

**MANUAL**



# **Ghid privind prevenirea utilizării ilegale a profilurilor în prezent și în viitor**

Conținutul acestui manual a fost finalizat în luna 2018.

Fotografiile (copertă și interior): © stock.adobe.com-Savvapanf Photo

Mai multe informații despre Uniunea Europeană sunt disponibile pe internet (<http://europa.eu>).

Luxemburg: Oficiul pentru Publicații al Uniunii Europene, 2022

Print	ISBN 978-92-9461-444-5	doi:10.2811/505260	TK-06-18-031-RO-C
PDF	ISBN 978-92-9461-429-2	doi:10.2811/11707	TK-06-18-031-RO-N

© Agenția pentru Drepturi Fundamentale a Uniunii Europene, 2022

Pentru utilizarea sau reproducerea fotografiilor sau a altor materiale care nu intră sub incidența drepturilor de autor ale FRA trebuie solicitată permisiunea direct de la deținătorul drepturilor de autor.

*Printed by the Publications Office in Luxembourg*

# Ghid privind prevenirea utilizării ilegale a profilurilor în prezent și în viitor



# Cuprins

FIGURI ȘI TABELE .....	5
ACRONIME ȘI ABREVIERI.....	6
INTRODUCERE .....	7
<b>1 PREZENTAREA CONTEXTULUI: CE ESTE CREAREA DE PROFILURI? .....</b>	<b>17</b>
1.1. Definiția creării de profiluri .....	17
1.1.1. Profilurile în contextul aplicării legii și al gestionării frontierelor .....	19
1.1.2. Definiția creării de profiluri pe bază de algoritmi .....	21
1.2. Când este ilegală utilizarea profilurilor? .....	26
1.2.1. Interzicerea discriminării .....	27
1.2.2. Dreptul la respectarea vieții private și la protecția datelor cu caracter personal.....	35
1.3. Care sunt potențialele efecte negative ale utilizării ilegale a profilurilor pentru activitățile de aplicare a legii și de gestionare a frontierelor? .....	43
1.3.1. Impactul asupra încrederii în poliție și în autoritățile de gestionare a frontierelor și asupra bunelor relații cu comunitatea.....	44
1.3.2. Eficacitatea utilizării profilurilor .....	55
<b>2 UTILIZAREA LEGALĂ A PROFILURILOR: PRINCIPII ȘI PRACTICĂ .....</b>	<b>57</b>
2.1. Respectarea demnității persoanelor .....	59
2.2. Motive rezonabile și obiective .....	63
2.2.1. Evitarea prejudecăților.....	64
2.2.2. Orientări clare pentru polițiști.....	65
2.2.3. Formare specifică.....	66
2.2.4. Motive rezonabile de suspiciune: utilizarea datelor operative și a informațiilor .....	72
2.2.5. Procesele-verbale de oprire și percheziționare folosite în activitățile de aplicare a legii care presupun profiluri .....	81
2.3. Răspunderea .....	85
2.3.1. Monitorizare internă.....	87
2.3.2. Camere de corp.....	92
2.3.3. Mecanisme de tratare a plângerilor.....	98
<b>3 CREAREA PROFILURILOR PE BAZĂ DE ALGORITMI.....</b>	<b>105</b>
3.1. Cadrul de protecție a datelor care reglementează crearea de profiluri pe bază de algoritmi.....	109
3.1.1. Datele trebuie prelucrate cu un scop specific.....	110
3.1.2. Persoanele fizice trebuie informate.....	113
3.1.3. Păstrarea datelor în siguranță: normele cu privire la evidențe, jurnale și stocare.....	115
3.1.4. Obligația de depistare și prevenire a prelucrării ilegale .....	116

3.2.	Utilizarea bazelor mari de date în scopuri de gestionare a frontierelor și de securitate .....	121
3.2.1.	Minimizarea riscurilor legate de drepturile fundamentale la prelucrarea datelor din baze mari de date .....	125
	CONCLUZIE .....	130
	ANEXĂ.....	131
	BIBLIOGRAFIE.....	134

## Figuri și tabele

Figura 1:	Procesul creării de profiluri pe bază de algoritmi în contextul aplicării legii și al gestionării frontierelor.....	24
Figura 2:	Încălcarea vieții private și a protecției datelor – procesul de evaluare.....	41
Figura 3:	Cele mai recente opriri ale poliției percepute ca motivate de profiluri etnice printre persoanele oprite în cei cinci ani anteriori sondajului UE-MIDIS II, pe state membre ale UE și pe grupuri vizate.....	49
Figura 4:	Ciclul profeției autoîmplinite.....	54
Figura 5:	Trei elemente ale unei interacțiuni respectuoase.....	61
Figura 6:	Procesul și obiectivele urmărite la elaborarea formării specifice.....	67
Figura 7:	Indicatori considerați utili sau foarte utili pentru recunoașterea eficientă a persoanelor care încearcă să intre în țară în mod neregular înainte ca agentul să li se adreseze.....	74
Figura 8:	Combinarea elementelor.....	79
Figura 9:	Elementele unui profil nediscriminatoriu.....	80
Figura 10:	Elementele monitorizării interne.....	89
Figura 11:	Instrument online care prezintă detalii despre acțiunile de oprire și percheziționare efectuate în Londra.....	93
Figura 12:	Prezentare generală a mecanismelor de tratare a plângerilor din statele membre ale UE.....	100
Tabelul 1:	Caracteristicile activităților polițienești bazate pe informații specifice și pe analiza predictivă.....	20
Tabelul 2:	Cerințe privind protecția datelor – diferențe între Directiva privind poliția și RGPD.....	37
Tabelul 3:	Tipuri și caracteristici ale orientărilor și implicarea părților interesate.....	65
Tabelul 4:	Identificarea cadrului juridic corect în funcție de scopul prelucrării.....	111
Tabelul 5:	Obligația de a furniza persoanelor informații referitoare la crearea de profiluri: tipul datelor, mijloacele de comunicare și excepțiile.....	113
Tabelul 6:	Selecție de instrumente ale UE care implică prelucrarea unor volume mari de date pentru gestionarea frontierelor și aplicarea legii.....	122
Tabelul 7:	Sisteme informatice la scară largă ale UE existente și planificate.....	131

## Acronime și abrevieri

<b>AEPD</b>	Autoritatea Europeană pentru Protecția Datelor
<b>CEaDO</b>	Convenția europeană a drepturilor omului
<b>CEDO</b>	Curtea Europeană a Drepturilor Omului
<b>CJUE</b>	Curtea de Justiție a Uniunii Europene
<b>EES</b>	Sistemul de intrare/ieșire
<b>EIPD</b>	Evaluare a impactului asupra protecției datelor
<b>ENISA</b>	Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor
<b>ETIAS</b>	Sistemul european de informații și de autorizare privind călătoriile
<b>EU-MIDIS</b>	Sondajul Uniunii Europene privind minoritățile și discriminarea
<b>FRA</b>	Agenția pentru Drepturi Fundamentale a Uniunii Europene
<b>Frontex</b>	Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă
<b>GL29/Grupul de lucru „Articolul 29”</b>	Grupul de lucru instituit prin articolul 29 privind protecția datelor
<b>IT</b>	Tehnologia informației
<b>OHCHR</b>	Oficiul Înaltului Comisar al Națiunilor Unite pentru Drepturile Omului
<b>ONU</b>	Organizația Națiunilor Unite
<b>OSCE</b>	Organizația pentru Securitate și Cooperare în Europa
<b>PCB</b>	Programa comună de bază
<b>RGPD</b>	Regulamentul general privind protecția datelor
<b>RTT</b>	Resortisant al unei țări terțe
<b>SIS II</b>	Sistemul de informații Schengen
<b>UE</b>	Uniunea Europeană
<b>UNHRC</b>	Comitetul pentru Drepturile Omului al ONU
<b>VIS</b>	Sistemul de informații privind vizele



# Introducere

Evoluțiile tehnologice au determinat intensificarea utilizării profilurilor într-o gamă largă de contexte, printre care marketing, ocuparea forței de muncă, sănătate, finanțe, aplicarea legii, controlul frontierelor și securitate. În ultimii ani, statele membre ale UE au acordat mai multă atenție utilizării instrumentelor prin care se creează profiluri pentru a sprijini activitatea agenților de aplicare a legii și de gestionare a frontierelor. Profilurile sunt utilizate în mod obișnuit și legitim de agenții de poliție și de polițiștii de frontieră pentru a preveni, a ancheta și a urmări penal infracțiunile, precum și pentru a preveni și a depista imigrația ilegală. Pe de altă parte, utilizarea ilegală a profilurilor poate submina încrederea în autorități, în special în poliție, și poate stigmatiza anumite comunități. La rândul său, acest lucru poate intensifica tensiunile dintre comunități și autoritățile de aplicare a legii atunci când crearea de profiluri este percepută ca fiind utilizată discriminator.

Prezentul ghid explică ce este crearea de profiluri, cadrele juridice care o reglementează și motivele pentru care utilizarea profilurilor în mod legal nu este doar necesară pentru respectarea drepturilor fundamentale, ci și esențială pentru eficiența activității polițienești și de gestionare a frontierelor. De asemenea, ghidul oferă îndrumări practice care să ajute la evitarea situațiilor în care utilizarea profilurilor în cadrul operațiunilor poliției și ale autorităților de gestionare a frontierelor este ilegală. Principiile și practicile prezentate în ghid sunt susținute de exemple, studii de caz și jurisprudență din întreaga UE și nu numai.

## De ce avem nevoie de acest ghid?

Crearea profilurilor generează o serie de îngrijorări legate de drepturile fundamentale<sup>1</sup>. Există riscul ca practicile folosite în acest scop să încalce principiile juridice consacrate precum cel al egalității și al nediscriminării, precum și drepturile la respectarea vieții private și la protecția datelor. În plus, au apărut întrebări referitoare la eficacitatea creării de profiluri în combaterea activităților ilegale, precum și la potențialele consecințe negative asupra relațiilor dintre autorități (inclusiv cele polițienești și de gestionare a frontierelor) și comunitățile pe care acestea le deservesc.

Ca răspuns la aceste îngrijorări, în 2010 Agenția Uniunii Europene pentru Drepturi Fundamentale (FRA) a publicat ghidul *În sprijinul unor practici polițienești mai eficiente. Ghid pentru înțelegerea și prevenirea creării profilurilor etnice discriminatorii*. Axat pe utilizarea creării de profiluri de către poliție, ghidul s-a concentrat în special asupra efectuării operațiunilor de oprire și percheziționare. Scopul ghidului a fost să ofere polițiștilor de nivel mediu instrumente pentru evitarea creării de profiluri discriminatorii pe baza etniei.

De atunci, evoluțiile tehnologice au schimbat considerabil natura activității de creare a profilurilor. O mare parte a acestora se bazează acum pe rezultatele analizei computerizate a unor seturi mari de date. Din punct de vedere juridic, normele de protecție a datelor reformate – mai stricte – aplicabile în întreaga UE începând din mai 2018 stabilesc noi standarde pentru colectarea, analiza și utilizarea datelor cu caracter personal.

Prezentul ghid actualizat ia în considerare aceste schimbări semnificative, valorificând și extinzând ghidul din 2010 astfel încât să reflecte noile realități de ordin juridic și practic. Totodată, adoptă o abordare mai cuprinzătoare a situațiilor în care utilizarea profilurilor este ilegală, incorporând:

- profilurile în contextul gestionării frontierelor;
- profilurile care sunt discriminatorii din orice motiv, inclusiv pe criterii de cetățenie, vârstă și sex, pe lângă originea etnică; și
- crearea de profiluri pe bază de algoritmi sau prin mijloace computerizate.

<sup>1</sup> Vezi FRA (2018e), p. 85-87; FRA (2017c), p. 88-89; și FRA (2016), p. 83-85.

De asemenea, această versiune din 2018 conține noi exemple și studii de caz, care reflectă evoluțiile și inovațiile din domeniul creării de profiluri.

## Cui i se adresează acest ghid?

Prezentul ghid este conceput în principal pentru cei responsabili de pregătirea agenților de aplicare a legii și de gestionare a frontierelor. De asemenea, poate ajuta direct agenții cu funcții de nivel mediu să aplice în mod legal tehnicile de creare a profilurilor. Scopul său este să asigure o mai bună înțelegere a teoriei și a practicii profilurilor și să ilustreze în termeni concreți modul în care acestea pot fi create cu respectarea drepturilor fundamentale.

Ghidul se referă la utilizarea profilurilor de polițiștii din prima linie – de exemplu, în cursul acțiunilor de oprire și percheziționare – și în cadrul verificărilor efectuate de polițiștii de frontieră la punctele de trecere a frontierei, și anume atunci când se ia decizia de a trimite o persoană către o verificare mai amănunțită „în linia a doua”. În activitatea de gestionare a frontierelor, ghidul este un material auxiliar destinat formatorilor care predau programa comună de bază pentru formarea profesională a polițiștilor de frontieră în conformitate cu articolul 36 alineatul (5) din Regulamentul privind Poliția de frontieră și garda de coastă la nivel european [Regulamentul (UE) 2016/1624].

De asemenea, ghidul abordează crearea de profiluri pe baza analizei unor seturi foarte mari de date, inclusiv a celor reglementate de legislația UE. Crearea de profiluri în alte situații, de exemplu în sectorul privat în scopuri comerciale, depășește sfera actualului ghid. FRA efectuează cercetări suplimentare pe această temă<sup>2</sup>.

## Cum se utilizează acest ghid

Prezentul ghid oferă o imagine de ansamblu asupra principalelor principii și practici ale creării de profiluri în contextul aplicării legii și al gestionării frontierelor. El poate fi citit în întregime sau utilizat ca referință în sprijinul activităților de formare.

Ghidul cuprinde trei capitole. Capitolul 1 explică noțiunea de creare de profiluri, clarifică situațiile în care aceasta devine ilegală și descrie impactul negativ pe care îl poate avea asupra persoanelor, asupra comunităților și asupra exercitării competențelor polițienești și de gestionare a frontierelor. Capitolul 2 detaliază principiile

2 Vezi proiectul FRA privind [inteligenta artificială](#), [volumele mari de date](#) și [drepturile fundamentale](#).

și practicile după care ar trebui să se ghideze agenții de aplicare a legii și polițiștii de frontieră în implementarea activităților legale de utilizare a profilurilor. În fine, capitolul 3 se concentrează asupra creării de profiluri pe bază de algoritmi. Având în vedere că practica în acest domeniu nu este foarte avansată, secțiunea respectivă conține mai puține exemple concrete. În schimb, prezintă principalele riscuri pentru drepturile fundamentale asociate creării computerizate de profiluri și stabilește principalele cerințe legale instituite de Regulamentul general privind protecția datelor (RGPD) și de Directiva privind poliția.

Diferitele aspecte ale ghidului sunt evidențiate printr-o serie de elemente vizuale. Aspectele esențiale sintetizează mesajele principale și sunt evidențiate în casete galbene. Casetele colorate în albastru deschis evidențiază aspectele de bază ale cadrului juridic, iar casetele verzi prezintă exemple practice. Alte casete evidențiază aspecte importante pe care trebuie să se pună accent, studii de caz și exemple din jurisprudență. În ciuda eforturilor de diversificare a studiilor de caz, un număr disproporționat de exemple provin din Regatul Unit. Motivul este acela că Regatul Unit combate utilizarea ilegală a creării de profiluri încă din anii 1980, în timp ce alte state membre au recunoscut practicile ilegale de acest tip abia mai recent. Astfel, Regatul Unit a dezvoltat politici și practici mai extinse și mai consacrate în domeniu, din care se pot extrage exemple.

## Cum a fost elaborat acest ghid?

FRA a organizat o reuniune cu experți din diverse domenii, invitându-i să dezbată proiectul inițial al ghidului și să contribuie la realizarea produsului final.

În acest sens, FRA dorește să transmită mulțumiri experților din cadrul Oficiului Înaltului Comisar al Națiunilor Unite pentru Drepturile Omului (OHCHR), al Agenției Europene pentru Poliția de Frontieră și Garda de Coastă (Frontex), al Biroului pentru Instituții Democratice și Drepturile Omului (ODIHR) din cadrul Organizației pentru Securitate și Cooperare în Europa (OSCE), celor din cadrul Amnesty International, al Rețelei Europene împotriva Rasismului (ENAR), al Centrului Internațional pentru Dezvoltarea Politicilor de Migrație (ICMPD), al FIZ Karlsruhe, al Leibniz Institut für Informationsinfrastruktur GmbH, al European Digital Rights, al Open Society Initiative for Europe și reprezentanților Ombudsmanului francez, ai forțelor de poliție din Țările de Jos, Danemarca și Austria, precum și ai polițiștilor de frontieră polonezi pentru feedbackul valoros oferit în cursul elaborării ghidului.

## Sinteza aspectelor principale

### 1. Caracteristicile protejate nu pot constitui niciodată unica bază a creării de profiluri

- Crearea de profiluri presupune **clasificarea persoanelor** în funcție de caracteristicile lor.
- Pentru colectarea și prelucrarea **datelor cu caracter personal**, autoritățile de aplicare a legii și de gestionare a frontierelor trebuie să se asigure că activitățile de colectare și prelucrare au un temei juridic, au un scop valabil și legitim și sunt necesare și proporționale.
- **Caracteristicile protejate**, cum sunt rasa, originea etnică, genul sau religia, se pot regăsi printre factorii pe care autoritățile de aplicare a legii și poliștii de frontieră îi iau în considerare în exercitarea competențelor lor, dar **nu pot să constituie singurul sau principalul motiv pentru a aplica unei persoane tratament diferențiat**. (Pentru informații suplimentare despre caracteristicile protejate, a se vedea secțiunea 1.2.1).
- Crearea de profiluri care se bazează exclusiv sau în principal pe una sau mai multe caracteristici protejate reprezintă o discriminare directă și, prin urmare, **încalcă drepturile și libertățile persoanei și este ilegală**.

### 2. Orice interacțiune cu persoanele fizice trebuie să fie respectuoasă, profesionistă și informativă

- O **interacțiune de bună calitate** nu înseamnă eliminarea completă a prejudecăților la utilizarea unui profil, dar are șanse mai mari să fie o interacțiune mai reușită și este de natură să reducă potențialul impact negativ al opririi persoanei de un agent de poliție sau de un polițist de frontieră. În gestionarea frontierelor, atitudinea profesionistă și respectuoasă este menționată în mod expres ca obligație legală.
- În general, o **atitudine profesionistă și respectuoasă** face ca persoana vizată să fie mai mulțumită de interacțiunea respectivă.
- **Explicarea motivelor opririi** contribuie la creșterea încrederii publicului în operațiunile agenților de poliție și de gestionare a frontierelor și reduce impresia că profilurile sunt realizate pe baza unor prejudecăți.
- Pe de altă parte, respectul și politețea **nu scuză niciodată realizarea unor verificări la frontieră sau a unor acțiuni de oprire și percheziționare care sunt ilegale**.

### 3. Profilurile trebuie să se bazeze pe motive obiective și rezonabile

- Pentru a fi legale, opririle și trimerile către verificări în linia a doua la frontieră trebuie să se bazeze pe motive rezonabile și obiective de suspiciune.
- Caracteristicile personale pot fi utilizate ca factori legitimi pentru crearea de profiluri, însă pentru ca acestea să nu fie discriminatorii, **trebuie să existe și motive rezonabile de suspiciune** bazate pe alte informații decât caracteristicile protejate.
- Acțiunile agenților de poliție și de gestionare a frontierelor care se bazează pe **informații specifice și actualizate** tind să fie mai **obiective**.
- Esențial este ca decizia de a opri o persoană și de a o trimite spre verificare în linia a doua la frontieră să nu se bazeze exclusiv pe **impresia agentului** cu privire la persoana respectivă, deoarece aceasta riscă să aibă la bază concepții părtinitoare, stereotipuri și/sau prejudecăți.

### 4. Utilizarea ilegală a creării de profiluri are un impact negativ asupra activității agenților de poliție și de gestionare a frontierelor

- **Utilizarea ilegală a creării de profiluri subminează încrederea în polițiști și în poliția de frontieră.** Poate duce la deteriorarea relației dintre polițiști/poliția de frontieră și membrii minorităților și ai altor comunități, care pot simți că li se aplică un tratament diferențiat. Sentimentul de nedreptate poate determina unele persoane și grupuri să-și piardă încrederea în poliție și în alte autorități, ceea ce poate duce la un nivel redus de denunțare a infracțiunilor la poliție și la o cooperare redusă cu autoritățile. La rândul lor, autoritățile pot privi anumite grupuri cu suspiciune, ceea ce poate determina intensificarea practicilor de utilizare ilegală a profilurilor.
- **Utilizarea ilegală a profilurilor subminează eficacitatea acestui instrument,** întrucât rata de oprire a persoanelor de către poliție sau la frontieră nu corespunde neapărat ratelor de infraționalitate înregistrate în cadrul diferitelor grupuri.
- Vizarea disproporționată a unui grup minoritar de către agenții de poliție sau de gestionare a frontierelor comportă riscul unei **profeții autoîmplinite**, având ca rezultat un număr mai mare de arestări sau de verificări la frontieră.

## 5. Utilizarea ilegală a creării de profiluri are consecințe juridice și financiare, iar agenții sunt răspunzători

- Agenții de aplicare a legii și de gestionare a frontierelor sunt **răspunzători** pentru utilizarea profilurilor în limitele legii.
- **Colectarea de date fiabile, exacte și oportune** este esențială pentru asigurarea răspunderii.
- Existența unor **mecanisme eficiente de tratare a plângerilor** poate să descurajeze abuzul de putere și totodată să contribuie la asigurarea și restabilirea încrederii publicului în operațiunile autorităților polițienești și de gestionare a frontierelor.
- Organizarea unor **reuniuni de feedback cu membri ai publicului** (pentru a le asculta părerea, a discuta despre profiluri și a primi feedback cu privire la operațiuni) oferă ocazia de a învăța lecții importante și de a îmbunătăți acțiunile legate de profiluri.

## 6. Crearea de profiluri pe bază pe algoritmi trebuie să respecte garanțiile specifice privind protecția datelor

- Când se concep și se utilizează algoritmi pentru crearea de profiluri, se pot strecura **prejudecăți** în fiecare etapă a procesului. Pentru a evita acest lucru și potențiale încălcări ulterioare ale drepturilor fundamentale, atât **experții în IT, cât și agenții care interpretează datele trebuie să înțeleagă clar drepturile fundamentale**.
- Este esențial să se utilizeze **date fiabile**. Introducerea în algoritm a unor date care reflectă prejudecăți existente sau care provin din surse ce nu prezintă încredere va genera rezultate părtinitoare și nefiabile.
- Crearea profilurilor pe bază de algoritmi trebuie să fie **legitimă, necesară și proporțională**.
- Prelucrarea datelor trebuie să aibă **un scop specific**.
- Oamenii au **dreptul de a fi informați**, primind informații despre datele cu caracter personal care se colectează și se stochează, despre prelucrare și scopul acesteia, precum și despre drepturile lor.
- Datele trebuie să fie **colectate, prelucrate și stocate în condiții de siguranță**. Autoritățile trebuie să țină evidența activităților de prelucrare (inclusiv a intervențiilor asupra datelor) și a jurnalelor aferente (inclusiv a informațiilor despre persoanele care accesează datele).
- Prelucrarea ilegală a datelor trebuie să fie **prevenită și detectată**: 1) prin evaluări ale impactului efectuate în prealabil și 2) prin utilizarea unor instrumente de criptare încorporate în algoritm „din faza de proiectare”.

## Site-uri relevante

### **Uniunea Europeană**

Curtea de Justiție a Uniunii Europene (CJUE): <http://www.curia.eu>

Legislația UE: <http://eur-lex.europa.eu>

Agenția pentru Drepturi Fundamentale a Uniunii Europene (FRA): <https://fra.europa.eu/ro>

Parlamentul European: <https://www.europarl.europa.eu/portal/ro>

### **Consiliul Europei**

Comitetul de Miniștri al Consiliului Europei: <http://www.coe.int/cm>

Curtea Europeană a Drepturilor Omului (CEDO): <http://www.echr.coe.int>

### **Organizația Națiunilor Unite**

Oficiul Înaltului Comisar al Națiunilor Unite pentru Drepturile Omului (OHCHR): <http://www.ohchr.org>

### **Lupta împotriva discriminării**

Comisia Europeană împotriva Rasismului și Intoleranței (ECRI): <http://www.coe.int/ecri>

Rețeaua europeană a organismelor naționale de promovare a egalității (Equinet): <http://www.equineteurope.org>

Organisme naționale de promovare a egalității: <https://equineteurope.org/members-map>

### **Protecția datelor**

Autoritatea Europeană pentru Protecția Datelor (AEPD): <https://edps.europa.eu>

Comitetul european pentru protecția datelor (CEPD): [https://edpb.europa.eu/edpb\\_ro](https://edpb.europa.eu/edpb_ro)

Autorități naționale pentru protecția datelor: [https://edpb.europa.eu/about-edpb/about-edpb/members\\_ro](https://edpb.europa.eu/about-edpb/about-edpb/members_ro)

### **Aplicarea legii**

Rețeaua autorităților independente de tratare a plângerilor împotriva poliției (IPCAN): <https://ipcan.org>

Agenția Uniunii Europene pentru Formare în Materie de Aplicare a Legii (CEPOL): <https://www.cepoleuropa.eu>

Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (EUROPOL): <https://www.europol.europa.eu/ro/about-europol>



***Gestionarea frontierelor***

Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (Frontex):

<https://frontex.europa.eu/ro>

Biroul European de Sprijin pentru Azil (EASO): <https://www.easo.europa.eu>

***Baze mari de date***

Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informa-  
tice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA):

<https://www.eulisa.europa.eu>



# 1

## Prezentarea contextului: Ce este crearea de profiluri?

Acest capitol descrie ce se înțelege prin crearea de profiluri și explică principalele drepturi fundamentale cărora le poate aduce atingere. Utilizarea profilurilor în contextul activităților de aplicare a legii și de gestionare a frontierelor este prezentată prin analiza a trei elemente esențiale:

- conceptul de creare de profiluri și utilizarea acestuia de către autoritățile de aplicare a legii și de gestionare a frontierelor. Această secțiune prezintă și câteva dintre diversele tipuri de profiluri;
- cele mai importante principii ale drepturilor fundamentale care trebuie respectate pentru ca profilurile să fie utilizate legal, și anume nediscriminarea, dreptul la respectarea vieții private și dreptul la protecția datelor;
- potențialul impact negativ al utilizării profilurilor, inclusiv posibilele consecințe asupra persoanelor și asupra relațiilor cu comunitățile, precum și asupra încrederii în autoritățile polițienești și de gestionare a frontierelor.

### 1.1. Definiția creării de profiluri

Crearea de profiluri presupune **clasificarea persoanelor** în funcție de caracteristicile lor personale. Aceste caracteristici pot fi „invariabile” (cum sunt vârsta sau înălțimea) sau „variabile” (de exemplu, îmbrăcămintea, obiceiurile, preferințele și alte elemente de comportament). Crearea de profiluri include activități de extragere de date, prin care persoanele sunt clasificate **„pe baza unora dintre caracteristicile lor**

**observabile, cu scopul de a deduce, cu o anumită marjă de eroare, altele care nu sunt observabile”<sup>3</sup>.**

## Aspecte esențiale

- Crearea de profiluri presupune **clasificarea persoanelor** în funcție de caracteristicile deduse ale acestora.
- Crearea de profiluri în contextul aplicării legii și al gestionării frontierelor are două scopuri principale: **identificarea persoanelor cunoscute pe baza informațiilor referitoare la o anumită persoană** și, ca **metodă predictivă**, identificarea persoanelor „necunoscute” care ar putea prezenta interes pentru autoritățile de aplicare a legii și de gestionare a frontierelor. În ambele cazuri pot exista prejudecăți conștiente sau inconștiente care pot avea efect discriminator.
- Activitățile de creare de profiluri ale polițiștilor de frontieră și ale agenților de aplicare a legii pot fi influențate de prejudecăți provenite fie din experiențele personale, fie din cele instituționale. Aceste prejudecăți pot interveni în evaluarea realizată în vederea creării profilurilor și o pot modifica, afectând atât legalitatea, cât și eficacitatea activităților polițieneste.
- Stereotipurile pot reflecta un anumit adevăr statistic. Totuși, chiar și în aceste cazuri, ele **rămân problematice** dacă au drept consecință tratarea unei persoane ca membru al unui grup, și nu pe baza situației sale individuale.
- În realizarea și utilizarea profilurilor create cu ajutorul algoritmilor, **se pot strecura prejudecăți în fiecare etapă a procesului**. Pentru a evita acest lucru și potențiale încălcări ulterioare ale drepturilor fundamentale, atât experții informaticieni care concep algoritmi, cât și agenții care colectează și interpretează datele trebuie să înțeleagă clar drepturile fundamentale și modul în care se aplică în acest context.

Practicile care implică profiluri se utilizează pentru:

- a genera cunoștințe, prin analizarea datelor existente cu scopul de a face presupuneri despre o persoană. Se folosesc experiențele anterioare și analiza statistică pentru a stabili corelații între anumite caracteristici și rezultate sau comportamente particulare;
- a sprijini procesele decizionale, prin utilizarea acestor corelații pentru a lua decizii cu privire la acțiunile care urmează să fie întreprinse.

3 Dinant J.-M., Lazaro C., Pouillet Y., Lefever N. și Rouvroy A. (2008), p. 3.

Toate acestea fac ca profilurile să fie un instrument puternic la dispoziția agenților de aplicare a legii și a polițiștilor de frontieră. Există însă și unele riscuri semnificative:

- profilurile stabilesc corelații generale care ar putea să nu fie adevărate pentru toate persoanele. Orice persoană poate fi „excepția de la regulă”;
- profilurile pot genera corelații incorecte, atât pentru anumite persoane, cât și pentru anumite grupuri;
- profilurile pot crea stereotipuri dăunătoare și pot duce la discriminare;
- unele stereotipuri pot reflecta un adevăr statistic. Totuși, chiar și în aceste cazuri, stereotipurile rămân problematice dacă au drept consecință tratarea unei persoane ca membru al unui grup, și nu ca individ.

### **Exemple**

#### **Profiluri potențial inexacte**

*Presupunerea că „femeile trăiesc mai mult decât bărbații” este susținută de cercetări factuale; însă un anumit bărbat poate trăi mai mult decât o anumită femeie. Prin urmare, orice decizie luată față de o femeie pe baza acestei presupuneri prezintă riscul de a fi inexactă într-un caz concret și ar rămâne adevărată doar în medie.*

*Oamenii își pot împrumuta mașina rudelor sau prietenilor, motiv pentru care nu se poate avea încredere într-un profil care sugerează un comportament riscant la volan pe baza faptului că persoana deține un anumit autoturism.*

## **1.1.1. Profilurile în contextul aplicării legii și al gestionării frontierelor**

Profilurile sunt utilizate în mod obișnuit și legitim de agenții de poliție și de polițiștii de frontieră pentru a preveni, a ancheta și a urmări penal infracțiunile, precum și pentru a preveni și a depista imigrația ilegală.

**Crearea de profiluri** înseamnă „orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau a preconiza aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia<sup>4</sup>”. Rezultatele acestei prelucrări de date se folosesc pentru a ghida acțiunile de gestionare a frontierelor și de aplicare a legii, cum ar fi oprirea și percheziționarea, arestările, refuzarea accesului în anumite zone sau trimiterea către „verificări în linia a doua” mai temeinice la frontieră. Există două utilizări principale ale profilurilor:

- identificarea persoanelor pe baza unor informații specifice. În acest scop se folosește un profil care enumeră caracteristicile unor suspecți specifici, pe baza dovezilor culese cu privire la un anumit eveniment;
- ca metodă predictivă, identificarea persoanelor „necunoscute” care ar putea prezenta interes pentru autoritățile de aplicare a legii și de gestionare a frontierelor. Aceasta se bazează pe analiza datelor și pe ipoteze fondate, derivate din experiență. În mod ideal, metodele predictive pun accentul pe comportament. În practică însă, accentul se pune deseori nu (sau nu doar) pe comportament, ci pe caracteristicile fizice vizibile, cum ar fi vârsta, genul sau etnia.

Tabelul 1 prezintă o comparație între caracteristicile esențiale ale acestor două tipuri de utilizare a profilurilor în contextul activităților polițienești.

**Tabelul 1: Caracteristicile activităților polițienești bazate pe informații specifice și pe analiza predictivă**

	<b>Activități polițienești bazate pe informații specifice</b>	<b>Activități polițienești bazate pe analiza predictivă</b>
<b>Context</b>	S-a comis o infracțiune sau s-a emis o alertă cu privire la o anumită persoană	Nu s-a comis nicio infracțiune sau nu s-a emis nicio alertă cu privire la o anumită persoană
<b>Abordare</b>	Reactivă	Proactivă

4 Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, JO L 119 (Directiva privind poliția), articolul 3 alineatul (4).

<b>Obiectiv</b>	Arestarea suspectului/suspecților	Anticiparea locului și a momentului în care ar putea avea loc infracțiuni sau a persoanelor care ar putea încerca să intre în țară în mod neregular
<b>Date utilizate</b>	Informații specifice referitoare la cazul respectiv („profil individual”)	Informații generice referitoare la mai multe cazuri
<b>Tip de proces</b>	Combinatie între procese bazate pe date și procese umane	În principal pe bază de date („analiza riscurilor”)

Sursa: FRA, 2018.

Ambele utilizări ale profilurilor pot fi ilegale dacă nu respectă garanții specifice, inclusiv necesitatea de a avea un obiectiv și o justificare rezonabilă pentru crearea profilurilor. **Capitolul 2** și **capitolul 3** cuprind informații practice despre modul în care trebuie să se asigure legalitatea utilizării profilurilor și conformitatea acestora cu drepturile omului.

## 1.1.2. Definiția creării de profiluri pe bază de algoritmi

Ca urmare a evoluțiilor tehnologice rapide, crearea profilurilor se bazează din ce în ce mai mult pe utilizarea datelor stocate în baze de date și pe sisteme de tehnologie a informației (sisteme IT). Crearea profilurilor cu ajutorul algoritmilor utilizează diferite tehnici pentru a crea profilurile persoanelor pe baza corelațiilor și a modelelor observate între date. Ea permite agenților de aplicare a legii și de gestionare a frontierelor să urmărească persoane sau grupuri specifice care prezintă un anumit risc pe baza analizei datelor.

Această practică ridică probleme importante legate de drepturile fundamentale, cum ar fi potențiale discriminări și încălcări ale dreptului la respectarea vieții private și la protecția datelor. Secțiunea de față a ghidului se concentrează asupra modului în care agenții de aplicare a legii și de gestionare a frontierelor pot să utilizeze și să trateze datele în conformitate cu principiile drepturilor fundamentale în activitatea lor de zi cu zi.

### **Prelucrarea datelor cu caracter personal: ce spune legea?**

Standardele juridice care reglementează prelucrarea datelor cu caracter personal în scopul construirii de profiluri sunt cuprinse în cadrul juridic al

UE privind protecția datelor. În conformitate cu articolul 4 alineatul (4) din Regulamentul general privind protecția datelor (RGPD) și cu articolul 3 alineatul (4) din Directiva privind poliția, „«creare de profiluri» înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia”.

Articolul 22 alineatul (1) din RGPD prevede că crearea de profiluri poate fi acceptată doar dacă decizia nu este bazată exclusiv pe prelucrarea automată și nu produce efecte care ar afecta într-o măsură semnificativă persoanele vizate.

Crearea profilurilor care intră sub incidența Directivei privind poliția (a se vedea [secțiunea 3.1](#) referitoare la crearea de profiluri pe bază de algoritmi și la protecția datelor) trebuie să respecte dispozițiile articolului 11 alineatul (3) din directiva respectivă. Acesta prevede că, „[i]n conformitate cu dreptul Uniunii, este interzisă crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza categoriilor speciale de date cu caracter personal menționate la articolul 10\*”.

\* Categoriile speciale de date sunt datele „cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, afilierea sindicală, prelucrarea datelor genetice, prelucrarea datelor biometrice pentru identificarea unică a unei persoane fizice sau prelucrarea datelor privind sănătatea sau a datelor privind viața sexuală și orientarea sexuală a unei persoane fizice”. A se vedea Directiva privind poliția, articolul 10 primul paragraf.

Metoda folosită pentru a genera profiluri pe bază de algoritmi este similară unei tehnici cunoscute sub denumirea de „**analiză comportamentală**”, care presupune realizarea de conexiuni între anumite caracteristici și tipare de comportament. [Figura 1](#) arată modul în care se pot utiliza algoritmi pentru a face predicții.



### **În obiectiv: utilizarea algoritmilor în sprijinul procesului decizional**

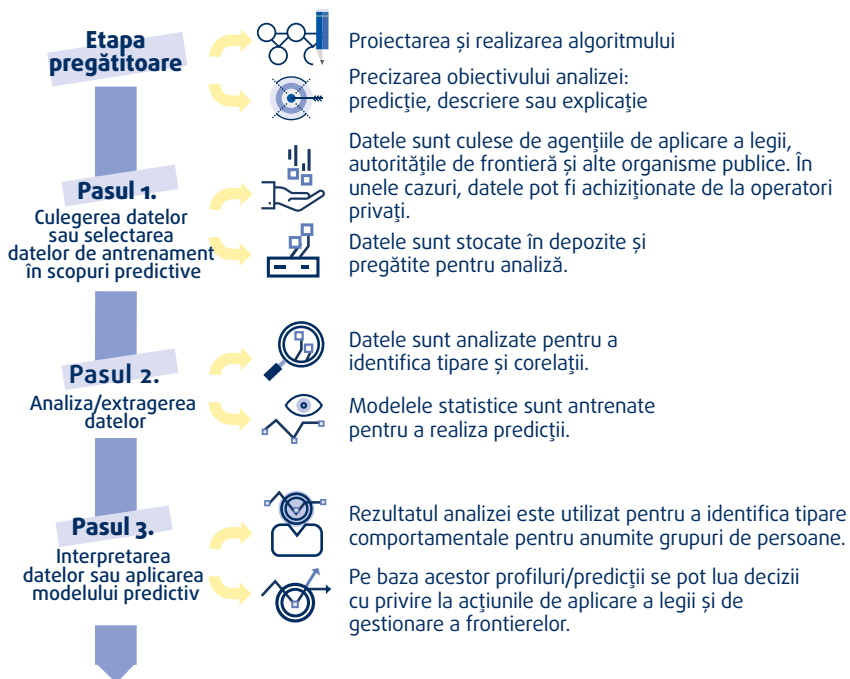
Odată cu creșterea disponibilității și a utilizării datelor, luarea deciziilor este facilitată tot mai mult sau chiar înlocuită de metode de modelare predictivă, denumite adesea „utilizare de algoritmi”. Un algoritm este o secvență de comenzi în urma căreia un computer transformă datele de intrare într-un rezultat. Mulți algoritmi se bazează pe metode statistice și utilizează tehnici care calculează relațiile dintre diferite variabile. De exemplu, datele despre cantitatea de alcool pe care o consumă un grup de persoane și datele despre speranța de viață a aceluiași grup pot fi utilizate împreună pentru a calcula influența medie a consumului de alcool asupra speranței de viață.

Rezultatul generat de algoritmi este întotdeauna o probabilitate, ceea ce înseamnă că există un grad de incertitudine cu privire la conexiunile sau clasificările realizate. De exemplu, furnizorii de e-mail folosesc algoritmi pentru a identifica mesajele spam și a le trimite în fișierul de corespondență nedorită. Algoritmii funcționează bine, dar nu sunt perfecți. Uneori mesajele spam nu sunt detectate și ajung în inbox; acesta este un rezultat fals negativ (adică mesajul este în mod fals neidentificat ca spam). Mai rar, se poate întâmpla ca un e-mail legitim să fie selectat de filtrul de spam și trimis în fișierul de corespondență nedorită; acesta este un rezultat fals pozitiv.

Atunci când înțeleg modul de bază în care algoritmii sprijină procesul decizional, practicienii pot să identifice și să adreseze întrebările corecte despre potențialele probleme legate de utilizarea algoritmilor, inclusiv despre potențialul acestora de discriminare și de încălcare a dreptului la respectarea vieții private și la protecția datelor.

*Pentru mai multe informații, a se vedea FRA (2018b).*

**Figura 1: Procesul creării de profiluri pe bază de algoritmi în contextul aplicării legii și al gestionării frontierelor**



Sursa: FRA, 2018 [adaptare după/bazată pe Perry, W.L., et al. (2013), p. 11-15, și Zarsky, T.Z. (2002-2003), p. 6-18].

Crearea de algoritmi pentru predicție este un proces complex, care implică luarea a numeroase decizii de către mai multe persoane implicate în proces. Ca atare, nu este vorba doar despre regulile urmate de computer, ci și despre procesul de colectare, pregătire și analizare a datelor. Acesta este un proces uman care cuprinde mai multe etape, inclusiv decizii ale dezvoltatorilor și managerilor. Metoda statistică este doar o parte a procesului prin care se elaborează regulile finale utilizate pentru predicție, clasificare sau decizie<sup>5</sup>. În orice caz, modul în care datele sunt colectate și utilizate poate fi discriminatoriu.

5 FRA (2018b), p. 4.

**Exemplu**

*Pentru a fi eficient și precis, software-ul de recunoaștere facială trebuie alimentat cu volume mari de imagini și date. Cu cât primește mai multe date, cu atât mai precise vor fi concluziile sale. Cu toate acestea, până în prezent imaginile introduse în algoritmi pentru antrenarea lor au fost în mare parte imagini de bărbați albi, numărul de reprezentări ale femeilor și/sau ale persoanelor cu altă origine etnică fiind comparativ scăzut. Ca urmare, rezultatele produse de software sunt mai puțin precise și prezintă un risc mai mare de inexactități în cazul persoanelor care aparțin acestor grupuri. Când sunt folosite de agenții de aplicare a legii sau de polițiștii de frontieră pentru a crea profiluri și pentru a decide, de exemplu, dacă să facă o arestare sau nu, aceste rezultate pot duce la greșeli cu un potențial impact grav asupra drepturilor și libertăților persoanei respective.*

*Pentru mai multe informații, a se vedea Center on Privacy and Technology at Georgetown Law (2016); și Buolamwini J., Gebru T. (2018).*

Se pot strecura prejudecăți în fiecare etapă a procesului de creare de profiluri pe bază de algoritmi. Pentru a evita prejudecățile discriminatorii și încălcările dreptului la protecția datelor și la viață privată, atât persoanele care concep algoritmi, cât și agenții de aplicare a legii și de gestionare a frontierelor care colectează și interpretează datele ar trebui să aibă o înțelegere clară a drepturilor fundamentale și a aplicării lor în acest context.

Este esențial să se utilizeze date fiabile. În crearea de profiluri pe bază de algoritmi, trebuie evaluată calitatea datelor utilizate pentru a se asigura că sunt de încredere: cu cât variabilitatea este mai mică, cu atât este mai mare fiabilitatea lor. Dacă la construirea unui algoritm se folosesc date care reflectă prejudecăți existente sau care provin din surse ce nu prezintă încredere, rezultatele generate vor fi pătinoare și nefiabile. Pot apărea erori și la realizarea de predicții pe baza acestor date:

- rezultate fals pozitive, adică acele cazuri în care sunt selectate și supuse unui control suplimentar persoane pe baza predicției eronate că prezintă un risc;
- rezultate fals negative, atunci când persoane care prezintă un risc real în contextul operațiunilor de aplicare a legii și de gestionare a frontierelor nu au fost identificate ca atare de către sistem.

## 1.2. Când este ilegală utilizarea profilurilor?

### Aspecte esențiale

- Caracteristicile personale pot fi utilizate ca factori legitimi pentru crearea de profiluri, însă pentru ca utilizarea profilurilor să nu fie discriminatorie și, deci, ilegală, trebuie să existe și motive rezonabile de suspiciune bazate pe alte informații decât **criteriile protejate**.
- Criteriile protejate sunt: sexul, rasa, culoarea, originea etnică sau socială, caracteristicile genetice, limba, religia sau convingerile, opiniile politice sau de altă natură, apartenența la o minoritate națională, averea, nașterea, un handicap, vârsta și orientarea sexuală.
- Criteriile protejate pot fi dezvăluite, deduse sau prezise pe baza altor date cu caracter personal.
- Pentru colectarea și prelucrarea **datelor cu caracter personal**, autoritățile de aplicare a legii și de gestionare a frontierelor trebuie să se asigure că activitățile de colectare și prelucrare au un temei juridic, au un scop valabil și legitim și sunt necesare și proporționale.
- Reprezintă date cu caracter personal orice informații care pot fi utilizate pentru a identifica – direct sau indirect – o persoană, cum ar fi: un nume, un număr de identificare, date de localizare sau orice elemente specifice, proprii identității fizice, fiziologice, genetice, psihice, economice, culturale sau sociale a unei persoane.

Atunci când sunt utilizate în mod legal, profilurile reprezintă o **tehnică de investigare legitimă**. Pentru a fi legală, utilizarea trebuie să se bazeze pe **justificări obiective și rezonabile** și să respecte drepturile fundamentale, printre care dreptul la nediscriminare și dreptul la protecția datelor cu caracter personal. Se va considera că utilizarea profilurilor nu are o justificare obiectivă și rezonabilă „dacă nu urmărește un scop legitim sau dacă nu există o relație rezonabilă de proporționalitate între mijloacele utilizate și scopul urmărit”<sup>6</sup>.

Utilizarea profilurilor poate aduce atingere multor drepturi fundamentale diferite. Secțiunea de față se concentrează asupra drepturilor fundamentale care sunt afectate cu precădere de utilizarea ilegală a profilurilor: dreptul la nediscriminare, dreptul la viață privată și dreptul la protecția datelor. Utilizarea profilurilor va fi considerată ilegală dacă:

6 Comisia Europeană împotriva Rasismului și Intoleranței (ECRI) (2007), punctul 28.

- include acte de tratament diferențiat nejustificat al persoanelor pe baza unor criterii protejate (a se vedea secțiunea 1.2.1), sau
- interferează în mod inutil cu viața privată a persoanelor și/sau nu respectă normele de prelucrare a datelor cu caracter personal (a se vedea secțiunea 1.2.2).

## 1.2.1. Interzicerea discriminării

### Interzicerea discriminării: ce spune legea?

„**Se interzice discriminarea de orice fel**, bazată pe motive precum sexul, rasa, culoarea, originea etnică sau socială, caracteristicile genetice, limba, religia sau convingerile, opiniile politice sau de orice altă natură, apartenența la o minoritate națională, averea, nașterea, un handicap, vârsta sau orientarea sexuală.”\*

*Articolul 21 din Carta drepturilor fundamentale a UE*

„**Exercitarea oricărui drept prevăzut de lege trebuie să fie asigurată fără nicio discriminare** bazată, în special, pe sex, pe rasă, culoare, limbă, religie, opinii politice sau orice alte opinii, origine națională sau socială, apartenența la o minoritate națională, avere, naștere sau oricare altă situație.

Nimeni nu va fi discriminat de o autoritate publică pe baza oricăruia dintre motivele menționate în paragraful 1.”

*Articolul 1 din Protocolul nr. 12 la Convenția Europeană a Drepturilor Omului*

*\* Trebuie precizat că, în practică, multe state membre au extins protecția împotriva discriminării la motive suplimentare celor enumerate în cartă și în Convenția Europeană a Drepturilor Omului (CEaDO).*

Se consideră discriminare „atunci când o persoană este tratată într-un mod mai puțin favorabil decât este, a fost sau va fi tratată într-o situație asemănătoare o altă persoană”, pe baza unei caracteristici personale reale sau percepute<sup>7</sup>. Aceste caracteris-

7 Directiva 2000/43/CE a Consiliului din 29 iunie 2000 de punere în aplicare a principiului egalității de tratament între persoane, fără deosebire de rasă sau origine etnică, JO L 180, articolul 2; și Directiva 2000/78/CE a Consiliului din 27 noiembrie 2000 de creare a unui cadru general în favoarea egalității de tratament în ceea ce privește încadrarea în muncă și ocuparea forței de muncă, JO L 303, articolul 2.

tici sunt denumite în legislația împotriva discriminării „criterii protejate” sau „caracteristici protejate”. Mai multe informații despre legislația și jurisprudența europeană în domeniul nediscriminării sunt disponibile în ediția din 2018 a Manualului de drept european privind nediscriminarea, publicat în comun de FRA și Consiliul Europei<sup>8</sup>.

Există mai multe tipuri de discriminare:

**Discriminarea directă** este cea în care o persoană beneficiază de un tratament mai puțin favorabil, *exclusiv sau în principal* pe baza unui criteriu protejat precum rasa, genul, vârsta, un handicap sau originea etnică<sup>9</sup>.

### **Exemplu**

*Ca răspuns la o amenințare teroristă, polițiștii primesc competența de a opri și percheziționa orice persoană despre care consideră că ar putea fi implicată în acte de terorism. Se crede că amenințarea provine de la o organizație teroristă activă într-o anumită regiune a lumii, dar nu există alte informații specifice. Dacă un polițist oprește un bărbat exclusiv sau în principal pentru că, după felul în care arată, el ar putea proveni din regiunea respectivă, aceasta ar constitui o discriminare directă și ar fi ilegală.*

**Discriminarea indirectă** (denumită și „discriminare cu impact disproporționat” în contextul activităților de aplicare a legii și de gestionare a frontierelor) se produce atunci când o dispoziție, un criteriu sau o practică *aparent neutră* poate avea drept consecință un dezavantaj special pentru persoane cu anumite caracteristici protejate în raport cu alte persoane, cu excepția cazului în care dispoziția, criteriul sau practica respectivă este obiectiv justificată de un obiectiv legitim, iar mijloacele de realizare a acestui obiectiv sunt necesare și proporționale<sup>10</sup>. În general, în cazul discriminării indirecte este nevoie de statistici pentru a evalua dacă o persoană a fost tratată, în practică, mai puțin favorabil decât o alta pe baza apartenenței la un grup cu anumite caracteristici protejate.

8 FRA și Consiliul Europei (2018).

9 *Ibid.*, p. 43.

10 [Directiva 2000/78/CE a Consiliului din 27 noiembrie 2000 de creare a unui cadru general în favoarea egalității de tratament în ceea ce privește încadrarea în muncă și ocuparea forței de muncă](#), JO L 303 (Directiva privind egalitatea de tratament în muncă), articolul 2; vezi de asemenea FRA și Consiliul Europei (2018), p. 53.

### **Exemplu**

*Autoritățile de aplicare a legii decid să oprească o mașină din zece între orele 21.00 și 01.00 în orașul X, pentru controale de rutină; 60 % din populația orașului X care este la volan în acest interval este de origine afro-caraibiană, în timp ce populația afro-caraibiană din oraș și zona înconjurătoare nu depășește 30 %. Deoarece este probabil ca acest grup să fie afectat într-o măsură mai mare decât altele, ar fi un caz de discriminare indirectă.*

Abordarea discriminării din perspectiva unui singur criteriu nu reușește să reflecte în mod adecvat diferitele manifestări ale inegalității de tratament. **Discriminarea multiplă** se referă la discriminarea pe baza mai multor criterii care funcționează separat. De exemplu, o persoană poate fi discriminată nu doar pentru originea sa etnică, ci și pentru vârsta și genul său<sup>11</sup>. **Discriminarea intersecțională** se referă la o situație în care există mai multe criterii care funcționează și interacționează simultan, astfel încât sunt inseparabile și generează tipuri specifice de discriminare (a se vedea caseta cu exemplul).

### **Exemplu**

*Un polițist oprește și percheziționează un tânăr de origine africană fără a avea suspiciuni rezonabile că a comis o infracțiune. Acesta este discriminat nu doar din cauza vârstei sale (nu toți tinerii sunt opriți) sau a originii sale etnice (nu toate persoanele de origine africană sunt oprite), ci tocmai pentru că este și tânăr, și de origine africană.*

Discriminarea poate apărea și prin prelucrarea automată a datelor cu caracter personal și utilizarea profilurilor create pe bază de algoritmi. Ea poate apărea în cursul conceperii și al execuției algoritmilor, ca urmare a încorporării – conștiente sau nu – de prejudecăți în algoritm, precum și atunci când se iau decizii pe baza informațiilor obținute.

Articolul 9 alineatul (1) din RGPD prevede în mod specific că se interzice prelucrarea categoriilor speciale de date cu caracter personal care dezvăluie caracteristici personale cum sunt originea rasială sau etnică, opiniile politice, confesiunea religioasă

11 FRA și Consiliul Europei (2018), p. 59.

sau convingerile filozofice (a se vedea figura 9 din secțiunea 2.2.4 pentru lista completă a criteriilor protejate). Această interdicție poate fi ridicată în cazuri specifice, de exemplu pentru protejarea interesului public, cu condiția ca exceptarea să aibă un temei juridic, să fie proporțională și necesară și să prevadă garanții adecvate<sup>12</sup>.

În mod similar, în contextul prevenirii, investigării, depistării și urmăririi penale a infracțiunilor, articolul 11 alineatul (3) din Directiva privind poliția, referitor la procesul decizional individual automatizat, interzice „crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza categoriilor speciale de date cu caracter personal”, inclusiv a celor care dezvăluie originea rasială sau etnică și confesiunea religioasă, precum și a datelor genetice și biometrice<sup>13</sup>. Din nou, în anumite cazuri sunt permise excepții de la această interdicție, dar ele trebuie să fie necesare, sprijinite de garanții adecvate și să aibă fie un temei juridic, fie scopul de a proteja interesele vitale ale unei persoane<sup>14</sup>.

### Interzicerea creării de profiluri discriminatorii: ce spune legea?

**„Crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza datelor cu caracter personal** care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale **este interzisă** în condițiile prevăzute la articolele 21 și 52 din Cartă [Carta drepturilor fundamentale].”

*Considerentul 38 din Directiva privind poliția*

**„În conformitate cu dreptul Uniunii, este interzisă crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza categoriilor speciale de date cu caracter personal menționate la articolul 10\*.”**

*Articolul 11 alineatul (3) din Directiva privind poliția*

*\*Articolul 10 din Directiva privind poliția: „[date] care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, afilierea sindicală, prelucrarea datelor genetice, prelucrarea datelor biometrice pentru*

12 Regulamentul general privind protecția datelor, articolul 9 alineatul (2) litera (g).

13 Pentru mai multe informații, vezi Grupul de lucru instituit prin articolul 29 (2017b).

14 [Directiva \(UE\) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului](#), JO L 119 (Directiva privind poliția), articolul 10.



*identificarea unică a unei persoane fizice sau prelucrarea datelor privind sănătatea sau a datelor privind viața sexuală și orientarea sexuală a unei persoane fizice”.*

„În cursul efectuării verificărilor la frontieră, polițiștii de frontieră **nu fac nicio discriminare** pe criterii de sex, rasă sau origine etnică, religie sau convingeri, handicap, vârstă sau orientare sexuală.”

*Articolul 7 din Codul Frontierelor Schengen*

Interzicerea discriminării nu înseamnă că nu se pot utiliza caracteristicile personale ca factori legitimi pentru crearea de profiluri în contextul anchetelor penale sau al controalelor la frontieră (a se vedea [secțiunea 2.3](#)). Trebuie însă să existe motive rezonabile de suspiciune bazate pe alte informații decât criteriile protejate. De exemplu, o persoană poate să corespundă descrierii specifice a unui suspect sau felul în care arată poate să nu coincidă cu informațiile cuprinse în documentul său de călătorie<sup>15</sup>.

### În obiectiv: discriminarea pe criteriul cetățeniei

Articolul 21 din Carta drepturilor fundamentale a UE **limitează la cetățenii UE interzicerea discriminării pe motiv de cetățenie**. Directiva privind egalitatea rasială nu include cetățenia printre criteriile protejate.

Totuși, statele membre au extins în diverse moduri sfera de aplicare a interzicerii discriminării astfel încât să includă și cetățenia. Una dintre modalități constă în recunoașterea faptului că cetățenia este uneori folosită ca substituent pentru rasă, origine etnică sau religie. În anumite cazuri de acest gen, „diferențele de tratament pe criteriul cetățeniei [...] [vor fi] considerate încălcări ale legislației care interzice discriminarea pe aceste criterii” (a se vedea Rețeaua europeană a experților juridici în domeniul egalității de gen și al nediscriminării, 2016, p. 99). În practică, este adesea dificil de diferențiat între discriminarea pe criteriul cetățeniei și discriminarea pe criteriul etniei.

Faptul că cetățenia nu este menționată în mod explicit ca motiv potențial de discriminare în articolul 21 din cartă reflectă în primul rând statutul

<sup>15</sup> Regatul Unit, Camera Lorzilor (2006), Lord Scott, Opinions of the Lords of appeal for judgment in *R (on the application of Gillan et al.) v. Commissioner of Police for the Metropolis et al.*, [2006] UKHL 12, 8 martie 2006, punctul 67.

diferit al cetățenilor UE (și al altor persoane care beneficiază de dreptul la liberă circulație în temeiul legislației UE) față de resortisanții țărilor terțe în baza dreptului UE. Acest lucru are o semnificație deosebită în procedurile la frontieră, în care cetățenia este factorul decisiv care determină dacă o persoană va fi supusă unui control amănunțit sau dacă trebuie să dețină o viză pentru a intra în spațiul Schengen – ori pentru a-l tranzita.

În același timp, trimiterea sistematică a tuturor persoanelor de o anumită cetățenie pentru verificare în linia a doua riscă să devină discriminatorie. Cetățenia poate fi o parte legitimă a profilurilor de risc folosite pentru depistarea migrației neregulamentare sau a presupuselor victime ale traficului de persoane, dar nu trebuie să fie unicul sau principalul factor declanșator al unei verificări în linia a doua. În plus, la fel ca în alte contexte, tratamentul diferențiat pe baza cetățeniei devine discriminatoriu și, prin urmare, ilegal când este utilizat ca substitut pentru discriminarea pe criterii protejate care sunt strâns legate de cetățenie, cum ar fi rasa, etnia sau religia.

În principiile și orientările recomandate din 2014 privind drepturile omului la frontierele internaționale, Oficiul Înaltului Comisar al Națiunilor Unite pentru Drepturile Omului include cetățenia printre criteriile protejate care nu trebuie utilizate pentru crearea de profiluri ale migranților (principiul 8).

### **Jurisprudență**

În cauza *Rosalind Williams Lecraft/Spania*, o femeie a fost oprită pe peronul unei gări din Spania de un polițist care i-a cerut să-i prezinte actele de identitate. Femeia l-a întrebat pe polițist de ce este singura persoană de pe peron care a fost oprită, iar acesta i-a răspuns: „Pentru că ești negresă”. În hotărârea sa, Comitetul Națiunilor Unite pentru Drepturile Omului a subliniat că, în general, este legitimă efectuarea de controale de identitate în interesul siguranței publice și pentru a preveni infracțiunile și a monitoriza imigrația ilegală. Totuși, a stabilit că, „atunci când efectuează aceste controale, autoritățile nu trebuie să considere caracteristicile fizice sau etnice ale persoanelor vizate drept indicii pentru situația posibil ilegală a acestora în țară. În plus, controalele de identitate nu trebuie efectuate astfel încât să fie vizate doar persoanele cu anumite caracteristici fizice sau origini etnice. Acest lucru nu numai că va afecta demnitatea celor vizați, ci va contribui și la

răspândirea atitudinilor xenofobe în rândul populației generale; de asemenea, ar fi incompatibil cu o politică eficientă de combatere a discriminării rasiale”.

În 2017 a fost depusă la CEDO o plângere similară, referitoare la modul în care a fost tratat un resortisant pakistanez în timpul și după ce a fost oprit de poliție în Spania. Instanța va trebui să decidă dacă reclamantul a fost discriminat pe motiv de origine etnică în cursul controlului de identitate și dacă s-a produs o încălcare a articolului 8 (dreptul la viață privată și de familie) prin faptul că autoritățile spaniole nu au luat toate măsurile pentru a descoperi eventualele motive rasiste ale incidentului. Hotărârea este pendinte la data redactării prezentului document.

*Pentru mai multe informații, a se vedea UNHRC, Rosalind Williams Lecraft/ Spania, com. nr. 1493/2006 și CEDO, Zeshan Muhammad/Spania, nr. 34085/17, acțiune introdusă la 6 mai 2017. A se vedea, de asemenea, FRA și Consiliul Europei (2018).*

În cauza *B.S./Spania*, o lucrătoare sexuală de origine nigeriană a cărei ședere în Spania era legală a susținut că poliția spaniolă a agresat-o fizic și verbal ca urmare a rasei, a genului și a profesiei sale. Ea a susținut că, spre deosebire de alte lucrătoare sexuale de origine europeană, a fost vizată de controale repetate ale poliției și a fost victima unor insulte rasiste și sexiste. Doi intervenienți terți – Centrul AIRE și Unitatea Europeană de Cercetare Socială din cadrul Universității din Barcelona – au apelat la CEDO pentru recunoașterea discriminării intersecționale. Instanța a constatat o încălcare a articolului 3 (interzicerea tratamentelor inumane și degradante), dar a mers și mai departe și a analizat separat dacă a existat, de asemenea, o încălcare a obligației de a investiga existența unei posibile legături de cauzalitate între presupusele atitudini rasiste și actele de violență ale poliției. Cu privire la această chestiune, CEDO a constatat o încălcare a articolului 14 (interzicerea discriminării), deoarece instanțele naționale nu au luat în considerare vulnerabilitatea deosebită a reclamantei, în calitate de femeie africană care lucra ca prostituată. Deși abordarea a fost intersecțională, în hotărâre nu s-a folosit termenul „intersecționalitate”.

*Pentru mai multe informații, a se vedea CEDO, B.S./Spania, nr. 47159/08, 24 iulie 2012.*

### **În obiectiv: sarcina probei**

În 2016, Curtea de Casație din Franța s-a pronunțat pentru prima dată asupra chestiunii controalelor de identitate discriminatorii. În *deciziile sale din 9 noiembrie 2016*, curtea a statuat că poliția a efectuat controale de identitate discriminatorii asupra a trei din 13 bărbați de origine africană sau arabă, constatând responsabilitatea statului în cauzele respective și obligându-l să plătească despăgubiri celor trei reclamânți. În alte opt cauze, instanța a statuat că controalele de identitate contestate au fost legale, întrucât s-au bazat pe elemente obiective și, prin urmare, nediscriminatorii. În celelalte două cauze judecătoria nu s-au pronunțat, ci le-au trimis înapoi la instanțele inferioare pentru rejudecare.

De asemenea, curtea a clarificat sarcina probei în astfel de cazuri. Controalele de identitate nu sunt înregistrate dacă nu conduc la proceduri judiciare sau administrative. Curtea a explicat că reclamânții trebuie să furnizeze instanțelor probe care să indice existența discriminării. Poliția trebuie să dovedească fie absența tratamentului diferențiat în efectuarea controalelor de identitate, fie faptul că tratamentul diferențiat a fost justificat de elemente obiective.

În plus, instanța a constatat că judecătoria pot lua în considerare, ca probe, studii și informații statistice care atestă frecvența controalelor de identitate efectuate, din motive discriminatorii, asupra aceluiași grup de populație din care face parte și reclamantul (minorități vizibile, determinate pe baza unor caracteristici fizice derivate din originea etnică reală sau presupusă). Totuși, doar aceste dovezi nu sunt suficiente pentru a sugera o discriminare.

Prin urmare, instanța a considerat că un control al identității bazat pe caracteristici fizice asociate cu o origine etnică reală sau presupusă, fără nicio justificare obiectivă prealabilă, este discriminatoriu și constituie o abatere gravă care, în aceste trei cauze, a angajat responsabilitatea statului.

*Pentru mai multe informații, a se vedea Franța, Curtea de Casație (Cour de Cassation), Décision 1245, 9 noiembrie 2016.*

## 1.2.2. Dreptul la respectarea vieții private și la protecția datelor cu caracter personal

În conformitate cu legislația UE, dreptul la respectarea vieții private (articolul 7 din cartă) și la protecția datelor cu caracter personal (articolul 8 din cartă) sunt drepturi distincte, deși strâns legate între ele. Dreptul la viață privată (sau dreptul la intimitate) este un drept mai larg, care interzice *orice interferență* în viața privată a unei persoane. Viața privată este înțeleasă nu doar ca ceea ce se dorește a se păstra confidențial, ci cuprinde și mijloacele prin care o persoană își exprimă personalitatea – de exemplu, atunci când alege cu cine să interacționeze sau cum să se îmbrace. Protecția datelor cu caracter personal se limitează la evaluarea legalității în legătură cu *prelucrarea datelor cu caracter personal*<sup>16</sup>. *Când nu se referă în mod specific la legislația UE, cele două sunt utilizate în mod interschimbabil în sensul prezentului ghid. Aceste drepturi nu sunt absolute și pot fi limitate în anumite circumstanțe (a se vedea articolul 8 din CEaDO și articolul 52 din cartă).*

### Dreptul la viață privată și dreptul la protecția datelor: ce spune legea?

„(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 acesta este prevăzut de lege și constituie, într-o societate democratică, o măsură necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protecția sănătății, a moralei, a drepturilor și a libertăților altora.”

*Articolul 8 din Convenția Europeană a Drepturilor Omului*

„Orice persoană are dreptul la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor.”

*Articolul 7 din Carta drepturilor fundamentale a UE*

„(1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.

16 FRA, AEPD și Consiliul Europei (2018).

(2) Asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora. [...]"

*Articolul 8 din Carta drepturilor fundamentale a UE*

„(1) Persoana vizată are dreptul de a nu face obiectul unei decizii **bazate exclusiv pe prelucrarea automată**, inclusiv crearea de profiluri, care **produce efecte juridice** care privesc persoana vizată **sau o afectează în mod similar într-o măsură semnificativă**.

(2) Alineatul (1) nu se aplică în cazul în care decizia:

- (a) este necesară pentru încheierea sau executarea unui contract [...];
- (b) este autorizată prin dreptul [...] care prevede [...] măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau
- (c) are la bază consimțământul explicit al persoanei vizate.”

*Articolul 22 alineatele (1) și (2) din Regulamentul general privind protecția datelor*

„Statele membre garantează că o decizie întemeiată exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce un efect juridic negativ pentru persoana vizată sau care o afectează în mod semnificativ, este interzisă, cu excepția cazului în care este autorizată de dreptul Uniunii sau de dreptul intern care se aplică operatorului și care prevede garanții adecvate pentru drepturile și libertățile persoanei vizate, cel puțin dreptul de a obține intervenția umană din partea operatorului.”

*Articolul 11 alineatul (1) din Directiva privind poliția*

Tabelul 2: Cerințe privind protecția datelor – diferențe între Directiva privind poliția și RGPD

Principiul protecției datelor	RGPD	Directiva privind poliția
<b>Legalitate, echitate, transparență</b>	Datele cu caracter personal trebuie să fie prelucrate în mod echitabil, legal <b>și transparent</b> .	Datele cu caracter personal trebuie să fie prelucrate în mod echitabil și legal.
<b>Limitarea scopului</b>	Datele cu caracter personal colectate pentru un anumit scop nu trebuie prelucrate ulterior pentru un scop incompatibil; <b>prelucrarea ulterioară în scop științific, istoric sau statistic nu este incompatibilă cu scopurile inițiale</b> .	Datele cu caracter personal colectate pentru un anumit scop nu trebuie prelucrate ulterior pentru un scop incompatibil; alte scopuri nu sunt incompatibile cu scopul inițial dacă prelucrarea este autorizată de lege și este necesară și proporțională.
<b>Reducerea la minimum a datelor</b>	Datele cu caracter personal colectate sunt adecvate, relevante <b>și limitate la ceea ce este necesar</b> în raport cu scopurile în care au fost colectate;	Datele cu caracter personal colectate sunt adecvate, relevante și <b>neexcesive</b> în ceea ce privește scopurile în care au fost colectate.
<b>Limitări legate de stocare</b>	Datele cu caracter personal sunt păstrate într-o formă care permite identificarea persoanelor vizate pe perioada necesară îndeplinirii scopurilor în care au fost colectate datele; <b>datele cu caracter personal pot fi stocate pe perioade mai lungi în scopuri științifice, istorice sau statistice</b> .	Datele cu caracter personal sunt păstrate într-o formă care permite identificarea persoanelor vizate pe perioada necesară îndeplinirii scopurilor pentru care au fost colectate datele.
<b>Exactitate</b>	Datele cu caracter personal colectate sunt exacte și actualizate. Datele cu caracter personal incorecte sau inexacte sunt șterse sau rectificate.	
<b>Integritate și confidențialitate</b>	Datele cu caracter personal sunt păstrate în condiții de securitate, protejate împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale.	

Sursa: FRA, 2018.

Legislația secundară a UE detaliază dreptul la viață privată și dreptul la protecția datelor cu caracter personal. Modul în care pot fi colectate și prelucrate datele cu caracter personal este specificat în două acte legislative. Regulamentul (UE) 2016/679, Regulamentul general privind protecția datelor (RGPD), stabilește

principiile generale și garanțiile cu privire prelucrarea datelor cu caracter personal. Cu mai multă precizie, Directiva (UE) 2016/680, cunoscută ca Directiva privind poliția, stabilește normele de prelucrare a datelor cu caracter personal în contextul operațiilor de aplicare a legii în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor. Cele mai importante principii ale celor două acte și câteva diferențe esențiale între ele sunt ilustrate în tabelul 2. Legile care instituie marile baze de date ale UE utilizate pentru gestionarea frontierelor, cum sunt Sistemul de informații privind vizele (VIS), Sistemul de intrare/ieșire (EES) sau Sistemul european de informații și de autorizare privind călătoriile (ETIAS), conțin de asemenea câte un cadru specific de protecție a datelor (a se vedea [secțiunea 3.2](#), referitoare la bazele mari de date).

### **Exemple**

*Un polițist de frontieră trimite lista pasagerilor dintr-un avion către persoane neautorizate. Odată comunicate, aceste date cu caracter personal pot fi utilizate pentru scopuri diferite și/sau private. Este o încălcare clară a principiilor protecției datelor.*

*O polițistă iese din birou lăsând afișată pe ecranul calculatorului o listă de date cu caracter personal ale unor suspecți. Prin faptul că subminează principiul securității datelor cu caracter personal, aceasta constituie o încălcare a principiilor protecției datelor.*

### **Jurisprudență**

Hotărârile instanțelor oferă orientări cu privire la modul în care aceste principii sunt aplicate în practică.

### **Limitarea scopului**

În cauza *Heinz Huber/Bundesrepublik Deutschland*, CJUE a evaluat legitimitatea Registrului central al străinilor din Germania (*Ausländerzentralregister*, AZR), care conține anumite date cu caracter personal referitoare la resortisanții străini – atât din UE, cât și din afara UE – a căror ședere în Germania depășește trei luni. CJUE a concluzionat că datele colectate cu un anumit scop nu pot fi utilizate în alt scop. Instanța a considerat că AZR este un instrument legitim de aplicare a normelor de ședere și că diferența de tratament dintre resortisanții străini și cei germani, despre care se păstrează mai puține date,



este justificată având în vedere scopul urmărit. Totuși, CJUE a stabilit că datele stocate în AZR nu pot fi utilizate pentru combaterea criminalității în general, deoarece acesta este un scop diferit de cel pentru care datele au fost colectate inițial.

*Pentru mai multe informații, a se vedea CJUE, cauza C-524/06, Heinz Huber/ Bundesrepublik Deutschland, 16 decembrie 2008.*

### Limitări legate de stocare

În cauza *S. și Marper/Regatul Unit*, reclamanții au solicitat ștergerea înregistrărilor lor (amprente, mostre celulare și profiluri ADN) din baza de date ADN utilizată pentru identificarea infractorilor în Regatul Unit. Procesele lor se încheiaseră cu achitare și erau îngrijorați cu privire la eventuale utilizări ale datelor lor în prezent sau în viitor. Poliția a refuzat. CEDO a concluzionat că păstrarea pe termen nedeterminat a mostrelor de ADN ale persoanelor arestate, dar care au fost ulterior achitate sau împotriva cărora au fost retrase acuzațiile reprezintă o încălcare a dreptului la viață privată. Instanța a subliniat că există riscul de stigmatizare, deoarece datele persoanelor care nu au fost condamnate pentru nicio infracțiune erau tratate în același mod ca și cele ale persoanelor condamnate. De asemenea, instanța a recunoscut că prejudiciul potențial cauzat de păstrarea acestor date este semnificativ îndeosebi în cazul copiilor, având în vedere importanța dezvoltării și integrării lor în societate.

*Pentru mai multe informații, a se vedea CEDO, S. și Marper/Regatul Unit, nr. 30562/04 și 30566/04, 4 decembrie 2008.*

Pentru a colecta și prelucra date cu caracter personal în scopul creării de profiluri, autoritățile de aplicare a legii și de gestionare a frontierelor trebuie să îndeplinească patru criterii juridice esențiale. Colectarea și prelucrarea datelor trebuie:

- **să fie definite și reglementate prin lege (temei juridic):** orice limitare a dreptului la respectarea vieții private și a dreptului la protecția datelor trebuie să fie stipulată de lege și să respecte esența acestor drepturi. Legea trebuie să respecte standardele de claritate și calitate, adică să fie accesibilă publicului și să fie suficient de clară și de precisă pentru ca publicul să înțeleagă aplicarea și consecințele ei;

- **să aibă un scop valid, legal și adecvat (*obiectiv legitim*):** obiectivele legitime sunt stabilite în legislație și nu pot fi extinse. Ele pot să vizeze securitatea națională, sănătatea, ordinea publică sau prevenirea criminalității;
- **să fie indispensabile pentru atingerea acestui scop (*necesitate*):** prelucrarea datelor cu caracter personal trebuie să se limiteze la ceea ce este necesar în scopul pentru care au fost colectate datele;
- **să nu fie excesive (*proporționalitate*):** autoritățile care prelucrează date cu caracter personal trebuie să realizeze un echilibru corect între scop și mijloacele utilizate pentru a-l atinge. Cu alte cuvinte, valoarea adăugată a prelucrării nu trebuie să depășească potențialul impact negativ al acesteia.

Capitolul 3 explică modul în care pot fi aplicate în practică aceste principii.

Figura 2 arată modul în care pot fi folosite principiile pentru a evalua dacă o acțiune ar putea încălca dreptul la respectarea vieții private și de familie și dreptul la protecția datelor (a se vedea și secțiunea 2.3.3 referitoare la mecanismele de tratare a plângerilor). Cauza *Gillan și Quinton/Regatul Unit*, referitoare la un caz de oprire și percheziționare, ilustrează modul în care CEDO a aplicat aceste principii pentru a stabili dacă a existat o încălcare a dreptului la protecția datelor și a vieții private (a se vedea caseta referitoare la jurisprudență).

Figura 2: Încălcarea vieții private și a protecției datelor – procesul de evaluare



Sursa: FRA, 2018 [având la bază Consiliul Europei (2003), *Dreptul la respectarea vieții private și de familie: Ghid privind punerea în aplicare a articolului 8 din Convenția Europeană a Drepturilor Omului*].

## Jurisprudență

În cauza *Gillan și Quinton/Regatul Unit*, reclamanții, doi cetățeni britanici, au contestat în instanță legalitatea opririi și percheziționării lor.

**Măsura adoptată este prevăzută de lege?** Măsura a fost în conformitate cu secțiunile 44-47 din Legea privind combaterea terorismului din 2000, care stabilește că: 1) pentru prevenirea actelor de terorism, polițiștii de rang superior pot autoriza orice polițist în uniformă dintr-o anumită zonă să desfășoare acțiuni de oprire și percheziționare; 2) autorizările trebuie să fie confirmate de către ministrul de interne și sunt limitate în timp, dar pot fi reînnoite pe termen nelimitat; 3) deși scopul acestor operațiuni de percheziționare este de a găsi obiecte care ar putea fi utilizate pentru acte

de terorism, nu este necesar ca acțiunile de oprire și percheziționare să se bazeze pe suspiciunea că persoana sau persoanele oprite au asupra lor astfel de obiecte; și 4) persoanele care refuză să se supună unei operațiuni de percheziționare sunt pasibile de închisoare, amendă sau ambele (*Gillan și Quinton*, punctele 76-80).

**Măsura adoptată constituie o ingerință în viața privată și/sau protecția datelor?** Folosirea competențelor coercitive de către autoritățile de aplicare a legii pentru a opri o persoană și a-i percheziționa îmbrăcămintea și obiectele personale reprezintă o clară ingerință în dreptul la respectarea vieții private. Gravitatea acesteia este sporită de expunerea publică a unor informații cu caracter personal, care este asociată unui element de umilință și rușine (*Gillan și Quinton*, punctul 63).

**Evaluarea proporționalității și a necesității:** Instanța a exprimat o serie de îngrijorări cu privire la proporționalitatea și necesitatea legii (*Gillan și Quinton*, punctele 80-86):

- standardul legal pentru autorizarea opririlor nu este împovăraător;
- competențele legale sunt atât de largi încât persoanelor le este foarte dificil să demonstreze că autorizația și confirmarea acesteia depășesc competențele autorităților relevante (*ultra vires*) sau reprezintă un abuz de putere;
- zonele geografice acoperite de autorizație sunt foarte întinse, iar termenul a fost prelungit în mod repetat, ceea ce reduce natura punctuală a autorizației;
- restricțiile privind dreptul discreționar al fiecărui polițist sunt mai mult de formă decât de substanță;
- există puține perspective de căi de atac judiciare, deoarece polițistul care efectuează oprirea nu trebuie să facă dovada unei bănuieli rezonabile; prin urmare, este aproape imposibil să se dovedească faptul că aceste drepturi au fost exercitate în mod necorespunzător.

Aceste considerații au determinat CEDO să concluzioneze că secțiunile relevante ale Legii privind combaterea terorismului „nu sunt suficient de clar reglementate și nici susceptibile de a oferi garanții legale împotriva abuzurilor” și, prin urmare, încalcă articolul 8 din CEaDO.

*Pentru mai multe informații, a se vedea CEaDO, Gillan și Quinton/Regatul Unit, nr. 4158/05, 12 ianuarie 2010.*

Cerințele legale referitoare la crearea de profiluri cuprinse în cadrul juridic reformat al UE în materie de protecție a datelor sunt detaliate în capitolul 3.

### 1.3. Care sunt potențialele efecte negative ale utilizării ilegale a profilurilor pentru activitățile de aplicare a legii și de gestionare a frontierelor?

Profilurile create doar pe baza unor categorii generice cum sunt rasa, originea etnică sau religia nu numai că sunt ilegale, dar pot avea și inconveniente pentru eficiența activităților polițienești și de gestionare a frontierelor. Secțiunea de față analizează două efecte negative potențiale:

- Cea mai mare dificultate constă în tensionarea relațiilor cu comunitățile. Profilurile pot genera resentimente în cadrul comunităților afectate în mod deosebit și pot scădea încrederea în autoritățile polițienești și de gestionare a frontierelor. La rândul său, acest lucru poate submina eficiența metodelor care se bazează pe cooperarea publică.
- De asemenea, există îndoieli cu privire la eficacitatea utilizării unor categorii generice de profiluri în activitățile de gestionare a frontierelor sau de aplicare a legii, de exemplu dacă se ajunge la situația în care o persoană este suspectată în mod eronat<sup>17</sup>.

În plus, în cazul în care profilurile sunt utilizate în mod ilegal, autoritățile vor fi expuse riscului de reclamații sau de acțiuni legale, care pot lua forma supravegherii interne derulate de autoritățile competente să examineze plângerile împotriva poliției, de organele specializate în tratarea plângerilor, de autoritățile de supraveghere sau de sistemul judiciar civil și penal (a se vedea [secțiunea 2.3](#)). Agenții individuali și managerii de nivel mediu pot primi sancțiuni administrative și/sau penale ca urmare a implicării lor în utilizarea de profiluri ilegale sau a încuviințării acestora. Acest lucru poate determina pierderi de resurse și poate știrbi moralul și reputația autorităților.

<sup>17</sup> FRA (2017d), p. 51.

## Aspecte esențiale

- **Utilizarea ilegală a profilurilor subminează încrederea** în autoritățile de aplicare a legii și de gestionare a frontierelor și poate duce la deteriorarea relațiilor cu comunitățile locale.
- Există **îndoieli cu privire la eficacitatea reală a utilizării profilurilor generice** pentru depistarea infracțiunilor sau în gestionarea frontierelor. Dovezile care atestă că aceste profiluri cresc rata de succes a operațiunilor de aplicare a legii sau de gestionare a frontierelor nu sunt concludente.

### 1.3.1. Impactul asupra încrederii în poliție și în autoritățile de gestionare a frontierelor și asupra bunelor relații cu comunitatea

Cercetările arată că utilizarea profilurilor generice are un impact negativ asupra persoanelor vizate și a comunităților din care fac parte<sup>18</sup>. Caseta de mai jos surprinde răspunsurile unor persoane după ce au fost oprite și percheziționate sau au fost controlate la frontieră.

#### **Exemple**

#### **Impactul acțiunilor de oprire și percheziționare și al controalelor la frontieră asupra persoanelor**

##### **1. Opririle efectuate de poliție – Keskinen, S. et al. (2018)**

*Între 2015 și 2017, Școala Suedeză de Științe Sociale din cadrul Universității din Helsinki a intervievat 185 de persoane cu privire la experiențele lor legate de aplicarea profilurilor etnice. Cercetarea a arătat că, pentru majoritatea respondenților, opririle reprezentaseră experiențe neplăcute, deranjante sau umilitoare. Oferim mai jos câteva extrase din mărturiile respondenților.*

*„Apoi, ceva mai târziu, am fost oprită din nou [...] de un alt polițist, în timp ce mergeam pe stradă cu doi prieteni albi: unul finlandez și celălalt olandez. Și a făcut exact același lucru... mi-a pus aceeași întrebare. M-am enervat*

18 FRA (2017d).

pentru că nu știam de ce sunt oprită doar eu. L-am întrebat și mi-a răspuns că își face doar meseria.” (Femeie între 30 și 40 de ani, de origine africană)

„Odată, mama și fratele meu mergeau prin oraș, când i-a oprit poliția și a cerut să le vadă pașapoartele. Consider că le-a fost aplicat un profil etnic. Și atunci fratele meu [a spus în finlandeză]: «Nu avem pașapoartele, nu le purtăm cu noi tot timpul». Când polițiștii au văzut că vorbește fluent finlandeză, au zis: «Lăsați, nu mai e nevoie». M-am înfuriat, pentru că știu că utilizarea profilurilor etnice este ilegală, dar mama și fratele meu nu știau. Așa că, vă dați seama, am simțit că au fost tratați abuziv. Și deci eram foarte supărată. La un moment dat le-am spus că e ilegal ce li s-a întâmplat, fiindcă, evident, și-au dat seama că au fost opriți pentru că [...] nu arată a finlandezi, ci a străini.” (Femeie între 20 și 30 de ani, somalo-finlandeză)

„Mereu se uită după persoane cu aceeași descriere. Chiar mă întreb – deci ei de 11 ani caută aceeași persoană, care mereu le scapă? Păi atunci, băieți, înseamnă că nu prea faceți treabă bună, fiindcă descrierea pe care o au [cei care se ocupă de controlul la frontieră] este mereu similară, iar eu de fiecare dată corespund descrierii [râde].” (Bărbat între 30 și 35 de ani, africano-finlandez)

Pentru informații suplimentare, a se vedea Keskinen, S. et al. (2018), *The Stopped – Ethnic Profiling in Finland*.

## **2. Controalele la frontieră – FRA (2014a și 2014b)**

„Înțeleg de ce m-a oprit [polițistul de frontieră], dar nu era nevoie să mă trimită aici [verificarea în linia a doua/secția de poliție] sau să mă trateze ca pe un infractor. Fac asta cu toți est-europenii.”

(Pasager din Serbia, bărbat, intervievat la aeroportul din Frankfurt)

Întrebare: „Cum considerați că ați fost tratat la verificarea din prima linie?”

Răspuns: „Consider că nu am fost bine tratat. A fost umilitor. S-a purtat urât cu mine. Doar mi-a luat pașaportul, s-a uitat la el și apoi i-a chemat pe cei de la Imigrări. Mi-a pus câteva întrebări și a ridicat vocea, dar n-am înțeles nimic. M-au scos afară din coadă, dar nu m-au respectat, și m-au speriat.”

Î: „De ce v-ați simțit speriat sau umilit?”

R: „Pentru că nu știam ce o să se întâmple și ei nu-mi explicau nimic. Și erau o mulțime de oameni în jur, iar polițistul vorbea cu ceilalți polițiști fără să vorbească și cu mine. Apoi a trebuit să aștept și tot nu știam de ce sunt acolo.”

(Pasager din Angola, bărbat, intervievat la aeroportul Schiphol)

„Chiar îi înțeleg [...] pe polițiștii de frontieră. Și pentru ei e foarte greu, să lucreze în cabină atâtea ore! De asta, din când în când, atitudinea lor mai lasă de dorit, de exemplu se răstesc la oamenii ca noi.” (Bărbat, cetățean turc, șofer de camion care trece frecvent granița, Kipi)

Suma acestor experiențe individuale se poate traduce în efecte de grup negative<sup>19</sup>. Acest lucru poate contribui la o deteriorare accentuată a relației dintre agenții de poliție și polițiștii de frontieră, pe de o parte, și membrii comunităților minoritare supuse unui număr mare de acțiuni de oprire și percheziționare sau unor controale mai amănunțite la frontieră.

### Studiu de caz

#### **Rolul acțiunilor de oprire și percheziționare în dezordinea publică (Regatul Unit 2011 și Franța 2005)**

În urma revoltelor care au avut loc în mai multe orașe importante din Regatul Unit în august 2011, London School of Economics și ziarul The Guardian au intervievat 270 de protestatari cu privire la motivul participării la revolte. Studiul a constatat că neîncrederea și antipatia față de poliție reprezentau un factor semnificativ și că „[c]ele mai frecvente plângeri se refereau la experiența zilnică a oamenilor cu acțiunile poliției, mulți exprimând o profundă frustrare față de modul în care erau vizate persoanele din comunitățile lor de acțiunile de oprire și percheziționare”.

*Pentru mai multe informații, a se vedea London School of Economics (2011).*

O dinamică similară a fost identificată și în alte state membre ale UE. În Franța, revoltele din noiembrie 2005 s-au dovedit a fi declanșate de un eveniment în cadrul căruia au murit accidental doi tineri minoritari, aparent

<sup>19</sup> Organizația Națiunilor Unite (ONU) (2007), punctul 57.



în timp ce erau urmăriți de poliție (a se vedea Jobard, 2008 și Body-Gendrot, 2016).

*Pentru mai multe informații, a se vedea Hörnqvist (2016).*

În contextul celor de mai sus, utilizarea profilurilor poate duce la creșterea nivelului de ostilitate în cursul altor întâlniri dintre oameni și poliție sau alte organe de aplicare a legii. O mai mare ostilitate sporește riscul ca întâlnirile de rutină să degereze în agresiune și conflict, ridicând probleme de siguranță atât pentru agenți, cât și pentru membrii comunității.

Într-un sens mai larg, cercetările recente arată că oamenii opriți, arestați, condamnați sau încarcerați tind să se țină departe și de alte servicii publice, din afara sistemului de justiție penală, precum cele de sănătate, ocupare a forței de muncă și învățământ<sup>20</sup>. Fără a submina motivele legitime care duc la arestarea persoanelor condamnate, ar trebui avut în vedere faptul că excluderea unor segmente deja marginalizate ale populației din astfel de instituții poate fi un obstacol în calea incluziunii sociale și a integrării grupurilor minoritare.

### **În obiectiv: concluziile sondajului EU-MIDIS II efectuat de FRA**

În 2015 și 2016, FRA a cules informații de la peste 25 500 de respondenți aparținând unor minorități etnice diferite și provenite din diverse contexte de imigrație, în cele 28 de state membre ale UE.

#### ***Ce informații au fost colectate?***

În domeniul creării de profiluri, respondenții au fost întrebați dacă consideră că au fost opriți de poliție din cauza apartenenței la comunitatea imigranților sau la o minoritate etnică, precum și despre modul în care au fost tratați de polițiști, inclusiv eventualele experiențe de agresiune fizică din partea acestora. Sondajul nu a întrebat despre experiențele avute cu agenții de gestionare a frontierelor.

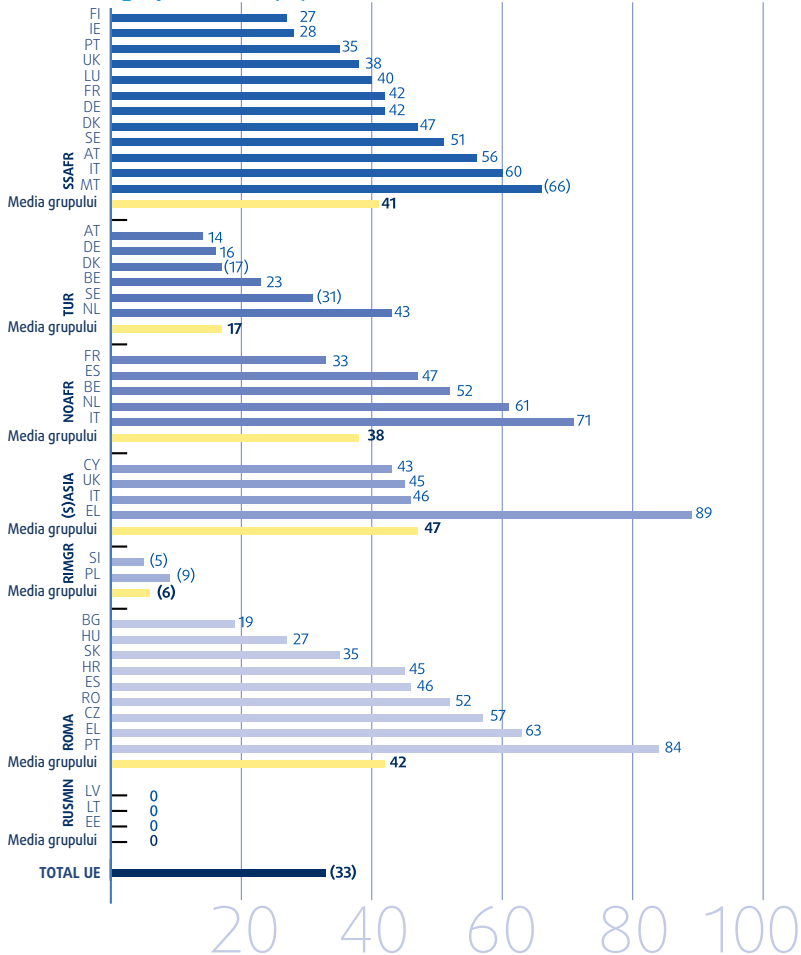
20 Brayne, S. (2014), p. 367-391.

### ***Ce indică rezultatele?***

**Opririle și originea etnică:** Rezultatele arată că 26 % din totalul respondenților din cadrul UE-MIDIS II au fost opriți de poliție în cei cinci ani anteriori sondajului. Dintre cei opriți în ultimii cinci ani anteriori sondajului, 33 % au spus că acest lucru s-a datorat originii lor etnice și de imigrație.

**Percepția de discriminare:** În medie, aproape unul din doi respondenți cu origini asiatice (47 %), subsahariene (41 %) și nord-africane (38 %) care a fost oprit în acest interval de timp a spus că a fost oprit din cauza faptului că este imigrant sau aparține unei etnii minoritare. În mod similar, dintre respondenții romi opriți, aproape unul din doi (42 %) considera că motivul opririi fusese originea sa etnică. În schimb, procentul este mult mai mic în rândul respondenților cu origini turce care au fost opriți (17 %) (a se vedea figura 3).

**Figura 3: Cele mai recente opriri ale poliției percepute ca motivate de profiluri etnice printre persoanele oprite în cei cinci ani anteriori sondajului UE-MIDIS II, pe state membre ale UE și pe grupuri vizate (%)** (a) (b) (c) (d)



Note: (a) Din totalul respondenților care au fost oprite de poliție în cei cinci ani anteriori sondajului (n=6 787); rezultate ponderate.

- (b) *Rezultatele bazate pe un număr mic de răspunsuri sunt mai puțin fiabile din punct de vedere statistic. De aceea, rezultatele bazate pe 20-49 de observații neponderate dintr-un total de grup sau bazate pe celule cu mai puțin de 20 de observații neponderate sunt notate între paranteze. Rezultatele bazate pe mai puțin de 20 de observații neponderate dintr-un total de grup nu sunt publicate.*
- (c) *Întrebări: „În ultimii cinci ani în care ați trăit în [ȚARA] (sau de când vă aflați în [ȚARA]), ați fost vreodată oprit(ă), percheziționat(ă) sau interogată(ă) de poliție?”; „Credeti că ULTIMA DATĂ când ați fost oprit(ă) acest lucru s-a datorat originii dumneavoastră etnice sau statutului de imigrant?”*
- (d) *Acronimele prin care sunt desemnate grupurile vizate se referă la imigrații din [țara/regiunea] și la descendenții acestora: TUR = Turcia, SSAFR = Africa subsahariană, NOAFR = Africa de Nord, SASIA = Asia de Sud, ASIA = Asia, ROMA = minoritatea romă.*

Sursa: FRA, 2017b.

**Respectul:** Constatările arată că majoritatea (59 %) respondenților care au fost opriți de poliție în cei cinci ani anteriori sondajului consideră că au fost tratați cu respect (25 % „tratament foarte respectuos”, 34 % „tratament destul de respectuos”). Unul din patru respondenți (24 %) a spus că modul în care a fost tratat de poliție nu a fost „nici respectuos, nici lipsit de respect”. În același timp, 17 % au spus că poliția i-a tratat fără respect (8 % „tratament destul de nerespectuos” și 9 % „tratament foarte nerespectuos”). Respondenții romi și cei cu origini nord-africane care au fost opriți au indicat un comportament lipsit de respect al poliției în timpul celei mai recente opriri (25 % și, respectiv, 21 %) – mai des decât alte grupuri vizate.

*Pentru mai multe informații, a se vedea FRA (2017b).*

### **În obiectiv: importanța și utilitatea colectării de date cu privire la opririle efectuate de poliție**

Dintre cele 28 de state membre ale UE, Regatul Unit este în prezent singurul în care colectarea datelor privind opririle efectuate de poliție include în mod sistematic informații despre originea etnică a persoanelor oprite (a se vedea și secțiunile 2.2.5 și 2.3.1).

Datele colectate măsoară „rata de oprire și percheziționare” pentru diferite grupuri etnice din Anglia și Țara Galilor. Categoriile etnice utilizate sunt cele enumerate în recensământul din 2001 al Regatului Unit. Acest recensământ a identificat 16 categorii, care au fost reunite în cinci grupuri mari:

- albi: englezi/galezi/scoțieni/nord-irlandezi/britanici; irlandezi; și orice persoane de altă origine albă;
- grupuri etnice mixte/multiple: caraibieni de origine albă și neagră; africani de origine albă și neagră; albi asiatici; și persoane de orice altă origine etnică mixtă/multiplă;
- asiatici/britanici asiatici: indieni; pakistanezi; persoane din Bangladesh; și de orice altă origine asiatică;
- negri/africani/caraibieni/britanici negri: africani; caraibieni; și orice altă origine neagră/africană/caraibiană;
- alte grupuri etnice: chinezi; și alte grupuri etnice.

Datele colectate cu privire la acțiunile de oprire și percheziționare compară numărul de persoane oprite și percheziționate dintr-un anumit grup etnic cu numărul total de persoane din acel grup etnic care locuiesc în zonă, calculând apoi rata la 1 000 de persoane.

Pentru perioada 2016-2017, analiza datelor colectate arată că au existat patru opriri la fiecare 1 000 de albi, comparativ cu 29 de opriri la fiecare 1 000 de negri. Datele indică, de asemenea, că cele mai mari rate s-au înregistrat în rândul celor trei grupuri etnice negre: altă origine neagră (70 de opriri la 1 000 de persoane), negri caraibieni (28 la 1 000 de persoane) și negri africani (19 la 1 000 de persoane).

Fără dovezile aduse de datele dezagregate, este dificil să se demonstreze dacă există diferențe în acțiunile poliției față de anumite grupuri etnice și – în caz afirmativ – dacă aceste diferențe ar putea fi rezultatul utilizării unor profiluri discriminatorii. Date dezagregate sunt disponibile în domeniul public în Anglia și Țara Galilor, defalcate pe unități de poliție. Acest lucru permite identificarea unor practici diferențiate între unități, care fie pot fi explicate ca legitime, fie ar putea fi utilizate pentru a identifica potențialele practici polițienești discriminatorii. De asemenea, se utilizează date la nivel de polițiști individuali, pentru a identifica practicile discriminatorii în activitatea acestora.

Pentru mai multe informații, a se vedea [pagina web privind acțiunile de oprire și percheziționare a Guvernului Regatului Unit \(Gov.uk\)](#), [site-ul Independent Office for Police Conduct](#) și [site-ul cu date deschise despre infracțiuni și activitatea polițienească al Ministerului Afacerilor Interne \(Home Office\)](#). A se vedea și *Regatul Unit (2018)*.

Pentru orientări privind metodologiile de înregistrare, a se vedea *Open Society Justice Initiative (2018b)*.

## Studiu de caz

### **Anchetă privind relațiile dintre poliție și cetățeni în Franța**

În 2016, Avocatul Poporului din Franța (*Défenseur des droits*) a realizat o anchetă privind accesul la drepturi. *Défenseur des droits* îndeplinește și rolul de comisie națională de tratare a plângerilor împotriva poliției. Ancheta a inclus un eșantion reprezentativ de peste 5 000 de persoane.

Prima parte a raportului prezintă rezultatele referitoare la comportamentul autorităților de aplicare a legii. În general, sondajul indică existența unor relații bune între cetățeni și poliție. Marea majoritate a respondenților a declarat că au încredere în poliție (82 %).

Referitor în mod special la controalele de identitate, sondajul arată că majoritatea oamenilor nu se confruntă cu astfel de verificări: 84 % dintre respondenți au declarat că nu au fost verificați în ultimii cinci ani (90 % dintre femei și 77 % dintre bărbați). Cei care au spus că au fost verificați semnalează în general puține cazuri de comportamente care au încălcat etica profesională a forțelor de securitate în timpul celui mai recent control de identitate, cum ar fi: neutilizarea pronumelor de politețe (16 %), brutalitate (8 %) sau insulte (7 %). Pe de altă parte, 29 % au semnalat o atitudine lipsită de politețe, iar mai mult de jumătate (59 %) dintre respondenții care fuseseră verificați au menționat că nu li s-a explicat motivele controlului. În general, controalele de identitate sunt percepute ca fiind mai legitime atunci când forțele de securitate explică motivele verificării.

Datele relevă, de asemenea, că anumite grupuri de persoane indică experiențe mai negative. Bărbații tineri cu vârste cuprinse între 18 și 24 de

ani prezintă o probabilitate de aproape șapte ori mai mare de a fi supuși unor controale de identitate frecvente (adică de peste cinci ori în ultimii cinci ani) decât populația generală, iar bărbații percepuți ca negri sau arabi sunt de 6-11 ori mai afectați de controale de identitate frecvente decât restul populației masculine. Combinând aceste două criterii, rezultă că 80 % din bărbații cu vârsta sub 25 de ani care sunt percepuți ca arabi sau negri au fost verificați cel puțin o dată în ultimii cinci ani (față de 16 % dintre ceilalți respondenți). În comparație cu populația generală, acest grup prezintă o probabilitate de 20 de ori mai mare să fie supus controalelor de identitate.

În plus, bărbații tineri percepuți ca negri sau arabi au semnalat o incidență mai mare a comportamentului problematic în timpul celui mai recent control al identității, de exemplu: nefolosirea pronumelor de politețe (40 % față de 16 % din eșantionul total), insulte (21 % față de 7 % din eșantionul total) sau brutalitate (20 % față de 8 % din eșantionul total). Aceste experiențe negative și frecvența controalelor sunt asociate cu un nivel scăzut de încredere în poliție. De altfel, acest grup a indicat o deteriorare a relațiilor cu poliția.

Ca ultimă constatare, rezultatele arată că puțini dintre respondenții (5 %) care menționează încălcări ale eticii profesionale în timpul controalelor de identitate iau măsuri pentru a denunța această situație. Ei declară, în principal, că nu reclamă experiențele avute deoarece consideră că ar fi inutil.

*Pentru mai multe informații, a se vedea Défenseur des droits (2017).*

În cazul în care unui grup minoritar i se aplică profiluri generice, acest lucru poate, împreună cu alte acțiuni politice stigmatizante, să determine apariția unei percepții negative despre sine în cadrul grupului respectiv. În plus, comunitatea mai largă poate căpăta o percepție negativă cu privire la acel grup. Grupul minoritar poate deveni o „comunitate suspectă”, asociată de către public cu infracționalitatea, ceea ce poate duce la prejudecăți din ce în ce mai mari.

Grupul minoritar poate fi urmărit de un volum disproporționat de resurse ale poliției, lucru care, la rândul său, este de natură să ducă la un număr mai mare de arestări sau de controale la frontieră. Se poate ajunge astfel la o relație de tipul profesiilor autoîmplinite între activitățile polițienești intensive și ratele mai mari de arestare (a se vedea caseta)<sup>21</sup>.

21 Observatorul European al Fenomenelor Rasiste și Xenofobe (2006), p. 54.

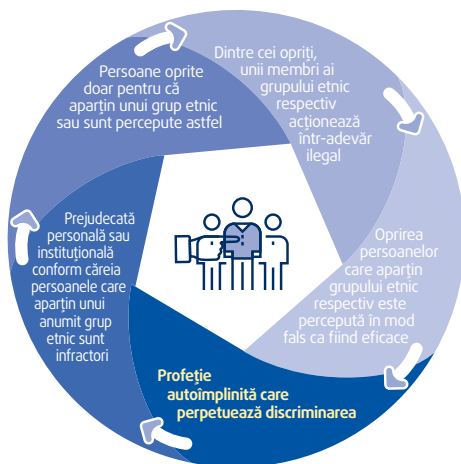
### În obiectiv: riscul de „profeție autoîmplinită”

Când creează profiluri nu pe bază de motive întemeiate, ci pe bază de prejudecăți, polițiștii tind să interpreteze informațiile într-un mod care să le confirme propriile preconcepții. Aceasta se numește „eroare de confirmare” și are loc atunci când prejudecățile creează în mintea polițiștilor așteptarea ca o persoană să acționeze ilegal pe baza rasei sale (reale sau percepute), a originii sale etnice, a genului, a orientării sexuale, a religiei sau a altor criterii protejate. Din cauza acestui tip de eroare, polițiștii cu astfel de prejudecăți tind să se concentreze mai mult pe persoanele care corespund descrierii.

Deoarece este mai probabil să se găsească dovezi ale infracționalității în rândul persoanelor oprite decât la cele care nu sunt oprite, aceste profiluri bazate pe prejudecăți întăresc stereotipurile existente în mintea polițiștilor. Această falsă „dovadă” a faptului că decizia de a opri persoanele respective a fost corectă poartă numele de „profeție autoîmplinită”. Acest tip de profiluri bazate pe prejudecăți sunt discriminatorii, ilegale, ineficiente și perpetuează stereotipurile.

Figura 4 descrie modul în care „profeția autoîmplinită” perpetuează incriminarea persoanelor.

Figura 4: Ciclul profeției autoîmplinite



Sursa: FRA, 2018.



### 1.3.2. Eficacitatea utilizării profilurilor

Există îndoieli și cu privire la eficacitatea utilizării profilurilor bazate pe categorii generice pentru a detecta infracțiunile. Nu este clar dacă profilurile determină într-adevăr creșterea ratei de succes (sau „rata de rezultate pozitive”) a operațiunilor de aplicare a legii.

Unele dovezi sugerează că ratele de oprire a persoanelor nu corespund neapărat ratelor infracționalității înregistrate în rândul diferitelor grupuri etnice sau rasiale (a se vedea caseta). Trebuie precizat că datele privind justiția penală din majoritatea statelor membre ale UE nu oferă o imagine de ansamblu asupra parcursului unei cauze individuale prin sistemul de justiție penală. Ca atare, nu se poate stabili dacă o arestare se soldează cu urmărire penală și condamnare.

#### Studiu de caz

##### **Schimbarea modelelor de percheziționare duce la creșterea „ratei de succes” (1998-2000, SUA)**

În 1998, 43 % din persoanele percheziționate de autoritățile vamale din SUA erau negri și latino-americani, ceea ce reprezintă un procent mult mai ridicat decât proporția acestor persoane în rândul călătorilor. Un număr deosebit de mare de percheziții, inclusiv percheziții corporale invazive și scanare cu raze X, vizau femei latino-americane și negrese suspectate a fi „cărăuși de droguri”, conform unui profil care se baza în mare măsură pe cetățenie și etnie. Ratele de succes ale acestor percheziții erau mici în toate grupurile: 5,8 % în cazul „albilor”, 5,9 % în cazul „negrilor” și 1,4 % în cazul „latino-americanilor”. O rată deosebit de mică se înregistra în cazul femeilor latino-americane, care erau de altfel cele mai puțin înclinate să transporte droguri asupra lor sau în corp. În 1999, autoritățile vamale din SUA și-au schimbat procedurile, eliminând rasa din rândul factorilor care trebuie luați în considerare când se efectuează opriri. În schimb, s-au introdus tehnici de observație axate pe comportamente precum nervozitatea și pe neconcordanțele din explicațiile pasagerilor, s-au utilizat mai multe date operative și s-a aplicat o supraveghere mai atentă a deciziilor de oprire și percheziționare. Până în 2000, disparitățile rasiale întâlnite în perchezițiile vamale aproape au dispărut. Numărul perchezițiilor efectuate a scăzut cu 75 %, iar rata de succes s-a îmbunătățit de la puțin sub 5 % la peste 13 % și a devenit aproape egală pentru toate grupurile etnice.

*Pentru mai multe informații, a se vedea Harris (2002), SUA (2000).*

### **Ineficiența profilurilor ilegale (2007-2008, Ungaria)**

Cercetările efectuate în Ungaria au arătat că romii erau vizați într-o măsură disproporționată de controalele de identitate. Aproximativ 22 % din totalul persoanelor verificate de poliție aparțineau comunității rome, în condițiile în care proporția de romi în cadrul populației era de aproximativ 6 %. Numărul disproporționat de mare al controalelor de identitate asupra persoanelor de etnie romă nu se reflecta în dovezi ale unui comportament ilegal: 78 % din controalele de identitate ale persoanelor de etnie romă nu au dus la întreprinderea vreunei acțiuni de către poliție, iar 19 % au depistat doar infracțiuni minore\* (față de 18 % din controalele efectuate asupra populației generale). În plus, s-au înregistrat rate de arestare similare pentru comunitatea de romi și pentru populația generală.

*Pentru mai multe informații, a se vedea Tóth, B.M. și Kádár, A. (2011).*

\* „Infracțiunile minore sunt infracțiuni cvasi-penale, a căror gravitate nu atinge nivelul penal (adică nu sunt prevăzute în Codul penal). Ele variază de la infracțiuni care se pedepsesc cu 60 de zile de închisoare, cum sunt prostituția sau amenințările fizice, la infracțiuni care se pedepsesc prin măsuri mai puțin severe (de exemplu amendă, confiscarea bunurilor sau interzicerea intrării la anumite evenimente). Exemple de astfel de infracțiuni sunt furturile mărunte sau încălcările legislației circulației.” A se vedea Kádár, A., Körner, J., Moldova, Z. și Tóth, B. (2008), p. 23.

Există neclarități și cu privire la motivele pentru care sunt oprite anumite persoane. Un studiu din Regatul Unit a arătat că „[o] proporție alarmantă de 27 % (2 338) din rapoartele examinate referitoare la acțiuni de oprire și percheziționare [...] nu conțin motive rezonabile pentru percheziționarea persoanelor, chiar dacă multe dintre aceste rapoarte au fost aprobate în prealabil de supraveghetori”<sup>22</sup>. Potrivit studiului, acest lucru sugerează că „este posibil ca forțele de poliție să nu respecte pe deplin obligația de tratament egal în sectorul public, care le impune să țină seama în mod corespunzător de necesitatea de a elimina discriminarea ilegală și de a promova egalitatea de șanse, de a încuraja bunele relații și, în acest scop, de a colecta, analiza și publica în mod adecvat date care să demonstreze că dispun de suficiente informații pentru a înțelege efectele activității lor.”

<sup>22</sup> Regatul Unit, Her Majesty's Inspectorate of Constabulary (HMIC) (2013), p. 6.

# 2

## Utilizarea legală a profilurilor: principii și practică

Acest capitol se concentrează asupra utilizării profilurilor de către polițiștii din prima linie, în special pentru acțiuni de oprire și percheziționare, și de către polițiștii de frontieră, în special pentru trimiterea către verificări la frontieră „în linia a doua”. Sunt explicate principalele principii și practici care pot contribui la reducerea riscului de utilizare ilegală a profilurilor. Aceste măsuri pot fi luate atât la nivel de conducere, cât și la nivel operațional. Sunt luate în considerare diferitele contexte juridice și practice ale acțiunilor de oprire și percheziționare și ale controalelor la frontieră.

În contextul gestionării frontierelor, Codul frontierelor Schengen [Regulamentul (UE) 2016/399]<sup>23</sup> stabilește norme unificate care reglementează controalele la frontierele externe ale UE. Aceasta înseamnă că unele dintre principiile prezentate în capitolul de față – de exemplu, cu privire la informațiile care trebuie furnizate resortisanților țărilor terțe supuși unei verificări în linia a doua – sunt prescrise prin lege și obligatorii pentru statele membre. În plus, Frontex are un rol important în promovarea unui standard constant ridicat al controalelor la frontieră. În special, Regulamentul privind Poliția de frontieră și garda de coastă la nivel european din 2016 impune statelor membre să urmeze programele de bază comune elaborate de Frontex în formarea polițiștilor de frontieră. Publicată în 2012, programa comună de bază cuprinde o componentă referitoare la drepturile fundamentale, care se referă și la profiluri (a se vedea secțiunea 2.2.3 privind formarea specifică).

23 Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2016 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen), JO L 77, 23 martie 2016.

### **În obiectiv: criteriile de verificare în linia a doua la frontieră**

Natura sistematică a controalelor la frontieră face ca fiecare călător să fie supus unei verificări de bază în prima linie, în cadrul căreia sunt verificate documentele de călătorie și orice alte condiții de intrare. În plus, unii călători pot fi trimiși către o verificare suplimentară în linia a doua. Motivele pot fi variate: o potrivire într-o bază de date, un document de călătorie suspect, potrivirea cu un profil de risc sau prezentarea unui comportament suspect.

În timpul verificării din prima linie, polițiștii de frontieră pot utiliza informații obținute prin compararea datelor din documentul de călătorie cu citire optică (care include identificatori biometrici) cu datele stocate în baze de date naționale, UE și internaționale, cum ar fi Sistemul de informații Schengen, Sistemul de informații privind vizele și bazele de date ale Europol și Interpol. În practică, trimiterea către o verificare în linia a doua este deseori urmarea unei potriviri în una dintre bazele de date.

Însă o persoană poate fi trimisă către verificările din linia a doua și din alte motive, de exemplu dacă corespunde unui profil de risc sau dacă polițistul are alte suspiciuni cu privire la persoana respectivă. Catalogul Schengen al UE prevede că, pe lângă efectuarea de controale la frontieră în conformitate cu Codul frontierelor Schengen, obiectivul verificărilor în prima linie ar trebui să fie acela de a crea profilul pasagerilor și de a selecta persoanele suspecte pentru verificări amănunțite în linia a doua.\* Prin urmare, polițiștii de frontieră trebuie să evalueze o combinație de alți indicatori și criterii pentru a stabili dacă o persoană ar putea încerca să intre în țară neregulamentară, să prezinte un risc de securitate sau, de exemplu, să fie victima traficului de persoane. Indiferent dacă aplică un profil de risc specific deja existent sau nu, în aceste situații polițiștii de frontieră utilizează profiluri.

Din nevoia de a fluidiza circulația călătorilor, polițiștii de frontieră au puțin timp la dispoziție pentru a evalua cu obiectivitate dacă să supună pe cineva unei verificări în linia a doua. Informațiile de la Frontex arată că agenții din statele membre ale UE au în medie doar 12 secunde pentru a decide dacă ar trebui să selecteze o persoană pentru o verificare ulterioară.\*\* Acest lucru creează o presiune semnificativă, pentru că trebuie să ia rapid decizia corectă.

\* *Consiliul Uniunii Europene (2009), Recomandarea 43.*

\*\* *Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (Frontex) (2015).*

Principiile și instrumentele practice din acest capitol oferă informații menite să încurajeze dezbaterile și întreprinderea de acțiuni care să ajute polițiștii și organizațiile lor în sens mai larg să își mențină activitățile de utilizare a profilurilor în limitele legii. Cele trei principii esențiale discutate sunt următoarele:

- respectarea demnității persoanelor;
- asigurarea faptului că profilurile se bazează pe criterii rezonabile și obiective;
- garantarea răspunderii.

Fiecare principiu este corelat cu importanța fundamentală a asigurării faptului că agenții de poliție și polițiștii de frontieră acționează în limitele legii atunci când crează și utilizează profiluri.

## 2.1. Respectarea demnității persoanelor

### Aspecte esențiale

- Asigurarea unei **interacțiuni de bună calitate** nu elimină în mod automat crearea de profiluri discriminatorii, însă poate face ca interacțiunea să aibă mai mult succes și poate reduce impactul negativ potențial al acțiunilor de oprire și percheziționare. În gestionarea frontierelor, conduita profesională și respectuoasă este o obligație legală.
- În general, o **atitudine profesionistă și respectuoasă** face ca persoana vizată să fie mai mulțumită de interacțiunea respectivă.
- **Explicarea motivelor opririi** contribuie la creșterea încrederii în operațiunile agenților de poliție și de gestionare a frontierelor și reduce impresia că profilurile sunt discriminatorii.
- Respectul și politețea **nu scuză niciodată realizarea unor verificări la frontieră sau a unor acțiuni de oprire și percheziționare care sunt ilegale.**

Respectarea demnității persoanelor nu este doar un drept fundamental în sine, ci și un principiu de bază al operațiunilor polițienești și de gestionare a frontierelor. În operațiunile din prima linie au o importanță crucială atât modul în care agenții de poliție și polițiștii de frontieră vorbesc și interacționează cu persoanele oprite, cât și informațiile pe care le furnizează.

Ar trebui să ne amintim întotdeauna că, indiferent cât de politicoși și de profesioniști sunt polițiștii, tratarea persoanelor în mod diferențiat este, totuși, o experiență intruzivă care trebuie să se bazeze întotdeauna pe motive legale. Impresia că se utilizează profiluri discriminatorii este determinată și de frecvența și numărul interacțiunilor cu poliția și cu autoritățile de gestionare a frontierelor. Acest lucru subliniază importanța asigurării faptului că există întotdeauna motive obiective și rezonabile pentru oprire.

### **Ce spun standardele?**

„Verificările la frontieră ar trebui să fie efectuate astfel încât demnitatea umană să fie respectată pe deplin. Controlul la frontieră ar trebui să fie efectuat într-un mod profesionist și respectuos și să fie proporțional cu obiectivele urmărite.”

*Considerentul 7 din Codul frontierelor Schengen*

„Toți călătorii au dreptul să fie informați cu privire la natura controlului și au dreptul la tratament profesional, prietenos și amabil, în conformitate cu dreptul internațional, dreptul Uniunii și dreptul național aplicabil.”

*Secțiunea 1.2 din Manualul practic pentru polițiștii de frontieră (Manualul Schengen)*

„Personalul poliției va acționa cu integritate și respect față de public și cu o atenție deosebită pentru situația persoanelor care aparțin unor grupuri deosebit de vulnerabile.”

*Recomandarea 44 din Codul european de etică al poliției*

Nu este întotdeauna ușor pentru agenții de poliție și polițiștii de frontieră să fie amabili și să ofere informații detaliate în situații tensionate și dificile. Dovezile arată însă că adoptarea unui ton respectuos crește semnificativ nivelul de satisfacție cu privire la interacțiune<sup>24</sup>. **Figura 5** ilustrează câteva elemente ale unei interacțiuni respectuoase.

24 FRA (2014b).

Figura 5: Trei elemente ale unei interacțiuni respectuoase



Sursa: FRA, 2018.

Unele elemente ale controalelor la frontieră sunt reglementate de Codul frontierelor Schengen, cum ar fi cerința de a efectua controale în mod profesionist și respectuos sau de a oferi informații cu privire la scopul și procedura verificării [Codul frontierelor Schengen, considerentul 7, articolul 7 și articolul 8 alineatul (5)]. Utilizarea unui limbaj comun, pe de altă parte, nu este o cerință absolută în contextul gestionării frontierelor, din cauza naturii inerent variate a traficului de frontieră. Totuși, Codul frontierelor Schengen impune statelor membre să încurajeze polițiștii de frontieră să învețe limbile străine necesare pentru îndeplinirea atribuțiilor lor [articolul 16 alineatul (1)]. Catalogul Schengen, care conține un set de recomandări și de bune practici pentru controlul frontierelor externe, recomandă ca polițiștii de frontieră să aibă capacitatea de a comunica în limbi străine în legătură cu sarcinile lor zilnice. Acesta menționează cunoașterea satisfăcătoare a limbilor țărilor învecinate, precum și a altor limbi, în funcție de natura traficului de frontieră. În mod ideal, în fiecare schimb ar trebui incluși polițiști cu cunoștințe lingvistice adecvate<sup>25</sup>.

Lipsa de considerație și de respect manifestată în timpul opririlor de către poliție poate avea efecte directe asupra eficacității activității polițienești (a se vedea secțiunea 1.3.2). Codul de practică al Legii privind probele polițienești și penale, elaborat în Regatul Unit, prevede următoarele: „Toate opririle și perchezițiile trebuie efectuate cu amabilitate, considerație și respect față de persoana în cauză. Acest lucru are un impact semnificativ asupra încrederii publicului în poliție. Trebuie depuse toate

25 Consiliul Uniunii Europene (2009), Recomandările 27 și 41.

eforturile rezonabile pentru a reduce la minimum stânjeneala pe care o poate resimți persoana percheziționată.”<sup>26</sup>

Unele componente importante ale respectării demnității, cum ar fi furnizarea de explicații pentru oprire și asigurarea faptului că persoanelor li se oferă posibilitatea de a-și exprima punctul de vedere, reprezintă elemente de bază ale procedurilor polițienești și de gestionare a frontierelor. Procesele-verbale de oprire și percheziționare pot oferi un mod structurat de furnizare a acestor informații (a se vedea secțiunea 2.3.1).

În contextul gestionării frontierelor, formularele tip sunt un instrument util pentru informarea călătorilor despre scopul și procedura de verificare în linia a doua. Ele pot facilita comunicarea cu călătorii, dacă sunt distribuite împreună cu explicații orale suplimentare care să le completeze atunci când este necesar. Codul frontierelor Schengen impune ca persoanelor supuse unui control în linia a doua să li se ofere informații scrise cu privire la scopul și procedura controlului, într-o limbă pe care o înțeleg sau despre care se presupune în mod rezonabil că o înțeleg. Informațiile trebuie:

- să fie disponibile în toate limbile oficiale ale UE și în limbile țărilor limitrofe țării în cauză;
- să precizeze posibilitatea călătorului de a solicita numele sau numărul matricol al polițistului care efectuează verificarea, numele punctului de trecere a frontierei și data trecerii frontierei.

Aceste elemente ale unei interacțiuni respectuoase, care țin de abilitățile interpersonale și de comunicare, sunt mai greu de prevăzut în procedurile de operare și pot necesita investiții suplimentare în cursuri de formare. Polițistului îi poate fi greu să adopte un ton pozitiv în cadrul interacțiunii din cauza:

- unor abilități de comunicare deficitare;
- incapacității de a explica motivul acțiunii; și

---

26 Regatul Unit, Home Office (2014a), secțiunea 3.1.



- incapacității de a depăși prejudecățile personale și instituționale și stereotipurile negative, precum și ostilitățile acumulate în cadrul anumitor grupuri din cadrul comunității.

## 2.2. Motive rezonabile și obiective

### Aspecte esențiale

- Acțiunile agenților de poliție și de gestionare a frontierelor care se bazează pe informații specifice și actualizate tind să fie mai obiective.
- Pentru a fi legale, acțiunile de oprire și percheziționare și trimerile către verificări în linia a doua la frontieră trebuie să se bazeze pe **motive rezonabile și obiective de suspiciune**. O „presimțire” nu constituie un motiv rezonabil sau obiectiv pentru a opri și percheziționa o persoană sau pentru a trimite o persoană către verificări în linia a doua la frontieră.
- Caracteristicile protejate, cum sunt rasa, originea etnică, genul sau religia, se pot regăsi printre factorii pe care autoritățile de aplicare a legii și polițiștii de frontieră îi iau în considerare în exercitarea competențelor lor, dar **nu pot să constituie singurul sau principalul motiv pentru a aplica unei persoane tratament diferențiat**.
- Profilurile bazate exclusiv sau în principal pe unul sau mai multe dintre criteriile protejate reprezintă discriminare directă și sunt ilegale.

Obiectivitatea este un principiu important al activității polițienești și de gestionare a frontierelor. În contextul utilizării profilurilor, persoanele ar trebui oprite și percheziționate sau supuse verificărilor în linia a doua la frontieră doar pe baza unor motive rezonabile și obiective de suspiciune. Pot reprezenta justificări obiective comportamentul persoanei în cauză, anumite informații specifice sau circumstanțe care asociază persoana cu o activitate ilegală suspectată.

Pentru asigurarea obiectivității în activitatea legată de profiluri este necesar:

- să se evite prejudecățile, de exemplu prin orientări clare și formare specifică; și
- să se utilizeze în mod eficient informațiile și datele operative.

## 2.2.1. Evitarea prejudecăților

Codul european de etică al poliției oferă orientări referitoare la conduita polițiștilor în domenii precum acțiunea și intervenția polițienească, răspunderea polițiștilor și supravegherea polițienească<sup>27</sup>. În el se subliniază principiul general conform căruia: „[p]oliția trebuie să își desfășoare activitatea în mod corect, ghidându-se în special după principiul imparțialității și al nediscriminării.”<sup>28</sup>

Aplicarea unui tratament diferențiat persoanelor folosind *ca factor unic sau determinant* rasa acestora, originea etnică, genul, orientarea sexuală, religia, un handicap (real sau perceput) sau alte criterii interzise încalcă drepturile fundamentale. De asemenea, aceasta poate avea consecințe negative semnificative atât pentru autoritățile publice, cât și pentru comunități (a se vedea [secțiunea 1.3](#)).

Profilurile discriminatorii pot reflecta atât prejudecăți individuale, cât și instituționale. Stereotipurile și comportamentul discriminatoriu față de anumite persoane pot apărea nu doar ca urmare a unor prejudecăți personale, ci și a unor practici specifice din cadrul autorităților de aplicare a legii și de gestionare a frontierelor. Creșterea transparenței procedurilor și practicilor instituționale poate contribui la combaterea discriminării și a perpetuării stereotipurilor.

Prejudecățile profunde pot fi dificil de recunoscut. Este posibil ca agenții de poliție și polițiștii de frontieră să creadă că selectează persoanele pe baza unor motive rezonabile și obiective (precum comportamentul), deși deciziile lor sunt de fapt reflexia unor prejudecăți.

Când efectuează opriri, polițiștii asociază adesea motivul selectării unei anumite persoane de o „presimțire” sau „intuiție”. Aceasta se bazează, probabil, pe o combinație între expertiză și experiențele anterioare, dar poate reflecta și o prejudecată conștientă sau subconștientă a polițistului. Pentru a evita folosirea unor profiluri ilegale, polițiștii ar trebui să analizeze dacă decizia lor este justificată de informații obiective. O „presimțire” nu constituie un motiv rezonabil sau obiectiv pentru a opri și percheziționa o persoană sau pentru a trimite o persoană către verificări în linia a doua la frontieră.

27 Consiliul Europei, Comitetul de Miniștri (2001), [Recomandarea Rec\(2001\)10 a Comitetului de Miniștri către statele membre cu privire la Codul european de etică al poliției](#), 19 septembrie 2001.

28 *Ibid.*, punctul 40.

## 2.2.2. Orientări clare pentru polițiști

Este deosebit de important să se furnizeze orientări practice, ușor de înțeles și de aplicat agenților de aplicare a legii și polițiștilor de frontieră, care să îi ajute să evite activitățile ilegale legate de profiluri. Orientările pot lua mai multe forme: pot fi anexate actelor legislative, emise chiar de autoritățile de aplicare a legii și de gestionare a frontierelor sau furnizate zilnic de către superiori. Utilizarea unor exemple din viața reală pentru a arăta ce trebuie făcut în anumite situații este de regulă mai eficientă decât explicarea regulilor și a procedurilor.

Ofițerii aflați în funcții de conducere trebuie să informeze personalul că rasa, originea etnică, genul, orientarea sexuală, religia (reale sau percepute) sau alte criterii interzise de discriminare nu pot constitui factorul determinant pentru inițierea unei acțiuni de aplicare a legii sau de gestionare a frontierelor împotriva unei persoane. Clarificarea situațiilor și a modurilor în care pot fi utilizate caracteristicile personale poate contribui la reducerea riscului de interpretări diferite, precum și a dependenței de stereotipuri și prejudecăți. Orientările ar trebui să vizeze și aspectele legate de protecția vieții private și a datelor.

Tabelul 3 arată câteva dintre tipurile de orientări care pot fi utilizate și caracteristicile importante care ar trebui luate în considerare.

**Tabelul 3: Tipuri și caracteristici ale orientărilor și implicarea părților interesate**

Tipurile de orientări	Caracteristici ale orientărilor	Implicarea părților interesate
<ul style="list-style-type: none"> <li>• proceduri standard de operare</li> <li>• coduri de conduită</li> <li>• îndrumare regulată din partea superiorilor</li> </ul>	<ul style="list-style-type: none"> <li>• detaliate și specifice</li> <li>• cuprinzând toate activitățile în care pot apărea profiluri bazate pe prejudecăți:</li> <li>• oprire și percheziționare</li> <li>• arestări</li> <li>• controale la frontieră</li> <li>• folosirea forței etc.</li> </ul>	<ul style="list-style-type: none"> <li>• elaborarea de orientări împreună cu alte părți interesate</li> <li>• punerea orientărilor la dispoziția comunităților</li> <li>• încurajarea comunităților să-și spună opinia cu privire la orientări</li> </ul>

Sursa: FRA, 2018.

## Studiu de caz

### Cod de bune practici și abordarea prin „ambasadori” (poliția neerlandeză)

Poliția neerlandeză a elaborat, împreună cu organizații ale societății civile precum Amnesty International, un cod de bune practici care descrie cele patru principii ale unei acțiuni de oprire profesioniste:

- ☑ selecția legitimă și justificabilă a persoanelor;
- ☑ explicarea motivului care stă la baza acțiunii de oprire și percheziționare;
- ☑ utilizarea unui mod de comunicare profesional;
- ☑ polițiști care reflectează asupra practicilor lor și își oferă feedback reciproc.

Practicile care nu sunt percepute ca problematice sunt greu de schimbat – de exemplu practica atitudinii proactive a polițiștilor, care poate duce la crearea de profiluri etnice. Poliția din Amsterdam a realizat o abordare ascendentă, în cadrul căreia în echipe sunt implicați polițiști de teren (ambasadori), asistați de superiorii lor și de formatori. Primul pas constă în sensibilizare prin prezentarea și discutarea impactului opririlor proactive asupra persoanelor vizate și prin introducerea unui cadru alternativ, corect și eficient. Al doilea pas constă în îmbrățișarea acestei noi practici de către polițiști.

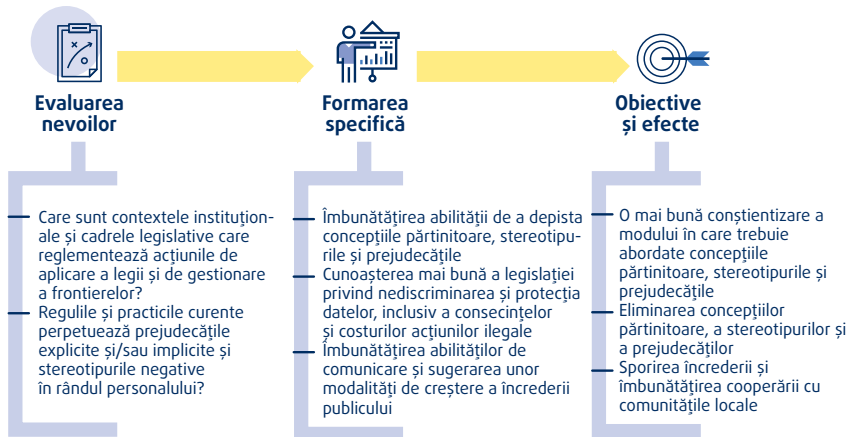
*Pentru mai multe informații în limba neerlandeză, a se vedea [site-ul poliției](#).*

## 2.2.3. Formare specifică

Formarea agenților de poliție și a polițiștilor de frontieră este un alt instrument important pentru reducerea la minimum a riscului de utilizare ilegală a profilurilor. Există multe tipuri diferite de formare, care pot interveni în diferite etape ale carierei unui ofițer, printre care: formarea inițială a recruților, formarea la locul de muncă și dezvoltarea profesională continuă. Indiferent de tip, modulele de formare ar trebui să ia în considerare cultura organizațională și să ofere cursuri care să includă strategii de înlocuire și contracarare a stereotipurilor. La final, este esențială evaluarea impactului formării pentru a monitoriza modul în care a contribuit la schimbarea percepției polițiștilor și la îmbunătățirea acțiunilor lor practice, precum și pentru a identifica lipsurile care pot necesita formare suplimentară. **Figura 6** evidențiază câteva aspecte care trebuie luate în considerare la elaborarea formării specifice.

Anumite tipuri de formare pentru agenții de aplicare a legii sau polițiștii de frontieră sunt deja bine dezvoltate în unele țări, cum ar fi „formarea în materie de diversitate” și „formarea în materie de sensibilitate culturală”. Formarea în materie de diversitate încearcă să abordeze sentimentele personale cu privire la originea etnică, diferențe și stereotipuri și modul în care acestea ne influențează viața de zi cu zi. Însă unele cursuri în materie de diversitate nu discută neapărat subiectul discriminării. Unele studii susțin că formarea culturală și în materie de diversitate poate chiar să aducă în prim plan și să întărească diferențele, sporind utilizarea stereotipurilor în loc să o reducă<sup>29</sup>. Formarea în materie de sensibilitate culturală (spre deosebire de formarea generală în materie de diversitate) are ca scop educarea agenților și a ofițerilor de poliție cu privire la cultura unor grupuri etnice specifice cu care se întâlnesc frecvent, dar cu care nu sunt familiarizați. Această formare abordează acțiunile recomandate și nerecomandate și oferă îndrumări despre ce înseamnă politețea din perspective etnice, religioase sau naționale diferite. Formarea în materie de sensibilitate culturală își atinge eficiența maximă atunci când este elaborată și desfășurată cu ajutorul și cu participarea unor persoane din comunitățile relevante.

Figura 6: Procesul și obiectivele urmărite la elaborarea formării specifice



Sursa: FRA, 2018.

<sup>29</sup> Wrench, J. (2007).

## **Studiu de caz**

### **Formare privind utilizarea legală a profilurilor**

#### **Formare legată de profiluri pentru polițiști (Italia)**

Începând din 2014, Observatorul Italian pentru Securitate împotriva Actelor de Discriminare (*Osservatorio per la sicurezza contro gli atti discriminatori*) desfășoară un modul de formare privind profilurile etnice, adresat polițiștilor și cadeților. În cadrul lui se pune accentul în principal pe prejudecățile prezumate care pot influența crearea de profiluri, pe consecințele lor în ceea ce privește eficiența activităților polițienești și pe impactul negativ asupra relațiilor cu comunitățile. Până acum, la acest modul au participat aproximativ 5 000 de persoane. Începând din 2017 se oferă și un modul de formare online în cadrul cursurilor de perfecționare pentru polițiști.

*Pentru mai multe informații, a se vedea [site-ul poliției naționale italiene](#).*

#### **Instrument referitor la drepturile fundamentale în cadrul formării polițiștilor de frontieră (UE)**

Programa comună de bază (PCB) pentru polițiștii de frontieră europeni stabilește nivelul minim de abilități și cunoștințe pe care trebuie să le dețină fiecare polițist de frontieră european. Conține capitole în domeniul sociologiei și al drepturilor fundamentale, precum și secțiuni specifice privind nediscriminarea (1.5.4) și crearea de profiluri etnice (1.7.10), pe care formatorii le pot folosi. PCB evidențiază riscurile potențiale ale prejudecăților, rasismului, discriminării rasiale, xenofobiei, islamofobiei, homofobiei și ale altor intoleranțe conexe care pot apărea în cursul utilizării de profiluri. Versiunea actualizată a PCB din 2017 include secțiuni referitoare la competențe noi, în special în domeniul drepturilor fundamentale.

În plus, Frontex a elaborat un manual pentru formatori, în consultare cu universități și organizații internaționale (a se vedea Frontex, 2013). Acesta oferă formatorilor metodologii pentru îmbunătățirea cunoștințelor și a abilităților polițiștilor de frontieră în domeniul drepturilor fundamentale și al protecției internaționale. Manualul menționează în mod explicit crearea și utilizarea profilurilor și stabilește reguli de bază pentru evitarea discriminării.

Cursurile au loc regulat. Totuși, nu există un mecanism permanent pentru evaluarea atingerii obiectivelor de formare.

*Pentru mai multe informații, a se vedea Frontex (2012).*

### **Zile de studiu pe tema creării de profiluri pentru ofițerii superiori (Belgia)**

Centrul pentru Poliție și Securitate (CPS) cu sediul la Gent (Belgia) a organizat în 2015, cu implicarea organismului belgian de promovare a egalității (Unia), o zi de studiu pe tema profilurilor etnice (*Profilage ethnique: l'égalité sous pression?*). Au fost abordate diverse aspecte ale acestei practici, printre care: dacă și cum pot fi îmbunătățite relațiile cu comunitățile minoritare etnice cu ajutorul polițiștilor proveniți din familii de migranți; cât de des sunt folosite profilurile etnice de către polițiști și cum a fost evaluată utilizarea lor.

În 2016, Unia a organizat două zile de studiu pentru ofițerii de poliție superiori din nordul Bruxelles-ului pentru a-i sensibiliza cu privire la utilizarea profilurilor etnice și a-i încuraja să reflecteze pe tema identificării practicilor legate de profiluri folosite de ofițerii din prima linie. Mai mulți polițiști din Spania și Regatul Unit au prezentat exemple de bune practici unui public format din agenți de aplicare a legii, cercetători și ONG-uri. Ca mențiune specială, ei au demonstrat că reducerea utilizării profilurilor bazate pe originea etnică a dus la creșterea numărului de arestări fructuoase ale persoanelor căutate. Totodată, au subliniat faptul că acest lucru a fost posibil prin păstrarea unor evidențe corecte ale fiecărei opriri, precum și prin asigurarea transparenței cu privire la motivele care au stat la baza opririlor. Formarea a avut ca scop ajungerea la o înțelegere comună a practicilor de utilizare a profilurilor etnice, în vederea realizării de cercetări viitoare privind practicile aplicate în prezent de poliție în acest domeniu.

*Pentru mai multe informații, a se vedea Belgia (2015 și 2017).*

Formarea ar trebui să abordeze eventualele prejudecăți și stereotipuri existente chiar în cadrul instituțiilor de aplicare a legii și de gestionare a frontierelor. Înainte de a desfășura cursuri cu privire la prevenirea utilizării ilegale a profilurilor, ar trebui examinate contextul instituțional mai larg și politicile interne în vigoare – cum ar fi mecanismele existente de tratare a plângerilor, prezența unui „cod al tăcerii” în rândul colegilor etc. Programele de formare ar trebui să abordeze prejudecățile și

stereotipurile integrate în acțiuni polițienești cum sunt acțiunile de oprire și percheziționare, arestările, detenția și folosirea forței.

Ofițerii de rang înalt sau de nivel mediu au un rol esențial în succesul formării, atât în calitate de participanți, cât și prin importanța pe care o acordă acesteia<sup>30</sup>. Ca beneficiari ai formării, ofițerii superiori pot deprinde noi practici și abilități, pe care le pot transmite polițiștilor din prima linie. Cultura organizațională, stabilită în mare parte de conducerea superioară, are un impact substanțial asupra comportamentului de zi cu zi al agenților de poliție și al polițiștilor de frontieră, inclusiv asupra modului în care aceștia interacționează cu publicul.

De asemenea, ofițerii superiori se pot asigura că formarea este privită pozitiv. Comportamentul personalului din funcții de conducere, de exemplu modul în care supraveghetorii comunică polițiștilor scopul formării sau bănuiala polițiștilor că au fost selectați aleatoriu sau pentru că sunt „problematici”, poate afecta nivelul de interes și de implicare în formare. Încurajarea polițiștilor să participe activ la programele de formare și să fie dispuși să își schimbe comportamentul pentru a-și îmbunătăți activitatea de zi cu zi poate spori impactul formării<sup>31</sup>.

După finalizarea formării, aceasta trebuie analizată și evaluată pentru a estima impactul pe care l-a avut în sensul creșterii gradului de conștientizare și al schimbării comportamentului.

### **În obiectiv: principiile directoare ale formării**

Formarea specializată este esențială pentru a asigura o utilizare legală a profilurilor. Comisia Europeană a elaborat un set de principii directoare de bază referitoare la modul în care trebuie asigurată o formare eficientă și de calitate privind infracțiunile motivate de ură. Aceleași principii se aplică și în cazul formării privind utilizarea legală a profilurilor.

**Formarea privind infracțiunile motivate de ură pentru autoritățile de aplicare a legii și de justiție penală: 10 principii directoare de bază**

30 Vezi Comisia Europeană (2017b).

31 Miller, J. și Alexandrou, B. (2016).



*Asigurarea impactului și a durabilității:*

- integrarea formării într-o abordare mai largă a combaterii discriminării;
- elaborarea unei metodologii pentru abordarea nevoilor de formare.

*Identificarea obiectivelor și crearea de sinergii:*

- adaptarea programelor la nevoile personalului;
- cooperarea cu societatea civilă într-o manieră structurată.

*Alegerea metodologiei potrivite:*

- combinarea unor metodologii diferite;
- formarea formatorilor.

*Transmiterea unui conținut de calitate:*

- conceperea unei programe de formare cu conținut de calitate;
- elaborarea de module de formare care vizează discriminarea.

*Monitorizare și evaluarea rezultatelor:*

- corelarea formării cu procesele de analiză a performanței;
- asigurarea monitorizării și a evaluării regulate a metodelor de formare.

*Pentru mai multe informații, a se vedea Comisia Europeană (2017a).*

Formarea nu va reuși însă să elimine prejudecățile implicite ale polițiștilor dacă nu va fi însoțită și de alte măsuri. Pentru aceasta este nevoie de o schimbare în gândirea instituțională. Prin urmare, autoritățile trebuie să ia în considerare intervenții multiple pentru a contracara prejudecățile personale și instituționale (a se vedea studiul de caz).

## Studiu de caz

### Combaterea „rasismului instituțional” în poliție

În urma îngrijorărilor apărute cu privire la importanța rasei lui Stephen Lawrence în proasta gestionare de către poliție a investigației legate de uciderea acestuia din motive rasiste în Regatul Unit, guvernul britanic a inițiat o anchetă de amploare pentru a identifica „lecțiile care trebuie învățate în ceea ce privește investigarea și urmărirea penală a infracțiunilor cu motivație rasială”.

Raportul anchetei, publicat în 1999, a evidențiat problema „rasismului instituțional” din cadrul Poliției Metropolitane, manifestat inclusiv prin numărul diferit de acțiuni de oprire și percheziționare, ca fiind un motiv de considerabilă îngrijorare pentru comunitățile afectate. Recomandările anchetei, care au cuprins măsuri diverse – de la formare pentru conștientizarea rasismului până la raportarea și înregistrarea incidentelor –, au fost completate de un apel general la sporirea deschiderii și a răspunderii poliției și la restabilirea încrederii în aceasta.

Analizele publicate în 2009, la zece ani de la anchetă, au arătat îmbunătățiri ale modului în care poliția interacționează cu comunitățile etnice minoritare și investighează infracțiunile cu motivație rasială. Se remarcă, totuși, tendința de a opri și percheziționa mult mai des persoane cu pielea neagră decât cu pielea albă.

*Pentru mai multe informații, a se vedea Regatul Unit, Home Office (1999), Regatul Unit, Comisia pentru Egalitate și Drepturile Omului (2009) și Regatul Unit, Comisia pentru Afaceri Interne a Camerei Comunelor (2009).*

## 2.2.4. Motive rezonabile de suspiciune: utilizarea datelor operative și a informațiilor

Atunci când agenții de poliție și de gestionare a frontierelor aleg persoanele pe care le controlează, de obicei își bazează decizia pe o combinație de elemente. Acestea pot fi informații mai „obiective”, de exemplu date operative specifice,

comportamentul persoanelor, îmbrăcămintea sau obiectele pe care le au asupra lor, dar și cunoștințe „subiective” bazate pe experiență.

Toate aceste elemente pot fi „semnalul” unei activități ilegale, însă informațiile trebuie combinate și utilizate cu prudență. Dovezile arată că, în practică, polițiștilor le poate fi greu să facă distincția între elementele obiective și cele subiective, ca în exemplul citat în casetă.

### **Exemplu**

*„Este foarte subiectiv. Pe de o parte este senzația pe care ți-o dă persoana sau cazul respectiv, dar unele dovezi țin de discrepanțele dintre ceea ce spun persoanele, inconsecvențele dintre ce spun ele și ce spune susținătorul reîntregirii familiei, inconsecvențele dintre spusele lor și documentele pe care le dețin, dintre spusele lor și toate lucrurile pe care pot să le aibă în bagaje. Deci există dovezi, dar [singure, aceste lucruri nu pot] să învinovățească pe cineva. Agentul trebuie să aibă în vedere o imagine completă despre persoana respectivă.”*

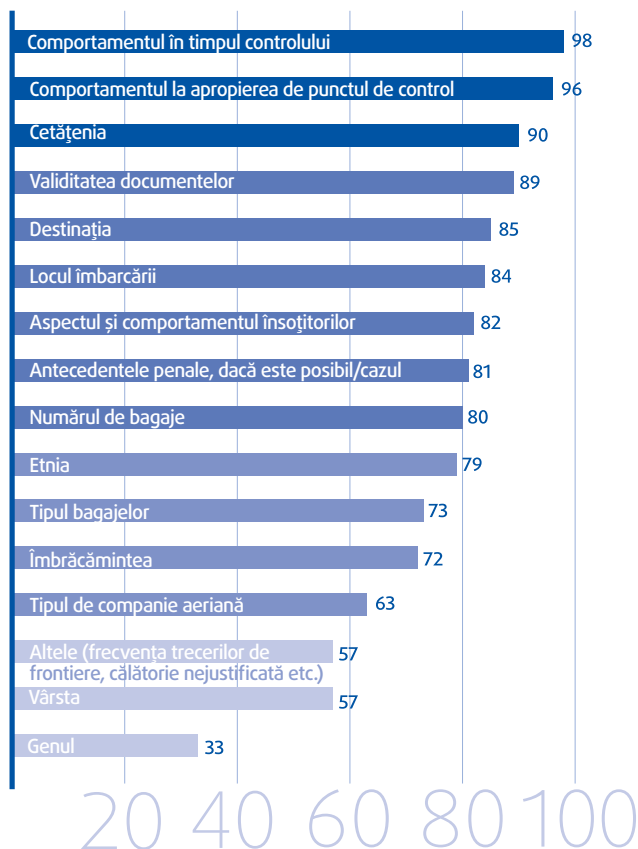
*Agent de imigrări la un aeroport important din Regatul Unit*

*Pentru mai multe informații, a se vedea FRA (2014a), p. 46.*

### **În obiectiv: depistarea persoanelor care încearcă să intre într-o țară în mod neregulamentar**

Cercetările FRA efectuate în 2012 într-o serie de aeroporturi majore arată că polițiștii de frontieră iau în considerare o serie de factori atunci când suspectează că o persoană încearcă să intre în țară în mod neregulamentar. Aceștia cuprind adesea o combinație între criterii „obiective” – de exemplu, comportamentul persoanei atunci când se apropie de punctul de control și în timpul controlului, tipul și numărul de bagaje și validitatea documentelor de călătorie – și experiența personală a controalelor la frontieră efectuate în trecut, după cum se arată în [figura 7](#).

**Figura 7: Indicații considerate utile sau foarte utile pentru recunoașterea eficientă a persoanelor care încearcă să intre în țară în mod neregular înainte ca agentul să li se adreseze (%)**



*Notă: S-au înregistrat între 206 și 216 răspunsuri valabile dintr-un total de 223. La calcularea rezultatelor, respondenții care nu au răspuns la o anumită întrebare au fost excluși. Numărul celor care nu au răspuns s-a situat între 7 și 17 persoane, în funcție de întrebare.*

*Sursa: FRA, Ancheta privind polițiștii de frontieră, 2012 (întrebarea 17).*

Polițiștii de frontieră au menționat comportamentul în timpul controlului sau la apropierea de punctul de control ca fiind cel mai util factor în recunoașterea

persoanelor care încearcă să intre în țară într-un mod neregular. Au fost însă considerați importanți și factori precum cetățenia și etnia, care ar putea indica profiluri discriminatorii.

Îmbrăcămintea, care a fost de asemenea considerată un indicator util, este un exemplu al modului în care informații aparent „obiective” pot fi utilizate în mod părtinitor în practică. Anumite haine pot fi asociate unor profiluri de risc specifice. De exemplu, este posibil ca victimele traficului de persoane de o anumită cetățenie să poarte de obicei anumite tipuri de haine; însă îmbrăcămintea poate indica și faptul că o persoană aparține unui anumit grup etnic sau religios. Chiar dacă există suficiente alte motive pentru a justifica trimiterea către verificarea în linia a doua, persoanele care se identifică puternic cu originea lor etnică sau religioasă, care au avut experiențe negative în trecut sau care nu primesc o explicație adecvată de la agent pot percepe tratamentul ca fiind discriminatoriu.

*Pentru mai multe informații, a se vedea FRA (2014a). În legătură cu profilurile victimelor traficului, a se vedea Frontex (2017).*

Obținerea de informații cât mai bune despre tiparele de comportament sau despre evenimente poate asigura aplicarea unor profiluri mai obiective. Informațiile pot avea legătură cu activități infracționale sau, în cazul gestionării frontierelor, cu migrația neregulară sau cu infracțiuni transfrontaliere. Atunci când acțiunile de aplicare a legii și de gestionare a frontierelor se bazează pe informații specifice și oportune, de exemplu informații despre o anumită persoană și/sau un context specific, cresc șansele să fie obiective și scade riscul să se bazeze pe stereotipuri.

Pe lângă informațiile și elementele obiective, pot fi utilizate în mod legitim și informații despre caracteristicile protejate, cum sunt rasa, originea etnică, cetățenia, genul sau religia (reale sau percepute), ca o componentă suplimentară în evaluarea necesară pentru crearea de profiluri în anumite circumstanțe. Pentru a fi legală, utilizarea acestor informații trebuie să fie reglementată prin lege, să respecte esența drepturilor și libertăților afectate, să fie proporțională (adică să respecte un echilibru de interese) și necesară (adică să nu fie disponibile alte mijloace mai puțin restrictive). Trebuie să existe un motiv justificat, diferit de criteriile protejate, pentru ca agenții să trateze o persoană diferit de ceilalți membri ai publicului. De asemenea, motivul trebuie să se refere în mod specific la persoana respectivă, ca în exemplul prezentat în casetă.

### **Exemplu**

*Martorii relatează că suspectul într-un caz de jaf purta pantofi de alergare roșii și o șapcă de baseball neagră, că are între 1,60 și 1,70 m înălțime și pare să fie de origine chineză. În aceste condiții, autoritățile de aplicare a legii ar putea considera în mod legitim că originea etnică este relevantă pentru a determina dacă o persoană devine un potențial suspect, întrucât este combinată cu informații specifice.*

### **În obiectiv: descrierile detaliate ale suspectilor**

O descriere bună a suspectului poate reduce riscul de ilegalitate a profilurilor. Descrierea unui suspect constă în detalii despre persoana respectivă, de exemplu culoarea pielii, a părului și a ochilor, înălțimea și greutatea, îmbrăcămintea. Aceste detalii sunt furnizate de victima infracțiunii, de martori sau pe baza altor date operative specifice. O descriere bună poate fi utilizată de agenți ca bază pentru acțiunile de oprire și percheziționare care urmăresc reținerea suspectilor sau pentru trimiterea persoanelor către verificări în linia a doua la frontieră.

Dacă însă agenții de aplicare a legii primesc o descriere prea generală care menționează rasa, etnia sau caracteristici similare ale suspectului, nu ar trebui să-și bazeze operațiunile pe descrierea respectivă. În astfel de cazuri, este posibil ca operațiunile să conducă la oprirea a numeroase persoane nevinovate care, din întâmplare, au aceleași caracteristici. Mai degrabă ar trebui căutate alte informații operaționale specifice care să orienteze investigațiile.

*Pentru mai multe informații, a se vedea Comisia Europeană (2017b).*

Unele informații care par obiective pot, de fapt, să încorporeze prejudecăți. Chiar și factori aparent obiectivi precum ora, ziua, locul etc. pot fi folosiți ca substitut pentru criterii interzise din cauză că sunt discriminatoare, cum ar fi rasa, țara de origine, genul, orientarea sexuală sau religia (reale sau percepute), așa cum se arată în exemplul de mai jos.

**Exemplu**

*Într-o zi de vineri, în jurul prânzului, se desfășoară o operațiune de oprire și percheziționare în zona X. Dar acest moment este cea mai importantă oră de rugăciune pentru musulmani. Deoarece zona X se află în apropierea unei moschei, ora, data și locul – aparent factori obiectivi – ar putea avea de fapt rolul unor substituenți pentru o operațiune de oprire și percheziționare bazată pe criteriul discriminatoriu interzis al religiei.*

În mod similar, urmărirea anumitor comportamente suspecte poate părea o modalitate obiectivă de identificare a posibilelor fapte ilicite. Agenții pot interpreta însă comportamentul unei persoane în moduri diferite, în funcție de alte caracteristici ale persoanei în cauză. Dovezile arată că cunoașterea și înțelegerea informațiilor operative pot să difere foarte mult de la un agent la altul și adesea nu corespund tiparelor reale ale infracționalității<sup>32</sup>.

Furnizarea de informații oportune și detaliate agenților, de exemplu prin scurte ședințe de informare înainte de intrarea în fiecare tură, ar trebui să restrângă puterea discreționară a agenților și să îi îndrume astfel încât să-și direcționeze mai bine competențele către tiparele de infracționalitate și către problemele de siguranță identificate la momentul respectiv. Se reduce astfel influența prejudecăților. Îmbunătățirea calității și a utilizării informațiilor, astfel încât să se pună accentul pe factorii comportamentali sau pe informațiile specifice, are eficiență maximă atunci când este combinată cu o supraveghere și o monitorizare sporită a modului în care agenții își folosesc competențele.

**Studiu de caz****Asigurarea obiectivității în utilizarea profilurilor****Informări înainte de intrarea în tură (UE)**

Catalogul Schengen recomandă ca, înainte de fiecare tură, agentul de serviciu să ofere informații cu privire la orice indicatori de risc și profiluri de risc. Asigurarea suprapunerilor între ture poate oferi suficient timp pentru

32 United Kingdom National Policing Improvement Agency (NPIA) (2012).

schimbul de informații între personalul care iese și cel care intră în tură, precum și informări adecvate.

*Pentru mai multe informații, a se vedea Consiliul Uniunii Europene (2009).*

### **Programul de formare SDR (Țările de Jos)**

Programul de formare privind percheziționarea, depistarea și reacția (Search, Detect and React – SDR) are drept scop prevenirea infracțiunilor sau a actelor teroriste înainte ca ele să aibă loc, prin îmbunătățirea capacității personalului de securitate în ceea ce privește profilurile comportamentale. Aceasta înseamnă ca polițiștii să nu-și mai îndrepte atenția către caracteristicile inalterabile, cum este culoarea pielii, ci să se concentreze în schimb asupra comportamentului individual atunci când decid asupra modului de acțiune. Deoarece indicatorii unui comportament suspect sunt specifici contextului, formarea este nuanțată în funcție de mediu. Se respinge ideea că ar exista o soluție universal valabilă. După ce detectează tipare de conduită relevante, agenții trebuie să acționeze într-o manieră „sensibilă”. În majoritatea cazurilor, ei vor purta o conversație informală cu suspectul în loc de a uza de puterile oficiale ale poliției. Programul constă în predare la clasă plus formare aplicată și formare la locul de muncă.

Pentru mai multe informații, a se vedea [site-ul SDR Academy](#).

### **Instrumentul de oprire și percheziționare „practica profesională autorizată” (Authorised Professional Practice – APP) (Regatul Unit)**

În Regatul Unit, College of Policing a elaborat orientări de practică profesională autorizată (APP), care acoperă diverse aspecte ale activității poliției. APP referitoare la oprire și percheziționare explică ce este o acțiune de acest tip, de ce este important să se utilizeze corect aceste competențe și care sunt caracteristicile acțiunilor legale de oprire și percheziționare. Se explică faptul că legalitatea și eficacitatea interacțiunilor de oprire și percheziționare vor fi susținute asigurând:

- **echitatea:** decizia agentului de a opri și percheziționa o persoană trebuie să se bazeze numai pe factori obiectivi corespunzători. O persoană nu poate fi oprită niciodată exclusiv sau în principal pe baza unor caracteristici protejate sau a unor factori precum existența unor condamnări anterioare;

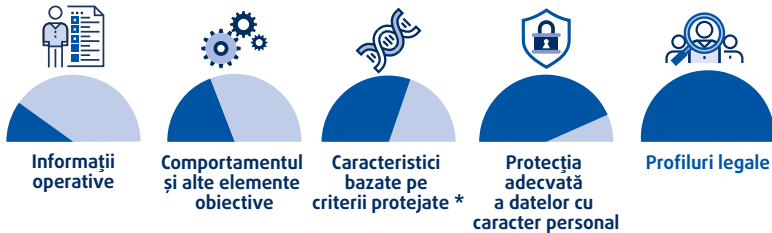


- **legalitatea:** oprirea și percheziționarea trebuie să aibă un temei juridic care să fie aplicat în mod legal;
- **profesionalismul:** în timpul interacțiunilor de oprire și/sau percheziționare, agenții trebuie să respecte standardele profesionale de conduită, în special Codul etic, să comunice eficient cu oamenii și să îi trateze cu demnitate și respect;
- **transparența:** interacțiunea individuală trebuie înregistrată cu precizie. Trebuie să se asigure supravegherea și monitorizarea eficientă a acțiunilor de oprire și percheziționare, precum și controlul public.

*Pentru mai multe informații, a se vedea Regatul Unit, College of Policing (2016).*

Figura 8 ilustrează diferitele elemente care pot fi utilizate pentru crearea unor profiluri legale; modul în care se combină acestea depinde de natura fiecărui caz în parte.

Figura 8: Combinarea elementelor

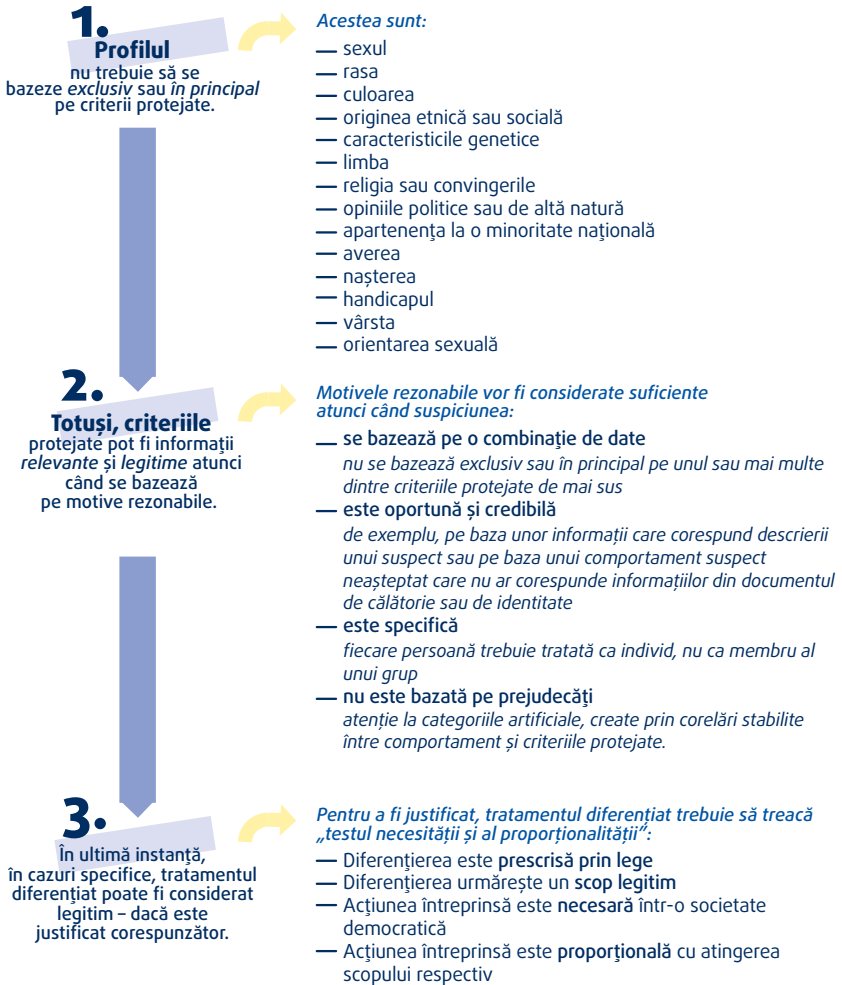


\* A se vedea în figura 9 lista criteriilor protejate în conformitate cu dreptul UE. Profilurile nu trebuie niciodată create exclusiv sau în principal pe baza unor caracteristici protejate.

Sursa: FRA, 2018.

Figura 9 arată cum pot fi combinate aceste elemente astfel încât profilurile rezultate să nu fie discriminatorii.

Figura 9: Elementele unui profil nediscriminatoriu



*Notă: Lista criteriilor protejate diferă de la un stat membru la altul. Pentru o prezentare generală a motivelor de discriminare incluse în codurile penale ale fiecărui stat membru, a se vedea FRA (2018d). A se vedea și site-ul Equinet, rețeaua europeană a organismelor naționale de promovare a egalității, care enumeră motivele de discriminare urmărite de organismele naționale de promovare a egalității.*

Sursa: FRA, 2018.

## 2.2.5. Procesele-verbale de oprire și percheziționare folosite în activitățile de aplicare a legii care presupun profiluri

Procesele-verbale de oprire și percheziționare îi pot ajuta pe agenți să stabilească dacă opririle pe care le efectuează se bazează pe motive rezonabile și fac posibilă monitorizarea de către ofițerii superiori a potențialelor practici discriminatorii utilizate de agenți în acțiunile de oprire și percheziționare. Deși uneori sunt considerate împovărătoare, ele asigură și o evidență a opririlor, iar atunci când sunt agregate oferă date care pot indica dacă opririle sunt efectuate în mod legal<sup>33</sup>. Acest lucru poate contribui la promovarea deschiderii și a asumării răspunderii. Pe lângă completarea proceselor-verbale pe hârtie, pentru înregistrarea acestor informații pot fi folosite și noile tehnologii, precum aplicațiile pentru dispozitivele mobile.

În casetă sunt descrise câteva aspecte importante care trebuie încorporate în conceperea proceselor-verbale de oprire și percheziționare.

### **În obiectiv: elementele unui proces-verbal de oprire și percheziționare bine structurat**

Pentru a fi utile, procesele-verbale folosite la oprire și percheziționare trebuie să fie bine concepute. În primul rând, completarea lor creează un volum de lucru suplimentar pentru agenți. Dacă nu sunt concepute clar și nu sunt rezonabil de scurte, există riscul ca agenții să nu completeze întregul formular sau să îl completeze superficial. În al doilea rând, procesele-verbale bine structurate fac posibilă extragerea și agregarea ușoară a datelor, facilitând monitorizarea și evaluarea acțiunilor de oprire și percheziționare.

Ori de câte ori este posibil, procesele-verbale de oprire și percheziționare trebuie:

- să conțină câmpuri cu mai multe variante de răspuns, care sunt mai rapid de completat și mai ușor de procesat statistic;
- să prezinte o listă exhaustivă de opțiuni pentru fiecare punct;
- să evite exprimările ambigue;
- să fie ușor de înțeles atât pentru agent, cât și pentru persoana oprită;

33 Regatul Unit, Stop Watch (2011).

- să includă:

- temeiurile juridice ale percheziției. Sunt de preferat explicațiile simple în locul unei liste de reguli;
- data, ora și locul percheziționării persoanei sau vehiculului;
- scopul percheziției, de exemplu obiectele căutate de agenți;
- rezultatul opririi;
- numele polițiștilor care efectuează percheziția și secția de poliție de care aparțin;
- pot fi notate date cu caracter personal ale persoanelor percheziționate, de exemplu numele, adresa și cetățenia. Totuși, persoana vizată poate refuza să furnizeze aceste informații.

Pentru a-și îndeplini scopul, procesele-verbale trebuie completate la momentul opririi.

Persoana oprită sau responsabilă de vehiculul percheziționat trebuie să primească un exemplar. În Regatul Unit, persoanele care au fost oprite au dreptul să solicite o copie a raportului aferent în termen de trei luni de la oprire. Astfel, procesul-verbal nu reprezintă o dovadă a opririi doar pentru poliție, ci și pentru persoanele oprite.

*Pentru mai multe informații, a se vedea Regatul Unit, Poliția West Midlands (2012), p. 7; și Regatul Unit, Home Office (2014a).*

## Studiu de caz

### Procesul-verbal de oprire și percheziționare (Regatul Unit)

În continuare este reprodus procesul-verbal de oprire și percheziționare folosit de Poliția West Midlands în Regatul Unit.

Se observă că persoanei oprite i se cere să se autoidentifice ca aparținând uneia dintre categoriile etnice enumerate, existând și opțiunea „alta” sau „nedeclarată”. Agentul care efectuează oprirea poate adăuga o observație cu privire la propria percepție asupra etniei persoanei, dacă nu este de acord cu cea declarată.

Codul de practică pentru exercitarea competențelor de oprire și percheziționare în Regatul Unit prevede că agenții trebuie să le explice celor

opriți că informațiile referitoare la etnie „sunt necesare pentru a obține o imagine reală a activității de oprire și percheziționare și pentru a contribui la îmbunătățirea monitorizării etnice, la combaterea practicilor discriminatorii și la promovarea unei utilizări eficiente a competențelor”.

WC332  
03/17

## Stop and Search

Call: 805 6666



### Power

- 1 Drugs
- 2 Section 1 PACE

A typical response would be "2,5" if the Power was "S1 PACE & Object 'Fireworks'. The Object of search will default if there is only 1 option.

- 3 S47 Firearms Act
- 4 Section 60 CJPO Act 1994
- 5 Section 43 Terrorism Act
- 6 New Psychoactive Substances Act 2016
- 7 Other (a Search contains list of additional powers)

### Object

- 1 Search for Drugs
- 1 Stolen Items
- 2 Offensive Weapon/Bladed Article
- 3 Articles for Burglary/Theft/Fraud/TWOC
- 4 Items for Criminal Damage
- 5 Fireworks
- 1 Firearms
- 1 Dangerous Items/Offensive Weapons
- 1 Evidence of Terrorism
- 1 Search for NPS

### Self Assessed Ethnicity (16+1)

- A1 Asian - Indian
- A2 Asian - Pakistani
- A3 Asian - Bangladeshi
- A9 Asian - Any Other Asian background
- B1 Black - Caribbean
- B2 Black - African
- B9 Black - Any Other Black background
- M1 Mixed - White & Black Caribbean
- M2 Mixed - White and Black African
- M3 Mixed - White & Asian
- M9 Mixed - Any Other Mixed Background
- O1 Other - Chinese
- O9 Other - Any Other Ethnic Group
- W1 White - British
- W2 White Irish
- W9 White - Any Other White background
- NS Not Stated

### Officer assessed Ethnicity (PNC)

- IC1 White North European
- IC2 White South European
- IC3 Black
- IC4 Asian
- IC5 Chinese/Japanese/South East Asian
- IC6 Middle Eastern
- IC9 Other

### Grounds for Search - Multi Select

- 1 Acting Suspiciously
- 2 Stopped in tasking area
- 3 Stopped in high crime area
- 4 Could not give reasonable explanation
- 5 Tried to avoid police
- 6 Seen to discard an item
- 7 Seen to conceal item
- 8 Smell of controlled drug
- 9 Current Intelligence
- 10 Matches Description

Grounds will be supported by a free text explanation

### Outcome

- |  |  |
|--|--|
| 1 Arrested - Consequence of Stop & Search            | 7 Street Summons                         |
| 2 Arrested - Unrelated Offence including Warrant/PNC | 8 Conditional Bail                       |
| 3 Community Resolution                               | 9 Out of custody Caution                 |
| 4 Fixed Penalty                                      | 10 Substance seized, person not arrested |
| 5 Cannabis Warning                                   | 11 NFA                                   |
| 6 Street Bail  |  |

*Pentru mai multe informații, a se vedea Regatul Unit, Poliția West Midlands (2017a) și Regatul Unit, Home Office (2014a), p. 19.*

În prezent, multe structuri polițienești renunță la colectarea datelor privind acțiunile de oprire și percheziționare pe formulare, folosind în schimb, tehnologii precum aplicații pentru telefoanele mobile, sisteme radio, terminale de date mobile sau laptopuri. Aceste tehnologii pot accelera procesul de înregistrare și pot reduce birocrăția, dar creează și riscuri noi, legate în special de utilizarea algoritmică a datelor cu caracter personal (a se vedea [capitolul 3](#)).

## Studiu de caz

### Înregistrarea în direct a acțiunilor de oprire și percheziționare

#### „eSearch” (Poliția West Midlands, Regatul Unit)

Adoptat în aprilie 2014, acest sistem se bazează pe o convorbire între agentul de pe teren și un membru al personalului aflat în centrul de contact (camera de control). Detaliile despre acțiunea de oprire și percheziționare sunt înregistrate imediat în centrul de contact și sunt incluse într-o bază de date. Ulterior, informațiile pot fi accesate și utilizate pentru a examina eficacitatea acțiunilor de oprire și percheziționare, atât la nivel intern, cât și extern. eSearch a transformat complet modul de înregistrare a acțiunilor de oprire și percheziționare. Înregistrările pot fi vizualizate mult mai rapid pe sistemele poliției, ceea ce prezintă avantaje din punctul de vedere al datelor operative și al integrării lor în activitățile operaționale ale poliției.

*Pentru mai multe informații, a se vedea Regatul Unit, Poliția West Midlands (2014) și Regatul Unit, Poliția West Midlands (2016).*

#### Aplicație pentru dispozitivele mobile destinată agenților din prima linie (Poliția West Midlands, Regatul Unit)

O nouă aplicație pentru dispozitivele mobile, lansată în octombrie 2017, își propune să scurteze și să eficientizeze acțiunile de oprire și percheziționare. Aplicația eSearch permite agenților să înregistreze detalii despre interacțiunile de stradă direct în aplicație prin intermediul telefoanelor inteligente, fără a mai fi nevoie să apeleze personalul centrului de contact. Fiecare oprire primește un număr de referință unic, iar GPS-ul înregistrează automat locul. Se preconizează că aplicația va reduce numărul apelurilor către centrul de contact cu aproape 1 000 de apeluri pe lună.

*Pentru mai multe informații, a se vedea Regatul Unit, Poliția West Midlands (2017b).*

Ofițerii superiori au un rol important în asigurarea legalității operațiunilor de oprire și percheziționare. Exemplul de mai jos arată modul în care ofițerii superiori pot ține aceste acțiuni sub supraveghere. Totodată, ei trebuie să se asigure că acțiunile

de oprire și percheziționare nu sunt utilizate ca indicator de performanță bazat pe numărul de opriri efectuate.

### Studiu de caz

#### Validarea rapoartelor de oprire și percheziționare (Regatul Unit)

Începând din august 2014, fiecare raport de oprire și percheziționare din Regatul Unit trebuie să fie validat de supraveghetorul agentului care a efectuat percheziția. Rapoartele sunt avizate ca fiind conforme sau neconforme cu standardele aplicabile. În caz de neconformitate, agentul evaluator trebuie să menționeze motivul pe raportul de oprire și percheziționare.

*Pentru mai multe informații, a se vedea Regatul Unit, Home Office (2014a).*

## 2.3. Răspunderea

### Aspecte esențiale

- Agenții de aplicare a legii și de gestionare a frontierelor **răspund** de utilizarea profilurilor în limitele legii.
- **Colectarea de date fiabile, exacte și oportune** cu privire la activitățile legate de profiluri este esențială pentru asigurarea răspunderii.
- **Existența unor mecanisme eficiente de tratare a plângerilor** poate să descurajeze abuzul de putere și totodată să asigure și să restabilească încrederea publicului în operațiunile autorităților polițienești și de gestionare a frontierelor.
- **Organizarea unor reuniuni de feedback cu membri ai publicului** pentru a le asculta părerea, a discuta despre profiluri și a primi feedback cu privire la operațiuni oferă ocazia de a învăța lecții importante și de a îmbunătăți acțiunile legate de profiluri.

Răspunderea reprezintă un principiu cheie al guvernantei democratice. În termeni foarte generali, aceasta implică furnizarea de răspunsuri către cei care au dreptul de a trage la răspundere<sup>34</sup>. Răspunderea se referă nu doar la deciziile individuale, ci și la

34 Bovens, M., Schillermans, T. și Goodlin, R.E. (2014), p. 1-11.

cele luate de instituții (așa-numita „răspundere instituțională”). În calitate de funcționari și organisme publice, agenții de aplicare a legii și de gestionare a frontierelor, precum și organizațiile conexe, răspund în fața publicului pentru deciziile și acțiunile lor – inclusiv pentru asigurarea utilizării profilurilor în limitele legii.

Colectarea de date fiabile, exacte și oportune este esențială pentru asigurarea răspunderii. Deoarece multe date conțin informații sensibile cu caracter personal, ele trebuie gestionate în conformitate cu normele și procedurile de protecție a datelor (a se vedea [capitolul 3](#)).

### Listă de verificare pentru asigurarea răspunderii

Lista de verificare de mai jos oferă o trecere în revistă minimală a pașilor pe care autoritățile de aplicare a legii și de gestionare a frontierelor îi pot urma pentru a asigura asumarea răspunderii pentru deciziile și acțiunile legate de profiluri. Această listă poate ajuta agenții să fie mai responsabili, dar nu trebuie înțeleasă ca procedură obligatorie pentru agenții de aplicare a legii și pentru cei de gestionare a frontierelor. În funcție de context, este posibil ca unele recomandări să nu se aplice particularităților gestionării frontierelor.

#### 1. Identificați problema

- Recunoașteți și **admițeți** problema legată de utilizarea ilegală a profilurilor. Prejudecățile și stereotipurile există cu adevărat și prezintă riscuri pentru persoanele implicate, inclusiv pentru polițiști și comunitățile locale.
- Colectați și utilizați date dezagregate**: sunt un instrument important pentru evaluarea eficacității și a performanței.
- Participați la dezbateri externe organizate de comunitate sau de societatea civilă pentru a primi **feedback** cu privire la practicile pe care le utilizați și pentru a spori încrederea în operațiunile pe care le desfășurați.

#### 2. Culegeți informații

- Garantați capacitatea de asumare a răspunderii **ținând evidența** activităților legate de profiluri.
- Cu condiția să se adopte garanțiile necesare, **supravegherea video** și/sau **camerele de corp** pot spori responsabilitatea și pot furniza



dovezi pe baza cărora să se ia măsuri de modificare a tiparelor de comportament părtinitor.

- ☑ Creați **procese-verbale de oprire și percheziționare** care să fie completate de polițiști după fiecare oprire.

### 3. Acționați și preveniți

- ☑ Efectuați **evaluări** pentru a afla dacă există norme și practici care perpetuează prejudecățile explicite sau implicite și stereotipurile negative.
- ☑ Introduceți cursuri specifice și/sau **sesiuni de formare** axate pe combaterea prejudecăților și a stereotipurilor personale și instituționale.
- ☑ **Furnizați informații** persoanelor pe care le opriți, pentru a consolida impresia de echitabilitate, și oferiți-le informații suficiente încât să poată decide dacă vor apela sau nu la o cale de atac. Furnizarea de informații reprezintă o obligație legală în cazul trimiterilor către verificări de linia a doua la punctele de trecere a frontierei.
- ☑ Arătați **toleranță zero** în cadrul organizației pentru incidentele care au la origine prejudecăți.
- ☑ Instituți **mecanisme interne** de supraveghere și control, de exemplu grupuri de dezbateri interne în cadrul cărora să se discute dacă opririle se fac pe baza unor motive rezonabile.
- ☑ Asigurați-vă că **indicatorii de performanță** sunt asociați cu evitarea prejudecăților și a stereotipurilor.
- ☑ Instituți **mecanisme de tratare a plângerilor** pentru a descuraja abuzurile de putere și pentru a asigura asumarea răspunderii.

*Sursa: FRA, 2018.*

## 2.3.1. Monitorizare internă

Conducerea autorităților polițienești și de gestionare a frontierelor joacă un rol important în crearea unei culturi care să susțină drepturile individuale și principiul nediscriminării, atât în cadrul organizației, cât și în relațiile acesteia cu publicul. De asemenea, cadrele de conducere contribuie la crearea unui climat de responsabilitate și transparență. Comunicarea deschisă între membrii personalului (atât pe orizontală, cât și pe verticală) și stabilirea unor standarde clare de comportament, cum

ar fi codurile de conduită profesională, sunt două dintre elementele interne care ar trebui să fie puse în aplicare pentru a spori nivelul de responsabilitate. Recrutarea și formarea au de asemenea roluri importante în acest sens (a se vedea secțiunea 2.2.3).

Conform legislației UE, orice autoritate sau organism public trebuie să desemneze un **responsabil cu protecția datelor**. Acesta consiliază structurile polițienești și de gestionare a frontierelor cu privire la obligațiile care le revin în ceea ce privește protecția datelor, printre care păstrarea evidenței activităților de prelucrare de date sau efectuarea de evaluări ale impactului asupra protecției datelor. În contextul profilurilor, responsabilul cu protecția datelor va recomanda și va supraveghea, de exemplu, ca datele cu caracter personal colectate pentru sau în timpul creării și utilizării de profiluri să fie prelucrate și stocate în mod legal.

#### **În obiectiv: rolul responsabililor cu protecția datelor**

**Directiva privind poliția** impune statelor membre să numească un responsabil cu protecția datelor, ale cărui atribuții să includă:

- monitorizarea respectării legislației aplicabile privind protecția datelor cu caracter personal, de exemplu prin:
  - alocarea responsabilităților;
  - sensibilizarea și formarea personalului;
  - audituri;
- furnizarea de consiliere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea punerii în aplicare a recomandărilor emise;
- asumarea rolului de punct de contact pentru autoritatea de supraveghere.

Responsabilul cu protecția datelor trebuie să se implice pe deplin și cu promptitudine în toate aspectele legate de protecția datelor cu caracter personal.

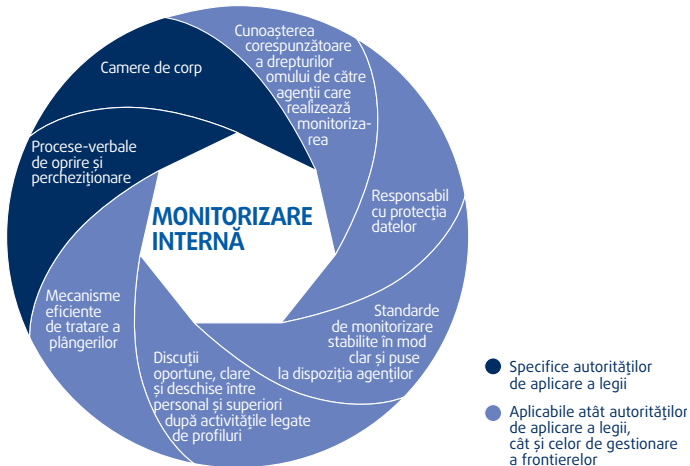
*A se vedea articolele 32-34 din Directiva privind poliția.*

În cadrul structurilor polițienești, monitorizarea internă a activității legate de profiluri poate fi efectuată ca parte a unei game largi de măsuri menite să țină evidența interacțiunilor dintre autorități și publicul larg (a se vedea figura 10). Acestea mai cuprind utilizarea de:

- **procese-verbale de oprire și percheziționare:** un instrument practic util pentru a încuraja agenții să își fundamenteze bine acțiunile de oprire și pentru a promova deschiderea și responsabilitatea față de public (a se vedea secțiunea 2.2.5);
- **camere de corp:** sub rezerva garanțiilor necesare, acestea pot spori încrederea între comunități și poliție și pot fi un factor de descurajare a abuzului de forță și a discriminării (a se vedea secțiunea 2.3.2).

Aceste măsuri pot fi utilizate și în activitățile de monitorizare internă din cadrul organizațiilor de gestionare a frontierelor. De exemplu, Catalogul Schengen recomandă înregistrarea numărului de trimeri către verificările din linia a doua și a motivelor aferente. În plus, diferitele contexte ale controalelor la frontieră, infrastructura existentă la punctele de trecere a frontierei și prezența superiorilor la fața locului creează alte ocazii de monitorizare internă. De pildă, pot fi disponibile echipamente tehnologice suplimentare, cum ar fi supravegherea video.

Figura 10: Elementele monitorizării interne



Sursa: FRA, 2018.

Dacă sunt instituite garanțiile necesare, înregistrările video pot furniza dovezi pentru evaluarea modului în care se efectuează activitatea de utilizare a profilurilor și pot reprezenta probe în cazul plângerilor specifice. De exemplu, ele pot confirma dacă comportamentul unei persoane aflate în așteptarea verificării din prima linie a dat suficiente motive pentru o trimitere către verificarea în linia a doua.

Spre deosebire de acțiunile de oprire și percheziționare, la punctele de trecere a frontierei pasagerii se așteaptă în general la prezența supravegherii video, având în vedere natura publică a acestor puncte și considerentele de securitate. Totuși, utilizarea acestor instrumente trebuie să respecte dreptul la intimitate și normele aplicabile de protecție a datelor.

Păstrarea de evidențe poate avea beneficii atât pe termen scurt, cât și pe termen lung. Exemplul proceselor-verbale de oprire și percheziționare arată că:

- pe **termen scurt**, acestea pot asigura responsabilitatea la fața locului. În Regatul Unit, toate persoanele oprite primesc un exemplar al procesului-verbal sau o recipisă care precizează de unde pot obține o copie. În el se oferă detalii despre motivul opririi, precum și informații despre locul și modalitatea de depunere a unei plângeri. Astfel, persoana în cauză poate să afle motivul și să îl conteste dacă îl consideră nedrept;
- pe **termen lung**, analiza evidențelor păstrate permite structurilor polițienești să afle dacă atribuțiile de oprire și percheziționare se îndreaptă în mod disproporționat asupra grupurilor minoritare și să ajusteze în consecință îndrumările oferite agenților. Evidențele pot fi făcute publice pentru a spori transparența și a promova încrederea publicului în exercitarea competențelor de oprire și percheziționare.

### **Păstrarea evidențelor: Ce spune legea?**

Pentru a asigura legalitatea prelucrării datelor, Directiva privind poliția impune ca autoritățile de aplicare a legii să țină evidența tuturor categoriilor de activități de prelucrare aflate în responsabilitatea lor. În plus, în sistemele de prelucrare automată trebuie să se păstreze jurnale pentru a ști cine a consultat sau a dezvăluit date cu caracter personal, când s-a întâmplat acest lucru, cine a primit datele și care a fost justificarea prelucrării datelor (a se vedea secțiunea 3.1.3).

*Articolele 24 și 25 din Directiva privind poliția*

## Studiu de caz

### Utilizarea evidențelor păstrate pentru a depista lipsa de proporționalitate în acțiunile de oprire și percheziționare (Regatul Unit)

Codul de practică al Legii privind probele polițienești și penale, elaborat în Anglia și Țara Galilor (Regatul Unit), impune structurilor polițienești obligația legală de a monitoriza modul în care sunt utilizate competențele de oprire și percheziționare pentru a depista dacă acestea sunt „exercitate pe baza unor imagini stereotipe sau a unor generalizări necorespunzătoare”. Trebuie identificată și investigată orice utilizare aparent disproporționată a competențelor de către anumiți agenți sau grupuri de agenți ori legate de anumite părți ale comunității și trebuie luate măsuri adecvate în vederea eliminării acesteia. În plus, poliția trebuie să asigure posibilitatea ca evidențele să fie examinate de reprezentanții comunității și să explice utilizarea competențelor de oprire și percheziționare la nivel local.

*Pentru mai multe informații, a se vedea Regatul Unit, Home Office (2014a).*

Poliția din Regatul Unit a dezvoltat mai multe instrumente de sporire a transparenței prin facilitarea accesului la datele privind acțiunile de oprire și percheziționare. Site-ul <http://www.police.uk> permite utilizatorilor să își introducă codul poștal pentru a vizualiza informații detaliate despre numărul și natura opririlor din zona lor. Informațiile publicate se bazează pe procesele-verbale de oprire și percheziționare completate. În plus, [tabloul de bord al acțiunilor de oprire și percheziționare](#) al Poliției Metropolitane oferă date despre toate opririle și percheziționările din Londra, inclusiv despre proporția persoanelor cu origine etnică minoritară oprite în raport cu populația generală. Utilizatorii pot accesa online date detaliate în diferite moduri, de exemplu:

- o hartă care arată locul exact al acțiunilor de oprire și percheziționare efectuate lunar într-o anumită zonă. Acest instrument oferă totodată informații detaliate despre fiecare oprire și percheziționare (obiect, tip, rezultat, dacă acțiunea a făcut parte dintr-o operațiune a poliției), despre persoana vizată (gen, interval de vârstă, etnie autodeclarată, etnie prezumată de agent) și despre legea care sprijină legalitatea acțiunii de oprire și percheziționare (a se vedea [figura 11](#)); și

- o imagine generală a statisticilor și a graficelor care prezintă acțiunile de oprire și percheziționare ale poliției. Informațiile pot fi agregate și descărcate.

Deși promovează transparența și încrederea, această practică ar putea să afecteze drepturile la intimitate și la protecția datelor ale persoanelor vizate. Este posibil ca identitatea unei persoane să poată fi dedusă din combinația de date disponibile în acest instrument sau în alte instrumente online. Aceste riscuri trebuie evaluate și, după caz, eliminate.

### 2.3.2. Camere de corp

Forțele de poliție folosesc din ce în ce mai des camere de corp. Acestea pot contribui la asumarea răspunderii, la îmbunătățirea calității interacțiunilor individuale și la modificarea tiparelor de comportament părtinitor. De asemenea, pot ajuta la dezamorsarea situațiilor periculoase. Pe lângă filmările realizate de polițiști, și membrii publicului filmează din ce în ce mai mult opririle și alte interacțiuni cu poliția. Filmările pot fi utilizate inclusiv pentru analizarea practicilor poliției.

Figura 11: Instrument online care prezintă detalii despre acțiunile de oprire și percheziționare efectuate în Londra

POLICE.UK Find your neighbourhood 🔍 Share this page ➦

Home > Metropolitan Police Service > London Fields > Stop and search >

## Stop and search map

In this neighbourh

- [Overview](#)
- [Crime map](#)
- [Stop and search](#)
- [Policing team](#)
- [News and events](#)
- [Performance](#)
- [Community Payback](#)

Next steps

- [Stop and search overview](#)
- [Metropolitan Police Service](#)

Related links

- [Stop and search FAQs](#)

Click on the dots on the map for information about individual stop and searches.

Showing: April 2018 Update

[View A-Z list of stop and search locations](#)

[View the crime map for London Fields](#)

1076 stop and searches were carried out by Metropolitan Police Service this month that could not be mapped to a location.

The British Transport Police are responsible for policing railways in the Metropolitan Police Service area. [View summary information for stop and searches conducted by the British Transport Police.](#)

Location anonymisation is accurate to 2012 population and housing developments. [Learn more](#)

Please [contact us](#) about any privacy concerns, or feedback about how useful and useable you find this stop and search information.

Sursa: Regatul Unit, Home Office, pagina web cu harta acțiunilor de oprire și percheziționare.

**Stop and searches on or near Forest Road in April 2018**

**Stop and search at 29 April 2018, 12:20 p.m.**

<b>Object of search:</b> Articles for use in criminal damage	<b>Self-defined ethnicity:</b> Black/African/Caribbean/Black British - Any other Black/African/Caribbean background
<b>Type of search:</b> Person search	<b>Officer-defined ethnicity:</b> Black
<b>Outcome:</b> A no further action disposal	<b>Removal of more than just outer clothing:</b> Unknown
<b>Part of a policing operation:</b> No	<b>Legislation:</b> Police and Criminal Evidence Act 1984 (section 1)
<b>Gender:</b> Male	<b>Outcome linked to object of search:</b> Unknown
<b>Age range:</b> over 34	

**Next steps**

- [View stop and search overview for Metropolitan Police Service](#)
- [Contact us regarding a privacy concern or to provide stop and search feedback](#)
- [Contact your local policing team](#)
- [Attend your next beat meeting](#)

**Related links**

- [Stop and search FAQs](#)

*Sursa: Regatul Unit, Home Office, [pagina web referitoare la perchezițiile specifice](#).*

## Studiu de caz

### Eficacitatea camerelor de corp

Un studiu realizat în 2015 în Regatul Unit cu privire la utilizarea a 500 de camere de către 814 agenți din cadrul Poliției Metropolitane a arătat că nu a existat „niciun impact general asupra numărului sau tipului de opriri și percheziționări efectuate; niciun efect asupra proporției de arestări pentru infracțiuni violente; și nicio dovadă că aceste camere au schimbat modul în care ofițerii s-au purtat față de victime sau de suspecți”. Rapoartele de evaluare a impactului unor experimente similare efectuate de alte structuri polițienești nu au adus decât cel mult puține dovezi că acestea ar fi avut vreun efect pozitiv în reducerea criminalității, a plângerilor față de agenți sau a cazurilor de folosire a forței.

*Pentru mai multe informații, a se vedea Big Brother Watch (2017).*



În Franța au fost introduse camere de corp în 300 de localități pentru o perioadă-pilot de doi ani. În iunie 2018, o analiză a Ministerului Afacerilor Interne a evidențiat efectele pozitive și rezultatele experimentului. În special, raportul a subliniat că purtarea camerelor de corp a avut drept efect descurajarea persoanelor oprite de a abuza sau de a insulta poliția. Rapoartele provenite de la unele municipalități au indicat că utilizarea camerelor individuale a redus agresivitatea și comportamentul ofensator față de polițiști. Unele municipalități au semnalat că utilizarea camerelor de corp pare să fi dezamorsat situații în care, în lipsa lor, s-ar fi putut ajunge la infracțiuni împotriva polițiștilor. Deși aceste rapoarte sugerează că utilitatea camerelor de corp constă în special în crearea unui efect disuasiv, unele imagini au fost folosite ca probe pentru identificarea infractorilor în justiție. Nu în ultimul rând, mai multe municipalități au subliniat utilitatea educațională a acestui dispozitiv, deoarece unii polițiști au beneficiat de formare cu privire la procedurile și tehnicile de intervenție vizionând înregistrările efectuate în timpul intervențiilor. În urma experimentului pilot, a fost depus la Parlamentul francez un proiect de lege având ca scop armonizarea utilizării camerelor de corp în toate structurile polițienești și extinderea utilizării acestora la pompieri și la polițiștii care lucrează în închisori.

*Pentru mai multe informații, a se vedea Franța, Ministerul Afacerilor Interne (2018).*

Un experiment amplu cu durata de 12 luni, care a studiat purtarea camerelor de corp în perioada 2012-2013 la Rialto, în Statele Unite, a analizat dacă aceste camere ar putea determina un comportament dezirabil din punct de vedere social în rândul agenților care le poartă. Rezultatele arată că, în comparație cu 2011, în perioada de 12 luni studiată, folosirea forței a scăzut de la 60 la 25 de cazuri, iar numărul plângerilor împotriva poliției a scăzut de la 28 la 3.

*Pentru mai multe informații, a se vedea Farrar, T. (2018).*

Pe de altă parte, utilizarea camerelor de corp de către poliție creează îngrijorări importante de ordin operațional și legate de drepturile fundamentale. Sunt necesare garanții și politici clare privind utilizarea lor pentru a aborda următoarele chestiuni:

- nu este clar **rolul camerelor de corp în depistarea și descurajarea utilizării ilegale a profilurilor**. Camerele surprind incidente individuale și nu permit

colectarea de date statistice care ar putea fi utilizate pentru a stabili dacă operațiunile de oprire și percheziționare sunt discriminatorii. Ele pot fi folosite mai degrabă pentru a analiza și a discuta despre interacțiunile individuale, contribuind la îmbunătățirea calității acestora;

- utilizarea camerelor de corp ar putea avea **efecte negative asupra relațiilor cu comunitățile minoritare**, dacă acestea simt că sunt vizate în mod specific. Insti-tuirea de garanții și de politici în consultare cu comunitățile locale poate contribui la promovarea ideii că aceste echipamente sunt un instrument de îmbunătățire a responsabilității, nu un mijloc de a stigmatiza grupurile minoritare;
- utilizarea camerelor de corp are **consecințe asupra drepturilor la viață privată și la protecția datelor**, precum și asupra altor drepturi fundamentale ale omului. De exemplu, ele ar putea afecta libertatea de întrunire pașnică dacă sunt utilizate pentru a monitoriza demonstrațiile publice. Adesea nu este clar când trebuie pornită și când trebuie oprită camera și ce se întâmplă dacă un agent uită sau decide să nu o pornească: sunt necesare îndrumări clare în această privință. Companiile private care furnizează acest serviciu trebuie să înțeleagă clar că nu au dreptul să prelucreze filmările în scopuri proprii. Utilizarea camerelor de corp ar trebui regle-mentată prin lege pentru a se asigura respectarea drepturilor fundamentale.

#### **În obiectiv: utilizarea eficientă a camerelor de corp**

Se poate contribui la asigurarea unei utilizări eficiente a camerelor de corp prin respectarea a trei principii importante:

- **autenticitate:** imaginile trebuie să fie legate în mod clar de incident. Trebuie înregistrate data și ora (de exemplu, prin marcaj temporal) și locul exact al incidentului (de exemplu, cu ajutorul GPS-ului);
- **fiabilitate:** imaginile trebuie încărcate în sistemul central într-un mod riguros, securizat și confidențial. Ele trebuie să respecte principiul protecției datelor și al respectării vieții private și, prin urmare, nu trebuie păstrate pentru o perioadă mai lungă decât cea specificată de lege;
- **admisibilitate:** pentru a fi utile în procedurile penale, filmările trebuie să fie admisibile în instanță. Aceasta poate presupune:

- evitarea înregistrării video continue, care constituie o ingerință inacceptabilă în dreptul la viață privată atât al polițiștilor, cât și al persoanelor filmate;
- informarea celor care pot fi filmați și obținerea acordului lor (atunci când este necesar);
- stocarea imaginilor cu asigurarea unui nivel adecvat de securitate și urmărirea accesării imaginilor atât de către polițiști, cât și de către cetățeni.

*Pentru mai multe informații, a se vedea Coudert et al. (2015), p. 8.*

Evoluțiile tehnologice suplimentare vor necesita elaborarea de noi garanții pentru a asigura utilizarea legală a camerelor de corp. De exemplu, camerele care pot recunoaște automat chipul unei persoane prin compararea și potrivirea cu înregistrări anterioare dintr-o bază de date existentă creează noi probleme legate de dreptul la viață privată și la protecția datelor.

## **Studiu de caz**

### **Camerele de corp ale poliției: un bilanț al politicilor (SUA)**

În vederea creșterii transparenței și a responsabilității la utilizarea camerelor de corp, organizațiile Leadership Conference on Civil and Human Rights și Upturn din Statele Unite au creat un instrument de evaluare și structurare a informațiilor care pot fi extrase din filmările realizate de camerele de corp.

Instrumentul propune opt criterii pentru evaluarea acestor imagini:

1. dacă filmările sunt făcute publice de către departamentul de poliție și sunt ușor accesibile;
2. dacă se specifică clar marja de apreciere a agenților cu privire la momentul pornirii înregistrării;
3. dacă sunt abordate problemele legate de viața privată;
4. dacă agenții trebuie să examineze filmările înainte de a redacta raportul scris inițial;

5. dacă secvențele nemarcate trebuie șterse într-o perioadă predefinită;
6. dacă filmările sunt protejate împotriva manipulării și a utilizării necorespunzătoare;
7. dacă filmările sunt puse la dispoziția persoanelor care depun plângeri;
8. dacă este restricționată sau nu utilizarea tehnologiilor biometrice de identificare a persoanelor din imagini.

Astfel de inițiative pot ajuta la consolidarea răspunderii prin stabilirea de standarde și încurajarea implementării unor mecanisme prin care să se evalueze dacă filmările sunt colectate și utilizate în mod corespunzător.

*Pentru mai multe informații, a se vedea Leadership Conference on Civil and Human Rights și Upturn, [site-ul privind tabloul de bord al politicilor](#).*

### 2.3.3. Mecanisme de tratare a plângerilor

Existența unor mecanisme eficiente de tratare a plângerilor poate să descurajeze abuzul de putere și totodată să contribuie la asigurarea și la restabilirea încrederii publicului în operațiunile autorităților polițienești și de gestionare a frontierelor. Aceste mecanisme există de obicei alături de canale legale oficiale care fac posibilă contestarea de către cetățeni a acțiunii sau a deciziei unei autorități publice în fața unei instanțe independente și imparțiale.

Pentru ca mecanismele de tratare a plângerilor să fie eficiente, este esențial ca:

- **cetățenii să le poată accesa cu ușurință:** dovezile arată invariabil că oamenii sunt reticenți să depună reclamații, de exemplu pentru că este un proces lung sau costisitor sau pentru că se tem de repercusiuni negative. Asigurarea accesului ușor la mecanismele de tratare a plângerilor, prin utilizarea de platforme online cum sunt site-urile sau aplicațiile, ar putea încuraja oamenii să le folosească. În plus, organizațiile pot sprijini persoanele în depunerea plângerilor, fie depunând plângerile în numele lor, fie prin mecanisme de acțiune colectivă în despăgubire, astfel cum se prevede la articolul 80 alineatul (2) din RGPD;

- **plângerile să fie gestionate în mod transparent:** acest lucru va contribui la creșterea încrederii în mecanismele de tratare a plângerilor;
- **organele de soluționare a plângerilor să fie independente** față de organizație sau de acea parte a organizației împotriva căreia este formulată plângerea.

Există o varietate de diferite mecanisme care gestionează diferite tipuri de reclamații. [Figura 12](#) oferă o prezentare generală a câtorva dintre mecanismele de tratare a plângerilor disponibile în statele membre ale UE și la nivelul Uniunii în ansamblu.

Figura 12: Prezentare generală a mecanismelor de tratare a plângerilor din statele membre ale UE



Mecanismele în cadrul cărora polițiștii se întâlnesc cu membri ai publicului pentru a le asculta plângerile, a discuta despre profiluri și a primi feedback cu privire la operațiunile lor oferă ocazia de a învăța lecții importante pentru îmbunătățirea proceselor care reglementează activitățile legate de profiluri. Totodată, creează un mijloc de implicare a publicului în activitățile de aplicare a legii (a se vedea studiul de caz).

## **Studiu de caz**

### **Mecanisme publice de tratare a plângerilor în sectorul aplicării legii**

#### **Grupuri de dezbatere pentru exercitarea controlului public (Poliția West Midlands – Regatul Unit)**

Fiecare dintre cele opt circumscripții de poliție din cadrul Poliției West Midlands (WMP) organizează o întâlnire bilunară a Grupului de examinare a operațiunilor de oprire și percheziționare, prezidată de membri ai publicului. Aceste dezbateri evaluează evidențele referitoare la operațiunile de oprire și percheziționare, se asigură că WMP respectă legea și oferă comunităților un canal de transmitere a plângerilor și de exprimare a îngrijorărilor. Ordinea de zi și procesele-verbale ale ședințelor se publică online. În plus, WMP a adoptat o serie de practici legate de implicarea comunității, în efortul de a spori echitatea și specificitatea acțiunilor de oprire pe stradă și de a responsabiliza suplimentar agenții.

*Pentru mai multe informații, a se vedea Poliția West Midlands, [pagina web privind operațiunile de oprire și percheziționare](#), și *Her Majesty's Inspectorate of Constabulary* (2016).*

#### **Grupuri de dezbatere privind motivele rezonabile (Poliția Northamptonshire – Regatul Unit)**

Poliția Northamptonshire a instituit grupuri de dezbatere privind motivele rezonabile cu scopul de a implica membrii publicului în îmbunătățirea operațiunilor de oprire și percheziționare. Aceste grupuri reprezintă un canal de discuții privind utilizarea competențelor de oprire și percheziționare și impactul acestora asupra comunităților. Ele sunt prezidate de un inspector-șef și formate dintr-un ofițer din prima linie și doi membri ai comunității, care pot fi inclusiv delincvenți sau foști delincvenți. Pe lângă îmbunătățirea

comunicării dintre poliție și public, grupul are autoritatea de a restrânge competențele agenților și de a le impune o instruire suplimentară în vederea îmbunătățirii operațiunilor de oprire și percheziționare.

*Pentru mai multe informații, a se vedea pagina web a grupului de dezbateri instituit de Poliția Northamptonshire și [Open Society Justice Initiative](#) (2018a).*

### **Rețea informală de mecanisme de tratare a plângerilor**

Rețeaua autorităților independente de tratare a plângerilor împotriva poliției (IPCAN) este o rețea informală de cooperare între structurile independente care răspund de controlul extern al forțelor de securitate. A fost creată în 2013 și reunește autorități de soluționare a plângerilor din aproximativ 20 de țări. Aceste organisme, în principal din statele membre ale UE, primesc și prelucrează plângeri împotriva forțelor de securitate publice și, uneori, și împotriva celor private.

*Pentru mai multe informații, a se vedea [site-ul IPCAN](#).*

În cadrul gestionării frontierelor, pot fi instituite mecanisme publice de tratare a plângerilor prin posibilitatea de a depune plângere la fața locului sau ulterior. Posibilitatea de a accesa astfel de mecanisme sporește transparența și responsabilitatea și încurajează respectul reciproc și relațiile bune între poliștii de frontieră și public. Opțiunea de a depune o plângere ulterior, la un organism superior, nu (doar) direct la punctul de trecere a frontierei, creează un anumit grad de supraveghere și poate influența pozitiv disponibilitatea călătorilor de a denunța eventualele incidente<sup>35</sup>.

### **Studiu de caz**

#### **Mecanisme publice de tratare a plângerilor în gestionarea frontierelor**

#### **Mecanismul intern de tratare a plângerilor de la aeroportul Manchester (Regatul Unit)**

La aeroportul din Manchester, Central Allocation Hub este un punct unic de contact pentru toți pasagerii care doresc să depună o plângere. Plângerile

35 FRA (2014b).



pot fi depuse prin e-mail, scrisoare, telefon sau fax sau față în față, în limba engleză sau galeză. Orientările Poliției de Frontieră a Regatului Unit prezintă modalitățile posibile de soluționare a plângerilor. Abaterile minore, cum ar fi impolitețea, bruscarea sau atitudinea necorespunzătoare pot fi rezolvate de obicei la nivel local, prin clarificarea problemelor cu clientul, explicarea procedurilor operaționale, convenirea unor acțiuni suplimentare și prezentarea de scuze, dacă este cazul. Plângerile privind abaterile grave sunt repartizate de obicei Unității de standarde profesionale. Orientările Poliției de Frontieră includ un test pentru identificarea semnelor unei eventuale discriminări, care ar constitui o abatere gravă. Dacă există dovezi inițiale puternice că modul în care a fost tratat un pasager poate fi explicat prin alți factori decât cei rasiali, cazul este trimis de obicei spre soluționare locală.

*Pentru mai multe informații, a se vedea FRA (2014a), p. 74.*

### **Mecanismul Frontex de tratare a plângerilor individuale (UE)**

În urma adoptării noului Regulament privind Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (Frontex) în 2016, Frontex a instituit un mecanism de tratare a plângerilor individuale pentru a monitoriza respectarea drepturilor fundamentale în cadrul activităților sale. Aceste activități cuprind proiecte pilot, operațiuni de returnare, operațiuni comune, intervenții rapide la frontieră, detașări de echipe de sprijin pentru gestionarea migrației și intervenții pentru returnare. Orice persoană ale cărei drepturi au fost afectate în mod direct de acțiuni ale personalului, inclusiv ale personalului autorităților publice naționale implicat în astfel de activități ale Frontex, poate depune o plângere la ofițerul Frontex pentru drepturile fundamentale. Ofițerul decide asupra admisibilității plângerii și o înaintează directorului executiv al Frontex, precum și autorităților din statul membru afectat dacă în presupusa încălcare a fost implicat și personal național. Plângerea poate fi depusă în orice limbă, prin e-mail, scrisoare sau prin formularul de plângere online disponibil pe site-ul Frontex: <http://frontex.europa.eu/complaints>.

### **În obiectiv: drepturile agenților de aplicare a legii**

Polițiștii se bucură de aceleași drepturi și libertăți ca și celelalte persoane și sunt protejați de standardele privind drepturile omului în timpul exercitării activității. Ei se pot prevala de drepturile lor prevăzute în diverse documente internaționale din domeniul drepturilor omului, cum sunt Convenția europeană a drepturilor omului (CEaDO) sau Pactul internațional cu privire

la drepturile civile și politice (PIDCP). Codul european de etică al poliției clarifică următoarele: „[c]a regulă generală, personalul de poliție beneficiază de aceleași drepturi civile și politice ca și ceilalți cetățeni. Se pot introduce restrângeri ale acestor drepturi numai atunci când sunt necesare pentru exercitarea funcțiilor poliției într-o societate democratică, în conformitate cu legislația și cu Convenția europeană a drepturilor omului.” În articolul 11 din CEaDO apare menționată o excepție referitoare la dreptul la libertatea de întrunire și de asociere.

Atunci când îndeplinește funcții polițienești, în special atunci când exercită atribuțiile cu care este abilitat, polițistul nu acționează în calitate de persoană privată, ci în calitate de organ al statului. Prin urmare, obligația statului de a respecta și a proteja drepturile omului are un efect direct asupra opțiunilor de răspuns pe care le are polițistul în fața agresiunilor. Drepturile polițiștilor, care pot risca să fie răniți sau chiar uciși în cursul îndeplinirii sarcinilor de serviciu, trebuie să fie la rândul lor respectate și protejate, de exemplu prin asigurarea de echipamente de protecție, prin planificarea atentă a operațiunilor polițienești sau prin luarea unor măsuri preventive. Este posibil să fie necesară restrângerea drepturilor polițiștilor în vederea exercitării atribuțiilor polițienești, dar orice restrângere trebuie să respecte principiul proporționalității. Dat fiind rolul său special de organ al statului, polițistul se poate confrunta cu o limitare mai puternică a drepturilor sale decât „cetățeanul de rând”. Luând ca exemplu cazul unei demonstrații care devine violentă, „cetățeanul de rând” poate să fugă sau să ceară ajutor, pe când polițistul este obligat să apere drepturile celorlalți oameni și să restabilească ordinea publică.

*Pentru mai multe informații, a se vedea FRA (2013).*

# 3

## Crearea profilurilor pe bază de algoritmi



Crearea profilurilor pe bază de algoritmi include orice tehnici computerizate care analizează date pas cu pas pentru a identifica tendințe, tipare sau corelații<sup>36</sup>. Prin aceste profiluri, individul este selectat „pe baza conexiunilor cu alte persoane identificate de algoritm, mai degrabă decât pe baza comportamentului real”, iar „alegerile indivizilor sunt structurate în funcție de informațiile despre grup” mai degrabă decât în funcție de propriile alegeri personale<sup>37</sup>.

Crearea profilurilor pe bază de algoritmi poate fi pentru organizațiile de gestionare a frontierelor și de aplicare a legii o modalitate eficientă de a utiliza date pentru a preveni, depista și investiga infracțiunile. Pe de altă parte, colectarea și prelucrarea unor seturi mari de date creează o serie de îngrijorări legate de drepturile fundamentale. Pe lângă importanța nevoii de a evita discriminarea, crearea de profiluri pe bază de algoritmi introduce noi riscuri, în special în ceea ce privește drepturile la viață privată și la protecția datelor. Secțiunea de față se concentrează mai întâi asupra acestor noi riscuri, după care ilustrează provocările legate de drepturile fundamentale asociate cu utilizarea algoritmilor pentru a crea profiluri pe baza unor baze mari de date în scopuri de securitate și de gestionare a frontierelor, sugerând câteva modalități de reducere la minimum a acestor riscuri.

36 Pentru mai multe informații despre algoritmi, vezi FRA (2018b), p. 4.

37 Mittelstadt, BD, Allo, P., Taddeo, M., Wachter, S. și Floridi, L. (2016).

### **În obiectiv: activitățile polițienești bazate pe analiza predictivă**

Autoritățile de aplicare a legii utilizează mai multe aplicații software pentru a prezice momentul și locul în care va fi comisă o infracțiune. Iată câteva exemple: PredPol în Regatul Unit și SUA, sistemul de conștientizare a criminalității (CAS) în Țările de Jos și Precobs în Germania și Elveția. Totuși, eficacitatea acestor metode predictive pentru prevenirea infracțiunilor nu a fost încă evaluată corespunzător. Dovezile de până acum arată constatări contradictorii, ca în exemplele de mai jos.

### **Testare pe teren a activităților polițienești bazate pe analiza predictivă în Kent (Regatul Unit) și la Los Angeles (SUA)**

Poliția din Regatul Unit și din SUA a efectuat un experiment pentru a compara – în opoziție cu abordarea mai tradițională – un algoritm complet automat de identificare a punctelor cu criminalitate ridicată și de planificare a patrulelor de poliție în consecință.

Rezultatele au arătat că algoritmul automat a identificat mai bine infracțiunile ulterioare. Acesta a prezis de 1,4-2,2 ori mai multe fapte penale decât un analist al criminalității care a folosit informații tradiționale în materie penală și practici clasice de cartografiere a criminalității. În plus, acțiunile de patrulare bazate pe instrumentul predictiv sunt mai eficiente, ducând la o reducere a numărului de infracțiuni cu 7,4 % în medie.

*Pentru mai multe informații, a se vedea Mohler, G.O., et al. (2016).*

### **Programul PILOT (Predictive Intelligence Led Operational Targeting) (Stabilirea țintelor operaționale pe bază de informații predictive) folosit la Shreveport (SUA)**

Acest program utilizează un model predictiv pentru identificarea zonelor restrânse cu risc crescut de infracțiuni contra patrimoniului și pentru implementarea unui model de intervenție în zonele respective pentru prevenirea acestui tip de infracțiuni. Rezultatele din trei districte care utilizează PILOT au fost comparate cu trei districte în care s-au desfășurat activități polițienești tradiționale. Nu au existat dovezi statistice ale unei reduceri mai mari a infracțiunilor contra patrimoniului în cele trei districte PILOT examinate.

*Pentru mai multe informații, a se vedea Hunt, P. et al. (2014).*

## Software-ul Beware (SUA)

„Beware” pune la dispoziția agenților care răspund apelurilor de urgență un cod de culori (roșu, galben și verde) care indică nivelul de pericol pentru persoana sau zona amenințată. Software-ul efectuează căutări în baze de date precum cele cu rapoarte de arestare, fișe ale proprietăților, baze de date comerciale, realizează căutări aprofundate pe internet, printre postările de pe platformele de comunicare socială și în alte baze de date disponibile publicului.

Nu au fost încă evaluate punctele tari și punctele slabe ale acestui sistem. Totuși, lipsa supravegherii procesului decizional și caracterul secret al algoritmului, care este protejat de secretul comercial, au creat îngrijorări cu privire la asumarea răspunderii. În plus, potențiala inexactitate a datelor colectate și/sau a informațiilor deduse din analiză poate reduce eficacitatea generală a instrumentului.

*Pentru mai multe informații, a se vedea Uniunea Americană pentru Libertăți Civile (2016).*

## Studiu de caz

### **Evaluarea impactului și a riscurilor activităților polițienești bazate pe analiza predictivă – instrumentul de evaluare ALGO-CARE**

Pentru a asigura o imagine de ansamblu echilibrată și transparentă a impactului pe care îl au activitățile polițienești bazate pe analiza predictivă asupra societății, trebuie luate în considerare potențialele efecte negative ale utilizării acestora. Analiza efectuată de un grup format din cadre universitare și polițiști a concluzionat că, întrucât activitățile polițienești bazate pe analiza predictivă se află încă într-o etapă experimentală în Regatul Unit, sunt necesare evaluări detaliate ale impactului lor asupra societății și a persoanelor. Cercetarea susține că unele dintre decizii ar putea avea un impact prea mare asupra societății și asupra unor persoane pentru a fi lăsate sub influența unei tehnologii emergente; în aceste situații nu ar trebui folosit un proces decizional pe bază de algoritmi.

Grupul a elaborat un cadru menit să ajute la luarea deciziilor privind implementarea instrumentelor de evaluare algoritmică în contextul activităților polițienești, numit ALGO-CARE. Acest cadru își propune să ofere îndrumare polițiștilor atunci când evaluează potențialele riscuri ale activităților polițienești bazate pe analiza predictivă. De asemenea, încearcă să transpună principiile-cheie ale dreptului public și ale drepturilor omului în considerente practice și în orientări care să poată fi utilizate de către organismele din sectorul public.

Instrumentul de evaluare invită polițiștii să examineze utilizarea analizei predictive în activitățile polițienești prin parcurgerea a opt pași complementari:

- **Consultare:** se evaluează amploarea intervenției umane;
- **Legalitate:** se evaluează justificarea juridică pentru utilizarea algoritmului;
- **Granularitate:** se evaluează dacă algoritmul poate prezenta un nivel suficient de detaliu în cazul respectiv;
- **Proprietate:** se asigură faptul că structura de poliție are proprietatea legală și capacitatea tehnică de a accesa, întreține, actualiza și corecta codul sursă cu regularitate;
- **Contestabilitate:** se garantează existența unor mecanisme de supraveghere și de audit;
- **Exactitate:** se evaluează dacă algoritmul corespunde scopului activității polițienești, dacă poate fi validat periodic și dacă probabilitatea și impactul unei eventuale inexactități reprezintă un risc acceptabil;
- **Responsabilitate:** se evaluează corectitudinea, responsabilitatea și transparența algoritmului;
- **Explicabilitate:** se evaluează accesibilitatea informațiilor, atât cu privire la regulile de luare a deciziilor, cât și la impactul pe care fiecare factor îl are asupra rezultatului final.

*Pentru mai multe informații, a se vedea Oswald, M. et al. (2017).*

### 3.1. Cadrul de protecție a datelor care reglementează crearea de profiluri pe bază de algoritmi

Dezvoltarea și utilizarea într-o măsură din ce în ce mai mare a noilor tehnologii – inclusiv utilizarea în creștere a seturilor mari de date în sprijinul luării deciziilor – a determinat UE să realizeze o amplă revizuire a normelor care reglementează prelucrarea datelor cu caracter personal în 2016. Cele două instrumente noi, Regulamentul general privind protecția datelor (RGPD) și Directiva privind poliția, stabilesc principii și standarde importante care se aplică oricărei decizii bazate pe procese computerizate, printre care se numără și crearea profilurilor pe bază de algoritmi.

RGPD și Directiva privind poliția au intrat în vigoare în mai 2018, de aceea la momentul redactării prezentului ghid există puține exemple practice de punere în aplicare. Secțiunea 1.2.2 descrie standardele legale care reglementează drepturile la viață privată și la protecția datelor și explică câteva diferențe principale dintre RGPD și Directiva privind poliția (a se vedea tabelul 2). Capitolul de față se bazează pe aceste informații pentru a descrie și a explica cerințele legale referitoare la crearea profilurilor pe bază de algoritmi introduse de RGPD și de Directiva privind poliția. Acestea sunt:

- Datele trebuie prelucrate în scopuri specifice, bazate pe un temei juridic specific.
- Persoanele fizice trebuie să fie informate atunci când le sunt prelucrate datele cu caracter personal.
- Datele trebuie păstrate în siguranță.
- Trebuie depistată și prevenită prelucrarea ilegală a datelor.

Agenții și ofițerii de poliție și polițiștii de frontieră care au nevoie de informații suplimentare despre cerințele legale descrise în prezentul capitol trebuie să se adreseze responsabililor cu protecția datelor din organizațiile lor. În plus, *Manualul de legislație europeană privind protecția datelor* elaborat de FRA, AEPD și Consiliul Europei oferă îndrumări suplimentare referitoare la aplicarea Directivei privind poliția și a RGPD<sup>38</sup>.

38 FRA, AEPD și Consiliul Europei (2018).

## Aspecte esențiale

- Crearea profilurilor pe bază de algoritmi trebuie să fie **legitimă, necesară și proporțională**.
- Datele nu trebuie să fie prelucrate fără un **scop specific bazat pe un temei juridic specific**.
- Persoanele fizice au anumite drepturi specifice, descrise detaliat în dispozițiile RGPD și ale Directivei privind poliția, printre care:
  - **dreptul de a fi informate**, inclusiv de a primi informații semnificative despre logica pe care se bazează algoritmul;
  - dreptul de **acces la propriile date cu caracter personal**;
  - dreptul de **a depune o plângere** la o autoritate de supraveghere; și
  - dreptul la o **cale de atac eficientă**.
- Datele trebuie să fie colectate, prelucrate și stocate **în condiții de siguranță**.
- Trebuie **prevenite și depistate** cazurile de prelucrare ilegală a datelor.

### 3.1.1. Datele trebuie prelucrate cu un scop specific

Orice prelucrare a datelor cu caracter personal trebuie să aibă un temei juridic, adică trebuie efectuată pentru atingerea unui **scop specific** prevăzut de lege.

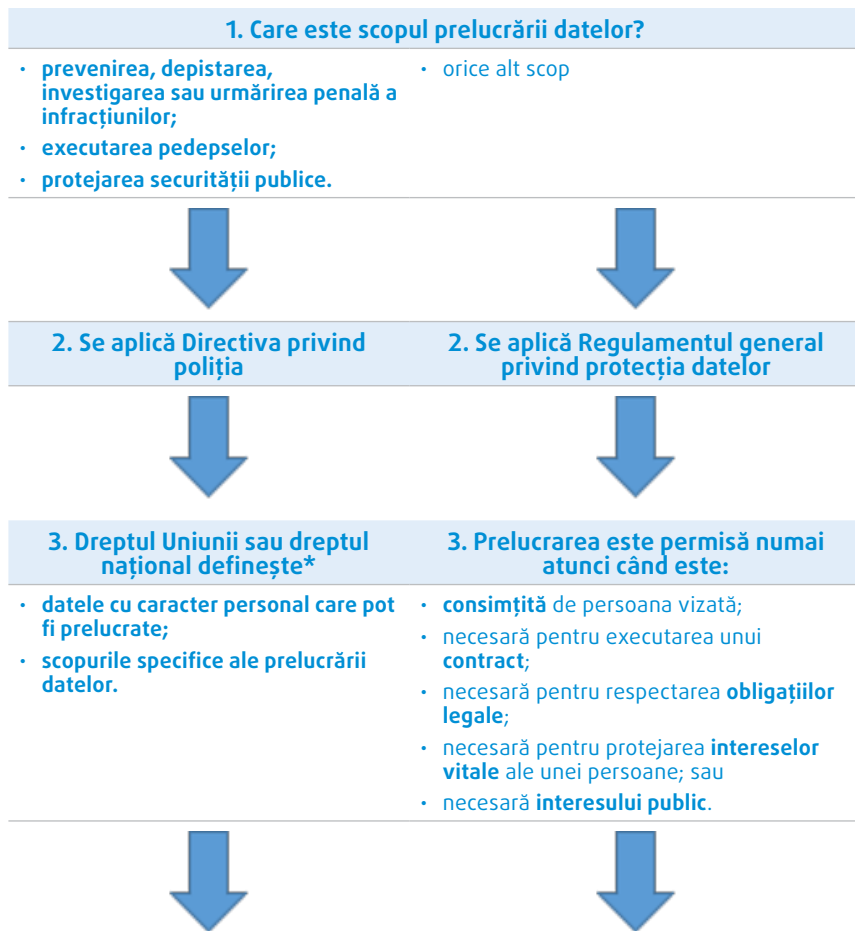
Înainte de orice prelucrare, agentul trebuie să cunoască scopul acesteia. Iată câteva exemple de scopuri:

- Datele sunt prelucrate pentru a depista o infracțiune?
- Sunt prelucrate pentru a menține siguranța publică?
- Sunt prelucrate pentru a combate terorismul?

După ce scopul este corect identificat, agenții vor ști ce cadru juridic se aplică și care sunt obligațiile legale relevante. [Tabelul 4](#) prezintă modul de identificare a cadrului juridic aplicabil.



Tabelul 4: Identificarea cadrului juridic corect în funcție de scopul prelucrării



#### 4. Scopul creării de profiluri este exceptat de la aplicarea Directivei privind poliția?

**Drepturile de a fi informat, de a avea acces la propriile date cu caracter personal și de a solicita modificarea sau ștergerea datelor pot fi restricționate (total sau parțial) în următoarele cazuri:**

- pentru a evita obstrucționarea **cercetărilor**, anchetelor sau procedurilor oficiale sau juridice;
- pentru a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;
- pentru protejarea securității publice;
- pentru protejarea securității naționale;
- pentru protejarea drepturilor și libertăților celorlalți.

#### 4. Scopul creării de profiluri este exceptat de la aplicarea RGPD?

Obligațiile (de transparență, de informare și de notificare a încălcărilor) și drepturile (de acces, rectificare, ștergere, opoziție sau de a nu face obiectul unui proces decizional automatizat) stabilite în RGPD **pot fi restricționate** de legislația națională sau a UE pentru a proteja:

- securitatea națională, apărarea sau securitatea publică;
- prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;
- alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale;
- protejarea independenței judiciare și a procedurilor judiciare;
- prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate;
- funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazuri specifice;
- protecția persoanei vizate sau a drepturilor și libertăților altora;
- punerea în aplicare a pretențiilor de drept civil.

Notă: *\*Legile naționale de transpunere a Directivei privind poliția sunt disponibile pe site-ul EUR-Lex.*

Sursa: *FRA, 2018.*

### 3.1.2. Persoanele fizice trebuie informate

Articolul 13 din Directiva privind poliția și articolele 13 și 14 din RGPD impun ca persoanele fizice să fie informate atunci când le sunt prelucrate datele cu caracter personal. Tabelul 5 descrie cum și când trebuie comunicate informații persoanei ale cărei date sunt prelucrate.

**Tabelul 5: Obligația de a furniza persoanelor informații referitoare la crearea de profiluri: tipul datelor, mijloacele de comunicare și excepțiile**

<b>Obligația de notificare – listă de verificare</b>	
<b>Cui?</b>	Persoanei ale cărei date sunt prelucrate
<b>Cum?</b>	<ul style="list-style-type: none"> <li>• limbaj simplu și clar</li> <li>• format ușor accesibil</li> <li>• în aceeași formă în care s-a formulat cererea – <i>preferabil prin mijloace electronice</i></li> </ul>
<b>Ce informații?</b>	<p><b>Despre prelucrare:</b></p> <ul style="list-style-type: none"> <li>• denumirea autorității pe care o reprezentați și datele de contact</li> <li>• datele de contact ale responsabilului cu protecția datelor</li> <li>• scopurile prelucrării</li> <li>• temeiul juridic al prelucrării</li> <li>• perioada maximă de stocare a datelor</li> <li>• tipurile de persoane/organizații care vor primi datele</li> </ul> <p><b>Despre drepturile persoanelor:</b></p> <ul style="list-style-type: none"> <li>• dreptul de a <b>depune o plângere</b> la o autoritate de supraveghere și datele de contact ale autorității de supraveghere</li> <li>• dreptul de a solicita <b>acces</b> la propriile date cu caracter personal</li> <li>• <b>rectificarea și/sau ștergerea</b> datelor cu caracter personal</li> <li>• dreptul de a solicita <b>restricționarea</b> prelucrării</li> </ul>
<b>Excepții</b>	<ul style="list-style-type: none"> <li>• În cazul cererilor excesive (adică repetitive) sau vădit nefondate</li> <li>• Atunci când identitatea solicitantului nu poate fi confirmată în mod clar</li> <li>• Atunci când comunicarea informațiilor ar obstrucționa investigațiile</li> <li>• Atunci când comunicarea informațiilor ar prejudicia prevenirea/investigarea infracțiunilor</li> <li>• Pentru a proteja securitatea publică sau națională</li> <li>• Pentru a proteja drepturile altor persoane</li> </ul>

Sursa: FRA, 2018.

### **În obiectiv: „dreptul la explicații”**

În cazurile în care se creează profiluri, RGPD impune ca persoanei vizate să îi fie furnizate „informații pertinente privind logica utilizată și privind importanța și consecințele preconizate” ale prelucrării datelor. Acestea trebuie furnizate atunci când datele sunt colectate (notificare), dar și în cazul în care persoana solicită informații suplimentare (dreptul de acces). Acest drept nu este menționat în mod explicit în Directiva privind poliția. Totuși, considerentul 38 precizează că „[prelucrarea automată] ar trebui să facă obiectul unor garanții corespunzătoare, inclusiv o informare specifică a persoanei vizate [...], în special [...] de a primi o explicație privind decizia luată în urma unei astfel de evaluări sau de a contesta decizia”.

Acest „drept la explicații” se poate dovedi dificil de pus în practică. Unele persoane pot avea competențele digitale necesare pentru a înțelege codul unui algoritm, în timp ce pentru altele sunt suficiente informații simplificate cu privire la scopul prelucrării și la interconectările datelor utilizate. Pentru a stabili dacă explicația furnizată este capabilă să fie înțeleasă, trebuie analizat obiectivul acesteia. O persoană trebuie să primească suficiente informații pentru a înțelege scopul, logica și criteriile care au condus la luarea unei decizii.

Dreptul la explicații nu este un drept absolut (a se vedea pasul 4 din [tabelul 4](#)). Statele membre pot restricționa acest drept prin lege într-o serie de cazuri, printre care: securitatea națională; apărarea; securitatea publică; prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor; executarea pedepselor; protecția persoanei vizate sau a drepturilor și libertăților altora; sau punerea în aplicare a pretențiilor de drept civil.

Furnizarea de informații rezonabile cu privire la scopul și consecințele preconizate ale prelucrării constituie totuși o bună practică și este recomandabilă. Conceperea unor modalități simple de a explica logica implicată și criteriile utilizate pentru a lua o decizie va avea în final efectul de a spori transparența și gradul de răspundere.

*Pentru mai multe informații, a se vedea RGPD, articolele 13-15 (dreptul la informare și dreptul de acces), articolul 22 (procesul decizional individual automatizat, inclusiv crearea de profiluri) și articolul 23 (restricții); precum și Directiva privind poliția, articolul 11 (procesul decizional individual*

*automatizat, inclusiv crearea de profiluri) și articolele 13-15 (dreptul la informare și dreptul de acces).*

*A se vedea și Grupul de lucru instituit prin articolul 29 privind protecția datelor (2018a).*

### 3.1.3. Păstrarea datelor în siguranță: normele cu privire la evidențe, jurnale și stocare

Autoritățile care colectează și prelucrează date cu caracter personal în scopuri legate de profiluri nu trebuie doar să prelucreze datele în mod legal, ci și să se asigure că datele nu sunt:

- accesate de persoane neautorizate;
- utilizate în alte scopuri decât scopul inițial; sau
- stocate mai mult timp decât este necesar.

În acest scop, autoritățile și agenții de aplicare a legii și de gestionare a frontiere-lor trebuie să se asigure că sunt puse în aplicare măsuri adecvate pentru a proteja integritatea și securitatea datelor. Aceștia trebuie să țină evidența tuturor accesărilor și utilizărilor datelor prin crearea și păstrarea de evidențe ale tuturor activităților de prelucrare sau a categoriilor de activități de prelucrare (articolul 30 din RGPD și articolul 24 din Directiva privind poliția). Evidențele trebuie să conțină:

- **numele și datele de contact** ale autorităților și ale responsabilului cu protecția datelor;
- **scopul** prelucrării;
- **categoriile de destinatari** cărora le-au fost sau le vor fi divulgate datele cu caracter personal;
- o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
- **utilizarea creării de profiluri;**

- indicarea **temeiului juridic** al operațiunii de prelucrare;
- acolo unde este posibil, **termenele-limită** preconizate pentru ștergerea diferitelor categorii de date cu caracter personal;
- acolo unde posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1) din RGPD sau la articolul 29 alineatul (1) din Directiva privind poliția.

În plus, atunci când se creează profiluri prin mijloace computerizate în scopuri reglementate de Directiva privind poliția (a se vedea [secțiunea 3.2](#)), autoritățile trebuie să păstreze jurnale privind: colectarea, modificarea, consultarea, divulgarea (inclusiv transferurile), combinarea și ștergerea datelor.

Aceste evidențe și jurnale vor ajuta agenții să demonstreze, în cadrul monitorizării interne și externe, că au respectat cerințele legale. De exemplu, dacă o persoană depune o plângere, autoritățile de aplicare a legii și de gestionare a frontierelor vor fi obligate să pună evidențele și jurnalele la dispoziția autorităților naționale de protecție a datelor.

Datele cu caracter personal nu trebuie stocate mai mult decât este necesar pentru a atinge scopul legitim stabilit. Stocarea pe perioade mai lungi trebuie justificată corespunzător. În astfel de cazuri, autoritățile trebuie să se asigure că modul de stocare este verificat regulat pentru a garanta integritatea și securitatea sa.

### 3.1.4. Obligația de depistare și prevenire a prelucrării ilegale

Depistarea și prevenirea prelucrării ilegale a datelor cu caracter personal nu sunt ușor de realizat. Asigurarea unor verificări adecvate este îngreunată de necesitatea unor competențe de specialitate pentru a înțelege algoritmiile complecși și bazele mari de date.

Pentru a soluționa această problemă, RGPD și Directiva privind poliția prevăd garanții menite să ofere îndrumare agenților de aplicare a legii și de gestionare a frontierelor înaintea, în timpul și după prelucrarea datelor. Acestea constau în:

- evaluări ale impactului asupra protecției datelor; și
- asigurarea protecției datelor începând cu momentul conceperii și în mod implicit.

## Evaluarea impactului

Cadrul juridic al UE impune poliției și autorităților de gestionare a frontierelor să realizeze evaluări ale impactului înainte de a efectua orice prelucrare de date care ar putea crea un risc ridicat pentru drepturile persoanelor (articolul 35 din RGPD și articolul 27 din Directiva privind poliția). Aceasta înseamnă că se vor efectua evaluări de impact nu doar atunci când rezultatul prelucrării riscă să încalce standardele de protecție a datelor sau de confidențialitate, ci în orice situație care poate duce la încălcarea *oricărui drept fundamental*, de exemplu drepturile la: egalitate și nediscriminare; libertatea de exprimare și informare; libertatea de gândire, conștiință și religie; educație; sănătate; azil; și protecție în caz de îndepărtare, expulzare sau extrădare. Evaluările impactului sunt deosebit de importante atunci când crearea de profiluri poate avea consecințe juridice pentru persoane. În astfel de cazuri, RGPD și Directiva privind poliția impun obligativitatea evaluărilor de impact.

Evaluările impactului trebuie efectuate înaintea prelucrării automate, iar obiectivul lor este unul dublu:

- *a priori*: înainte de prelucrarea datelor, o evaluare a impactului având ca obiect calitatea datelor și/sau a algoritmului pe care se bazează prelucrarea va ajuta la depistarea și, după caz, la remedierea potențialelor încălcări ale drepturilor fundamentale;
- *a posteriori*: după ce datele sunt prelucrate, agentului i se poate cere să demonstreze că a acționat în mod legal. Evaluarea impactului îl poate ajuta să dovedească faptul că au fost puse în aplicare toate măsurile necesare pentru a asigura respectarea legii.

De asemenea, evaluările impactului vor ajuta agenții să depisteze prejudecățile ascunse care pot încălca drepturile la protecția datelor și la nediscriminare și pot influența calitatea profilurilor (a se vedea [secțiunea 1.3.2](#)).

### În obiectiv: utilizarea „algoritmilor dinamici”

„Algoritmii dinamici” sunt algoritmi care sunt redefiniți în mod constant și „îmbunătățiți” pe baza unor „bucle de feedback”. Aceste bucle sunt create chiar de sistemele algoritmice și nu pot fi nici înțelese corect, nici măcar exprimate într-un limbaj simplu (a se vedea articolul 35 din RGPD și articolul

27 din Directiva privind poliția). Spre deosebire de „algoritmii statici”, care se bazează pe criterii predeterminate, „algoritmii dinamici” generează **noi corelații**, redefinindu-se în permanență.

Algoritmii dinamici creează riscul ca, la un moment dat, experții programatori să nu mai știe logica din spatele algoritmului. Acest lucru creează un **risc semnificativ de reproducere involuntară a prejudecăților existente** și de perpetuare a inegalităților sociale și a stigmatizării anumitor grupuri. În astfel de cazuri, devine foarte dificil să se asigure asumarea răspunderii și acordarea de măsuri reparatorii persoanelor afectate.

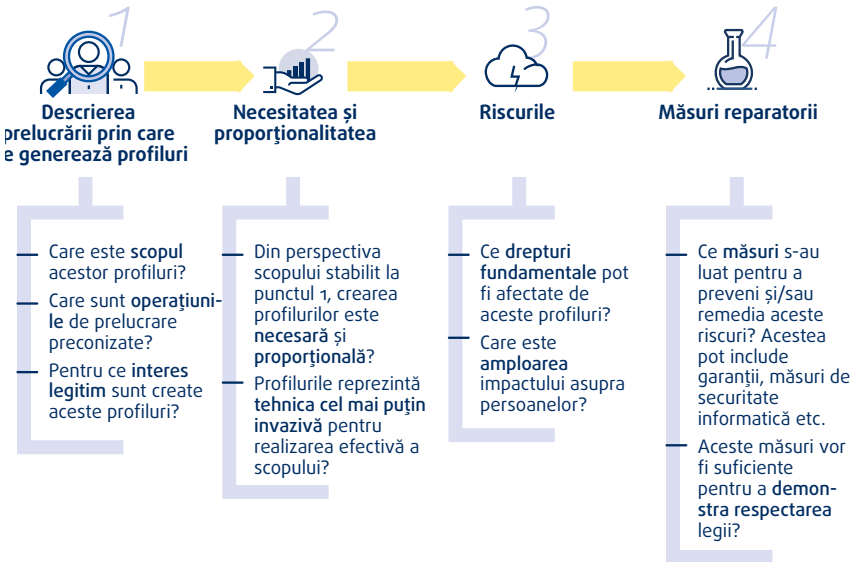
Prin urmare, utilizarea algoritmilor dinamici trebuie **evitată sau redusă** pentru a reduce la minimum riscul de a pierde din vedere criteriile de evaluare. Astfel, auditorii interni și externi pot să evalueze algoritmii și să-i modifice dacă se constată că sunt ilegali. În cazul în care se justifică utilizarea algoritmilor dinamici, indicatorii de risc vor fi revizuiți și testați pentru a se asigura că nu generează profiluri ilegale.

*Pentru mai multe informații, a se vedea Gandy, O. (2010) și Korff, D. (2015).*

Evaluarea impactului poate varia semnificativ în funcție de tipul și volumul datelor cu caracter personal prelucrate, precum și în funcție de tipul și scopul prelucrării. Ea poate include verificarea calității datelor, controale tehnice ale algoritmilor de prelucrare a datelor și/sau o analiză completă a obiectivelor prelucrării etc. **Figura 13** prezintă criteriile minime care trebuie evaluate.



Figura 13: Cerințele minime ale evaluărilor de impact



Sursa: FRA, 2018.

Grupul de lucru instituit prin articolul 29 privind protecția datelor (în prezent înlocuit de [Comitetul european pentru protecția datelor](#)), care reunește autoritățile naționale de protecție a datelor din statele membre ale UE, a elaborat orientări care furnizează informații suplimentare despre evaluările impactului asupra protecției datelor. Orientările includ o cartografiere detaliată a criteriilor care trebuie utilizate la efectuarea evaluărilor de impact<sup>39</sup>.

### ***Integrarea conceptului de legalitate „începând cu momentul conceperii” și „în mod implicit”***

Indiferent dacă o evaluare a impactului a identificat sau nu posibilitatea unei încălcări a drepturilor fundamentale, pot fi puse în aplicare măsuri care să prevină absolut orice risc de ilegalitate. Acestea sunt denumite „protecția datelor începând cu momentul conceperii” și „protecția datelor în mod implicit” (articolul 25 din RGPD și articolul 20 din Directiva privind poliția).

39 Grupul de lucru instituit prin articolul 29 (2017a).

Protecția datelor începând cu momentul conceperii are ca scop asigurarea faptului că, atât *înaintea*, cât și *în timpul* prelucrării datelor, sunt puse în aplicare măsuri tehnice și organizatorice care să garanteze principiile protecției datelor. De exemplu, dacă este posibil, datele cu caracter personal ar putea fi „pseudonimizate”. Pseudonimizarea este o măsură în urma căreia datele cu caracter personal nu pot fi atribuite persoanei vizate fără informații suplimentare, care sunt păstrate separat.

„Cheia” care permite reidentificarea persoanelor vizate trebuie păstrată separat, în condiții de siguranță<sup>40</sup>. Spre deosebire de datele anonimizate, datele pseudonimizate sunt în continuare date cu caracter personal și, prin urmare, trebuie să respecte regulile și principiile de protecție a datelor.

Protecția datelor în mod implicit asigură că „sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării”<sup>41</sup>. Aceasta are impact asupra:

- volumului de date personale colectate și stocate;
- tipurilor de prelucrare care pot implica date cu caracter personal;
- perioadei maxime de stocare;
- numărului de persoane autorizate să acceseze aceste date cu caracter personal.

### **În obiectiv: asumarea răspunderii**

Obiectivul principal al protecției datelor începând din momentul conceperii și al protecției datelor în mod implicit este de a ajuta autoritățile și agenții de aplicare a legii și de gestionare a frontierelor să conceapă programe de creare a profilurilor pe bază de algoritmi care să respecte cerințele drepturilor fundamentale, în special principiile **legalității, transparenței și securității**.

Aceste măsuri pot demonstra însă și modul în care autoritățile respectă cerința legală a **asumării răspunderii**. Autoritățile care prelucrează date au obligația legală să pună în aplicare „măsuri tehnice și organizatorice adecvate” prin care să demonstreze conformitatea cu dreptul Uniunii. De

40 FRA, AEPD și Consiliul European (2018), p. 83.

41 Regulamentul general privind protecția datelor (RGPD), articolul 25.

exemplu, dacă o persoană depune o plângere, autoritățile naționale judiciare și de protecție a datelor pot solicita autorităților să demonstreze fiecare dintre elementele următoare:

- legitimitatea, necesitatea și proporționalitatea profilurilor create prin mijloace computerizate;
- legalitatea scopului;
- informațiile furnizate persoanelor;
- integritatea și securitatea datelor;
- măsurile și controalele de calitate efectuate înaintea și în timpul operațiunilor legate de profiluri.

## 3.2. Utilizarea bazelor mari de date în scopuri de gestionare a frontierelor și de securitate

UE a dezvoltat mai multe sisteme sau mecanisme informatice la scară largă pentru colectarea și prelucrarea datelor care pot fi utilizate pentru gestionarea frontierelor și a migrației și, într-o anumită măsură, pentru asigurarea respectării legii. Acestea servesc ca exemple prin care se pot ilustra unele dintre provocările uzuale legate de crearea profilurilor pe bază de algoritmi, precum și garanțiile posibile.

Tabelul 6 prezintă pe scurt aceste sisteme și mecanisme informatice ale UE. Anexa oferă o prezentare detaliată a sistemelor informatice la scară largă existente și planificate ale UE, valabilă în martie 2018.

**Tabelul 6: Selecție de instrumente ale UE care implică prelucrarea unor volume mari de date pentru gestionarea frontierelor și aplicarea legii**

Baza de date	Acronim	Scopul principal
<b>Sistemul de informații Schengen</b>	<i>SIS II</i>	Introducerea și prelucrarea de alerte cu privire la persoanele căutate sau dispărute în scopul protejării siguranței, introducerea și prelucrarea de alerte cu privire la resortisanții țărilor terțe (RTT) în scopul refuzării intrării sau a șederii, introducerea și prelucrarea de alerte privind RTT care fac obiectul unei decizii de returnare.
<b>Sistemul de informații privind vizele</b>	<i>VIS</i>	Facilitarea schimbului de date între statele membre Schengen cu privire la cererile de viză.
<b>Sistemul dactiloscopic european</b>	<i>EURODAC</i>	Stabilirea statului membru responsabil pentru examinarea unei cereri de protecție internațională și aducerea unei contribuții la controlul imigrației ilegale și al deplasărilor secundare.
<b>Sistemul de intrare/ieșire</b>	<i>EES</i>	Calcularea și monitorizarea duratei de ședere autorizată a RTT și identificarea persoanelor care au depășit această durată.
<b>Registrul cu numele pasagerilor</b>	<i>PNR</i>	Colectarea, prelucrarea și schimbul de date cu privire la pasagerii zborurilor din țări terțe („zboruri din afara UE”)*. Utilizat strict în scopuri de asigurare a respectării legii.
<b>Informații prealabile privind pasagerii</b>	<i>API</i>	Colectarea și prelucrarea de date cu privire la pasagerii zborurilor din țări terțe (zboruri din afara UE) pentru gestionarea frontierelor și aplicarea legii.
<b>Sistemul european de informații și de autorizare privind călătoriile</b>	<i>ETIAS</i>	Evaluarea posibilității ca un RTT scutit de viză să prezinte un risc de securitate, de migrație neregulamentară sau pentru sănătatea publică.
<b>Sistemul european de informații cu privire la cazierile judiciare ale resortisanților țărilor terțe</b>	<i>ECRIS-TCN</i>	Transmiterea de informații cu privire la condamnările anterioare ale RTT.

*Notă: \* În plus, articolul 2 din Directiva (UE) 2016/681 oferă statelor membre opțiunea de a prelucra date provenite de la zborurile din interiorul UE.*

*Sursa: FRA, 2018.*

Sistemele informatice la scară largă ale UE sunt utilizate într-o serie de procese legate de migrație, printre care: procesul de evaluare a riscului înainte de sosire, procesul de azil, procesul de solicitare a vizelor, în timpul controalelor la frontieră,

la eliberarea permiselor de ședere, la reținerea migranților în situație neregulamentară, în timpul procedurilor de returnare și pentru emiterea de interdicții de intrare. Sistemele IT create de UE, inclusiv cele create inițial în scopul azilului și al gestionării migrației, sunt utilizate din ce în ce mai mult și în contextul securității interne, de exemplu pentru verificările poliției și în lupta împotriva infracțiunilor grave și a terorismului.

Majoritatea sistemelor instituite prin legislația UE se axează pe identificarea unei persoane specifice prin asocierea datelor alfanumerice sau biometrice (în prezent, amprente digitale) cu informații deja existente în sistem. Cu câteva excepții notabile (a se vedea „În obiectiv: crearea de profiluri pe bază de algoritmi în cadrul instrumentelor UE”), ele nu conțin, în sine, un algoritm care să permită asocierea unei persoane cu un profil. Totuși, pot fi utilizate pentru a produce statistici anonimizate, inclusiv cu privire la caracteristicile care sunt considerate criterii protejate, cum ar fi sexul sau vârsta (a se vedea [secțiunea 1.2.1](#)).

Astfel de statistici ar putea fi utilizate pentru a crea profiluri de risc care să fie aplicate în viitoarele decizii din activitatea de gestionare a frontierelor sau de poliție. Ca parte a cadrului mai larg de interoperabilitate a sistemelor informatice ale UE, Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA) va fi responsabilă pentru gestionarea registrului central de raportare și statistici. Acest registru se va baza pe date din bazele de date existente ale UE (Sistemul de intrare/ieșire, ETIAS, Sistemul de informații Schengen și Sistemul de informații privind vizele) pentru a genera statistici și rapoarte analitice pentru organismele UE și naționale<sup>42</sup>.

### **În obiectiv: crearea de profiluri pe bază de algoritmi în cadrul instrumentelor UE**

Unele instrumente existente ale UE prevăd utilizarea statisticilor derivate din datele lor pentru a genera profiluri de risc. Pe lângă faptul că permit depistarea suspecțiilor specifice „cunoscuți”, acestea conțin și o funcție

<sup>42</sup> Comisia Europeană (2017), *Propunere de Regulament al Parlamentului European și al Consiliului privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE (în materie de frontiere și vize) și de modificare a Deciziei 2004/512/CE a Consiliului, a Regulamentului (CE) nr. 767/2008, a Deciziei 2008/633/JAI a Consiliului, a Regulamentului (UE) 2016/399 și a Regulamentului (UE) 2017/2226*, COM(2017) 793 final, Strasbourg, 12 decembrie 2017; Comisia Europeană (2017), *Propunere de Regulament al Parlamentului European și al Consiliului privind instituirea unui cadru de interoperabilitate între sistemele de informații ale UE (cooperare polițienească și judiciară, azil și migrație)*, COM(2017) 794 final, Bruxelles, 12 decembrie 2017.

de creare de profiluri pe bază de algoritmi care identifică persoanele „necunoscute” care ar putea prezenta interes pentru autoritățile de aplicare a legii și de gestionare a frontierelor.

**Sistemul european de informații și de autorizare privind călătoriile (ETIAS)**<sup>43</sup>, care a fost adoptat în septembrie 2018, dar încă nu intrase la momentul finalizării prezentului ghid, va evalua dacă resortisanții țărilor terțe scutite de viză prezintă un risc în ceea ce privește migrația neregulamentară, securitatea sau sănătatea publică înainte de li se acorda autorizația de călătorie. Informațiile furnizate de călători în timpul procesului de depunere a cererilor vor fi comparate automat cu bazele de date relevante ale UE și internaționale, precum și cu un set de indicatori de risc („reguli de verificare”) cuprinși chiar în sistemul ETIAS. Un algoritm dezvoltat de Frontex va compara profilul individual al călătorului (pe baza unor indicatori precum vârsta, sexul, cetățenia, locul de reședință, nivelul de studii și ocupația) cu acești indicatori de risc pentru a stabili dacă cererea trebuie analizată manual.

**Datele din registrul cu numele pasagerilor (PNR)** sunt colectate de transportatorii aerieni din informațiile furnizate de pasageri în sistemele de rezervare a zborurilor, de exemplu: ziua și itinerariul călătoriei, datele de contact și de plată, informațiile despre bagaje și alte „observații generale”, cum ar fi preferințele alimentare. Nu există o bază de date centrală a UE care să colecteze aceste date, însă Directiva privind PNR a UE<sup>44</sup> impune transportatorilor aerieni să transmită datele către unitățile de informații despre pasageri (UIP) naționale, care apoi analizează informațiile în scopul combaterii terorismului și a criminalității grave. Pe lângă depistarea deplasării transfrontaliere a persoanelor cunoscute, aceste date pot fi folosite și pentru a identifica amenințările încă necunoscute, prelucrând datele pasagerilor pe baza anumitor indicatori de risc specifici („criterii prestabilite”). Aceste criterii sunt stabilite de UIP și actualizate pe baza noilor date și tipare disponibile în sistem.

43 Comisia Europeană (2018), *Regulamentul (UE) 2018/1240 al Parlamentului European și al Consiliului din 12 septembrie 2018 de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS) și de modificare a Regulamentelor (UE) nr. 1077/2011, (UE) nr. 515/2014, (UE) 2016/399, (UE) 2016/1624 și (UE) 2017/2226*, COM(2016) 731 final, Bruxelles, 16 noiembrie 2016, articolul 33 alineatul (5).

44 *Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave*, JO L 119, articolul 6 alineatul (4).

### 3.2.1. Minimizarea riscurilor legate de drepturile fundamentale la prelucrarea datelor din baze mari de date

La crearea profilurilor, inclusiv pe bază de algoritmi, se vor utiliza date cuprinzătoare privind călătorii, precum cetățenia, sexul și vârsta, la o scară care nu era posibilă în trecut. Chiar dacă aceste date sunt anonimizate, prelucrarea lor nu este lipsită de riscuri. Prejudecățile, conștiente sau inconștiente, manifestate în selectarea indicatorilor de risc, în proiectarea algoritmilor sau în interpretarea rezultatelor ar putea avea ca rezultat acțiuni operaționale care să ducă la discriminarea anumitor categorii de persoane<sup>45</sup>.

Secțiunea de față analizează unele dintre aceste riscuri și propune câteva modalități de a le minimiza. La baza ei stă publicația FRA *Twelve operational fundamental rights considerations for law enforcement when processing PNR data* (Douăsprezece considerente operaționale privind drepturile fundamentale destinate activității de prelucrare a datelor din PNR desfășurate de autoritățile de aplicare a legii) (a se vedea studiul de caz). Deși dezvoltate în contextul specific al prelucrării datelor din PNR, unele dintre aceste considerații au aplicabilitate mai generală și pot fi considerate garanții de diminuare a riscurilor care decurg din crearea de profiluri pe bază de algoritmi.

#### Studiu de caz

##### Ghidul operațional al FRA pentru înființarea sistemelor PNR naționale

În 2014, deoarece nu exista o legislație a Uniunii Europene privind PNR, Comisia Europeană a solicitat agenției FRA un ghid practic referitor la prelucrarea datelor din PNR în scopul aplicării legii pentru statele membre care intenționează să își creeze propriile sisteme PNR naționale. Ghidul s-a axat pe drepturile la respectarea vieții private (articolul 7 din cartă), la protecția datelor cu caracter personal (articolul 8 din cartă) și la nediscriminare (articolul 21 din cartă). Unele dintre garanțiile propuse au fost ulterior introduse în Directiva UE privind PNR.

45 Pentru mai multe informații, vezi FRA (2017e) și FRA (2018a).

Cele douăsprezece considerente privind drepturile fundamentale destinate activității de prelucrare a datelor din PNR desfășurate de autoritățile de aplicare a legii sunt următoarele:

- folosiți datele din PNR doar pentru a combate terorismul și infracțiunile transnaționale grave;
- acordați acces la baza de date PNR doar unei unități specializate;
- nu solicitați acces direct la bazele de date ale companiilor aeriene;
- ștergeți datele PNR sensibile;
- instituiți garanții stricte de securitate și trasabilitate împotriva abuzurilor;
- reduceți probabilitatea rezultatelor fals pozitive;
- demonstrați transparență față de pasageri;
- permiteți persoanelor să-și acceseze și să-și rectifice datele din PNR;
- nu permiteți identificarea persoanelor vizate sau păstrarea datelor mai mult decât este necesar;
- transferați datele extrase din PNR numai către autoritățile publice naționale competente;
- transferați datele extrase din PNR către țări terțe numai în condiții stricte;
- efectuați o evaluare obiectivă și transparentă a sistemului PNR.

*Pentru mai multe informații, a se vedea FRA (2014c).*

### ***Prelucrarea datelor care dezvăluie caracteristici protejate trebuie să fie necesară și proporțională***

Prin natura activității de creare a profilurilor pe bază de algoritmi, utilizarea caracteristicilor personale care sunt legate de criterii protejate implică un risc de discriminare deosebit de mare<sup>46</sup>. În contextul UE, atât legislația privind ETIAS, cât și cea privind PNR interzic bazarea indicatorilor de risc pe criterii care implică un risc ridicat de discriminare, cum sunt rasa, originea etnică sau convingerile religioase. Totuși, chiar și în absența unor astfel de date, există alte tipuri de date care pot fi puternic

46 Autoritatea Europeană pentru Protecția Datelor (2018).



corelate cu aceste caracteristici, acționând efectiv ca substitute pentru aceste caracteristici protejate. De exemplu, categoria „observații generale” din PNR, care poate conține preferințele alimentare ale călătorilor, ar putea dezvălui anumite convingeri religioase.

O anumită combinație de date utilizată de algoritm poate, de asemenea, să pună o categorie de persoane în dezavantaj; de exemplu, poate dezavantaja persoanele pe baza originii lor etnice sau sociale sau a apartenenței la o minoritate națională, care sunt caracteristici protejate conform articolului 21 din cartă. Astfel, dacă un profil de risc din ETIAS referitor la riscul de migrație neregulamentară se bazează pe combinația dintre o anumită cetățenie și un grup profesional, acesta poate avea ca rezultat vizarea persoanelor dintr-un anumit grup etnic sau cu o anumită cetățenie care, în țara respectivă, lucrează de obicei într-un anumit sector economic, cum ar fi construcțiile sau agricultura<sup>47</sup>.

- Prelucrarea datelor care dezvăluie caracteristici protejate prin articolul 21 din cartă trebuie să fie proporțională și limitată la ceea ce este strict necesar și să nu ducă niciodată la discriminare. Înainte de orice prelucrare, autoritatea competentă trebuie să evalueze datele pentru a depista orice caracteristici protejate și a elimina orice date a căror prelucrare nu ar fi legală. Ca bună practică, acest lucru ar trebui completat prin rularea unui program de potrivire și eliminare care să folosească un glosar de „termeni sensibili” actualizat periodic.

### ***Criteriile pe care se bazează profilurile trebuie să fie specifice și clar direcționate***

Utilizarea unor **criterii generale pentru crearea de profiluri** comportă un alt risc. Instrumentele UE existente permit o marjă de apreciere semnificativă în dezvoltarea algoritmilor pentru crearea de profiluri. Pentru a evalua riscul de migrație neregulamentară, ETIAS are în vedere utilizarea statisticilor UE și naționale cu privire la rata de depășire a perioadei permise de ședere și la rata de nepermitere a intrării. Totuși, în ceea ce privește riscurile de securitate, ETIAS se referă doar la informații privind anumiți indicatori de securitate și anumite amenințări. Directiva privind PNR oferă indicații generale pentru proiectarea algoritmilor, dar nu specifică ce criterii să se utilizeze pentru a identifica persoanele care ar putea fi implicate într-o infracțiune de terorism sau o infracțiune gravă, nici ce pondere ar trebui să se atribuie unui anumit criteriu.

<sup>47</sup> Vezi și FRA (2017a).

Criteriile excesiv de generale conduc la un număr semnificativ de rezultate „fals pozitive”, ceea ce înseamnă că persoanele sunt în mod greșit asociate cu un anumit profil de risc. În plus, unele dintre aceste rezultate „fals pozitive” ar putea fi discriminatorii. De exemplu, o definiție generică a criteriului „condamnare penală anterioară” ar obliga persoanele LGBT să declare cazieri judiciare asociate cu anumite conduite sexuale care sunt incriminate de unele țări din afara UE.

- Criteriile de evaluare trebuie să fie predefinite, clar direcționate, specifice, proporționale și bazate pe fapte. Ele trebuie testate pe eşantioane anonimizate și revizuite periodic de către un auditor intern pentru a stabili dacă sunt în continuare justificate de obiectivele lor specifice.
- Înainte de a transmite o alertă bazată pe prelucrarea automată cu scopul de a lua măsuri suplimentare, autoritatea competentă trebuie să examineze manual datele, împreună cu alte informații, pentru a stabili dacă persoana respectivă corespunde profilului de risc și pentru a elimina rezultatele fals pozitive. Destinatarul datelor trebuie să ofere feedback cu privire la acțiunile întreprinse pe baza alertei.

### ***Datele prelucrate trebuie să fie corecte și fiabile***

Cercetările FRA confirmă faptul că sistemele informatice la scară largă existente conțin un volum semnificativ de date inexacte<sup>48</sup>. **Datele inexacte sau nefiabibile** pot avea efecte negative multiple în contextul creării de profiluri pe bază de algoritmi în vederea gestionării frontierelor sau a aplicării legii. Datele inexacte pot afecta persoanele, dar pot duce și la corelații incorecte și la o imagine distorsionată, compromițând eficacitatea activității polițienești și de gestionare a frontierelor.

Acest lucru este deosebit de relevant în cazul datelor introduse de cetățeni, ca și în cazul datelor din PNR și din cererile depuse prin ETIAS, care pot fi mai predispuse la greșeli decât înregistrările oficiale. În mod similar, examinarea conturilor de pe platformele sociale, care este prevăzută de unele sisteme de autorizare a călătoriilor din afara UE, implică un risc ridicat de a introduce informații nefiabibile în procesul de creare de profiluri. În plus, comportă un risc deosebit de a colecta date care dezvăluie informații sensibile cu caracter personal care sunt protejate de cartă, cum sunt opiniile politice sau informații despre viața sexuală.

48 Vezi FRA (2018c), p. 81-98.

- Furnizați persoanelor informații corecte despre colectarea, stocarea și prelucrarea datelor lor și despre principiile aplicabile de protecție a datelor. Persoanele trebuie să fie informate despre drepturile pe care le au, inclusiv despre mecanismele de atac disponibile.
- Permiteți persoanelor să solicite rectificarea datelor dacă sunt inexacte și să fie informate dacă datele au fost rectificate sau șterse.
- Asigurați o reparație administrativă și judiciară eficientă în cazul în care s-au încălcat drepturile de protecție a datelor, inclusiv dacă s-a refuzat accesul sau dacă datele inexacte nu au fost rectificate sau șterse.

## Concluzie

Profilurile sunt un instrument legitim utilizat de agenții de aplicare a legii și de polițiștii de frontieră pentru a preveni, a ancheta și a urmări penal activitățile infracționale, precum și pentru a preveni și depista imigrația ilegală.

Pentru a fi legale, corecte și eficiente, activitățile legate de profiluri trebuie să rămână în limitele legii. În mod special, ele trebuie să respecte cerințele privind tratamentul egal și protecția datelor cu caracter personal.

Acest obiectiv se va realiza printr-o combinație de elemente. Orice activitate care implică profiluri trebuie:

- să trateze persoanele în mod egal, respectuos și demn;
- să evite profilurile bazate pe prejudecăți;
- să fie rezonabilă, obiectivă și bazată pe informații operative; și
- să protejeze în mod adecvat datele cu caracter personal și viața privată a persoanelor.













Agenții și ofițerii de poliție și polițiștii de frontieră au la dispoziție diferite instrumente pentru a se asigura că aceste principii sunt cunoscute, înțelese și respectate în practică:








- înainte de a crea și utiliza profiluri, agenții trebuie să primească orientări și formare;
- în timpul activităților care implică profiluri trebuie înregistrate și stocate detaliile activității;
- ulterior, acțiunile agenților trebuie monitorizate și evaluate pentru a identifica domeniile care necesită îmbunătățiri.

Prevenirea utilizării ilegale a profilurilor va asigura nu doar respectarea legii de către agenții de aplicare a legii și polițiștii de frontieră, ci și înțelegerea și acceptarea acțiunilor lor de către publicul larg. Creșterea încrederii în activitățile de aplicare a legii și de gestionare a frontierelor duce la îmbunătățirea eficacității acestora și, prin urmare, contribuie la creșterea nivelului de siguranță și securitate în societate în ansamblu.

# Anexă

Tabelul 7: Sisteme informatice la scară largă ale UE existente și planificate

Sistem informatic	Scopul principal	Persoanele vizate	Aplicabilitate	Instrument juridic/propunere	Identificatori biometrici
Sistemul dactiloscopic european (Eurodac)	Stabilirea statutului membru responsabil pentru examinarea cererii de protecție internațională <i>Sprijinirea ținerii sub control a imigrației ilegale și a deplasărilor secundare</i>	Solicitanții și beneficiarii de protecție internațională, <i>migranții aflați în situație neregulară</i>	28 SM ale UE + TAS	Regulamentul (UE) nr. 603/2013 (Regulamentul Eurodac)  <i>COM(2016) 272 final (propunere privind Eurodac)</i>	 
Sistemul de informații privind vizele (VIS)	Facilitarea schimbului de date între statele membre Schengen cu privire la cererile de viză	Solicitanții de viză și susținătorii reîntregirii familiei	24 SM ale UE (fără CY, HR, IE, UK) <sup>1</sup> + TAS	Regulamentul (CE) nr. 767/2008 (Regulamentul VIS)	
Sistemul de informații Schengen (SIS II) – poliție	Garantarea securității în UE și în statele membre	Persoanele dispărute sau căutate	26 SM ale UE (fără CY, IE) <sup>2</sup> + TAS	Decizia 2007/533/JAI a Consiliului (Decizia SIS II)  <i>COM(2016) 883 final (propunere privind SIS II)</i>	  
Sistemul de informații Schengen (SIS II) – frontiere	Introducerea și prelucrarea de alerte în scopul nepermitterii intrării sau a șederii în statele membre Schengen	Migranții aflați în situație neregulară	25 SM ale UE (fără CY, IE, UK) <sup>2</sup> + TAS	Regulamentul (CE) nr. 1987/2006 (Regulamentul SIS II)  <i>COM(2016) 882 final (propunere privind SIS II frontiere)</i>	  
Sistemul de informații Schengen (SIS II) – returnare	<i>Introducerea și prelucrarea de alerte cu privire la resortanții țărilor terțe care fac obiectul unei decizii de returnare</i>	<i>Migranții aflați în situație neregulară</i>	<i>25 SM ale UE (fără CY, IE, UK)<sup>2</sup> + TAS</i>	<i>COM(2016) 881 final (propunere privind SIS II returnare)</i>	  

<p><b>Sistemul de intrare/ieșire (EES)</b></p>	<p>Calcularea și monitorizarea duratei de ședere autorizată a resortisanților țărilor terțe și identificarea persoanelor care au depășit această durată</p>	<p>Călătorii care vin pentru o ședere de scurtă durată</p>	<p>22 SM ale UE (fără BG, CY, HR, IE, RO, UK)<sup>3</sup> + TAS</p>	<p>Regulamentul (UE) 2017/2226 (Regulamentul EES)</p>	 
<p><b>Sistemul european de informații și de autorizare privind călătoriile (ETIAS)</b></p>	<p>Evaluarea posibilității ca un resortisant al unei țări terțe scutit de viză să prezinte un risc de securitate, de migrație neregulamentară sau pentru sănătatea publică.</p>	<p>Călătorii scutiți de viză</p>	<p>26 SM ale UE (fără IE, UK)<sup>3</sup> + TAS</p>	<p>COM(2016) 731 final (propunere privind ETIAS)</p>	<p>Niciunul</p>
<p><b>Sistemul european de informații cu privire la cazier-rele judiciare ale resortisanților țărilor terțe (ECRIS-TCN)</b></p>	<p>Transmiterea de informații cu privire la condamnările anterioare ale resortisanților țărilor terțe</p>	<p>Resortisanți ai țărilor terțe care au cazier judiciar</p>	<p>27 SM ale UE (fără DK)<sup>4</sup></p>	<p>COM(2017) 344 final (propunere privind ECRIS-TCN)</p>	 
<p><b>Interoperabilitatea – registrul comun de date de identitate</b></p>	<p>Stabilirea unui cadru pentru interoperabilitatea dintre EES, VIS, ETIAS, Eurodac, SIS II și ECRIS-TCN</p>	<p>Resortisanții țărilor terțe vizați de Eurodac, VIS, SIS II, EES, ETIAS și ECRIS-TCN</p>	<p>28 SM ale UE<sup>5</sup> + TAS</p>	<p>COM(2017) 793 final (propunere privind interoperabilitatea în materie de frontiere și vize)  COM(2017) 794 final (propunere privind interoperabilitatea în materie de cooperare polițienească, azil și migrație)</p>	  

Notă: Sistemele planificate și modificările planificate în cadrul sistemelor sunt marcate cu litere cursive sau apar pe un fundal albastru.

  : amprente digitale;  : amprente palmare;  : imagine facială;  
 : profil ADN.

SM ale UE: statele membre ale UE.

TAS: țările asociate spațiului Schengen, adică Islanda, Liechtenstein, Norvegia și Elveția.

<sup>1</sup> Irlanda și Regatul Unit nu participă la VIS. Danemarcei nu i se aplică regulamentul, dar a ales să participe la VIS. VIS nu este încă aplicabil Croației și Ciprului și este doar parțial aplicabil Bulgariei și României, în conformitate cu Decizia (UE) 2017/1908 a Consiliului din 12 octombrie 2017.

<sup>2</sup> Cipru și Irlanda nu sunt încă conectate la SIS. Danemarcei nu i se aplică

*regulamentul și nici decizia Consiliului, dar a ales să participe la SIS II și va trebuie să opteze din nou la momentul adoptării propunerilor privind SIS II. Regatul Unit participă la SIS, dar nu poate utiliza sau accesa alerte privind nepermiterea intrării sau a șederii în spațiul Schengen. Bulgaria, România și Croația nu pot emite alerte Schengen de nepermitere a intrării sau a șederii în spațiul Schengen, deoarece nu fac încă parte din spațiul Schengen.*

- <sup>3</sup> *Danemarca poate decide să participe la EES și la ETIAS.*
- <sup>4</sup> *ECRIS-TCN nu se aplică Danemarcei. Regatul Unit și Irlanda pot decide să participe.*
- <sup>5</sup> *Danemarca, Irlanda și Regatul Unit vor participa, deoarece participă la sistemele informatice pentru care a fost asigurată interoperabilitatea.*

*Sursa: FRA, pe baza instrumentelor juridice existente și propuse, 2018.*

## Bibliografie

Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (FRONTEX) (2012), *Common core curriculum, EU border guard basic training*, martie 2012.

Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (FRONTEX) (2013), *Fundamental rights training for border guards, Trainers' Manual*, 2013.

Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (FRONTEX) (2015), *Twelve seconds to decide. In search of excellence: Frontex and the principle of best practice*, 2015.

Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (FRONTEX) (2017), *Handbook on risk profiles on Trafficking in Human Beings*, 2017.

Akhgar, B., Saathoff, G.B., Arabia, H.R., Hill, R., Staniforth, A. și Bayerl, P. S. (2015), *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*, Butterworth-Heinemann, 2015.

American Civil Liberties Union (ACLU) (2016), *Eight Problems With Police "Threat Scores"*, 13 ianuarie 2016.

Autoritatea Europeană pentru Protecția Datelor (AEPD) (2015), *Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of the terrorist offences and serious crime, Avizul 5/2015*, Bruxelles, 24 septembrie 2015.

Autoritatea Europeană pentru Protecția Datelor (AEPD) (2018), *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Bruxelles, 18 aprilie 2018.

Belgia, Unia, *Raport anual 2016*, Bruxelles, septembrie 2017.

Belgia, Unia, *Rapport annuel Convention entre Unia et la police fédérale, Budget 2015*, Bruxelles, 2015.

Big Brother Watch, *Smile you're on body worn camera Part II – Police, The use of body worn cameras by UK police forces*, august 2017.



Body-Gendrot, S. (2016), „*Making sense of French urban disorders in 2005*”, *European Journal of Criminology*, vol. 13, nr. 5, p. 556-572.

Bovens et al. (2014), „Public accountability” în: Bovens, M., Schillermans, T. și Goodlin, R.E. (ed.), *The Oxford handbook of public accountability*, Oxford, Oxford University Press, 2014.

Brayne, S. (2014), „Surveillance and system avoidance: criminal justice contact and institutional attachment”, *American Sociological Review*, vol. 79, nr. 3, p. 367-391.

Buolamwini, J., Gebru, T. (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, MIT Media Lab and Microsoft Research, 2018.

Center on Privacy and Technology at Georgetown Law (2016), *The Perpetual Line-up, Unregulated Police Face Recognition in America*, 18 octombrie 2016.

Centre d'analyse stratégique (2006), *Enquête sur les violences urbaines - Comprendre les émeutes de novembre 2005 : les exemples de Saint-Denis et d'Aulnay-Sous-Bois*, Paris, La Documentation française, 2006.

Comisia Europeană (2017a), *Hate crime training for law enforcement and criminal justice authorities: 10 key guiding principles*, februarie 2017.

Comisia Europeană (2017b), *Improving the recording of hate crime by law enforcement authorities, Key guiding principles*, decembrie 2017.

Comisia Europeană împotriva Rasismului și Intoleranței (ECRI) (2007), *Recomandarea de politică generală CERI nr. 11 privind combaterea rasismului și discriminare rasială în activitățile poliției, adoptată la data de 29 iunie 2007*, Strasbourg, 4 octombrie 2007.

Comisia Europeană, Subgrupul privind metodologiile pentru înregistrarea și colectarea datelor referitoare la infracțiunile motivate de ură (2017), *Improving the recording of hate crime by law enforcement authorities - Key guiding principles*, Bruxelles, decembrie 2017.

Consiliul Europei, Comitetul de Miniștri (2001), *Recommendation Rec(2001)10 of the Committee of Ministers to Member States on the European Code of Police Ethics adopted by the Committee of Ministers*, 19 septembrie 2001.

Consiliul Uniunii Europene (2009), *Catalogul Schengen actualizat al UE privind controlul la frontierele externe, returnarea și readmisia*, 19 martie 2009.

Coudert, F., Butin, D. și Le Metayer, D. (2015), „*Body-worn cameras for police accountability: opportunities and risks*”, *Computer Law and Security Review*, vol. 31, p. 749-762.

De Hert, P. și Lammerant, H. (2016), „Predictive profiling and its legal limits: effectiveness gone forever?” în: van der Sloot, B., Broeders, D. și Schrijvers, E. (ed.), The Netherlands Scientific Council for Government Policy, *Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, p. 145-173.

Défenseur des droits (2017), *Enquête sur l'accès aux droits. Volume 1 – relations police/population: le cas des contrôles d'identité*, 2017.

Dinant, J.-M., Lazaro, C., Pouillet, Y., Lefever, N. și Rouvroy, A. (2008), *Application of Convention 108 to the Profiling Mechanism - Some ideas for the future work of the consultative committee (T-PD)*, doc. T-PD 01, p. 3.

Farrar, T. (2018), *Self-awareness to being watched and socially-desirable behavior: A field experiment on the effect of body-worn cameras on police use-of-force*, Police Foundation, 2018.

FRA (2014a), *Fundamental rights at airports: border checks at five international airports in the European Union*, Luxemburg, Oficiul pentru Publicații, 2014.

FRA (2014b), *Fundamental rights at land borders: findings from selected European Union border crossing points*, Luxemburg, Oficiul pentru Publicații, 2014.

FRA (2014c), *Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data*, februarie 2014.

FRA (2016), *Fundamental Rights Report 2016*, Luxemburg, Oficiul pentru Publicații, 2016.

FRA (2017a), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)*, Avizul FRA 2/2017 [ETIAS], iunie 2017.

FRA (2017b), *Second European Union Minorities and Discrimination Survey - Main results*, Luxemburg, Oficiul pentru Publicații, decembrie 2017.

FRA (2017c), *Fundamental Rights Report 2017*, Luxemburg: Oficiul pentru Publicații, mai 2017.

FRA (2017d), *Second European Union Minorities and Discrimination Survey: Muslims – Selected findings*, Luxemburg, Oficiul pentru Publicații al Uniunii Europene, septembrie 2017

FRA (2017e), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxemburg, Oficiul pentru Publicații, mai 2017.

FRA (2018a), *Interoperability and fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights*, Avizul FRA 1/2018 [Interoperabilitate], aprilie 2018.

FRA (2018b), *#BigData: Discrimination in data-supported decision making*, publicație tematică a FRA, mai 2018.

FRA (2018c), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxemburg, Oficiul pentru Publicații, februarie 2018.

FRA (2018d), *Hate crime recording and data collection practice across the EU*, Luxemburg, Oficiul pentru Publicații, iunie 2018.

FRA (2018e), *Fundamental Rights Report 2018*, Luxemburg, Oficiul pentru Publicații, iunie 2018.

FRA (Agenția pentru Drepturi Fundamentale a Uniunii Europene) (2013), *Formare pentru polițiști din perspectiva drepturilor fundamentale – Manual pentru formatorii polițiștilor*, Luxemburg, Oficiul pentru Publicații, decembrie 2013.

FRA (Agenția pentru Drepturi Fundamentale a Uniunii Europene), Autoritatea Europeană pentru Protecția Datelor (AEPD) și Consiliul Europei (2018), *Manual de legislație europeană privind protecția datelor – Ediția 2018*, Luxemburg, Oficiul pentru Publicații, mai 2018.

FRA și Consiliul Europei (2018), *Manual de drept european privind nediscriminarea – Ediția 2018*, Luxemburg, Oficiul pentru Publicații, februarie 2018.

Franța, Ministerul Afacerilor Interne (2018), *Rapport d'évaluation sur l'expérimentation de l'emploi des caméras mobiles par les agents de police municipale*, 7 iunie 2018.

Gandy, O. (2010), „Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems”, *J Ethics Inf Technol*, vol. 12, nr. 1, p. 29-42, 2010.

Gross, S. R. (2002), „*Racial Profiling under Attack*”, D. Livingston, coautor. *Colum. L. rev.* 102, nr. 5, p. 1413-1438.

Grupul de lucru instituit prin articolul 29 privind protecția datelor (2014), *Avizul 01/2014 privind aplicarea noțiunilor de necesitate și de proporționalitate și protecția datelor în sectorul asigurării respectării legii*, 536/14/RO, WP 211, Bruxelles, 27 februarie 2014.

Grupul de lucru instituit prin articolul 29 privind protecția datelor (2017a), *Ghid privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679*, WP 248 rev. 01, 4 octombrie 2017.

Grupul de lucru instituit prin articolul 29 privind protecția datelor (2017b), *Aviz cu privire la unele aspecte esențiale ale Directivei privind asigurarea respectării legii (UE 2016/680)*, 7 decembrie 2017.

Grupul de lucru instituit prin articolul 29 privind protecția datelor (2018a), *Orientări privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului (UE) 2016/679*, WP 251 rev. 01, 6 februarie 2018.

Grupul de lucru instituit prin articolul 29 privind protecția datelor (2018b), *Opinion on Commission proposals on establishing a framework for interoperability*, WP 266, Bruxelles, 23 aprilie 2018.

Harcourt, B. (2004), „Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally”, *University of Chicago Law Review*, Vol. 71, 2004.

- Harris, D. (2002), „Flying While Arab: Lessons from the Racial Profiling Controversy”, *Civil Rights Journal*, vol. 6, nr. 1, iarna 2002.
- Harris, D. (2003), *Profiles in Injustice: Why Racial Profiling Cannot Work*, The New Press, 2003.
- Hildebrandt, M. și de Vries, K. (2013), *Privacy, due process and the computational turn: the philosophy of law meets the philosophy of technology*, New York, Routledge, 2013.
- Hildebrandt, M. și Gutwirth, S. (ed.) (2008), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Berlin, Springer, 2008.
- Hörnqvist, M. (2016), „*Riots in the welfare state: The contours of a modern-day moral economy*”, *European Journal of Criminology*, Vol. 13, Nr. 5, p. 573-589.
- Hunt, P., Saunders, J. și Hollywood, J. S. (2014), *Evaluation of the Shreveport predictive policing experiment*, RAND Corporation, 2014.
- Jobard, F. (2008), „The 2005 French urban unrests: data-based interpretations”, *Sociology Compass*, Vol. 2, Nr. 4, p. 1287-1302.
- Kádár, A., Körner, J., Moldova, Z. și Tóth, B. (2008), *Control(led) Group, Final Report on the Strategies for Effective Police Stop and Search (STEPSS) Project*, Budapesta, p. 23.
- Keskinen, S. et al (2018), *The Stopped – Ethnic Profiling in Finland*, Swedish School of Social Science, University of Helsinki, Helsinki, 3 aprilie 2018.
- Korff, D. (2015), „Passenger Name Records, data mining & data protection: the need for strong safeguards”, T-PD(2015)11, Strasbourg, 15 iunie 2015.
- Miller, J. și Alexandrou, B. (2016), „College of policing stop and search training experiment: Impact evaluation”, College of Policing Limited, 2016.
- Mittelstadt, BD., Allo, P., Taddeo, M., Wachter, S. și Floridi, L. (2016), „*The ethics of algorithms: Mapping the debate*”, *Big Data & Society*, 1 decembrie 2016.

Mohler, G.O., Short, M. B., Malinowski, S., Johnson, M., Tita, G. E., Bertozzi, A.L., Brantingham, P.J., „Randomized Controlled Field Trials of Predictive Policing”, 15 ianuarie 2016.

Nisbet, R., Elder, J. și Miner, G. (2009), „Handbook of Statistical Analysis & Data Mining Applications”, Sydney (Canada), Elsevier, 2009.

Observatorul European al Fenomenelor Rasiste și Xenofobe (2016), *Perceptions of discrimination and islamophobia – Voices from members of Muslim communities in the European Union*, 2006.

Oficiul Înaltului Comisar al Națiunilor Unite pentru Drepturile Omului (OHCHR) (2014), *Recommended Principles and Guidelines on Human Rights at International Borders*, 23 iulie 2014.

Open Society Justice Initiative (2018a), „Regulating Police Stop and Search: An Evaluation of the Reasonable Grounds Panel”, decembrie 2018

Open Society Justice Initiative (2018b), „The Recording of Police Stops: Methods and Issues”, decembrie 2018.

Organizația Națiunilor Unite (ONU) (2007), *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, A/HRC/4/26, 29 ianuarie 2007.

Oswald, M., Grace, J., Urwin, S. și Barnes, G., „Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and ‘Experimental’ Proportionality”, *Information & Communications Technology Law*, 31 august 2017.

Regatul Unit, Camden și London Prepared (2006), *Major Incident Procedures, What businesses and the voluntary sector need to know*, aprilie 2006.

Regatul Unit, Camera Lorzilor (2006), *Opinions of the Lords of appeal for judgment in the cause R (on the application of Gillan (FC) and another (FC)) (Appellants) v. Commissioner of Police for the Metropolis and another (Respondents)*, [2006] UKHL 12, 8 martie 2006.

Regatul Unit, College of Policing (2016), *Stop and Search*, Authorised Professional Practice (APP), 29 septembrie 2016.

Regatul Unit, Comisia pentru Afaceri Interne a Camerei Comunelor (2009), *The Macpherson Report – Ten Years On*, Al doisprezecelea raport din sesiunea 2008-2009, 22 iulie 2009.

Regatul Unit, Comisia pentru Egalitate și Drepturile Omului (2009), *Police and racism: what has been achieved 10 years after the Stephen Lawrence Inquiry report?*, 2009.

Regatul Unit, Her Majesty's Inspectorate of Constabulary (HMIC) (2016), *PEEL: Police legitimacy 2015 An inspection of West Midlands Police*, februarie 2016.

Regatul Unit, Her Majesty's Inspectorate of Constabulary (HMIC), (2013), *Stop and Search Powers: Are the police using them effectively and fairly?*, 2013.

Regatul Unit, Home Office (1999), *The Stephen Lawrence Inquiry. Report of An Inquiry by Sir William Macpherson of Cluny*, februarie 1999.

Regatul Unit, Home Office (2014a), *CODE A: Revised code of practice for the exercise by: police officers of statutory powers of stop and search; police officers and police staff of requirements to record public encounters*, Norwich, The Stationery Office (TSO), 2014.

Regatul Unit, Home Office (2014b), *Best use of stop and search scheme*, 2014.

Regatul Unit, London School of Economics (2011), *Reading the Riots*, decembrie 2011.

Regatul Unit, National Policing Improvement Agency (NPIA) (2012), *Stop and search, the use of intelligence and geographic targeting, Findings from case study research*, 2012.

Regatul Unit, Poliția Northamptonshire (2018), *Get Involved – Reasonable Grounds Panel*, accesat în aprilie 2018.

Regatul Unit, Poliția West Midlands (2012), *Stop and Search Policy*, noiembrie 2012.

Regatul Unit, Poliția West Midlands (2016), *Stop and Search Recommendations*, iulie 2015 (ultima modificare – iunie 2016).

Regatul Unit, Poliția West Midlands (2017a), *Stop and Search in the West Midlands: Presentation to Den Hague City Council*, aprilie 2017.

Regatul Unit, Poliția West Midlands (2017b), *New “app” set to speed up Stop & Search process*, august 2017.

Regatul Unit, Poliția West Midlands (2018), *Stop and Search Scrutiny Panels*, accesat în aprilie 2018.

Regatul Unit, Serviciul de Poliție și Prevenire a Infracțiunilor West Midlands (2014), *Stop and Search Action Plan – Outcome of consultation*, ianuarie 2014.

Regatul Unit, Staffordshire PCC Matthew Ellis, Ethics, Transparency and Audit Panel (2015), *An Independent Report into Stop & Search Encounters by Staffordshire Police*, ianuarie 2015.

Regatul Unit, Stop Watch (2011), *„Carry on Recording” Why police stops should still be recorded*, mai 2011.

Rețeaua europeană de experți juridici în domeniul egalității de gen și al nediscriminării (2016), *Links between migration and discrimination - A legal analysis of the situation in EU Member States*, iulie 2016.

Schauer, F. (2003), *Profiles Probabilities and Stereotypes*, Cambridge (MA), The Belknap Press of Harvard University Press, 2003.

Scheinin, M. (2007), raportorul special al ONU privind promovarea și protecția drepturilor omului în combaterea terorismului, *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, UN Doc. A/HRC/4/L.27, 29 ianuarie 2007.

SUA, GAO (General Accounting Office) (2000), *U.S. Customs Office: better targeting of airline passengers for personal searches could produce better results*, GAO/GGD-00-38, martie 2000.

The Guardian (2015), *Northamptonshire police ban stop and search by officers who abuse powers*, 18 august 2015.



Tóth, B.M. și Kádár, A. (2011), „Ethnic profiling in ID checks by the Hungarian police”, *Policing and Society*, vol. 21, nr. 4, p. 383-394.

Van Brakel, R. (2016), „Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing’ in: van der Sloot, B., Broeders, D. and Schrijvers, E. (ed.), *The Netherlands Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid), Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, p. 117-141.

Wrench, J. (2007), *Diversity management and discrimination: immigrants and ethnic minorities in the EU*, Aldershot, Ashgate, 2007.

Zarsky, T.Z. (2011), „Governmental Data Mining and its Alternatives”, *Penn State Law Review*, vol. 11, nr. 2, p. 285-330.

## Legislație UE

### Drepturile fundamentale

[Carta drepturilor fundamentale a Uniunii Europene](#), 2012/C 326/02, JO 2012 C 326.

[Explicații cu privire la Carta drepturilor fundamentale a Uniunii Europene](#), 2007/C 303/02, JO 2007 C 303/17.

### Nediscriminarea

[Directiva 2000/43/CE a Consiliului](#) din 29 iunie 2000 de punere în aplicare a principiului egalității de tratament.

[Directiva 2000/78/CE a Consiliului](#) din 27 noiembrie 2000 de creare a unui cadru general în favoarea egalității de tratament în ceea ce privește încadrarea în muncă și ocuparea forței de muncă.

### Protecția datelor

[Regulamentul \(UE\) 2016/679](#) al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)

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

### **Gestionarea frontierelor**

[Decizia 2007/533/JAI a Consiliului](#) din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II), JO 2007 L 205/63 (SIS II).

[Directiva \(UE\) 2016/681](#) a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, JO 2016 L 119/132.

[Regulamentul \(CE\) nr. 1987/2006](#) al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație (SIS II), JO 1987 L 381/4.

[Regulamentul \(CE\) nr. 767/2008](#) al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere, JO 2008 L 218/60 (*Regulamentul VIS*).

[Regulamentul \(UE\) nr. 603/2013](#) al Parlamentului European și al Consiliului din 26 iunie 2013 privind instituirea sistemului „Eurodac” pentru compararea amprentelor în scopul aplicării eficiente a Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentată într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid și privind cererile autorităților de aplicare a legii din statele membre și a Europol de comparare a datelor Eurodac în scopul asigurării respectării aplicării legii și de modificare a Regulamentului (UE) nr. 1077/2011 de instituire a Agenției europene pentru gestionarea operațională a sistemelor informatice la scară largă, în spațiul de libertate, securitate și justiție, JO 2013 L 180/1.

[Regulamentul \(UE\) 2016/1624](#) al Parlamentului European și al Consiliului din 14 septembrie 2016 privind Poliția de frontieră și garda de coastă la nivel european și de modificare a Regulamentului (UE) 2016/399 al Parlamentului European și al Consiliului și de abrogare a Regulamentului (CE) nr. 863/2007 al Parlamentului European și al Consiliului, a Regulamentului (CE) nr. 2007/2004 al Consiliului și a Deciziei 2005/267/CE a Consiliului, JO 2016 L 251/1.

[Regulamentul \(UE\) nr. 1052/2013](#) al Parlamentului European și al Consiliului din 22 octombrie 2013 de instituire a Sistemului european de supraveghere a frontierelor (EUROSUR), JO 2013 L 295/11.

[Regulamentul \(UE\) 2016/399](#) al Parlamentului European și al Consiliului din 9 martie 2016 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen).

## Jurisprudență

Franța, Curtea de Casație (*Cour de Cassation*), [Décision 1245](#), 9 noiembrie 2016.

Regatul Unit, Camera Lorzilor, *R (on the application of Gillan et al.) v. Commissioner of Police for the Metropolis et al.*, [2006] UKHL 12, 8 martie 2006.

CJUE, C-524/06, [Heinz Huber/Bundesrepublik Deutschland](#), 16 decembrie 2008.

CEDO, [B.S./Spania](#), nr. 47159/08, 24 iulie 2012.

CEDO, [S. și Marper/Regatul Unit](#), nr. 30562/04 și 30566/04, 4 decembrie 2008.

CEDO, [Gillan și Quinton/Regatul Unit](#), nr. 4158/05 2010, 12 ianuarie 2010.

UNHRC, *Rosalind Williams Lecraft/Spania*, com. nr. 1493/2006, 30 iulie 2009.



## **CONTACTAȚI UE**

### **În persoană**

În întreaga Uniune Europeană există sute de centre de informare Europe Direct.

Puteți găsi adresa centrului cel mai apropiat de dumneavoastră la:

[https://europa.eu/european-union/contact\\_ro](https://europa.eu/european-union/contact_ro)

### **La telefon sau prin e-mail**

Europe Direct este un serviciu care vă oferă răspunsuri la întrebările privind Uniunea Europeană. Puteți accesa acest serviciu:

– apelând numărul gratuit 00 800 6 7 8 9 10 11 (unii operatori pot taxa aceste apeluri);

– apelând numărul standard: +32 22999696; sau

– prin e-mail, la: [https://europa.eu/european-union/contact\\_ro](https://europa.eu/european-union/contact_ro)

## **GĂSIȚI INFORMAȚII DESPRE UE**

### **Online**

Informații despre Uniunea Europeană în toate limbile oficiale ale UE sunt disponibile pe site-ul Europa, la: [https://europa.eu/european-union/index\\_ro](https://europa.eu/european-union/index_ro)

### **Publicații ale UE**

Puteți descărca sau comanda publicații ale UE gratuite și contra cost la adresa:

<https://op.europa.eu/ro/publications>. Mai multe exemplare ale publicațiilor gratuite pot fi obținute contactând Europe Direct sau centrul dumneavoastră local de informare (a se vedea [https://europa.eu/european-union/contact\\_ro](https://europa.eu/european-union/contact_ro)).

### **Dreptul UE și documente conexe**

Pentru accesul la informații juridice din UE, inclusiv la ansamblul legislației UE începând din 1952 în toate versiunile lingvistice oficiale, accesați site-ul EUR-Lex, la:

<https://eur-lex.europa.eu>

### **Datele deschise ale UE**

Portalul de date deschise al UE (<https://data.europa.eu/euodp/ro>) oferă acces la seturi de date din UE. Datele pot fi descărcate și reutilizate gratuit, atât în scopuri comerciale, cât și necomerciale.

Evoluțiile tehnologice au determinat intensificarea utilizării profilurilor într-o gamă largă de contexte, iar utilizarea instrumentelor bazate pe profiluri pentru a sprijini activitatea autorităților de aplicare a legii și de gestionare a frontierelor beneficiază în ultima perioadă de o atenție sporită din partea statelor membre ale UE. Profilurile sunt utilizate în mod legitim pentru prevenirea, anchetarea și urmărirea penală a infracțiunilor, precum și pentru prevenirea și depistarea imigrației ilegale. În schimb, utilizarea ilegală a profilurilor poate submina încrederea în autorități și poate stigmatiza anumite comunități.

Prezentul ghid explică ce este crearea de profiluri, cadrele juridice care o reglementează și motivele pentru care utilizarea profilurilor în mod legal este necesară pentru respectarea drepturilor fundamentale și, totodată, esențială pentru eficiența activității polițienești și de gestionare a frontierelor. De asemenea, ghidul oferă îndrumări practice care să ajute la evitarea situațiilor în care utilizarea profilurilor în cadrul operațiunilor poliției și ale autorităților de gestionare a frontierelor este ilegală.



---

**FRA – AGENȚIA PENTRU DREPTURI FUNDAMENTALE A UNIUNII EUROPENE**

Schwarzenbergplatz 11 – 1040 Viena – Austria

T +43 158030-0 – F +43 158030-699

[fra.europa.eu](http://fra.europa.eu)

[facebook.com/fundamentalrights](https://facebook.com/fundamentalrights)

[linkedin.com/company/eu-fundamental-rights-agency](https://linkedin.com/company/eu-fundamental-rights-agency)

[twitter.com/EURightsAgency](https://twitter.com/EURightsAgency)



Oficiul pentru Publicații  
al Uniunii Europene