarea pe scară largă de date fiscale cu caracter personal;
- *Bédat împotriva Elveției* (MC), 2016 (pct. 44-82), care privea condamnarea unui jurnalist pentru publicarea de informații protejate de secretul urmăririi penale;
- *Mediengruppe Österreich GmbH împotriva Austriei,* 2022 (pct. 44-73), care priveau interdicția impusă de instanțele naționale unui ziar de a publica fotografia, însoțită de mențiunea „neonazist condamnat”, a unei persoane care avea o legătură indirectă cu

campania unui candidat la președinție, publicarea în cauză apărând la mai mult de 20 de ani de la condamnarea persoanei vizate;

- *Gafiuc împotriva României*, 2020 (pct. 85-90), care privea retragerea acreditării acordate unui jurnalist pentru efectuarea de cercetări în arhivele Securității, în urma divulgării, în mai multe articole pe care le publicase, a unor date cu caracter personal în forma brută a unor diverși sportivi cunoscuți, fără a evalua relevanța acestora în raport cu scopul declarat al cercetării sale, care era sportul în perioada comunistă;
- *Giesbert și alții împotriva Franței*, 2017 (pct. 77-103), care privea condamnarea unui ziar pentru publicarea unor acte dintr-o procedură penală înainte de citirea acestora în ședință publică;
- *Verlagsgruppe Droemer Knaur GmbH & Co. KG împotriva Germaniei*, 2017 (pct. 36-62), care privea acordarea de despăgubiri pentru neefectuarea de cercetări amănunțite de către o editură și pentru atingere gravă adusă drepturilor personalității;
- *Kurier Zeitungsverlag und Druckerei GmbH împotriva Austriei*, 2012 (pct. 47-56), care privea obligația de a despăgubi un copil victimă a unui abuz sexual a cărui identitate fusese dezvăluită într-un articol de presă. Având în vedere vulnerabilitatea lor, victimele infracțiunilor trebuie să beneficieze de o protecție specială a identității lor;
- *MGN Limited împotriva Regatului Unit*, 2011 (pct. 152), în care Curtea s-a considerat convinsă, printre altele, de faptul că divulgarea în presă a anumitor date privind terapia urmată de o celebritate pentru dependența de droguri era dăunătoare și foarte probabil să îi afecteze recuperarea;
- *Editions Plon împotriva Franței*, 2004 (pct. 22-57), care privea întreruperea temporară a difuzării unei cărți care conținea date care protejate de secretul medical cu privire la un șef de stat decedat.
- *Mitov și alții împotriva Bulgariei* (dec.), 2023 (pct. 30-41), privind normele de anonimizare emise de președintele Curții Administrative Supreme și legislația care instituie o normă ce impune amânarea publicării anumitor decizii pronunțate în cauze penale, în urma cărora reclamanții, jurnaliști de investigație, nu au putut consulta în mod liber pe internet toate elementele scanate ale dosarului care se aflau în baza de date a instanței în cauză.
- *Ramadan împotriva Franței* (dec.), 2024 (pct. 28-46), în care reclamantul, care fusese acuzat de agresiune sexuală pentru care a făcut obiectul unei proceduri penale în curs, a difuzat într-o carte, precum și în alte două canale mass-media informații privind identitatea presupusei victime, fără a obține consimțământul acesteia, chiar dacă identitatea persoanei vizate fusese deja dezvăluită de terți pe un canal mass-media.

350. În ceea ce privește difuzarea de imagini personale în presa scrisă sau prin intermediul mijloacelor de informare audiovizuale sau ordinul de a nu difuza astfel de date cu caracter personal, Curtea a constatat o încălcare a art. 10 într-o serie de cauze, între care: *Pinto Coelho împotriva Portugaliei (nr. 2)*, 2016 (pct. 31-56), care privea condamnarea unui jurnalist pentru difuzarea înregistrării unei ședințe de judecată fără autorizație; *Haldimann și alții împotriva Elveției*, 2015 (pct. 63-68), care privea condamnarea a patru jurnaliști pentru înregistrarea și difuzarea, în scopuri de interes public, a unui interviu cu un broker de asigurări realizat cu o cameră ascunsă; *Krone Verlag GmbH & Co. KG împotriva Austriei*, 2002, (pct. 21-39), care privea ordinul de a nu publica fotografia unui anumit om politic; *News Verlags GmbH & Co.KG împotriva Austriei*, 2000 (pct. 37-60), care privea interdicția impusă unui ziar de a publica fotografia unui suspect în cadrul unei proceduri penale inițiate împotriva acestuia din urmă.

351. În schimb, difuzarea unor astfel de imagini sau ordinul de a nu le difuza nu au condus la constatarea unei încălcări a art. 10 în cauzele: *Société de Conception de Presse et d'Édition împotriva Franței*, 2016 (pct. 32-54), care privea un ordin judecătoresc de a obtura, într-o revistă deja aflată în vânzare, fotografia unei persoane sechestrate și torturate; *Axel Springer SE și RTL Television GmbH*

împotriva Germaniei, 2017 (pct. 43-59), care privea decizia de a interzice publicarea de imagini care ar fi permis recunoașterea unei persoane judecate pentru omucidere; *Egeland și Hanseid împotriva Norvegiei*, 2009 (pct. 56-65), care privea condamnarea redactorilor-șefi ale unor ziare pentru publicarea fotografiilor unei persoane care urma să fie dusă în penitenciar pentru a executa o pedeapsă cu închisoarea de lungă durată care tocmai fusese pronunțată împotriva acesteia. A se vedea, de asemenea, supra, pct. 17 și 65 care privesc cauza *Vučina împotriva Croației* (dec.) 2019. În cauza *Standard Verlagsgesellschaft mbH împotriva Austriei (nr. 3)*, hotărârile nemotivate prin care se dispusese ca o societate media să divulge date referitoare la autorii unor comentarii injurioase încărcate pe portalul său de știri în contextul unei dezbateri politice au dus la constatarea unei încălcări a art. 10 din Convenție.

352. În cauza *Alpha Doryforiki Tileorasi Anonymi Etairia împotriva Greciei*, 2018 (pct. 59-69, 77-78), difuzarea în scopuri jurnalistice a mai multor înregistrări video cu supravegherea secrete cu o cameră ascunsă a unei personalități publice a condus la constatarea unei încălcări, respectiv la constatarea unei neîncălcări a art. 10, în funcție de faptul că înregistrarea fusese efectuată într-un spațiu public sau într-un spațiu privat.

353. În ceea ce privește difuzarea pe Internet, de către persoane de drept privat, a unor imagini ale altor persoane surprinse în secret, fără consimțământul persoanei vizate, în cauza *Khadija Ismayilova împotriva Azerbaidjanului*, 2019 (pct. 158-166), Curtea a condamnat statul pârât pentru neprotejarea reclamantei, jurnalistă de profesie, care fusese filmată de persoane necunoscute prin intermediul unor camere ascunse instalate în apartamentul său. Divulgarea nejustificată de către autorități, într-un comunicat de presă care pretindea că furnizează un raport privind evoluția unei anchete penale, a unor date cu caracter personal precum numele părții interesate și adresele rudelor și ale colegilor săi de la locul de muncă nu a făcut decât să agraveze situația, contrar spiritului unui mediu de protecție în ceea ce privește jurnalismul (ibidem, pct. 165).

354. Într-o cauză care punea în discuție protecția libertății de exprimare a avertizorului și divulgarea de informații confidențiale referitoare la siguranța statului, Curtea a concluzionat că a fost încălcat art. 10 în ceea ce privește condamnarea penală a reclamantului pentru că a făcut publice nereguli în colectarea datelor cu caracter personal de către serviciile de informații, pe care le constatase în contextul exercitării atribuțiilor sale profesionale (*Bucur și Toma împotriva României*, 2013, pct. 95-120). Într-o altă cauză care privea un avertizor, medicul-șef adjunct al unui spital public a fost concediat după ce a semnalat că își suspecta superiorul ierarhic că practică eutanasierea – suspiciune care s-a dovedit nefondată. Curtea a concluzionat că nu a fost încălcat art. 10, întrucât suspiciunile reclamantului se bazau pe informații disponibile în dosarele electronice de sănătate, însă reclamantul știa că aceste dosare nu conțineau toate informațiile referitoare la sănătatea pacienților, spre deosebire de dosarele pe suport de hârtie. Astfel, chiar dacă acționase cu bună-credință, nu verificase în mod corespunzător exactitatea și fiabilitatea informațiilor pe care le divulgase (*Gawlik împotriva Liechtensteinului*, 2021, pct. 74-78).

355. Problema protecției datelor cu caracter personal ale jurnaliștilor sau a datelor aflate în posesia jurnaliștilor, care poate conduce la descoperirea identității surselor acestora, a fost examinată de Curte în mai multe cauze, între care:

- *Sedletska împotriva Ucrainei*, 2021 (pct. 59-60 și 64-73), în care autoritățile de anchetă obținuseră din partea judecătorului autorizația de a colecta datele de comunicare unei jurnaliste – datele, orele și localizarea prin antenele de telefonie mobilă a impulsurilor de pe telefoanele sale mobile în apropierea anumitor străzi și locații pe o perioadă de șaisprezece luni – de la operatorul său de telefonie mobilă, și în care Curtea a constatat o încălcare a art. 10 pe motivul că măsura în litigiu nu era justificată de o „cerință imperioasă de interes public” și nu prezenta garanții procedurale suficiente;
- *Jecker împotriva Elveției*, 2020 (pct. 37-43), în care un ordin împotriva unei jurnaliste de a divulga identitatea unei surse pentru a sprijini autoritățile penale să identifice un vânzător

de droguri a fost considerat de Curte ca fiind contrar art. 10, în lipsa unei evaluări *in concreto* a diferitelor interese aflate în joc;

- *Telegraaf Media Nederland Landelijke Media B.V. și alții împotriva Țărilor de Jos*, 2012 (pct. 102), în care supravegherea unor jurnaliștilor autorizată fără controlul prealabil al unui organ independent și ordinul de divulgare a documentelor care ar fi putut conduce la identificarea surselor lor au constituit o încălcare a art. 8 și 10, coroborate. Controlul ulterior nu ar fi fost suficient întrucât, odată distrusă, confidențialitatea surselor jurnalistice nu putea fi restabilită (*ibidem*, pct. 100-101);
- *Financial Times Ltd și alții împotriva Regatului Unit*, 2009 (pct. 63), în care Curtea a precizat că comportamentul sursei nu putea fi niciodată decisiv pentru a stabili dacă era necesar să se ia în considerare un ordin de divulgare și nu trebuia să reprezinte decât un factor, desigur important, care trebuia luat în considerare în contextul exercițiului de punere în balanță;
- *Weber și Saravia împotriva Germaniei* (dec.), 2006 (pct. 143-153), în care Curtea a declarat vădit nefondat un capăt de cerere întemeiat pe o încălcare a libertății de exprimare rezultată din dispozițiile unei legi care autoriza supravegherea strategică a telecomunicațiilor și care împiedica jurnaliștii să se asigure că informațiile primite în contextul activităților lor rămâneau confidențiale;
- *Ernst și alții împotriva Belgiei*, 2003 (pct. 94-105), în care perchezițiile și confiscările în masă din sediile profesionale ale reclamanților, jurnaliști, cu scopul de a le identifica sursele, au constituit o încălcare a art. 10. [A se vedea, de asemenea, cauzele *Roemen și Schmit împotriva Luxemburgului*, 2003, pct. 47-60, care privea perchezițiile la domiciliul unui jurnalist pentru a-i identifica sursele; *Tillack împotriva Belgiei*, 2007, pct. 56-68, care privea perchezițiile și sechestrele la domiciliul și la biroul unui jurnalist suspectat de coruperea unui funcționar european pentru a obține informații confidențiale referitoare la anchetele în curs în cadrul instituțiilor europene, în vederea identificării autorului acestor divulgări; *Sanoma Uitgevers B.V. împotriva Țărilor de Jos* (MC), 2010, pct. 64-100, care privea confiscare de către poliție de probe care ar fi putut permite identificarea surselor jurnalistice; *Nagla împotriva Letoniei*, 2013, pct. 78-102, care privea perchezițiile urgente la domiciliul unei jurnaliste, implicând confiscarea unor dispozitive de stocare a datelor care conțineau sursele sale de informații; *Sérvulo & Associados - Sociedade de Advogados, RL, și alții împotriva Portugaliei*, 2015, pct. 101-120, care privea confiscarea de mare amploare de documente informatice și mesaje electronice dintr-un cabinet de avocatură; și *Görmüş și alții împotriva Turciei*, 2016, pct. 32-77, care privea protecția surselor jurnalistice care erau funcționari care constataseră și raportaseră comportamente sau practici pe care le considerau contestabile la locul de muncă în contextul confidențialității chestiunilor de ordin militar], și
- *Big Brother Watch și alții împotriva Regatului Unit* (MC), 2021, pct. 442-458, care privea un regim de interceptare în masă a comunicațiilor care permitea serviciilor de informații accesul accidental la materiale jurnalistice confidențiale, prin includerea accidentală a unor astfel de elementele în „plasele" unei interceptări în masă, care putea conduce astfel la colectarea unui număr mare de materiale jurnalistice confidențiale. Curtea a concluzionat că a fost încălcat art. 10 din Convenție.

3. Protecția datelor și interzicerea discriminării (art. 14 din Convenție)

356. În cauza *Sheffield și Horsham împotriva Regatului Unit* (MC), 1998 (pct. 51-61, 76-77), care privea întrebarea dacă statul pârât avea obligația de a recunoaște juridic noua identitate sexuală a reclamantelor, doi persoane transsexuale operate de la sexul masculin la cel feminin, Curtea a concluzionat că nu a fost încălcat art. 8, considerat singur sau coroborat cu art. 14. În opinia Curții, situațiile în care reclamantele ar fi putut fi nevoite să își divulge datele cu caracter personal nu se produseseră cu o asemenea frecvență încât să se poată considera că aduceau atingere în mod disproporționat drepturilor lor la respectarea vieții lor private. De asemenea, Curtea a arătat că statul

pârât făcuse eforturi, într-o anumită măsură, pentru a reduce la minimum riscul ca persoanelor transsexuale să li se pună întrebări deranjante cu privire la sexul lor, permițându-le să obțină permise de conducere, pașapoarte și alte tipuri de documente oficiale întocmite sub noile prenume și sex și că utilizarea certificatelor de naștere ca mijloc de identificare era în mod oficial descurajată (*ibidem*, pct. 59; *Cossey împotriva Regatului Unit*, 1990, pct. 36-42).

357. Într-o serie de cauze în care Curtea a examinat aspecte strâns legate de protecția datelor cu caracter personal din punctul de vedere al articolelor 8 sau 9, Curtea a hotărât că nu se ridica nicio problemă separată în temeiul art. 14 [*Sinan Işık împotriva Turciei,* 2010, pct. 57, care privea problema menționării, obligatorie sau facultativă, a religiei reclamantului pe cartea sa de identitate; *Avilkina și alții împotriva Rusiei,* 2013, pct. 61, care privea divulgarea dosarelor medicale ale mai multor membri ai Martorilor lui Iehova care refuzaseră să facă transfuzii de sânge; *Christine Goodwin împotriva Regatului Unit* (MC), 2002, pct. 92-93, 108, și *I. împotriva Regatului Unit* (MC), 2006, pct. 72-73, 88, care privea problema recunoașterii juridice a schimbării de sex a unei persoane).

4. Protecția datelor și dreptul la respectarea bunurilor (art. 1 din Protocolul nr. 1)

358. Curtea a examinat protecția datelor cu caracter personal și a dreptului la respectarea bunurilor în timpul percheziților și confiscărilor.

359. În cauza *Smirnov împotriva Rusiei*, 2007 (pct. 53-59), Curtea a hotărât că autoritățile naționale nu păstraseră un „just echilibru” între cerințele de interes general și cerințele privind protecția dreptului reclamantului la respectarea bunurilor și că, prin urmare, a fost încălcat art. 1 din Protocolul nr. 1 ca urmare a percheziției domiciliare a reclamantului, avocat de profesie, urmată, printre altele, de ridicarea unității centrale a calculatorului său care conținea hard diskurile cu datele sale cu caracter personal. Deși păstrarea probelor materiale putea fi necesară în interesul unei bune administrări a justiției, calculatorul în sine nu era nici obiectul, nici instrumentul, nici produsul unei infracțiuni. Întrucât informațiile care se aflau înregistrate pe hard disk, care puteau fi utile și decisive pentru anchetă, fuseseră examinate de anchetator, imprimate și depuse la dosar, nu exista niciun motiv pentru a continua păstrarea unității centrale, care, în plus, era instrumentul de lucru al reclamantului, care era, de altfel, utilizat pentru a păstra datele clienților săi.

360. În cauza *Kruglov și alții împotriva Rusiei*, 2020 (pct. 145-146), percheziția și confiscarea de către poliție la domiciliile și birourile reclamanților, avocaților sau clienților acestora a calculatoarelor și a hard diskurilor care conțineau informații cu caracter personal și documente care intrau sub incidența secretului profesional și care nu constituiau în sine un obiect, un instrument sau un produs al unei infracțiuni au condus la încălcarea art. 1 din Protocolul nr. 1.

361. În cauza *Pendov împotriva Bulgariei*, 2020 (pct. 43-51), Curtea a hotărât că păstrarea pentru o perioadă prelungită inutil a serverului informatic al reclamantului în contextul unei proceduri penale împotriva unor terți a condus la o încălcare a art. 1 din Protocolul nr. 1. Faptul că serverul informatic al reclamantului nu fusese niciodată examinat în scopul urmăririi penale, vizând numai terți, posibilitatea autorităților de a copia informațiile necesare, importanța serverului pentru activitatea profesională a reclamantului și faptul că parchetul rămăsese parțial inactiv a făcut ca păstrarea serverului reclamantului timp de șapte luni și jumătate să constituie o măsură disproporționată (*ibidem*, pct. 51).

5. Protecția datelor și libertatea de circulație (art. 2 din Protocolul nr. 4)

362. Curtea a trebuit să examineze o serie de cauze în care libertatea de circulație a unei persoane fizice a fost limitată din cauza datelor sale cu caracter personal stocate de autorități. În general, acestea au fost examinate din perspectiva art. 8.

363. Astfel, în cauza *Dalea împotriva Franței* (dec.), 2010, stocarea de către poliție în baza Sistemului de Informații Schengen de date a căror exactitate era contestată de partea interesată, îl împiedica pe reclamant să călătorească liber în spațiul Schengen. Reclamantul se afla în imposibilitatea de a accesa și de a obține rectificarea datelor cu caracter personal conținute în dosar. Curtea a reiterat faptul că art. 8 nu garanta, ca atare, un drept de intrare sau de ședere al unui străin într-un stat al cărui resortisant nu este. În speță, atingerea adusă vieții private a reclamantului ca urmare a înscrierii sale în baza Schengen de către autoritățile franceze era prevăzută de lege, urmărea scopul legitim de a proteja securitatea naționale, era proporțională cu scopul urmărit și necesară într-o societate democratică. Reclamantul nu invocase art. 2 din Protocolul nr. 4.

364. În cauza *Shimovolos împotriva Rusiei*, 2011 (pct. 64-71), informațiile privind deplasările cu trenul și cu avionul ale reclamantului fuseseră înregistrate în „baza de date de supraveghere” ca urmare a apartenenței sale la o organizație pentru apărarea drepturilor omului. De fiecare dată când o persoană al cărei nume figura pe această listă achiziționa un bilet de tren sau de avion, Departamentul intern al transporturilor era informat în mod automat. Astfel, atunci când reclamantul s-a deplasat la Samara cu ocazia unui summit Uniunea Europeană - Rusia și a unui protest în acest oraș, trei ofițeri de poliție i-au verificat documentele de identitate și l-au întrebat care era motivul călătoriei sale. Curtea a hotărât că, prin colectarea și păstrarea datelor privind deplasările reclamantului în temeiul unui decret ministerial care nu fusese nici publicat, nici pus altfel la dispoziția publicului, autoritățile îi încălcaseră viața privată într-un mod incompatibil cu dreptul garantat la art. 8. De asemenea, a considerat că nu se ridica nicio problemă separată din perspectiva art. 2 din Protocolul nr. 4 (*ibidem*, pct. 73).

365. În cauza *Beghal împotriva Regatului Unit*, 2019 (pct. 89-109), în care se ridica problema importanței monitorizării deplasărilor teroriștilor la nivel internațional, Curtea a considerat, înainte de a concluziona în sensul unei încălcări a art. 8, că puterea conferită în temeiul legislației antiterorism agenților de poliție și de imigrare, precum și agenților vamali desemnați în acest scop de a aresta, a interoga și a percheziționa pasageri în porturile, aeroporturile și terminalele feroviare internaționale nu era nici suficient delimitată, nici însoțită de garanții juridice adecvate împotriva abuzurilor. În special, nu era necesară nicio autorizare prealabilă, iar puterea de a reține și de interoga putea fi exercitată chiar și în lipsa suspiciunii de participare la activități teroriste.

366. În cauza *Willems împotriva Țărilor de Jos* (dec.), 2021, care privea obligația, în temeiul legii pașapoartelor, de a preleva amprente digitale atunci când se solicita un pașaport și păstrarea amprentelor digitale pe un cip electronic, ca urmare a încorporării în dreptul național (fără nicio marjă de manevră pentru autoritățile naționale), a Regulamentului UE privind elementele de securitate și elementele biometrice din documentele de călătorie, Curtea a respins ca vădit nefondate capetele de cerere ale reclamantului formulate în temeiul art. 8 și al art. 2 din Protocolul nr. 4, având în vedere „prezumția unei protecții echivalente” în temeiul dreptului UE (*ibidem*, pct. 26-36).

B. Protecția datelor și drepturile procedurale

Articolul 6 din Convenție

„1. Orice persoană are dreptul la judecarea în mod echitabil, în mod public și într-un termen rezonabil a cauzei sale, de către o instanță independentă și imparțială, instituită de lege, care va hotărî fie asupra încălcării drepturilor și obligațiilor sale cu caracter civil, fie asupra temeiniciei oricărei acuzații în materie penală îndreptate împotriva sa. Hotărârea trebuie sa fie pronunțată în mod public, dar accesul în sala de ședințe poate fi interzis presei și publicului pe întreagă durata a procesului sau a unei părți a acestuia în interesul moralității, al ordinii publice ori al securității naționale într-o societate democratică, atunci când interesele minorilor sau protecția vieții private a părților la proces o impun, sau în măsura considerată absolut necesară de către instanță atunci când, în împrejurări speciale, publicitatea ar fi de natură să aducă atingere intereselor justiției.

2. Orice persoană acuzată de o infracțiune este prezumată nevinovată până ce vinovăția sa va fi legal stabilită.

3. Orice acuzat are, în special, dreptul:

a) să fie informat, în termenul cel mai scurt, într-o limbă pe care o înțelege și în mod amănunțit, asupra naturii și cauzei acuzației aduse împotriva sa;

b) să dispună de timpul și de înlesnirile necesare pregătirii apărării sale;

c) să se apere el însuși sau să fie asistat de un apărător ales de el și, dacă nu dispune de mijloacele necesare pentru a plăti un apărător, să poată fi asistat în mod gratuit de un avocat din oficiu, atunci când interesele justiției o cer;

d) să întrebe sau să solicite audierea martorilor acuzării și să obțină citarea și audierea martorilor apărării în aceleași condiții ca și martorii acuzării;

e) să fie asistat în mod gratuit de un interpret, dacă nu înțelege sau nu vorbește limba folosită la audiere.

Articolul 13 din Convenție

„Orice persoană, ale cărei drepturi și libertăți recunoscute de prezenta Convenție au fost încălcate, are dreptul să se adreseze efectiv unei instanțe naționale, chiar și atunci când încălcarea s-ar datora unor persoane care au acționat în exercitarea atribuțiilor lor oficiale.” “

1. Dreptul la un proces echitabil (art. 6 din Convenție)[12]

367. Orice persoană ale cărei date cu caracter personal fac obiectul unei prelucrări automate în contextul unei proceduri judiciare trebuie să beneficieze de garanțiile prevăzute la art. 6, oricare ar fi poziția sa în cadrul procedurii, reclamant, pârât, martor, acuzat sau simplu terț.

a. Garanții generale (art. 6 § 1 din Convenție)

368. Într-o serie de cauze, Curtea a examinat, din perspectiva art. 6 § 1, necesitatea de a proteja datele cu caracter personal ale părților sau ale terților în contextul examinării diferitelor garanții generale pentru a asigura echitatea procedurilor judiciare, și anume, printre altele, egalitatea armelor

[12] Acest capitol trebuie citit în lumina și coroborat cu ghidurile privind art. 6 în materie *civilă* (pag. 60-91) și *penală* (pag 32-100).

și respectarea procedurii contradictorii, publicitatea dezbaterilor și a pronunțării hotărârii, administrarea probelor, caracterul rezonabil al duratei procedurii și cerința motivării hotărârilor.

i. Egalitatea armelor și respectarea procedurii contradictorii în contextul procedurilor care implică date sensibile sau confidențiale

369. În cauza *Eternit împotriva Franței* (dec.), 2012 (pct. 35-42), o procedură inițiată de angajator împotriva deciziei unei case de asigurări de sănătate de a recunoaște natura profesională a bolii unuia dintre angajații săi, procedură în cursul căreia angajatorului nu i se comunicaseră observațiile medicale ale medicului consultant al casei de sănătate, nu a fost considerată contrară art. 6 § 1. Necomunicarea către angajator a datelor medicale ale angajatului său se putea explica prin cerința de a proteja confidențialitatea datelor medicale ale acestuia, pe care instanțele au fost obligate să o ia în considerare în același mod cu dreptul societății reclamante la o procedură contradictorie, astfel încât niciunul dintre aceste drepturi să nu fie afectat în substanța sa. Acest echilibru era realizat atunci când angajatorul putea solicita instanței să desemneze un medic expert independent, căruia să îi fie prezentate documentele care alcătuiau dosarul medical al angajatului și al cărui raport, întocmit cu respectarea secretului medical, avea drept scop să fie adusă o clarificare instanței și părților (*ibidem*, pct. 37). Faptul că nu fusese dispus un raport de expertiză în toate cazurile în care angajatorul solicita acest lucru, ci numai în cazul în care instanța considera că este insuficient informată, nu era un fapt contrar art. 6 § 1 în ceea ce privește cerințele unui proces echitabil (*ibidem*, pct. 35-39).

370. În cauza *Kennedy împotriva Regatului Unit*, 2010 (pct. 184-191), restricțiile aduse principiilor egalității armelor și al contradictorialității în fața Tribunalului pentru Litigii referitoare la Competențele de Investigare, un organ independent însărcinat cu examinarea oricărei plângeri formulate de persoane care considerau că comunicațiile lor au fost interceptate ilegal de autorități, nu au fost considerate incompatibile cu art. 6 § 1. Interesele legate de securitatea națională sau de necesitatea de a păstra secrete anumite metode de cercetare în materie penală trebuiau să fie puse în balanță cu dreptul la o procedură contradictorie. În opinia Curții, era necesar să fie ascunse informații sensibile și confidențiale a căror divulgare ar fi împiedicat atingerea obiectivului urmărit (*ibidem*, pct. 186-187).

371. În termeni mai generali, Curtea a subliniat că dreptul la o procedură penală contradictorie implica, atât pentru acuzare, cât și pentru apărare, posibilitatea de a lua cunoștință și de a formula observații cu privire la observațiile sau probele prezentate de cealaltă parte, precum și de a le comenta, de exemplu o înregistrare video a unei persoane acuzate, reținută ca probă incriminatoare [*Murtazaliyeva împotriva Rusiei*, (MC), 2018, pct. 90-95].

ii. Motivarea hotărârilor și protecția datelor

372. În cauza *Surikov împotriva Ucrainei*, 2017 (pct. 102-103), Curtea a concluzionat că a fost încălcat art. 6 § 1 pe motiv că instanțele naționale nu abordaseră anumite aspecte relevante și importante invocate. Partea interesată susținea că angajatorul său colectase și păstrase în mod arbitrar date sensibile și caduce cu privire la sănătatea sa mintală, apoi le utilizase în contextul examinării cererii sale de promovare și le divulgase în mod ilegal în fața colegilor săi și a instanței. Curtea a reafirmat faptul că art. 6 nu obliga instanțele să își motiveze hotărârile. Deși această obligație nu ar putea fi înțeleasă ca necesitând un răspuns detaliat la toate argumentele, în cazul în care instanțele naționale ar ignora un aspect specific, relevant și important formulat de un reclamant, acest lucru ar fi contrar principiului echității (*ibidem*, pct. 101 și exemplele de jurisprudență citate acolo).

373. În cauza *Samoylova împotriva Rusiei*, 2021 (pct. 50-52), care privea difuzarea într-un reportaj televizat a adresei exacte a reședinței reclamantei, a numărului său de identificare fiscală și a imaginilor din interiorul casei sale de la țară, Curtea a hotărât că instanțele naționale nu furnizaseră un răspuns specific și explicit la argumentele care ar fi fost decisive pentru soluționarea procedurii inițiate de partea interesată, cu încălcarea dreptului la un proces echitabil garantat de art. 6 § 1 din Convenție.

374. În cauza *Kennedy împotriva Regatului Unit*, 2010 (pct. 185-191), politica autorităților de „a nu confirma și nega” că avusese loc o interceptare a comunicațiilor nu a fost considerată incompatibilă cu art. 6 § 1. Astfel, Tribunalul pentru Litigii referitoare la Competențele de Investigare, care era însărcinat cu examinarea plângerilor formulate de persoane care considerau că făcuseră obiectul unei interceptări ilegale a comunicărilor lor, se putea limita la a informa reclamanții că nu a fost luată nicio decizie în favoarea lor, întrucât, în cazul în care o cale de atac în fața acestui tribunal putea conduce la a dezvălui reclamanților punerea în aplicare a unei operațiuni de interceptare, politica guvernului de „a nu confirma și a nu nega” ar fi fost repusă în discuție (*ibidem*, pct. 189).

iii. Administrarea de date cu caracter personal de probe colectate în mod ilegal sau contrar art. 8

375. Chestiunea utilizării ca probe materiale, în cadrul unei proceduri judiciare, a datelor cu caracter personal colectate într-un mod care contravine cerințelor dreptului intern sau ale art. 8 a fost abordată până în prezent de Curte într-o serie de cauze, în contextul unor proceduri administrative (*Vukota-Bojic împotriva Elveției*, 2016, pct. 77, care privea utilizarea într-un litigiu cu o persoană asigurată de informații colectate în secret de o societate de asigurări în contextul competențelor care îi erau conferite de sistemul public de asigurări); civile [*Bărbulescu împotriva României* (MC), 2017, pct. 140-141, care privea utilizarea datelor colectate de un angajator cu privire la utilizarea Internetului de către un angajat la locul de muncă pentru a justifica concedierea acestuia; *Florindo de Almeida Vasconcelos Gramaxo împotriva Portugaliei*, 2022, pct. 130-140, privind utilizarea kilometrajului înregistrat de sistemul GPS al vehiculului de serviciu al unui delegat medical pentru a justifica concedierea persoanei vizate] sau penale [*Bykov împotriva Rusiei* (MC), 2009, pct. 80-83, care privea interceptarea unei conversații în contextul unei operațiuni secrete a poliției și utilizarea probelor astfel colectate pentru a justifica o condamnare].

376. Curtea a considerat că admiterea și utilizarea, într-o procedură judiciară, a unor astfel de probe nu conduce în mod automat la constatarea unei inechități în cazul în care, în ansamblu, procedurile s-a desfășurat într-un mod echitabil [*Bykov împotriva Rusiei* (MC), 2009, pct. 89-91; *Vukota-Bojic împotriva Elveției*, 2016, pct. 91-100].

377. Curtea a concluzionat că a fost încălcat art. 6 § 1 în ceea ce privește informațiile colectate, grație intervenției unui informator al poliției, printr-un dispozitiv de înregistrare secretă a conversațiilor în celula reclamantului, faptă care nu era „prevăzută de lege” (*Allan împotriva Regatului Unit*, 2002, pct. 45-53). Mărturiile făcute de reclamant nu erau spontane, ci fuseseră provocate de întrebările continue ale informatorului, care, la cererea poliției, condusese conversațiile lor în condiții care puteau fi considerate drept constituind echivalentul unui interogatoriu, dar fără garanțiile care trebuie să-l însoțească. Deși nu exista nicio relație specială între reclamant și informator și nu se constatase nicio constrângere directă, reclamantul fusese supus unor presiuni psihologice care aduseseră atingere caracterului voluntar al mărturiilor sale. În aceste condiții, informațiile colectate puteau fi considerate ca fiind obținute împotriva voinței reclamantului și utilizarea acestora în cadrul procesului întrucât aduseseră atingere dreptului său la tăcere și de a nu se autoincrimina.

iv. Publicarea dezbaterilor și a pronunțării hotărârii și confidențialitatea datelor[13]

378. În cauza *P. și B. împotriva Regatului Unit*, 2001 (pct. 38-41, 46-49), lipsa publicității dezbaterilor și pronunțarea, în ședință în camera de consiliu, a unei hotărâri într-o cauză care privea încredințarea copiilor nu au fost considerate contrare art. 6 § 1. În opinia Curții, procedurile de încredințare a copilului sunt exemple tipice ale unei situații în care poate fi justificat să se interzică accesul presei și al publicului în sala de judecată, pentru a proteja datele cu caracter personal ale copilului în cauză și ale părților și pentru a evita să se aducă atingere intereselor justiției (*ibidem*, pct. 38). Faptul că orice

[13] A se vedea, de asemenea, supra, partea din prezentul ghid privind „Divulgarea de date în contextul procedurilor judiciare”, din perspectiva art. 8 din Convenție.

persoană care poate justifica un interes avea dreptul de a consulta sau de a obține o copie a textului integral al ordinelor și hotărârilor și că hotărârile judecătorești erau publicate automat, fără numele părților interesate, permitea în mod suficient să se remedieze lipsa unei pronunțări făcute publice (*ibidem*, pct. 47).

379. În cauza *Kennedy împotriva Regatului Unit*, 2010 (pct. 188), Curtea a amintit că, în temeiul art. 6 § 1, securitatea națională putea justifica excluderea publicului de la o procedură și a hotărât că natura întrebărilor adresate Tribunalului pentru Litigii referitoare la Competențele de Investigare, care priveau nelegalitatea interceptării comunicațiilor, justificau lipsa unei ședințe publice.

380. Curtea a constatat o dublă încălcare a art. 6 în cauza *Vasil Vasilev împotriva Bulgariei*,2021, care punea în discuție lipsa totală a publicității (excluderea publicului de la toate ședințele și lipsa pronunțării publice a hotărârii) în cadrul unei acțiuni în despăgubire introduse de reclamant în urma interceptării, înregistrării și transcrierii unei conversații telefonice între acesta și unul dintre clienții săi, supravegheat în secret în cadrul unei cauze penale. Excluderea publicului de la toate ședințele și lipsa pronunțării publice a hotărârii se baza exclusiv pe prezența în dosar a unor informații clasificate (probele rezultate din interceptarea secretă a convorbirii telefonice a reclamantului). Potrivit Curții, lipsa totală a publicității nu poate fi justificată de necesitatea de a proteja informațiile clasificate la care se referea cauza. Natura întrebărilor adresate în cursul procedurii, care priveau răspunderea autorităților statului pentru o pretinsă încălcare a drepturilor garantate de art. 8, nu avea un caracter foarte tehnic, iar reclamantul nu renunțase la dreptul său la o ședință publică (*ibidem*, pct. 107-111). Atunci când o cauză privește o presupusă încălcare a unui drept fundamental de către autoritățile statului, controlul public al procedurilor este esențial pentru a menține încrederea în statul de drept. Prezența unor informații clasificate în dosarul cauzei nu putea constitui în sine un motiv pentru a refuza să se comunice publicului textul integral al hotărâri. Dacă o cauză implică informații clasificate, există tehnici care permit un anumit grad de acces al publicului la deciziile care sunt pronunțate, menținând în același timp confidențialitatea informațiilor sensibile (*ibidem*, pct. 116-118).

v. Durata procedurilor judiciare care se pronunță cu privire la chestiunea protecției datelor

381. În cauza *Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei* (MC), 2017 (pct. 215), Curtea a hotărât că durata totală, șase ani și șase luni pentru două grade de jurisdicție, a unei proceduri care privea legalitatea, în temeiul dreptului intern și al dreptului Uniunii, al publicării la scară largă de date cu caracter personal cu caracter fiscal de către societățile reclamante nu îndeplinea cerința unui termen rezonabil garantat de art. 6 § 1. Procedura în fața Curții de Justiție a Uniunii Europene, sesizată cu o întrebare preliminară, nu putea fi luată în considerare în evaluarea duratei imputabile autorităților interne (*ibidem*, pct. 208).

382. În schimb, în cauza *Surikov împotriva Ucrainei*, 2017 (pct. 104-106), Curtea a declarat vădit nefondat un capăt de cerere întemeiat pe durata unei proceduri care privea păstrarea, de către un angajator, a unor date sensibile și caduce privind sănătatea mintală a unui angajat și utilizarea acestora în contextul examinării cererii sale de promovare. Curtea a hotărât că o perioadă mai mică de șase ani pentru trei grade de jurisdicție nu putea ridica o problemă în ceea ce privește cerința unei durate rezonabile, prevăzută la ar. 6 § 1 (*ibidem*, pct. 101).

b. Garanții speciale (art. 6 §§ 2 și 3 din Convenție)

383. În materie penală, orice persoană ale cărei date cu caracter personal au reprezentat temeiul unei acuzații împotriva sa trebuie să beneficieze de anumite garanții speciale.

i. Protecția datelor și respectarea prezumției de nevinovăție (art. 6 § 2 din Convenție)

384. În cauza *Batiashvili împotriva Georgiei*, 2019 (pct. 87-97), Curtea a recunoscut că art. 6 § 2 era aplicabil într-o situație în care autoritățile manipulaseră, înainte de arestarea unei persoane, apoi

difuzaseră pe un canal de televiziune, o înregistrare audio a convorbirilor sale telefonice. Potrivit Curții, implicarea autorităților a contribuit la a face să pară vinovată o persoană, chiar dacă vinovăția acesteia nu fusese stabilită de o instanță, încălcând astfel această dispoziție. În opinia sa, cronologia faptelor, privită în ansamblu, indica faptul că autoritățile de anchetă se comportaseră într-un mod care avusese un impact semnificativ asupra situației reclamantului (*ibidem*, pct. 94). Chiar dacă acuzația de nedenunțare a unei infracțiuni a fost abandonată în cursul procedurii în primă instanță, actul de inculpare trimis instanței la aproape patru luni după ce înregistrarea a fost făcută publică o menționa încă, în timp ce organele de urmărire penală trebuie să fi avut deplină cunoștință de falsitatea probelor pe care se întemeia acuzația (*ibidem*, pct. 95).

385. În cauza *Y.B. și alții împotriva Turciei*, 2004 (pct. 43-51), declarațiile făcute presei de poliție cu privire la suspecți, fotografiați de jurnaliști în cadrul unei conferințe de presă organizate la sediul poliției, au condus la o încălcare a art. 6 § 2. Publicarea, în cadrul unei proceduri penale, a fotografiilor prezintând-i pe suspecți nu poate constitui în sine o încălcare a dreptului acestora la prezumția de nevinovăție. Autoritățile naționale pot informa publicul cu privire la anchetele penale în curs, cu condiția să facă acest lucru cu toată discreția și rezerva necesare. Atunci când fac publice probe obiective derivate din procedurile penale, aceste probe trebuie totuși să fie prezentate fără subiectivitate sau antepronunțarea vinovăției (*ibidem*, pct. 47-48). În speță, atitudinea autorităților polițienești, în măsura în care reflecta o evaluare apreciere a acuzațiilor care puteau fi reținute împotriva reclamanților și punea la dispoziția presei mijloace materiale care permiteau identificarea lor cu ușurință, nu se reconcilia cu respectarea dreptului lor la prezumția de nevinovăție (*ibidem*, pct. 50).

386. În cauza *Panteleyenko împotriva Ucrainei,* 2006 (pct. 68-71), termenii de redactare a hotărârilor judecătorești prin care se finalizase urmărirea penală împotriva reclamantului, care, potrivit Curții, nu lăsau nicio îndoială că judecătorii considerau că acesta săvârșise infracțiunea de care era acuzat, a condus la constatarea unei încălcări a art. 6 § 2. Rezoluția de neîncepere a urmăririi penale din „motive de exonerare” a fost luată pe baza informațiilor care conțineau datele cu caracter personal ale reclamantului, notar de profesie, obținute în urma unei percheziții efectuate la biroul său fără a respecta obligația prevăzută de lege de notificare prealabilă a ocupantul sediului în ceea ce privește mandatul de percheziție și cu încălcarea interdicției, din dreptul intern, de a confisca documente și obiecte fără un raport direct cu ancheta (*ibidem*, pct. 70)[14].

ii. Protecția datelor și dreptul la apărare [art. 6 § 3 b) din Convenție]

387. În cauza *Rook împotriva Germaniei*, 2019 (pct. 69), un termen de trei luni și jumătate pentru a analiza o masă voluminoasă de date și fișiere electronice ale reclamantului rezultate din supravegherea telecomunicațiilor sale reprezenta, în opinia Curții, un termen suficient, în lumina art. 6 § 3 b), pentru a permite avocatului să își pregătească apărarea. Ținând seama de complexitatea procedurii penale în discuție, nu era necesar să i se acorde avocatului reclamantului posibilitatea de a citi și de a asculta fiecare element al datelor de supraveghere, care făcuse posibilă în cursul anchetei colectarea a 45 000 de apeluri telefonice și 34 000 seturi de alte date provenite din telecomunicații și 14 milioane de fișiere electronice pe care poliția le confiscase din apartamentul reclamantului și din alte locații (*ibidem*, pct. 7-8, 67-71).

388. În termeni mai generali, Curtea a subliniat faptul că mijloacele de investigare actuale pot genera cantități enorme de date, a căror integrare într-o procedură penală nu ar trebui să provoace întârzieri inutile. Dreptul reclamantului de a i se comunica masa brută a datelor nu trebuie confundat cu dreptul acestuia de a avea acces la toate documentele pe care autoritățile le consideră deja relevante, ceea ce impune, în general, ca partea interesată să fie în măsură să înțeleagă tot conținutul acestora (*ibidem*, pct. 67). Simplul fapt că procedura judiciară fusese deja inițiată atunci când avocatul primise

[14] A se vedea, de asemenea, *Ghid privind art. 6 din Convenție* [Dreptul la un proces echitabil (aspectul civil) cu privire la motivarea hotărârilor (pct. 168-176].

o copie integrală a dosarului nu poate conduce la concluzia că nu a beneficiat de un timp de pregătire suficient. Art. 6 § 3 b) nu impune ca pregătirea unui proces de o anumită durată să fie finalizată înainte de desfășurarea primei ședințe (*ibidem*, pct. 72)[15].

389. În cauza *Sigurður Einarsson și alții împotriva Islandei*, 2019 (pct. 88-93), Curtea a concluzionat lipsa unei încălcări a art. 6 §§ 1 și 3 b) în ceea ce privește excluderea de la apărare a unei mase de date colectate în mod neselectiv de parchet și nedepuse la dosarul anchetei, precum și a sortării electronice a acestora de către parchet în vederea selectării informațiilor relevante pentru anchetă. În ceea ce privește „întreaga compilație", parchetul ignorase conținutul masei datelor și, ca atare, nu beneficiase de niciun avantaj în raport cu apărarea. În ceea ce privește datele care fuseseră „marcate", ar fi fost, în principiu, oportun să i se acorde apărării posibilitatea de a efectua cercetări în vederea identificării unor elemente potențial dezincriminatoare. Cu toate acestea, reclamanții nu solicitaseră niciodată în mod formal pronunțarea unei hotărâri în acest sens și nu furnizaseră nicio precizare cu privire la tipul de probe pe care le solicitau.

2. Dreptul la un recurs efectiv (art. 13 din Convenție)[16]

390. În materie de divulgare a datelor medicale, în cauza *Anne-Marie Anderson împotriva Suediei*, 1997 (pct. 41-42), Curtea a concluzionat că nu a fost încălcat art. 13 coroborat cu art. 8 în ceea ce privește lipsa unei căi de atac înainte ca o autoritate medicală să comunice date medicale cu caracter personal și confidențiale unui serviciu social. Printre altele, măsura fusese notificată părții interesate și avea un domeniu de aplicare limitat, întrucât informațiile în cauză nu fuseseră făcute publice, ci beneficiau de același grad de confidențialitate ca și dosarele psihiatrice.

391. În cauza *Mik și Jovanović împotriva Serbiei* (dec.), reclamanții se plângeau, în temeiul art. 8 considerat separat și coroborat cu art. 13, că statul continua să nu le furnizeze informații credibile cu privire la soarta fiilor lor, despre care li se spusese că decedaseră la scurt timp după naștere și că nu le-au fost niciodată arătate corpurile. Curtea a constatat că o lege adoptată recent instituise un mecanism (inclusiv o bază de date ADN) pentru a răspunde situației cu care se confruntau reclamanții și alte persoane. În special, a observat că noul cadru juridic prevedea atât proceduri judiciare, cât și proceduri extrajudiciare pentru a investiga situația reală a nou-născuților despre care se presupunea că au fost răpiți în centre publice de maternitate, permițând părinților în cauză să obțină reparații. A observat, de asemenea, că fuseseră luate anumite măsuri importante pentru punerea în aplicare a acestui nou cadru, inclusiv formarea completă a judecătorilor și numirea, pentru procedura extrajudiciară, de membri (în principal reprezentanți ai asociațiilor de părinți înființate) ai unei comisii cu competențe extinse de investigare, colectare de date și raportare. Constatând că reclamanții înșiși aleseseră să recurgă la acest nou mecanism, a concluzionat că nu mai era justificat să continue examinarea cererii, în sensul art. 37 § 1 c) din Convenție.

392. În cauza *Panteleyenko împotriva Ucrainei*, 2006 (pct. 82-84), Curtea a concluzionat că a fost încălcat art. 13 coroborat cu art. 8, luând în considerare lipsa unui recurs efectiv care să permită reclamantului să se plângă de divulgarea de informații confidențiale privind sănătatea sa mintală în cadrul unei ședințe publice. În opinia Curții, procedurile legale existente s-au dovedit ineficiente, întrucât nu au condus la încetarea divulgării de date psihiatrice confidențiale din dosar și nici nu au condus la acordarea de daune-interese părții interesate pentru prejudiciul suferit ca urmare a atingerii aduse dreptului său la viață privată. Desfășurarea unei ședințe în camera de consiliu ar fi permis să se evite divulgarea către public a informațiilor în litigiu, dar nu ar fi împiedicat ca acestea să fie aduse la cunoștința părților și să fie depuse la dosarul cauzei.

[15] A se vedea, de asemenea *Ghid privind art. 6 din Convenție* [Dreptul la un proces echitabil (aspectul civil) cu privire la înlesnirile necesare acuzatului în pregătirea apărării sale.

[16] Prezentul capitol trebuie citit în lumina și coroborat cu *Ghid privind art. 13 din Convenție* (a se vedea în special pag. 49-51).

393. În ceea ce privește publicarea pe Internet a unei hotărâri care divulga informații referitoare la adopția copiilor reclamanților, Curtea a concluzionat, în cauza *X și alții împotriva Rusiei*, 2020 (pct. 73-79), că a fost încălcat art. 13 coroborat cu art. 8, în lipsa unei căi de atac care să poată oferi o despăgubire pentru prejudiciul moral cauzat de funcționarea defectuoasă a sistemului de justiție.

394. Într-o cauză care privea înscrierea unei persoane ca „delincvent" în registrele poliției, după ce a fost interogată cu privire la un viol și păstrarea acestei mențiuni fără întocmirea ulterioară a unui act de punere sub învinuire, Curtea a concluzionat că a fost încălcat art. 13 coroborat cu art. 8, după ce a constatat că partea interesată nu dispusese la momentul faptelor de nicio cale de atac pentru a se plânge de această măsură (*Dimitrov-Kazakov împotriva Bulgariei*, 2011, pct. 37-39).

395. Lipsa unui recurs efectiv pentru a solicita eliminarea numelui reclamantului de pe lista anexată la ordonanța privind talibanii a constituit o încălcare a art. 13 coroborat cu art. 8 în cauza *Nada împotriva Elveției* (MC), 2012 (pct. 209-214). Reclamantul avusese posibilitatea să sesizeze instanțele interne, însă acestea nu îi examinaseră capetele sale de cerere pe fond.

396. În ceea ce privește utilizarea datelor cu caracter personal în context profesional, lipsa unui recurs efectiv pentru încălcarea dreptului la viață privată al reclamanților în ceea ce privește anchetele indiscrete privind viața privată a homosexualilor care au condus la excluderea lor din armată a constituit o încălcare a art. 13 coroborat cu art. 8 în cauza *Smith și Grady împotriva Regatului Unit*, 1999 (pct. 136-139).

397. În cauza *Karabeyoğlu împotriva Turciei*, 2016 (pct. 128-132), indisponibilitatea unei căi de recurs interne pentru examinarea utilizării, în cadrul unei anchete disciplinare, a datelor provenite din interceptarea convorbirilor telefonice din cadrul unei anchete penale a determinat Curtea să concluzioneze o încălcare a art. 13, citit în lumina art. 8.

398. În cauza *Peck împotriva Regatului Unit*, 2003 (pct. 101-114), Curtea a considerat că reclamantul nu dispusese de niciun recurs efectiv pentru a se plânge de transmiterea către media a unui material video provenit de la o cameră de televiziune cu circuit închis în timp ce încerca să se sinucidă într-un loc public. În ceea ce privește posibilitatea unui control jurisdicțional, întrucât singura întrebare adresată instanțelor naționale era dacă politica urmată în ceea ce privește imaginile captate de camerele video în locuri publice putea fi considerată „irațională", era exclusă orice examinare a aspectului dacă ingerința în drepturile reclamantului răspundea unei nevoi sociale imperioase sau dacă era proporțională (*ibidem*, pct. 106-107). De asemenea, comisiile competente în domeniul media nu ofereau nicio formă de recurs efectiv, întrucât nu aveau competența de a acorda daune-interese (*ibidem*, pct. 108-109). În ceea ce privește posibilitatea de a introduce o acțiune pentru abuz de încredere, era puțin probabil ca instanțele să fi acceptat la momentul faptelor că imaginile aveau „calitatea necesară de încredere" sau ca informațiile să fi fost „comunicate în circumstanțe care impun o obligație de discreție" (*ibidem*, pct. 111).

399. În materie de supraveghere secretă, caracterul secret al măsurilor face foarte dificil, dacă nu chiar imposibil, ca partea interesată să exercite un recurs, în special atât timp cât durează supravegherea. Un „recurs efectiv" în sensul art. 13 trebuie înțeles ca fiind efectiv atât cât poate fi având în vedere domeniul său de aplicare limitat, inerent oricărui sistem de supraveghere (*Klass și alții împotriva Germaniei*, 1978, pct. 68-69). Un mecanism obiectiv de control poate fi suficient cât timp măsurile rămân secrete. Dar, odată ce măsurile sunt dezvăluite, este necesar ca persoanei să i se pună la dispoziție căi de atac într-un termen rezonabil [*Rotaru împotriva României* (MC), 2000, pct. 69].

400. În domeniul măsurilor de supraveghere secretă țintite, în care abuzurile pot surveni destul de ușor în cazuri individuale și pot antrena consecințe negative pentru societatea democratică în ansamblu, se recomandă în principiu ca acest control să fie încredințat unui judecător, deoarece puterea judecătorească oferă cele mai bune garanții de independență, imparțialitate și procedură legală. Este dezirabilă informarea persoanei vizate după ridicarea măsurilor de supraveghere de îndată ce notificarea poate fi emisă fără a pune în pericol scopul restrângerii. Pentru a oferi părții interesate

mijlocul de a obține controlul procedurii aferente ingerinței în exercitarea dreptului său la respectarea vieții private, este necesar, în principiu, să i se ofere un nivel minim de informații privind decizia pe care ar putea să o conteste, ca de exemplu data adoptării și instanța emitentă [*Roman Zakharov împotriva Rusiei* (MC), 2015, pct. 233, 287, 294; *Irfan Güzel împotriva Turciei*, 2017, pct. 96, 98-99].

401. În cauza *Klass și alții împotriva Germaniei*, 1978 (pct. 65-72), în care legea „G 10" permitea deschiderea și controlul corespondenței și al trimiterilor poștale, citirea mesajelor telegrafice, ascultarea și înregistrarea convorbirilor telefonice atunci când era vorba de apărarea țării împotriva unor „pericole iminente", Curtea a hotărât că toate căile de atac prevăzute de dreptul german îndeplineau, în circumstanțele excepționale ale cauzei, cerințele art. 13 în lumina art. 8, în ceea ce privește respectarea vieții private și a corespondenței. Chiar dacă, potrivit acestei legi, adoptarea și executarea unor măsuri restrictive nu puteau fi atacate cu recurs în instanță, alte căi de atac erau deschise oricărei persoane care credea că este supravegheată. Potrivit termenilor deciziei Curții Constituționale Federale din 1970, autoritatea competentă trebuia să notifice partea interesată de îndată ce măsurile de supraveghere erau ridicate și notificarea putea fi emisă fără a pune în pericol scopul restrângeri. De la data acestei comunicări, deveneau posibile pentru persoană diverse căi de atac în justiție: printr-o acțiune în constatare, să solicite unei instanțe administrative să examineze dacă legea „G 10" fusese aplicată persoanei în mod legitim și dacă măsurile de supraveghere dispuse erau prevăzute de lege; să introducă în fața unei instanțe civile o acțiune în despăgubiri dacă suferise un prejudiciu; să intenteze o acțiune în vederea distrugerii sau, după caz, a restituirii documentelor; în ultimul rând, dacă niciuna dintre aceste acțiuni nu avea succes, să sesizeze Curtea Constituțională Federală pentru ca aceasta să se pronunțe cu privire la o eventuală încălcare a legii fundamentale. A se vedea, de asemenea, în același sens, cauzele *Leander împotriva Suediei*, 1987 (pct. 78-84), care privea un sistem de control secret al candidaților pentru posturi importante din punct de vedere al securității naționale, și *Amann împotriva Elveției* (MC), 2000 (pct. 89-90), care privea interceptarea și înregistrarea unui apel telefonic, precum și păstrarea datelor cu caracter personal în dosarele serviciilor de securitate.

402. În lipsa unui răspuns la îndoielile exprimate de un inculpat cu privire la legalitatea deciziei de interceptare a convorbirilor telefonice, Curtea a concluzionat că a fost încălcat art. 13 coroborat cu art. 8 în cauza *Irfan Güzel împotriva Turciei*, 2017 (pct. 100-109).

403. În cauza *Allan împotriva Regatului Unit*, 2002 (pct. 55), Curtea a concluzionat că a fost încălcat art. 13 coroborat cu art. 8 pe motiv că, la data faptelor, nu exista nicio dispoziție legală care să reglementeze dispozitivele de înregistrare secretă a conversațiilor în celula reclamantului și utilizarea acestora de către poliție.

404. Într-o cauză în care controlul global al unui sistem de supraveghere secretă ținea exclusiv de competența Ministerului Afacerilor Interne, care era direct implicat în cererea de punere în aplicare a mijloacelor de supraveghere speciale pentru a proteja securitatea națională, și nu de organe independente, Curtea a concluzionat că fost încălcat art. 13 citit în lumina art. 8, în lipsa unui recurs efectiv (*Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdjiev împotriva Bulgariei,* 2007, pct. 98-103).

405. În lipsa unei căi de atac pentru a contesta păstrarea de către agenții de stat a datelor privind viața privată a unei persoane sau veridicitatea acestor informații, Curtea a concluzionat că art. 13 coroborat cu art. 8 a fost încălcat în cauza *Rotaru împotriva României* (MC), 2000 (pct. 68-73). Situația a fost una similară în cauza *Segerstedt-Wiberg și alții împotriva Suediei*, 2006 (pct. 116-122), în lipsa unei căi de atac care să permită să fie obținute toate informațiile conținute în dosarele de securitate, distrugerea dosarelor păstrate de serviciul de securitate, sau ștergerea ori corectarea informațiilor cu caracter personal conținute în acestea.

3. Dreptul la libertate și la siguranță (art. 5 din Convenție)

406. În cauza *Akgün împotriva Turciei*, 2021 (pct. 178-181), în care utilizarea de către reclamant a serviciului de mesagerie criptată ByLock constituia singura probă pe baza căreia, la momentul arestării sale preventive, era suspectat, în sensul art. 5 § 1 c), de săvârșirea infracțiunii de apartenență la o organizație teroristă, Curtea a constatat o încălcare a art. 5 § 1 c) din Convenție. Presupusele fapte ilicite se încadrau în sfera criminalității organizate. Utilizarea unei probe electronice care să ateste că o persoană utilizează mesageria criptată care a fost special concepută și utilizată exclusiv de o organizație criminală în scopul comunicațiilor interne ale acestei organizații poate constitui un instrument foarte important în lupta împotriva criminalității organizate. În consecință, o astfel de probă poate justifica în mod valabil, de la bun început, privarea de libertate a unei persoane, în măsura în care poate indica în mod clar că persoana respectivă aparține unei astfel de organizații. În aceste condiții, atunci când o astfel de probă constituie temeiul unic sau exclusiv al suspiciunilor în privința unui suspect, instanța națională trebuie să dispună de informații suficiente cu privire la o astfel de probă înainte de a examina cu prudență eventuala sa valoare probantă în dreptul intern. În speță, guvernul nu a fost în măsură să demonstreze că, la momentul arestării preventive a reclamantului, probele aflate la dispoziția judecătorului de pace îndeplineau criteriul existenței unei „bănuieli întemeiate” prevăzut la art. 5 § 1 c), și puteau astfel convinge un observator obiectiv că reclamantul a fost în măsură să săvârșească infracțiunea pentru care fusese privat de libertate. Potrivit Curții, documentul referitor la constatarea utilizării ByLock de către reclamant, ca atare, nu evidențiază activitatea ilegală a reclamantului, în măsura în care nu preciza nici datele acestei pretinse activități, nici frecvența acesteia ori alte detalii referitoare la aceasta. Pe de altă parte, nici acest document, nici ordinul de plasare în arest preventiv nu explica modul în care această pretinsă activitate a reclamantului indica apartenența sa la o organizație teroristă.

IV. Provocări moderne în materie de protecție a datelor

B. Progrese tehnologice, algoritmi și inteligență artificială[17]

407. În cauzele care priveau prelevarea și păstrarea de către autorități, în scopul prevenirii infracțiunilor, a amprentelor digitale, a mostrelor de celule și a profilurilor ADN ale persoanelor suspectate de săvârșirea de infracțiuni sau condamnate, Curtea a indicat cu claritate că utilizarea tehnicilor științifice moderne nu poate fi permisă în orice moment și fără o punere în balanță atentă a avantajelor care pot rezulta, pe de o parte, din utilizarea pe scară largă a unor astfel de tehnici și interesele esențiale legate de viața privată, pe de altă parte [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 112; *Podchasov împotriva Rusiei*, 2024, pct. 62]. Orice stat care își revendică rolul de pionierat în dezvoltarea de noi tehnologii are responsabilitatea specială de a găsi justul echilibru în materie [*S. și Marper împotriva Regatului Unit* (MC), 2008, pct. 112]. Având în vedere ritmul ridicat al inovațiilor în domeniile geneticii și al tehnologiilor informației, nu poate fi exclusă posibilitatea ca aspectele legate de viața privată atașat informațiilor genetice să fie afectate în viitor prin noi mijloace, care nu pot fi prevăzute cu precizie în prezent (*ibidem*, pct. 71).

408. În opinia Curții, dezvoltarea rapidă a unor tehnici din ce în ce mai sofisticate, care permit, printre altele, recunoașterea sau cartografierea facială pornind de la fotografii ale persoanelor, face captarea imaginii acestora, păstrarea datelor astfel colectate și posibila lor difuzare să fie problematice. Acest aspect trebuie luat în considerare de instanțele naționale atunci când analizează necesitatea ingerinței în dreptul la viață privată al persoanei în cauză (*Gaughran împotriva Regatului Unit*, pct. 70). În cauza

[17] Prezentul capitol trebuie citit coroborat cu părțile din prezentul ghid referitoare Culegerea de date în scopul combaterii criminalității și Colectarea de date de către autorități prin intermediul supravegherii secrete.

Gaughran împotriva Regatului Unit, 2020 (pct. 96-98), Curtea a subliniat că tehnologia utilizată actual era mai complexă și că instanțele naționale nu luaseră suficient în considerare acest aspect în momentul examinării necesității ingerinței în dreptul la respectarea vieții private al persoanei a cărei imagine fusese captată de autorități în urma săvârșirii unei infracțiuni minore și păstrată chiar și după ce condamnarea fusese ștearsă din cazierul său judiciar, la expirarea termenului prevăzut de lege.

409. În cauza *Breyer împotriva Germaniei*, 2020 (pct. 88), Curtea a admis că, în ceea ce privește combaterea criminalității organizate și a terorismului, metodele de investigare trebuie să fie adaptate la mijloacele de comunicare moderne și la schimbările comportamentelor societale în materie de comunicare. În viziunea sa, obligația impusă operatorilor de telefonie mobilă de a păstra datele și de a le pune la dispoziția autorităților constituie, în general, un răspuns adecvat la evoluția mijloacelor de telecomunicații și a comportamentelor în materie de comunicare. În schimb, în cauza *Podchasov împotriva Rusiei*, 2024 (pct. 70-79), dreptul intern a impus furnizorilor de servicii de comunicații prin internet să păstreze și să stocheze conținutul tuturor comunicațiilor prin internet timp de șase luni și datele privind comunicațiile timp de un an, precum și să acorde forțelor de ordine sau serviciilor de securitate acces, la cerere, la datele astfel stocate și la informațiile necesare pentru decriptarea mesajelor electronice criptate: Curtea a fost uimită de întinderea extremă a acestei obligații de păstrare și a considerat că o astfel de ingerință avea o amploare și o gravitate excepționale. Aceasta a observat, de asemenea, că dreptul intern nu impunea forțelor de ordine și serviciilor de securitate obligația de a prezenta o autorizație judiciară furnizorului de servicii de comunicații în cauză înainte de a obține accesul la comunicațiile unei anumite persoane. De fapt, furnizorii de servicii de comunicații au fost obligați să instaleze echipamente care să permită autorităților relevante să acceseze direct datele stocate. Deși, într-un astfel de sistem, nevoia de garanții împotriva arbitrariului și a abuzurilor este deosebit de mare, dreptul intern nu prevedea astfel de garanții. În ceea ce privește obligația legală de decriptare a comunicațiilor, Curtea a concluzionat că măsurile în cauză nu erau limitate la anumite persoane, ceea ce a avut ca efect slăbirea dispozițiilor privind criptarea pentru toți utilizatorii, afectând astfel pe toată lumea fără discriminare, inclusiv pe cei care nu reprezentau o amenințare la adresa intereselor legitime; prin urmare, Curtea a considerat că astfel de măsuri nu pot fi considerate proporționale (pct. 77-79).

410. Într-o cauză care privea supravegherea în masă a comunicațiilor, *Szabó și Vissy împotriva Ungariei*, 2016 (pct. 68), Curtea a admis că formele luate de terorism actual aveau drept consecință naturală recurgerea de către guverne la tehnologii de ultimă generație, în special tehnici de supraveghere în masă a comunicațiilor, pentru a evita incidente iminente. În speță, Curtea a hotărât că legislația care autoriza supravegherea în masă nu oferea garanțiile necesare împotriva abuzurilor, întrucât noile tehnologii permiteau autorităților să intercepteze cu ușurință o cantitate foarte mare de date referitoare la persoane chiar și din afara categoriei vizate inițial de operațiune. În plus, o astfel de măsură putea fi dispusă de puterea executivă fără niciun control, fără a fi supusă unei evaluări care să stabilească dacă era strict necesară și în lipsa unei recurs efectiv, judiciar sau de altă natură (*ibidem*, pct. 73-89).

411. În cauza *Roman Zakharov împotriva Rusiei* (MC), 2015 (pct. 302-305), Curtea a hotărât că riscul de abuz inerent oricărui sistem de supraveghere secretă era deosebit de ridicat într-un sistem în care serviciile secrete și poliția se bucurau de acces direct, prin mijloace tehnice, la toate comunicațiile de telefonie mobilă ale populației. Curtea a concluzionat că a fost încălcat art. 8, considerând că dispozițiile din dreptul rus care permiteau interceptarea generală a comunicațiilor nu includeau garanții adecvate și eficiente împotriva arbitrariului și a riscului de abuz inerent oricărui sistem de supraveghere secretă.

412. În cauza *Akgün împotriva Turciei*, 2021 (pct. 178-181), în care utilizarea de către reclamant a mesageriei ByLock prescrise constituia singurul element de probă care, la momentul arestării sale preventive, dădea naștere unei suspiciuni, în sensul art. 5 § 1 c), Curtea a subliniat că utilizarea unor astfel de probe ca temei exclusiv pentru o suspiciune putea da naștere la o serie de probleme delicate, întrucât, prin natura lor, procedura și tehnologiile aplicate colectării unor astfel de probe sunt

complexe și pot așadar diminua capacitatea judecătorilor naționali de a le stabili autenticitatea, exactitatea și integritatea (a se vedea supra, pct. 373).

413. În cauzele *Centrum för rättvisa împotriva Suediei* (MC), 2021, pct. 261, și *Big Brother Watch și alții împotriva Regatului Unit* (MC), 2021, pct. 322-323, Curtea a admis în mod expres că utilizarea interceptării în masă nu era în sine contrară art. 8, având în vedere proliferarea amenințărilor la adresa statelor pe care le reprezintă în prezent rețelele de actori internaționali care utilizează Internetul pentru a comunica și care adesea nu sunt detectate prin utilizarea unor tehnologii sofisticate. Cu toate acestea, Curtea a subliniat că, având în vedere evoluția constantă a tehnologiilor moderne de comunicare, abordarea sa obișnuită în ceea ce privește regimurile de supraveghere țintită trebuia să fie adaptată la particularitățile unui regim de interceptare în masă, atât din cauza riscului de abuz inerent acestui tip de interceptare, cât și din cauza necesității legitime, care o caracterizează, de a opera în secret. În special, procesul trebuie să fie încadrat de „garanții de la un capăt la altul", și anume, la nivel național, necesitatea și proporționalitatea măsurilor luate ar trebui evaluate în fiecare etapă a procesului, activitățile de interceptare în masă ar trebui să facă obiectul autorizării de către o autoritate independentă încă de la început, iar operațiunile ar trebui să facă obiectul unei supravegheri și al unui control independent efectuat *a posteriori*.

414. În cauza *Glukhin împotriva Rusiei*, 2023, Curtea a examinat pentru prima dată problema utilizării de către poliție a tehnologiei de recunoaștere facială. Această tehnologie a fost utilizată, mai întâi, pentru a-l identifica pe reclamant pe baza fotografiilor și a înregistrărilor video publicate pe un canal public pe Telegram, iar apoi pentru a-l identifica și a-l reține în timp ce călătorea cu metroul. Curtea a observat caracterul foarte intruziv al acestor măsuri, subliniind că, prin urmare, era necesar un nivel ridicat de justificare pentru ca acestea să fie considerate „necesare, într-o societate democratică", cu cel mai înalt nivel de justificare necesar pentru utilizarea tehnologiei de recunoaștere facială în timp real (*ibidem*, pct. 86). În această privință, ea a arătat că reclamantul era urmărit penal pentru o infracțiune minoră, și anume pentru participarea, singur, la o demonstrație fără o declarație prealabilă, că nu fusese niciodată acuzat de săvârșirea unei infracțiuni în timpul demonstrației (blocarea traficului, pagube materiale sau acte de violență) și că nu s-a susținut nici că acțiunile sale ar fi prezentat un risc pentru ordinea publică sau pentru siguranța transporturilor. Având în vedere aceste împrejurări, Curtea a statuat că utilizarea tehnologiei de recunoaștere facială pentru identificarea reclamantului și, *a fortiori*, utilizarea unei astfel de tehnologii în timp real pentru identificarea și interpelarea sa nu răspundea niciunei „nevoi sociale imperioase" și, prin urmare, nu putea fi considerată „necesară, într-o societate democratică" (*ibidem*, pct. 88-90).

B. Internet și motoare de căutare

415. Site-urile Internet sunt instrumente de informare și comunicare deosebit de distincte de presa scrisă, în special în ceea ce privește capacitatea lor de a înmagazina și de a difuza informații [*Węgrzynowski și Smolczewski împotriva Poloniei*, 2013, pct. 58; *M.L. și W.W. împotriva Germaniei*, 2018, pct. 91; *Hurbain împotriva Belgiei* (MC), 2023, pct. 236]. Grație accesibilității lor, precum și capacității de a stoca și de a difuza cantități mari de date, site-urile Internet contribuie în mod semnificativ la îmbunătățirea accesului publicului la știri și, în general, la facilitarea comunicării de informații [*Times Newspapers Ltd împotriva Regatului Unit (nr. 1 și 2)*, 2009, pct. 27].

416. Comunicările on-line și conținutul acestora sunt mult mai susceptibile decât presa să aducă atingere exercitării și beneficiului drepturilor și libertăților fundamentale, în special dreptului la viață privată, nu în ultimul rând datorită rolului important pe care îl joacă motoarele de căutare [*Hurbain împotriva Belgiei* (MC), 2023, pct. 236; *M.L. și W.W. împotriva Germaniei*, 2018, pct. 91 și trimiterile citate].

417. Informațiile care conțin date cu caracter personal puse la dispoziția motoarelor de căutare de către mass-media pot fi identificate cu ușurință de către internauți. Dat fiind efectul amplificator în ceea ce privește gradul de difuzare a informațiilor și natura activității din care face parte publicarea

de informații, obligațiile motoarelor de căutare față de persoana vizată de informații pot fi diferite de cele ale editorului aflat la originea informațiilor [*Hurbain împotriva Belgiei* (MC), 2023, pct. 207; *M.L. și W.W. împotriva Germaniei*, 2018, pct. 97]. Ținând seama de distincția dintre activitățile și obligațiile operatorilor de motoare de căutare și cele ale redactorilor de presă, persoanele vizate care urmăresc să obțină protecția datelor lor cu caracter personal în acest context nu sunt obligate să se adreseze, înainte sau în același timp, site-ului internet de origine pentru a-și exercita drepturile față de motoarele de căutare, întrucât este vorba despre două forme diferite de prelucrare, fiecare dintre acestea având propria legitimitate și implicații specifice pentru drepturile și interesele persoanelor. Examinarea unei acțiuni împotriva redactorului unui site internet de presă nu poate fi condiționată nici de o cerere de dezindexare prealabilă [*Hurban împotriva Belgiei* (MC), 2023, pct. 208]. A se vedea, de asemenea, punctele de mai sus din prezentul ghid pentru mai multe informații privind „Dreptul de a fi uitat”.

418. Potrivit Curții, punerea la dispoziție a arhivelor pe Internet contribuie la păstrarea și la accesibilitatea știrilor și a informațiilor [*Times Newspapers Ltd împotriva Regatului Unit (nr. 1 și 2)*, 2009, pct. 45]. Astfel de arhive reprezintă o sursă valoroasă de educație și cercetare istorică, în special prin faptul că sunt imediat accesibile publicului și, în general, gratuite [*Hurbain împotriva Belgiei* (MC), 2023, pct.180]. Statele dispun de o marjă de apreciere mai largă pentru a stabilii un just echilibru între interesele concurente atunci când informațiile sunt arhivate și se referă la evenimente din trecut decât atunci când se referă la evenimente actuale [*Times Newspapers Ltd împotriva Regatului Unit (nr 1 și 2)*, pct. 45]. Obligația presei de a respecta principiile unui jurnalism responsabil prin verificarea exactității informațiilor publicate este mai strictă în cazul informațiilor referitoare la trecut, a căror difuzare nu are niciun caracter de urgență, decât în ceea ce privește actualitatea, perisabilă prin natură (*ibidem*, pct. 45).

419. În cauza *Hurbain împotriva Belgiei* (MC), 2023 (pct. 180-185), Curtea a remarcat apariția în Europa a unui consens cu privire la importanța arhivelor, precizând că arhivele trebuie, ca regulă generală, să rămână autentice, fiabile și integrale pentru ca presa să își poată îndeplini misiunea. Curtea a dedus, astfel, că integritatea arhivelor de presă trebuie să fie principiul director al oricărei examinări a unei cereri de ștergere sau de modificare integrală sau parțială a unui articol arhivat, în special dacă este vorba despre un articol a cărui legalitate nu a fost niciodată pusă în discuție. Aceasta a adăugat că astfel de cereri necesită o vigilență deosebită și o examinare aprofundată de către autoritățile naționale.

C. Transferuri de date și fluxuri de date

420. Într-o cauză care privea fluxul masiv de date cu caracter personal, *Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei* (MC), 2017, datele de natură fiscală a 1,2 milioane de persoane fizice fuseseră publicate într-o revistă și ulterior diseminate prin intermediul unui serviciu SMS. Potrivit Curții, existența unui interes general pentru ca astfel de cantități atât de mari de date fiscale să fie accesibile și să poată fi colectate în scopuri jurnalistice nu semnifică în mod necesar sau automat că există, de asemenea, un interes general de a difuza în masă astfel de date brute, ca atare, fără niciun aport analitic. Trebuie să se facă o distincție între prelucrarea datelor în scopuri jurnalistice și difuzarea de date brute la care jurnaliștii au acces în condiții privilegiate (*ibidem*, pct. 175). În acest context, fapta de a împiedica difuzarea în masă de date cu caracter personal de natură fiscală, potrivit unor modalități contrare reglementărilor naționale și normelor Uniunii Europene în materie de protecția datelor cu caracter personal, nu constituie, în sine, o sancțiune, chiar dacă limitările impuse în ceea ce privește volumul de date publicate ar fi putut, în practică, să fi făcut ca activitățile comerciale ale societăților reclamante să fie mai puțin profitabile (*ibidem*, pct. 197).

421. Cauza *Big Brother Watch și alții împotriva Regatului Unit* (MC), 2021 ridica, printre altele, problema compatibilității cu art. 8 din Convenție a schimbului de informații interceptate de servicii de informații străine, în speță Agenția Națională de Securitate americană („NSA”). Curtea a indicat că

schimbul de informații trebuia să fie încadrat de norme clare și precise care să indice în mod suficient toate circumstanțele și condițiile în care autoritățile au dreptul să formuleze astfel de cereri și care să ofere garanții eficiente împotriva utilizării acestei puteri în scopul eludării dreptului intern și/sau a obligațiilor statelor în temeiul Convenției. În momentul primirii materialului interceptat, statul destinatar trebuie să dispună de garanții suficiente pentru examinarea, utilizarea, stocarea, transmiterea către terți, ștergerea și distrugerea acestora. Garanțiile în cauză se aplică, de asemenea, primirii de către un stat contractant a elementelor interceptate solicitate de la un serviciu de informații străin. În cazul în care statele nu au întotdeauna cunoștință dacă materialele primite de la servicii de informații străine sunt rezultatul interceptării, aceleași standarde trebuie să se aplice tuturor materialelor primite care ar putea fi rezultatul interceptării. În sfârșit, orice regim care permite serviciilor de informații să solicite unor state necontractante să intercepteze sau să le transmită materiale interceptate trebuie să facă obiectul unei supravegheri independente și, de asemenea, trebuie să se prevadă, posibilitatea unui control *a posteriori* independent (*ibidem*, pct. 498-499).

Lista cauzelor citate

Jurisprudența citată în prezentul ghid face trimitere la hotărâri și decizii pronunțate de Curte, precum și, după caz, la decizii și rapoarte ale Comisiei Europene a Drepturilor Omului („Comisia”).

Dacă nu se specifică altfel, trimiterea este la o hotărâre pe fond, pronunțată de o Cameră a Curții. Abrevierea „(dec.)” arată că este vorba despre o decizie a Curții, iar „(MC)” că respectiva cauză a fost examinată de Marea Cameră.

Hotărârile pronunțate de o Cameră care nu sunt „definitive” în sensul art. 44 din Convenție, la data acestei actualizări, sunt marcate în lista de mai jos cu un asterisc (*). Art. 44 § 2 din Convenție prevede următoarele: „Hotărârea unei Camere devine definitivă: a) atunci când părțile declară că ele nu vor cere retrimiterea cauzei în fața Marii Camere; sau b) la 3 luni de la data hotărârii, dacă retrimiterea cauzei în fața Marii Camere nu a fost cerută; sau c) atunci când Colegiul Marii Camere respinge cererea de retrimitere formulată potrivit art. 43.” În cazul în care cererea de retrimitere este admisă de Colegiul Marii Camere, hotărârea pronunțată ulterior de Marea Cameră este cea care devine definitivă, și nu cea a Camerei.

Hiperlinkurile cauzelor citate în versiunea electronică a ghidului direcționează spre baza de date HUDOC (*http://hudoc.echr.coe.int*) care oferă acces la jurisprudența Curții (hotărâri și decizii pronunțate de Marea Cameră, de Cameră și de Comitet, cauze comunicate, avize consultative și rezumate juridice extrase din Nota de informare privind jurisprudența) și la jurisprudența Comisiei (decizii și rapoarte), precum și la rezoluțiile Comitetului de Miniștri.

Curtea pronunță hotărârile și deciziile în limba engleză și/sau franceză, cele două limbi oficiale. Baza de date HUDOC oferă, de asemenea, acces la traduceri ale unora dintre cele mai importante cauze ale Curții, în peste treizeci de limbi neoficiale. În plus, include linkuri către aproximativ o sută de culegeri de jurisprudență online, elaborate de terți.

—A—

A.B. împotriva Țărilor de Jos, nr. 37328/97, 29 ianuarie 2002
A.P., Garçon și Nicot împotriva Franței, nr. 79885/12 și alte 2 cereri, CEDO 2017
A.P împotriva Armeniei, nr. 58737/14, 18 iunie 2024
Adomaitis împotriva Lituaniei, nr. 14833/18, 18 ianuarie 2022
Akgün împotriva Turciei, nr. 19699/18, 20 iulie 2021
Allan împotriva Regatului Unit, nr. 48539/99, CEDO 2002-IX
Alexandridis împotriva Greciei, nr. 19516/06, 21 februarie 2008
Alkaya împotriva Turciei, nr. 42811/06, 9 octombrie 2012
Alpha Doryforiki Tileorasi Anonymi Etairia împotriva Greciei, nr. 72562/10, 22 februarie 2018
Amann împotriva Elveției (MC), nr. 27798/95, CEDO 2000-II
Anchev împotriva Bulgariei (dec.), nr. 38334/08 și 68242/16, 5 decembrie 2017
André și alții împotriva Franței, nr. 18603/03, 24 iulie 2008
Antoneta Tudor împotriva României, nr. 23445/04, 24 septembrie 2013
Antović și Mirković împotriva Muntenegrului, nr. 70838/13, 28 noiembrie 2017
Apostu împotriva României, nr. 22765/12, 3 februarie 2015
Armonienė împotriva Lituaniei, nr. 36919/02, 25 noiembrie 2008
Asociația „21 decembrie 1989” și alții împotriva României, nr. 33810/07 și 18817/08, 24 mai 2011
Asociația pentru integrarea europeană și drepturile omului și Ekimdjiev împotriva Bulgariei, nr. 62540/00, 28 iunie 2007
Avilkina și alții împotriva Rusiei, nr. 1585/09, 6 iunie 2013
Axel Springer AG împotriva Germaniei (MC), nr. 39954/08, 7 februarie 2012

Axel Springer SE și RTL Television GmbH împotriva Germaniei, nr. 51405/12, 21 septembrie 2017
Aycaguer împotriva Franței, nr. 8806/12, 22 iunie 2017

—B—

B.B. împotriva Franței, nr. 5335/06, 17 decembrie 2009
Batiashvili împotriva Georgiei, nr. 8284/07, 10 octombrie 2019
Bărbulescu împotriva României (MC), nr. 61496/08, 5 septembrie 2017 (extrase)
Bédat împotriva Elveției (MC), nr. 56925/08, CEDO 2016
Beghal împotriva Regatului Unit, nr. 4755/16, 28 februarie 2019
Benedik împotriva Sloveniei, nr. 62357/14, 24 aprilie 2018
Ben Faiza împotriva Franței, nr. 31446/12, 8 februarie 2018
Bernh Larsen Holding AS și alții împotriva Norvegiei, nr. 24117/08, 14 martie 2013
Biancardi împotriva Italiei, nr. 77419/16, 25 noiembrie 2021
Big Brother Watch și alții împotriva Regatului Unit (MC), nr. 58170/13 și alte 2 cereri, 25 mai 2021
Biriuk împotriva Lituaniei, nr. 23373/03, 25 noiembrie 2008
Bogomolova împotriva Rusiei, nr. 13812/09, 20 iunie 2017
Boljević împotriva Serbiei, nr. 47443/14, 16 iunie 2020
Borislav Tonchev împotriva Bulgariei, nr. 40519/15, 16 aprilie 2024
Brunet împotriva Franței, nr. 21010/10, 18 septembrie 2014
Breyer împotriva Germaniei, nr. 50001/12, 30 ianuarie 2020
Buck împotriva Germaniei, nr. 41604/98, CEDO 2005-IV
Buturugă împotriva României, nr. 56867/15, 11 februarie 2020
Bykov împotriva Rusiei (MC), nr. 4378/02, 10 martie 2009

—C—

C.C. împotriva Spaniei, nr. 1425/06, 6 octombrie 2009
Cakicisoy și alții împotriva Ciprului (dec.), nr. 6523/12, 23 septembrie 2014
Canonne împotriva Franței (dec.), nr. 22037/13, 2 iunie 2015
Caruana împotriva Maltei (dec.), nr. 41079/16, 15 mai 2018
Casarini împotriva Italiei (dec.), nr. 25578/11, 5 noiembrie 2024
Catt împotriva Regatului Unit, nr. 43514/15, 24 ianuarie 2019
Cherrier împotriva Franței, nr. 18843/20, 30 ianuarie 2024
Centrul pentru democrație și statul de drept împotriva Ucrainei, nr. 10090/16, 26 martie 2020
Centrum för rättvisa împotriva Suediei (MC), nr. 35252/08, 25 mai 2021
Cemalettin Canlı împotriva Turciei, nr. 22427/04, 18 noiembrie 2008
Cevat Özel împotriva Turciei, nr. 19602/06, 7 iunie 2016
Christine Goodwin împotriva Regatului Unit (MC), nr. 28957/95, CEDO 2002-VI
Ciubotaru împotriva Moldovei, nr. 27138/04, 27 aprilie 2010
Coban împotriva Spaniei (dec.), nr. 17060/02, 25 septembrie 2006
Comitetul de redacție al Pravoye Delo și Shtekel împotriva Ucrainei, nr. 33014/05, CEDO 2011 (extrase)
Copland împotriva Regatului Unit, nr. 62617/00, CEDO 2007-I
Cossey împotriva Regatului Unit, 27 septembrie 1990, seria A nr. 184
Craxi împotriva Italiei (nr. 2), nr. 25337/94, 17 iulie 2003

—D—

D.H. și alții împotriva Macedoniei de Nord, nr. 44033/17, 18 iulie 2023
D.L. împotriva Bulgariei, nr. 7472/14, 19 mai 2006
Dalea împotriva Franței (dec.), nr. 964/072, februarie 2010
DELTA PEKÁRNY a.s. împotriva Republicii Cehe, nr. 97/11, 2 octombrie 2014
Demirtepe împotriva Franței, nr. 34821/97, CEDO 1999-IX (extrase)
Denisiuk și alții împotriva Ucrainei, nr. 22790/19 și alte 3 cereri, 13 februarie 2025
Deveci împotriva Turciei (dec.), nr. 42785/11, 28 iunie 2022
Dimitras și alții împotriva Greciei, nr. 42837/06 și alte 4 cereri, 3 iunie 2010
Dimitrov-Kazakov împotriva Bulgariei, nr. 11379/03, 10 februarie 2011
Doerga împotriva Țărilor de Jos, nr. 50210/99, 27 aprilie 2004
Dragan Petrović împotriva Serbiei, nr. 75229/10, 14 aprilie 2020
Dragojević împotriva Croației, nr. 68955/11, 15 ianuarie 2015
Drakšas împotriva Lituaniei, nr. 36662/04, 31 iulie 2012
Drelon împotriva Franței, nr. 3153/16 și 27758/18, 8 septembrie 2022
Dudgeon împotriva Regatului Unit, 22 octombrie 1981, seria A nr. 45
Dumitru Popescu împotriva României (nr. 2), nr. 71525/01, 26 aprilie 2007
Dupuis și alții împotriva Franței, nr. 1914/02, 7 iunie 2007

—E—

Éditions Plon împotriva Franței, nr. 58148/00, CEDO 2004-IV
Egeland și Hanseid împotriva Norvegiei, nr. 34438/04, 16 aprilie 2009
Ekimdzhiev și alții împotriva Bulgariei, nr. 70078/12, 11 ianuarie 2022
Elberte împotriva Letoniei, nr. 61243/08, CEDO 2015
Erdem împotriva Germaniei, nr. 38321/97, CEDO 2001-VII (extrase)
Ernst și alții împotriva Belgiei, nr. 33400/96, 15 iulie 2003
Eternit împotriva Franței (dec.), nr. 20041/10, 27 martie 2012

—F—

Fédération nationale des associations et syndicats de sportifs (FNASS) și alții împotriva Franței, nr. 48151/11 și 77769/13, 18 ianuarie 2018
Financial Times Ltd și alții împotriva Regatului Unit, nr. 821/03, 15 decembrie 2009
Florindo de Almeida Vasconcelos Gramaxo împotriva Portugaliei, nr. 26968/16, 13 decembrie 2022
Foxley împotriva Regatului Unit, nr. 33274/96, 20 iunie 2000
Frâncu împotriva României, nr. 69356/13, 13 octombrie 2020
Friedl împotriva Austriei, nr. 15225/89, raport al Comisiei, 19 mai 1994

—G—

G.S.B. împotriva Elveției, nr. 28601/11, 22 decembrie 2015
Gafiuc împotriva României, nr. 59174/13, 13 octombrie 2020
Gardel împotriva Franței, nr. 16428/05, CEDO 2009
Garnaga împotriva Ucrainei, nr. 20390/07, 16 mai 2013
Gaskin împotriva Regatului Unit, 7 iulie 1989, seria A nr. 160
Gaughran împotriva Regatului Unit, nr. 45245/15, 13 februarie 2020
Gauvin-Fournis și Silliau împotriva Franței, nr. 21424/16 și 45728/17, 7 septembrie 2023

Gawlik împotriva Liechtensteinului, nr. 23922/19, 16 februarie 2021
Giesbert și alții împotriva Franței, nr. 68974/11 și alte 2 cereri, 1 iunie 2017
Gillan și Quinton împotriva Regatului Unit, nr. 4158/05, CEDO 2010 (extrase)
Gîrleanu împotriva României, nr. 50376/09, 26 iunie 2018
Glukhin împotriva Rusiei, nr. 11519/20, 4 iulie 2023
Godelli împotriva Italiei, nr. 33783/09, 25 septembrie 2012
Gorlov și alții împotriva Rusiei, nr. 27057/06 și alte 2 cereri, 2 iulie 2019
Görmüş și alții împotriva Turciei, nr. 49085/07, 19 ianuarie 2016
Grande Oriente d'Italia împotriva Italiei, nr. 29550/17, 19 decembrie 2024
Grant împotriva Regatului Unit, nr. 32570/03, CEDO 2006-VII
Greuter împotriva Țărilor de Jos (dec.), nr. 40045/98, 19 martie 2002
Guerra și alții împotriva Italiei, nr. 14967/89, *Culegere de hotărâri și decizii* 1998-I
Guillot împotriva Franței, 24 octombrie 1996, *Culegere de hotărâri și decizii* 1996-VI
Guiorgui Nikolaïchvili împotriva Georgiei, nr. 37048/04, 13 ianuarie 2009
Güzel Erdagöz împotriva Turciei, nr. 37483/02, 21 octombrie 2008

—H—

Haldimann și alții împotriva Elveției, nr. 21830/09, CEDO 2015
Halford împotriva Regatului Unit, 25 iunie 1997, *Culegere de hotărâri și decizii* 1997-III
Hämäläinen împotriva Finlandei (MC), nr. 37359/09, CEDO 2014
Haralambie împotriva României, nr. 21737/03, 27 octombrie 2009
Hájovský împotriva Slovaciei, nr. 7796/16, 1 iulie 2021
Haščák împotriva Slovaciei, nr. 58359/12 și alte 2 cereri, 23 iunie 2022
Hassine împotriva României, nr. 36328/13, 9 martie 2021
Heglas împotriva Republicii Cehe, nr. 5935/02, 1 martie 2007
Henry Kismoun împotriva Franței, nr. 32265/10, 5 decembrie 2013
Hurbain împotriva Belgiei, (MC), nr. 57292/16, 4 iulie 2023
Huvig împotriva Franței, 24 aprilie 1990, seria A nr. 176-B

—I—

I. împotriva Finlandei, nr. 20511/03, 17 iulie 2008
I. împotriva Regatului Unit (MC), nr. 25680/94, 11 iulie 2006
Iordachi și alții împotriva Republicii Moldova, nr. 25198/02, 10 februarie 2009
İrfan Güzel împotriva Turciei, nr. 35285/08, 7 februarie 2017
Ivashchenko împotriva Rusiei, nr. 61064/10, 13 februarie 2018

—J—

J.L. împotriva Italiei, nr. 5671/16, 27 mai 2021
J.P.D. împotriva Franței (dec.), nr. 55432/10, 16 septembrie 2016
J.S. împotriva Regatului Unit (dec.), 445/10, 3 martie 2015
Jäggi împotriva Elveției, nr. 58757/00, CEDO 2006-X
Jarnea împotriva României, nr. 41838/05, 19 iulie 2011
Jecker împotriva Elveției, nr. 35449/14, 6 octombrie 2020
Joanna Szulc împotriva Poloniei, nr. 43932/08, 13 noiembrie 2012

—K—

K.H. și alții împotriva Slovaciei, nr. 32881/04, CEDO 2009 (extrase)
K.S. și M.S. împotriva Germaniei, nr. 33696/11, 6 octombrie 2016
K.U. împotriva Finlandei, nr. 2872/02, CEDO 2008
Kaczmarek împotriva Poloniei, nr. 16974/14, 22 februarie 2024
Kahn împotriva Germaniei, nr. 16313/10, 17 martie 2016
Karabeyoğlu împotriva Turciei, nr. 30083/10, 7 iunie 2016
Kennedy împotriva Regatului Unit, nr. 26839/05, 18 mai 2010
Khadija Ismayilova împotriva Azerbaidjanului, nr. 65286/13 și 57270/14, 10 ianuarie 2019
Khan împotriva Regatului Unit, nr. 35394/97, CEDO 2000-VII
Khoujine și alții împotriva Rusiei, nr. 13470/02, 23 octombrie 2008
Khelili împotriva Elveției, nr. 16188/07, 18 octombrie 2011
Kinnunen împotriva Finlandei, nr. 18291/91, decizie a Comisiei, 13 octombrie 1993
Kinnunen împotriva Finlandei, nr. 24950/94, decizie a Comisiei, 15 mai 1996
Kırdök și alții împotriva Turciei, nr. 14704/12, 3 decembrie 2019
Kiyutin împotriva Rusiei, nr. 2700/10, CEDO 2011
Klass și alții împotriva Germaniei, 6 septembrie 1978, seria A nr. 28
Khmel împotriva Rusiei, nr. 20383/04, 12 decembrie 2013
Konovalova împotriva Rusiei, nr. 37873/04, 9 octombrie 2014
Köpke împotriva Germaniei (dec.), nr. 420/07, 5 octombrie 2010
Kotilainen și alții împotriva Finlandei, nr. 62439/12, 17 septembrie 2020
Krone Verlag GmbH & Co. KG împotriva Austriei, nr. 34315/96, 26 februarie 2002
Kruglov și alții împotriva Rusiei, nr. 11264/04 și alte 15 cereri, 4 februarie 2020
Kruslin împotriva Franței, 24 aprilie 1990, seria A nr. 176-B
Kurier Zeitungsverlag und Druckerei GmbH împotriva Austriei, nr. 3401/07, 17 ianuarie 2012
Kvasnica împotriva Slovaciei, nr. 72094/01, 9 iunie 2009

—L—

L.B. împotriva Ungariei (MC), nr. 36345/16, 9 martie 2023
L.F. împotriva Franței (dec.), nr. 3866/20 și 9292/20, 13 februarie 2024
L.H. împotriva Letoniei, nr. 52019/07, 29 aprilie 2014
L.L. împotriva Franței, nr. 7508/02, CEDO 2006-XI
Labita împotriva Italiei (MC), nr. 26772/95, CEDO 2000-IV
Lambert împotriva Franței, nr. 23618/94, *Culegere de hotărâri și decizii* 1998-V
Lavents împotriva Letoniei, nr. 58442/00, 28 noiembrie 2002
Le Marrec împotriva Franței (dec.), nr. 52319/22, 5 noiembrie 2024
Leander împotriva Suediei, 26 martie 1987, seria A nr. 116
Libert împotriva Franței, nr. 588/13, 22 februarie 2018
Liberty și alții împotriva Regatului Unit, nr. 58243/00, 1 iulie 2008
Liblik și alții împotriva Estoniei, nr. 173/15 și alte 5 cereri, 28 mai 2019
Liebscher împotriva Austriei, nr. 5434/17, 6 aprilie 2021
López Ribalda și alții împotriva Spaniei (MC), nr. 1874/13 și 8567/13, 17 octombrie 2019
Lüdi împotriva Elveției, nr. 12433/86, seria A nr. 238
Lupker și alții împotriva Țărilor de Jos, nr. 18395/91, decizie a Comisiei, 7 decembrie 1992

—M—

M.B. împotriva Franței, nr. 22115/06, 17 decembrie 2009
M.C. împotriva Regatului Unit, nr. 51220/13, 30 martie 2021
M.D. și alții împotriva Spaniei, nr. 36584/17, 28 iunie 2022
M.G. împotriva Regatului Unit, nr. 39393/98, 24 septembrie 2002
M.K. împotriva Franței, nr. 19522/09, 18 aprilie 2013
M.L. și W.W. împotriva Germaniei, nr. 60798/10 și 65599/10, 28 iunie 2018
M.M. împotriva Regatului Unit, nr. 24029/07, 13 noiembrie 2012
M.N. și alții împotriva San Marino, nr. 28005/12, 7 iulie 2015
M.P. împotriva Portugaliei, nr. 27516/14, 7 septembrie 2021
M.S. împotriva Suediei, 27 august 1997, pct. 35, *Culegere* 1997-IV
MGN Limited împotriva Regatului Unit, nr. 39401/04, 18 ianuarie 2011
Magyar Helsinki Bizottság împotriva Ungariei (MC), nr. 18030/11, CEDO 2016
Malanicheva împotriva Rusiei (dec.), nr. 50405/06, 31 mai 2016
Malone împotriva Regatului Unit, 2 august 1984, seria A nr. 82
Marchiani împotriva Franței (dec.), nr. 30392/03, 27 mai 2008
Margari împotriva Greciei, nr. 36705/16, 20 iunie 2023
Matheron împotriva Franței, nr. 57752/00, 29 martie 2005
McGinley și Egan împotriva Regatului Unit, 9 iunie 1998, *Culegere de hotărâri și decizii* 1998-III
McVeigh, O'Neill și Evans împotriva Regatului Unit, nr. 8022/77, 8025/77 și 8027/77, raport al Comisiei, 18 martie 1981
Mediengruppe Österreich GmbH împotriva Austriei, nr. 37718/18, 26 aprilie 2022
Mehmedovic împotriva Elveției (dec.), nr. 17331/11, 11 decembrie 2018
Mentzen împotriva Letoniei (dec.), nr. 71074/01, CEDO 2004-XII
Messina împotriva Italiei (nr. 2), nr. 25498/94, CEDO 2000-X
Michaud împotriva Franței, nr. 12323/11, CEDO 2012
Mik și Jovanović împotriva Serbiei (dec.), nr. 9291/14 și 63798/14, 23 martie 2021
Mikulić împotriva Croației, nr. 53176/99, CEDO 2002-I
Mifsud împotriva Maltei, nr. 62257/15, 29 ianuarie 2019
Mitov și alții împotriva Bulgariei (dec.), nr. 80857/17, 28 februarie 2023
Mityanin și Leonov împotriva Rusiei, nr. 11436/06 și 22912/06, 7 mai 2018
Mockutė împotriva Lituaniei, nr. 66490/09, 27 februarie 2018
Modestou împotriva Greciei, nr. 51693/13, 16 martie 2017
Moldovan împotriva Ucrainei, nr. 62020/14, 14 martie 2024
Montera împotriva Italiei (dec.), nr. 64713/01, 9 iulie 2002
Moskalev împotriva Rusiei, nr. 44045/05, 7 noiembrie 2017
Mosley împotriva Regatului Unit, nr. 48009/08, 10 mai 2011
Murray împotriva Regatului Unit (MC), 28 octombrie 1994, seria A nr. 300-A
Murtazaliyeva împotriva Rusiei (MC), nr. 36658/05, 18 decembrie 2018
Mustafa Sezgin Tanrıkulu împotriva Turciei, nr. 27473/06, 18 iulie 2017

—N—

N.F. și alții împotriva Rusiei, nr. 3537/15 și alte 8 cereri, 12 septembrie 2023
N. Š. împotriva Croației, nr. 36908/13, 10 septembrie 2020
Nada împotriva Elveției (MC), nr. 10593/08, CEDO 2012
Nagla împotriva Letoniei, nr. 73469/10, 16 iulie 2013
Negru împotriva Republicii Moldova, nr. 7336/11, 27 iunie 2023
News Verlags GmbH & Co.KG împotriva Austriei, nr. 31457/96, CEDO 2000-I
Niedbała împotriva Poloniei, nr. 27915/95, 4 iulie 2000

Nuh Uzun împotriva Turciei, nr. 49341/18 și alte 13 cereri, 29 martie 2022

—O—

Odièvre împotriva Franței (MC), nr. 42326/98, CEDO 2003-III
Oleynik împotriva Rusiei, nr. 23559/07, 21 iunie 2016

—P—

P.G. și J.H. împotriva Regatului Unit, nr. 44787/98, CEDO 2001-IX
P.N. împotriva Germaniei, nr. 74440/17, 11 iunie 2020
P.T. împotriva Republicii Moldova, nr. 1122/12, 26 mai 2020
P. și B. împotriva Regatului Unit, nr. 36337/97 și 35974/97, CEDO 2001-III
P. și S. împotriva Poloniei, nr. 57375/08, 30 octombrie 2012
Panteleyenko împotriva Ucrainei, nr. 11901/02, 29 iunie 2006
Peck împotriva Regatului Unit, nr. 44647/98, CEDO 2003-I
Peers împotriva Greciei, nr. 28524/95, CEDO 2001-III
Pendov împotriva Bulgariei, nr. 44229/11, 26 martie 2020
Peruzzo și Martens împotriva Germaniei (dec.), nr. 7841/08 și 57900/12, 4 iunie 2013
Perry împotriva Regatului Unit, nr. 63737/00, CEDO 2003-IX (extrase)
Petrova împotriva Letoniei, nr. 4605/05, 24 iunie 2014
Pietrzak și Bychawska-Siniarska și alții împotriva Poloniei, nr. 72038/17 și 25237/18, 28 mai 2024
Pinto Coelho împotriva Portugaliei (nr. 2), nr. 48718/11, 22 martie 2016
Podchasov împotriva Rusiei, nr. 33696/19, 13 februarie 2024
Polanco Torres și Movilla Polanco împotriva Spaniei, nr. 34147/06, 21 septembrie 2010
Prado Bugallo împotriva Spaniei, nr. 58496/00, 18 februarie 2003
Pruteanu împotriva României, nr. 30181/05, 3 februarie 2015

—R—

R.E. împotriva Regatului Unit, nr. 62498/11, 27 octombrie 2015
Radio Twist a.s. împotriva Slovaciei, nr. 62202/00, CEDO 2006-XV
Radu împotriva Republicii Moldova, nr. 50073/07, 15 aprilie 2014
Ramadan împotriva Franței (dec.), nr. 23443/23, 9 ianuarie 2024
Rees împotriva Regatului Unit, nr. 9532/81, seria A nr. 106
Reklos și Davourlis împotriva Greciei, nr. 1234/05, 15 ianuarie 2009
Reznik împotriva Ucrainei, nr. 31175/14, 23 ianuarie 2025
Ricci împotriva Italiei, nr. 30210/06, 8 octombrie 2013
Robathin împotriva Austriei, nr. 30457/06, 3 iulie 2012
Roche împotriva Regatului Unit (MC), nr. 32555/96, CEDO 2005-IX
Roemen și Schmit împotriva Luxemburgului, nr. 26419/10, CEDO 2003-IV
Roman Zakharov împotriva Rusiei (MC), nr. 47143/06, CEDO 2015
Rook împotriva Germaniei, nr. 1586/15, 25 iulie 2019
Rotaru împotriva României (MC), nr. 28341/95, CEDO 2000-IV

—S—

S. și Marper împotriva Regatului Unit (MC), nr. 30562/04 și 30566/04, CEDO 2008
S.V. împotriva Italiei, nr. 55216/08, 11 octombrie 2018
Sanoma Uitgevers B.V. împotriva Țărilor de Jos (MC), nr. 38224/03, 14 septembrie 2010
Samoylova împotriva Rusiei, nr. 49108/11, 14 decembrie 2021
Šantare și Labazņikovs împotriva Letoniei, nr. 34148/07, 31 martie 2016
Sârbu împotriva României, nr. 34467/15, 28 martie 2023
Särgava împotriva Estoniei, nr. 698/19, 16 noiembrie 2021
Satakunnan Markkinapörssi Oy și Satamedia Oy împotriva Finlandei (MC), nr. 931/13, CEDO 2017 (extrase)
Schmidt împotriva Germaniei (dec.), nr. 32352/02, 5 ianuarie 2006
Sciacca împotriva Italiei, nr. 50774/99, CEDO 2005-I
Sedletska împotriva Ucrainei, nr. 42634/18, 1 aprilie 2021
Segerstedt-Wiberg și alții împotriva Suediei, nr. 62332/00, CEDO 2006-VII
Sérvulo & Associados - Sociedade de Advogados, RL, și alții împotriva Portugaliei, nr. 27013/10, 3 septembrie 2015
Sheffield și Horsham împotriva Regatului Unit, 30 iulie 1998, *Culegere de hotărâri și decizii* 1998-V
Sher și alții împotriva Regatului Unit, nr. 5201/11, CEDO 2015 (extrase)
Shimovolos împotriva Rusiei, nr. 30194/09, 21 iunie 2011
Silver și alții împotriva Regatului Unit, 25 martie 1983, seria A nr. 61
Sinan Işık împotriva Turciei, nr. 21924/05, CEDO 2010
Smirnov împotriva Rusiei, nr. 71362/01, 7 iunie 2007
Smith și Grady împotriva Regatului Unit, nr. 33985/96 și 33986/96, *Culegere de hotărâri și decizii* 1999-VI
Société de Conception de Presse et d'Édition împotriva Franței, nr. 4683/11, 25 februarie 2016
Söderman împotriva Suediei (MC), nr. 5786/08, CEDO 2013
Sommer împotriva Germaniei, nr. 73607/13, 27 aprilie 2017
Sõro împotriva Estoniei, nr. 22588/08, 3 septembrie 2015
Standard Verlagsgesellschaft mbH împotriva Austriei (nr. 3), nr. 39378/15, 7 decembrie 2021
Stolkosa împotriva Poloniei (dec.), nr. 68562/14, 14 septembrie 2021
Succession Kresten Filtenborg Mortensen împotriva Danemarcei (dec.), nr. 1338/03, CEDO 2006-V
Suprunenko împotriva Rusiei (dec) [comitet], nr. 8630/11, 19 iunie 2018
Surikov împotriva Ucrainei, nr. 42788/06, 26 ianuarie 2017
Szabó și Vissy împotriva Ungariei, nr. 37138/14, 12 ianuarie 2016
Szuluk împotriva Regatului Unit, nr. 36936/05, CEDO 2009

—T—

Taylor-Sabori împotriva Regatului Unit, nr. 47114/99, 22 octombrie 2002
Telegraaf Media Nederland Landelijke Media B.V. și alții împotriva Țărilor de Jos, nr. 39315/06, 22 noiembrie 2012
Tena Arregui împotriva Spaniei, nr. 42541/18, 11 ianuarie 2024
Martorii lui Iehova împotriva Finlandei, nr. 31172/19, 9 mai 2023
Tillack împotriva Belgiei, 20477/05, 27 noiembrie 2007
Times Newspapers Ltd împotriva Regatului Unit (nr. 1 și 2), nr. 3002/03 și 23676/03, CEDO 2009
Toma împotriva României, nr. 42716/02, 24 februarie 2009
Tønsbergs Blad A.S. și Haukom împotriva Norvegiei, nr. 510/04, 1 martie 2007
Thoma împotriva Luxemburgului, nr. 38432/97, CEDO 2001-III
Trabajo Rueda împotriva Spaniei, nr. 32600/12, 30 mai 2017
Trajkovski și Chipovski împotriva Macedoniei de Nord, nr. 53205/13 și 63320/13, 13 februarie 2020

—U—

Ungváry și Irodalom Kft. împotriva Ungariei, nr. 64520/10, 3 decembrie 2013
Uzun împotriva Germaniei, nr. 35623/05, CEDO 2010 (extrase)

—V—

Valašinas împotriva Lituaniei, nr. 44558/98, CEDO 2001-VIII
Valenzuela Contreras împotriva Spaniei, nr. 2767/95, *Culegere de hotărâri și decizii* 1998-V
Van der Velden împotriva Țărilor de Jos (dec.), nr. 29514/05, CEDO 2006-XV
Van Vondel împotriva Țărilor de Jos, nr. 38258/03, 25 octombrie 2007
Vasil Vasilev împotriva Bulgariei, nr. 7610/15, 16 noiembrie 2021
Vasylchuk împotriva Ucrainei, nr. 24402/07, 13 iunie 2013
Verlagsgruppe Droemer Knaur GmbH & Co. KG împotriva Germaniei, nr. 35030/13, 19 octombrie 2017
Vetter împotriva Franței, nr. 59842/00, 31 mai 2005
Vicent Del Campo împotriva Spaniei, nr. 25527/13, 6 noiembrie 2018
Vinci Construction și GTM Génie Civil et Services împotriva Franței, nr. 63629/10 și 60567/10, 2 aprilie 2015
Visy împotriva Slovaciei, nr. 70288/13, 16 octombrie 2018
Volodina împotriva Rusiei (nr. 2), nr. 40419/19, 14 septembrie 2021
Von Hannover împotriva Germaniei, nr. 59320/00, CEDO 2004-VI
Von Hannover împotriva Germaniei (nr. 2) (MC), nr. 40660/08 și 60641/08, CEDO 2012
Vučina împotriva Croației (dec.), nr. 58955/13, 24 septembrie 2019
Vukota-Bojić împotriva Elveției, nr. 61838/10, 18 octombrie 2016

—W—

W. împotriva Țărilor de Jos (dec.), nr. 20689/08, 20 ianuarie 2009
Weber și Saravia împotriva Germaniei (dec.), nr. 54934/00, CEDO 2006-XI
Węgrzynowski și Smolczewski împotriva Poloniei, nr. 33846/07, 16 iulie 2013
Wieser și Bicos Beteiligungen GmbH împotriva Austriei, nr. 74336/01, CEDO 2007-IV
Willems împotriva Țărilor de Jos (dec.), nr. 57294/16, 9 noiembrie 2021
Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH împotriva Austriei (nr. 2) (dec.), nr. 62746/00, CEDO 2002-X
Wisse împotriva Franței, nr. 71611/01, 20 decembrie 2005

—X—

X și alții împotriva Rusiei, nr. 78042/16 și 66158/14, 14 ianuarie 2020

—Y—

Y. împotriva Turciei (dec.), nr. 648/10, 17 februarie 2015
Y.B. și alții împotriva Turciei, nr. 48173/99 și 48319/99, 28 octombrie2004
Y.G. împotriva Rusiei, nr. 8647/12, 30 august 2022
Y.Y. împotriva Rusiei, nr. 40378/06, 23 februarie 2016
Yonchev împotriva Bulgariei, nr. 12504/09, 7 decembrie 2017

Youth Initiative for Human Rights împotriva Serbiei, nr. 48135/06, 25 iunie 2013
Yvonne Chave, născută Jullien, împotriva Franței, nr. 14461/88, decizie a Comisiei, 9 iulie 1991

—Z—

Z împotriva Finlandei, 25 februarie 1997, *Culegere de hotărâri și decizii* 1997-I
Zoltán Varga împotriva Slovaciei, nr. 58361/12 și alte 2 cereri, 20 iulie 2021