Orientările nr. 5/2022 privind utilizarea tehnologiei de recunoaștere facială în domeniul aplicării legii

Versiunea 2.0

Adoptată la 26 aprilie 2023

Istoricul versiunilor

Versiunea 1.0	12 mai 2022	Adoptarea orientărilor pentru consultare publică
Versiunea 2.0	26 aprilie 2023	Adoptarea orientărilor în urma consultării publice

Cuprins

REZUMAT

Din ce în ce mai multe autorități de aplicare a legii (AAL) aplică sau intenționează să aplice tehnologia de recunoaștere facială (TRF). Aceasta poate fi utilizată pentru **autentificarea** sau **identificarea** unei persoane și poate fi aplicată pe materiale video (de exemplu, TVCI) sau pe fotografii. TRF poate fi utilizată în diverse scopuri, inclusiv pentru a căuta persoane aflate pe listele de supraveghere ale poliției sau pentru a monitoriza deplasările unei persoane în spațiul public.

TRF se bazează pe prelucrarea **datelor biometrice** și, prin urmare, cuprinde prelucrarea categoriilor speciale de date cu caracter personal. Această tehnologie utilizează adesea componente ale **inteligenței artificiale** (IA) sau ale învățării automate. Deși permite prelucrarea datelor pe scară largă, TRF creează și riscul de discriminare și de rezultate false. Tehnologia de recunoaștere facială poate fi folosită în situații controlate unu la unu, dar și pentru mulțimi uriașe și noduri de transport importante.

Această tehnologie este un **instrument sensibil pentru autoritățile de aplicare a legii**. Autoritățile de aplicare a legii sunt autorități de executare și au competențe suverane. TRF este predispusă să interfereze cu drepturile fundamentale – inclusiv dincolo de dreptul la protecția datelor cu caracter personal – și poate afecta stabilitatea socială și politica democratică.

Pentru protecția datelor cu caracter personal în contextul aplicării legii, trebuie îndeplinite **cerințele Directivei privind protecția datelor în materie de aplicare a legii (LED)**. Un anumit cadru privind utilizarea TRF este prevăzut în LED, în special la articolul 3 punctul 13 (termenul „date biometrice”), la articolul 4 (principiile referitoare la prelucrarea datelor cu caracter personal), la articolul 8 (legalitatea prelucrării), la articolul 10 (prelucrarea de categorii speciale de date cu caracter personal) și la articolul 11 (procesul decizional individual automatizat).

Mai multe alte drepturi fundamentale pot fi afectate, de asemenea, de aplicarea TRF. Prin urmare, **Carta drepturilor fundamentale a UE** („Carta”) este esențială pentru interpretarea LED, în special dreptul la protecția datelor cu caracter personal prevăzut la articolul 8 din Cartă, dar și dreptul la viață privată prevăzut la articolul 7 din Cartă.

Măsurile legislative care servesc drept temei legal pentru prelucrarea datelor cu caracter personal interferează în mod direct cu drepturile garantate de articolele 7 și 8 din Cartă. Prelucrarea datelor biometrice în toate situațiile constituie în sine o atingere gravă adusă drepturilor. Aceasta nu depinde de rezultat, de exemplu un rezultat pozitiv al combinării. Orice restrângere a exercitării drepturilor și libertăților fundamentale trebuie să fie prevăzută de lege și să respecte substanța acestor drepturi și libertăți.

Temeiul legal trebuie să aibă prevederi **suficient de clare** pentru a oferi cetățenilor indicii adecvate în ceea ce privește condițiile și circumstanțele în care autoritățile sunt împuternicite să recurgă la orice măsuri de colectare a datelor și de supraveghere secretă. O simplă transpunere în dreptul intern a clauzei generale de la articolul 10 din LED ar fi lipsită de precizie și previzibilitate.

Înainte ca legiuitorul național să creeze un nou temei legal pentru orice formă de prelucrare a datelor biometrice care utilizează recunoașterea facială, ar trebui **consultată** autoritatea competentă de supraveghere a protecției datelor.

Măsurile legislative trebuie să fie **adecvate** pentru realizarea obiectivelor legitime urmărite de legislația în cauză. Un **obiectiv de interes general** – oricât de important ar fi – nu justifică, în sine, restrângerea unui drept fundamental. Măsurile legislative ar trebui **să diferențieze** și să țintească persoanele care intră sub incidența acestora, ținând seama de obiectivul urmărit, de exemplu,

combaterea unor infracțiuni grave specifice. Dacă măsura acoperă toate persoanele la modul general, fără o astfel de diferențiere, limitare sau excepție, acest lucru intensifică atingerea adusă drepturilor. De asemenea, se aduce o atingere gravă drepturilor dacă prelucrarea datelor acoperă o parte semnificativă a populației.

Datele trebuie să fie prelucrate într-un mod care să asigure aplicabilitatea și eficacitatea normelor și a principiilor UE privind protecția datelor. În funcție de fiecare situație, **evaluarea necesității și a proporționalității** trebuie, de asemenea, să identifice și să ia în considerare toate implicațiile posibile pentru alte drepturi fundamentale. Dacă datele sunt prelucrate în mod sistematic fără ca persoanele vizate să aibă cunoștință de acest lucru, există probabilitatea să se genereze un **sentiment general de supraveghere constantă**. Acest lucru poate duce la efecte disuasive în ceea ce privește o parte sau toate drepturile fundamentale în cauză, de exemplu demnitatea umană în temeiul articolului 1 din Cartă, libertatea de gândire, de conștiință și de religie în temeiul articolului 10 din Cartă, libertatea de exprimare în temeiul articolului 11 din Cartă, precum și libertatea de întrunire și de asociere în temeiul articolului 12 din Cartă.

Prelucrarea categoriilor speciale de date, cum ar fi datele biometrice, poate fi considerată „**strict necesară**" (articolul 10 din LED) numai dacă atingerea adusă protecției datelor cu caracter personal și restrângerile acesteia se limitează la ceea ce este absolut necesar, adică indispensabil, și exclude orice prelucrare de natură generală sau sistematică.

Faptul că o fotografie a fost **făcută publică în mod manifest** (articolul 10 din LED) de către persoana vizată nu înseamnă că datele biometrice conexe, care pot fi extrase din fotografie prin mijloace tehnice specifice, sunt considerate ca fiind făcute publice în mod manifest. Setările implicite ale unui serviciu, de exemplu, punerea la dispoziția publicului a modelelor, sau absența posibilității de alegere, de exemplu modelele sunt făcute publice fără ca utilizatorul să poată modifica această setare, nu ar trebui interpretate în niciun fel ca fiind date făcute publice în mod manifest.

Articolul 11 din LED stabilește un cadru pentru un **proces decizional individual automatizat**. Utilizarea TRF implică utilizarea categoriilor speciale de date și poate duce la crearea de profiluri, în funcție de modul și de scopul în care se aplică TRF. În orice caz, în conformitate cu dreptul Uniunii și cu articolul 11 alineatul (3) din LED, este interzisă crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza categoriilor speciale de date cu caracter personal.

Articolul 6 din LED se referă la necesitatea de a face **distincție între diferitele categorii de persoane vizate**. În ceea ce privește persoanele vizate pentru care nu există dovezi de natură să sugereze că comportamentul lor ar putea avea o legătură, chiar indirectă sau îndepărtată, cu scopul legitim în conformitate cu LED, cel mai probabil nu există nicio justificare pentru a aduce atingere drepturilor.

Principiul reducerii la minimum a datelor [articolul 4 alineatul (1) litera (e) din LED] impune, de asemenea, ca orice material video care nu este relevant pentru scopul prelucrării să fie întotdeauna eliminat sau anonimizat (de exemplu, prin estompare fără capacitate retroactivă de recuperare a datelor) înainte de implementare.

Operatorul trebuie să analizeze cu atenție modul în care îndeplinește (sau dacă poate să îndeplinească) cerințele privind **drepturile persoanei vizate** înainte de lansarea oricărei prelucrări prin TRF, deoarece tehnologia în cauză implică adesea prelucrarea categoriilor speciale de date cu caracter personal fără nicio interacțiune evidentă cu persoana vizată.

Exercitarea efectivă a drepturilor persoanei vizate depinde de îndeplinirea de către operator a **obligațiilor de informare** care îi revin (articolul 13 din LED). Atunci când se evaluează dacă există un

„anumit caz” în conformitate cu articolul 13 alineatul (2) din LED, trebuie luați în considerare mai mulți factori, inclusiv dacă datele cu caracter personal sunt colectate fără știrea persoanei vizate, deoarece aceasta ar fi singura modalitate de a permite persoanelor vizate să-și exercite în mod efectiv drepturile. În cazul în care procesul decizional se realizează exclusiv pe baza TRF, atunci persoanele vizate trebuie informate cu privire la caracteristicile procesului decizional automatizat.

În ceea ce privește **cererile de acces**, atunci când datele biometrice sunt stocate și legate de o identitate și prin date alfanumerice, în conformitate cu principiul reducerii la minimum a datelor, acest lucru ar trebui să permită autorității competente să confirme o cerere de acces pe baza unei căutări după aceste date alfanumerice și fără a lansa o prelucrare suplimentară a datelor biometrice ale altor persoane (de exemplu, prin căutarea cu TRF într-o bază de date).

Riscurile pentru persoanele vizate sunt deosebit de grave dacă date inexacte sunt stocate într-o bază de date a poliției și/sau sunt partajate cu alte entități. Operatorul trebuie să **corecteze** datele stocate și sistemele bazate pe tehnologia de recunoaștere facială în consecință (vezi și considerentul 47 din LED).

Dreptul la **restricționare** devine deosebit de important atunci când este vorba despre tehnologia de recunoaștere facială [bazată pe algoritm(i) și care, prin urmare, nu prezintă niciodată un rezultat definitiv] în situațiile în care sunt colectate cantități mari de date, iar exactitatea și calitatea identificării pot varia.

O **evaluare a impactului asupra protecției datelor (EIPD)** înainte de utilizarea TRF este o cerință obligatorie, vezi articolul 27 din LED. CEPD recomandă publicarea rezultatelor acestor evaluări sau cel puțin a principalelor lor constatări și concluzii, ca măsură de consolidare a încrederii și a transparenței.

Cele mai multe cazuri de implementare și utilizare a TRF prezintă un risc ridicat intrinsec pentru drepturile și libertățile persoanelor vizate. Prin urmare, autoritatea care implementează TRF ar trebui să **consulte** autoritatea de supraveghere competentă înainte de implementarea sistemului.

Având în vedere natura unică a datelor biometrice, autoritatea care implementează și/sau utilizează TRF ar trebui să acorde o atenție deosebită **securității prelucrării**, conform articolului 29 din LED. Autoritatea de aplicare a legii ar trebui, în special, să se asigure că sistemul respectă standardele relevante și pune în aplicare măsuri de protecție a modelelor biometrice. Principiile și garanțiile privind protecția datelor trebuie să fie integrate în tehnologie înainte de începerea prelucrării datelor cu caracter personal. Prin urmare, chiar și atunci când o autoritate de aplicare a legii intenționează să aplice și să utilizeze TRF de la furnizori externi, aceasta trebuie să se asigure, de exemplu prin procedura de achiziții, că sunt implementate numai TRF bazate pe principiile **asigurării protecției datelor începând cu momentul conceperii și în mod implicit**.

Înregistrarea (vezi articolul 25 din LED) este o garanție importantă pentru verificarea legalității prelucrării, atât la nivel intern (adică monitorizarea proprie de către operatorul în cauză/persoana împuternicită de operatorul în cauză), cât și de către autoritățile de supraveghere externe. În contextul sistemelor de recunoaștere facială, se recomandă și înregistrarea modificărilor bazei de date de referință și a încercărilor de identificare sau de verificare, inclusiv a utilizatorului, a rezultatului și a scorului de încredere. Înregistrarea este însă doar un element esențial al **principiului general al responsabilității** [vezi articolul 4 alineatul (4) din LED]. Operatorul trebuie să poată demonstra conformitatea prelucrării cu principiile de bază ale protecției datelor prevăzute la articolul 4 alineatele (1)-(3) din LED.

CEPD reamintește **solicitarea** sa și a AEPD **de interzicere** a anumitor tipuri de prelucrare în legătură cu (1) identificarea biometrică la distanță a indivizilor în spații accesibile publicului, (2) sistemele de recunoaștere facială sprijinite de IA care clasifică indivizii pe baza datelor lor biometrice în grupuri bazate pe origine etnică, gen, precum și pe orientarea politică sau sexuală sau alte criterii de discriminare, (3) utilizarea recunoașterii faciale sau a unor tehnologii similare, pentru a deduce emoțiile unei persoane fizice și (4) prelucrarea datelor cu caracter personal într-un context de aplicare a legii care s-ar baza pe o bază de date populată prin colectarea de date cu caracter personal la scară largă și în mod generalizat, de exemplu prin extragerea („scraping") fotografiilor și a imaginilor faciale accesibile online.

O garanție esențială pentru drepturile fundamentale în cauză este **supravegherea eficientă** de către autoritățile competente de supraveghere a protecției datelor. Prin urmare, statele membre trebuie să se asigure că resursele autorităților de supraveghere sunt adecvate și suficiente pentru a le permite să-și îndeplinească mandatul.

Aceste **orientări se adresează** legiuitorilor de la nivelul UE și de la nivel național, precum și autorităților de aplicare a legii și funcționarilor acestora care implementează și utilizează sisteme bazate pe TRF. Orientările li se adresează persoanelor fizice în măsura în care sunt interesate la modul general sau în calitate de persoane vizate, în special în ceea ce privește drepturile persoanelor vizate.

Orientările sunt menite să informeze cu privire la anumite proprietăți ale TRF și la cadrul juridic aplicabil în contextul aplicării legii (în special LED).

- În plus, oferă un **instrument pentru a sprijini o primă clasificare a sensibilității unui caz de utilizare dat** (anexa I).
- Conține și **îndrumări practice pentru autoritățile de aplicare a legii care doresc să achiziționeze și să utilizeze un sistem bazat pe TRF** (anexa II).
- Descrie, de asemenea, mai multe **cazuri** tipice **de utilizare și prezintă numeroase considerente relevante**, în special cu privire la testul necesității și proporționalității (anexa III).

1 INTRODUCERE

1. Tehnologia de recunoaștere facială (TRF) poate fi folosită pentru recunoașterea automată a persoanelor fizice pe baza feței lor. TRF se bazează adesea pe inteligența artificială, de exemplu tehnologiile de învățare automată. Aplicațiile tehnologiei de recunoaștere facială sunt testate și folosite din ce în ce mai mult în diferite domenii, de la utilizarea individuală până la utilizarea de către organizații private și administrația publică. Autoritățile de aplicare a legii se așteaptă, de asemenea, să obțină avantaje de pe urma utilizării TRF. Aceasta promite soluții la provocările relativ noi, de exemplu investigațiile care implică o cantitate mare de probe obținute, dar și pentru probleme cunoscute, în special cu privire la lipsa de personal pentru sarcinile de observare și căutare.

2. În foarte mare măsură, interesul crescut pentru TRF se bazează pe eficiența și scalabilitatea ei. Odată cu acestea apar și dezavantajele inerente tehnologiei și aplicării acesteia – de asemenea la scară largă. Deși pot exista mii de seturi de date cu caracter personal analizate prin simpla apăsare a unui buton, efectele deja ușoare ale discriminării algoritmice sau ale identificării eronate pot duce la un număr mare de persoane afectate grav în comportamentul lor și în viața de zi cu zi. Alt element-cheie al TRF este amploarea prelucrării datelor cu caracter personal și, în special, a datelor biometrice, deoarece prelucrarea datelor cu caracter personal constituie o atingere adusă dreptului fundamental la protecția

datelor cu caracter personal în conformitate cu articolul 8 din Carta drepturilor fundamentale a Uniunii Europene (Carta).

3. Aplicarea TRF de către autoritățile de aplicare a legii va avea – și, într-o anumită măsură, are deja – implicații semnificative asupra persoanelor și grupurilor de persoane, inclusiv asupra minorităților. Aceste implicații vor avea efecte considerabile și asupra modului în care trăim împreună și asupra stabilității noastre sociale și politice democratice, apreciind importanța mare a pluralismului și a opoziției politice. Dreptul la protecția datelor cu caracter personal este adesea esențial ca o condiție prealabilă pentru garantarea altor drepturi fundamentale. Aplicarea TRF este în foarte mare măsură predispusă să interfereze cu drepturile fundamentale dincolo de dreptul la protecția datelor cu caracter personal.

4. Prin urmare, CEPD consideră că este important să contribuie la integrarea în curs a TRF în domeniul aplicării legii care intră sub incidența Directivei privind protecția datelor în materie de aplicare a legii[1], respectiv a legislației naționale de transpunere a acesteia, și să furnizeze prezentele orientări. Orientările sunt menite să furnizeze informații relevante pentru legiuitorii de la nivelul UE și de la nivel național, precum și pentru autoritățile de aplicare a legii și funcționarii acestora când implementează și utilizează sisteme bazate pe TRF. Domeniul de aplicare al orientărilor se limitează la TRF. Cu toate acestea, alte forme de prelucrare a datelor cu caracter personal bazate pe date biometrice de către autoritățile de aplicare a legii, în special dacă sunt prelucrate de la distanță, pot implica riscuri similare sau suplimentare pentru persoane, grupuri și societate. În funcție de circumstanțele respective, unele aspecte ale orientărilor pot servi drept sursă utilă și în aceste cazuri. În cele din urmă, persoanele care sunt interesate în general sau în calitate de persoane vizate pot găsi, de asemenea, informații importante, în special în ceea ce privește drepturile persoanelor vizate.

5. Orientărilor sunt alcătuite din documentul principal și trei anexe. Documentul principal de față prezintă tehnologia și cadrul juridic aplicabil. Pentru a contribui la identificarea unora dintre aspectele majore pentru clasificarea gravității atingerii aduse drepturilor fundamentale într-un anumit domeniu de aplicare, în anexa I este disponibil un model. Autoritățile de aplicare a legii care doresc să achiziționeze și să utilizeze un sistem bazat pe TRF pot găsi îndrumări practice în anexa II. În funcție de domeniul de aplicare al TRF, ar putea fi relevante diferite considerente. O serie de scenarii ipotetice și considerente relevante pot fi găsite în anexa III.

2 TEHNOLOGIA

2.1 O tehnologie biometrică, două funcții distincte

6. Tehnologia de recunoaștere facială este o tehnologie probabilistică ce poate recunoaște automat persoanele fizice pe baza feței, pentru a le autentifica sau identifica.

7. TRF se încadrează în categoria mai largă a tehnologiei biometrice. Biometria cuprinde toate procesele automatizate folosite pentru a recunoaște o persoană prin cuantificarea caracteristicilor fizice, fiziologice sau comportamentale (amprente digitale, structura irisului, vocea, mersul, modelele vaselor de sânge etc.). Aceste caracteristici sunt definite ca „date biometrice” deoarece permit sau confirmă identificarea unică a persoanei respective.

[1] 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.

8. Acest lucru este valabil pentru fețele oamenilor sau, mai precis, pentru prelucrarea tehnică a acestora cu dispozitive de recunoaștere facială: prin preluarea imaginii unei fețe (o fotografie sau un material video), numită „eșantion" biometric, se poate extrage o reprezentare digitală a caracteristicilor distincte ale feței respective (numită „model").

9. Un model biometric este o reprezentare digitală a caracteristicilor unice care au fost extrase dintr-un eșantion biometric și care pot fi stocate într-o bază de date biometrice[2]. Se presupune că acest model este unic și specific fiecărei persoane și este, în principiu, permanent în timp[3]. În faza de recunoaștere, dispozitivul compară acest model cu alte modele produse anterior sau calculate direct din eșantioane biometrice, de exemplu fețele dintr-o imagine, dintr-o fotografie sau dintr-un material video. „Recunoașterea facială" este, prin urmare, un proces în două etape: colectarea imaginii faciale și transformarea ei într-un model, urmată de recunoașterea acestei fețe prin compararea modelului corespunzător cu unul sau mai multe alte modele.

10. Ca orice proces biometric, recunoașterea facială poate îndeplini două funcții distincte:

- **autentificarea** unei persoane, care are scopul de a verifica dacă o persoană este cine pretinde că este. În acest caz, sistemul va compara un model sau un eșantion biometric preînregistrat (de exemplu, stocat pe un card inteligent sau pe un pașaport biometric) cu o singură față, cum ar fi cea a unei persoane care se prezintă la un post de frontieră, pentru a verifica dacă este vorba de una și aceeași persoană. Prin urmare, această funcționalitate se bazează pe compararea a două modele. Aceasta se numește și **verificare** unu la unu;

- **identificarea** unei persoane, care are scopul de a găsi o persoană dintr-un grup de persoane, într-o anumită zonă, o imagine sau o bază de date. În acest caz, sistemul trebuie să prelucreze fiecare captură facială, pentru a genera un model biometric și apoi să verifice dacă aceasta se potrivește cu o persoană cunoscută de sistem. Această funcționalitate se bazează deci pe compararea unui model cu o bază de date de modele sau eșantioane (de referință). Se mai numește și identificare realizată prin compararea mai multor serii de date. De exemplu, poate face legătura între o înregistrare a numelui (nume, prenume) și o față, în cazul în care comparația se face cu o bază de date cu fotografii asociate numelor și prenumelor. Aceasta poate implica și urmărirea unei persoane într-o mulțime, fără a face neapărat legătura cu identitatea civilă a persoanei respective.

11. În ambele cazuri, tehnicile de recunoaștere facială utilizate se bazează pe o corespondență estimată între modele: cel care este comparat și cel (cele) de referință. Din acest punct de vedere, ele sunt probabilistice: comparația deduce o probabilitate, mai mare sau mai mică, că persoana în cauză este într-adevăr persoana care trebuie autentificată sau identificată; dacă această probabilitate depășește un anumit prag din sistem, definit de utilizator sau de dezvoltatorul sistemului, sistemul va presupune că există o corespondență.

12. Deși cele două funcții – autentificarea și identificarea – sunt distincte, ambele se referă la prelucrarea datelor biometrice referitoare la o persoană fizică identificată sau identificabilă și, prin urmare, constituie o prelucrare a datelor cu caracter personal și, mai exact, o prelucrare a unor categorii speciale de date cu caracter personal.

13. Recunoașterea facială face parte dintr-un spectru mai larg de tehnici de prelucrare a imaginilor și a materialelor video. Unele camere video pot filma persoane dintr-o zonă delimitată, în special fețele

[2] Orientări privind recunoașterea facială, Comitetul consultativ al Convenției 108, Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, Consiliul Europei, iunie 2021.
[3] Acest lucru ar putea depinde de tipul de biometrie și de vârsta persoanei vizate.

lor, dar nu pot fi utilizate ca atare pentru recunoașterea automată a persoanelor. Același lucru este valabil și pentru fotografia simplă: un aparat de fotografiat nu este un sistem de recunoaștere facială, deoarece fotografiile persoanelor trebuie prelucrate într-un mod specific pentru a extrage datele biometrice.

14. Nici simpla depistare a fețelor de către așa-numitele camere „inteligente” nu constituie neapărat un sistem de recunoaștere facială. Deși ridică, de asemenea, întrebări importante în ceea ce privește etica și eficacitatea, tehnicile digitale de detectare a comportamentelor anormale sau a evenimentelor violente ori de recunoaștere a emoțiilor faciale sau chiar a siluetelor nu pot fi considerate sisteme biometrice care prelucrează categorii speciale de date cu caracter personal, cu condiția ca acestea să nu aibă drept scop identificarea unică a unei persoane și ca prelucrarea datelor cu caracter personal în cauză să nu includă alte categorii speciale de date cu caracter personal. Aceste exemple nu sunt complet independente de recunoașterea facială și sunt supuse în continuare normelor de protecție a datelor cu caracter personal.[4] În plus, acest tip de sistem de depistare poate fi utilizat împreună cu alte sisteme care au drept scop identificarea unei persoane, fiind astfel considerat o tehnologie de recunoaștere facială.

15. Spre deosebire de sistemele de captare și prelucrare video, de exemplu, care necesită instalarea unor dispozitive fizice, recunoașterea facială este o funcționalitate software care poate fi implementată în cadrul sistemelor existente (camere de luat vederi, baze de date de imagini etc.). Prin urmare, o astfel de funcționalitate poate fi conectată sau interfațată cu o multitudine de sisteme și combinată cu alte funcționalități. Această integrare într-o infrastructură deja existentă necesită o atenție deosebită, deoarece implică riscuri inerente din cauză că tehnologia de recunoaștere facială ar putea fi pe deplin compatibilă și ar putea fi ascunsă cu ușurință[5].

2.2 O mare varietate de scopuri și aplicații

16. În afara domeniului de aplicare al acestui ghid și în afara domeniului de aplicare al LED, recunoașterea facială poate fi utilizată pentru o gamă largă de obiective, atât pentru utilizarea comercială, cât și pentru abordarea preocupărilor legate de siguranța publică sau de aplicare a legii. Ea poate fi aplicată în numeroase contexte diferite: în relația personală dintre un utilizator și un serviciu (accesul la o aplicație), pentru accesul într-un anumit loc (filtrare fizică) sau, fără nicio limitare specială, în spațiul public (recunoaștere facială în timp real). Aceasta se poate aplica oricărui tip de persoană vizată: clientul unui serviciu, un angajat, un simplu privitor, o persoană căutată sau o persoană implicată în proceduri judiciare sau administrative etc. Unele utilizări sunt deja obișnuite și larg răspândite; altele sunt, în acest moment, în stadiu experimental sau speculativ. Deși aceste orientări nu vor aborda toate aceste utilizări și aplicații, CEPD reamintește că pot fi puse în aplicare numai dacă sunt conforme cu cadrul juridic aplicabil, în special cu RGPD și cu legislația națională relevantă.[6] Chiar și în contextul LED, ca urmare a funcțiilor de autentificare sau de identificare, datele prelucrate cu ajutorul tehnologiei de recunoaștere facială pot fi prelucrate ulterior și în alte scopuri, cum ar fi clasificarea.

17. Mai exact, ar putea fi avută în vedere o scară de utilizări potențiale în funcție de gradul de control pe care îl au persoanele asupra datelor lor cu caracter personal, de mijloacele efective de care dispun pentru exercitarea acestui control și de dreptul lor la inițiativă pentru declanșarea și utilizarea acestei

[4] Cu toate acestea, articolul 10 din LED (sau articolul 9 din RGPD) se aplică sistemelor care sunt utilizate pentru a clasifica persoanele fizice pe baza biometriei lor în grupuri în funcție de originea etnică, precum și de orientarea politică sau sexuală sau de alte categorii speciale de date cu caracter personal.
[5] De exemplu, în camerele purtate pe corp, care sunt folosite tot mai mult în practică.
[6] Vezi și Ghidul CEPD 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video, adoptat la 29 ianuarie 2020, pentru îndrumări suplimentare.

tehnologii, de consecințele pentru acestea (în cazul recunoașterii sau nerecunoașterii) și de amploarea prelucrării efectuate. Recunoașterea facială bazată pe un model stocat pe un dispozitiv personal (card inteligent, telefon inteligent etc.) care aparține persoanei respective, utilizat pentru autentificare și de uz strict personal printr-o interfață dedicată, nu prezintă aceleași riscuri ca, de exemplu, utilizarea în scopuri de identificare, într-un mediu necontrolat, fără implicarea activă a persoanelor vizate, în care modelul fiecărei fețe care intră în zona de monitorizare este comparat cu modelele aparținând unui segment amplu al populației stocate într-o bază de date. Între aceste două extreme se află un spectru foarte variat de utilizări și probleme asociate legate de protecția datelor cu caracter personal.

18. Pentru a ilustra mai bine contextul în care tehnologiile de recunoaștere facială sunt, în prezent, dezbătute sau implementate, fie pentru autentificare, fie pentru identificare, CEPD consideră că este relevant să menționeze o serie de exemple. Exemplele de mai jos sunt pur descriptive și nu trebuie considerate ca fiind vreun fel de evaluare preliminară a conformității lor cu acquis-ul UE în domeniul protecției datelor.

Exemple de autentificare prin recunoaștere facială

19. Autentificarea poate fi concepută astfel încât utilizatorii să dețină controlul deplin asupra acesteia, de exemplu pentru a permite accesul la servicii sau la aplicații doar în mediul casnic. Ca atare, acest tip de autentificare este utilizat pe scară largă de către proprietarii de telefoane inteligente pentru a-și debloca dispozitivul, în locul autentificării cu parolă.

20. Autentificarea prin recunoaștere facială poate fi folosită și pentru a verifica identitatea unei persoane care dorește să beneficieze de servicii publice sau private oferite de terți. Așadar, aceste procese oferă o modalitate de a crea o identitate digitală utilizând o aplicație mobilă (telefon inteligent, tabletă etc.), care poate fi utilizată apoi pentru a accesa serviciile administrative online.

21. În plus, autentificarea prin recunoaștere facială poate avea scopul de a controla accesul fizic într-unul sau în mai multe locuri prestabilite, de exemplu intrările în clădiri sau puncte de trecere specifice. Această funcționalitate este implementată, de exemplu, în anumite operațiuni de prelucrare în scopul trecerii frontierei, unde dispozitivul postului de frontieră compară fața persoanei cu cea stocată în documentul de identitate (pașaport sau permis de ședere securizat).

Exemple de identificare prin recunoaștere facială

22. Identificarea poate fi aplicată în multe moduri, chiar mai diverse. Acestea includ, în special, dar nu numai, utilizările enumerate mai jos, care sunt, în prezent, observate, experimentate sau planificate în UE:

- căutarea, într-o bază de date cu fotografii, a identității unei persoane neidentificate (victimă, suspect etc.);
- monitorizarea deplasărilor unei persoane în spațiul public. Fața sa este comparată cu modelele biometrice ale persoanelor care călătoresc sau au călătorit în zona monitorizată, de exemplu atunci când un bagaj este lăsat în urmă sau după comiterea unei infracțiuni;
- reconstituirea călătoriei unei persoane și a interacțiunilor ulterioare cu alte persoane, printr-o comparare întârziată a acelorași elemente în încercarea de a identifica, de exemplu, contactele acestora;
- identificarea biometrică la distanță în spații publice a persoanelor căutate. Toate fețele surprinse în timp real de camerele de protecție video sunt verificate, în timp real, într-o bază de date deținută de forțele de securitate;

- recunoașterea automată a persoanelor dintr-o imagine pentru a identifica, de exemplu, relațiile lor pe o rețea socială care folosește acest tip de recunoaștere. Imaginea este comparată cu modelele tuturor celor din rețea care și-au dat acordul pentru această funcționalitate pentru a sugera identificarea nominală a acestor relații;

- accesul la servicii, unele distribuitoare de numerar recunoscându-și clienții, prin compararea unei capturi faciale efectuate de o cameră de luat vederi cu baza de date a imaginilor faciale deținute de bancă;

- urmărirea călătoriei unui pasager într-o anumită etapă a călătoriei. Modelul, calculat în timp real, al oricărei persoane care se înregistrează la porțile situate în anumite etape ale călătoriei (puncte de predare a bagajelor, porți de îmbarcare etc.) este comparat cu modelele persoanelor înregistrate anterior în sistem.

23. Pe lângă utilizarea TRF în domeniul aplicării legii, gama largă de aplicații observate necesită cu siguranță o dezbatere și o abordare politică cuprinzătoare pentru a asigura consecvența și conformitatea cu acquis-ul UE în domeniul protecției datelor.

2.3 Fiabilitate, exactitate și riscuri pentru persoanele vizate

24. Ca fiecare tehnologie, recunoașterea facială poate fi supusă și unor provocări în ceea ce privește implementarea sa, în special cu privire la fiabilitatea și eficiența sa în materie de autentificare sau de identificare, precum și la problema generală a calității și a exactității datelor „sursă” și a rezultatului prelucrării prin tehnologia de recunoaștere facială.

25. Aceste provocări tehnologice implică riscuri speciale pentru persoanele vizate, care sunt cu atât mai semnificative sau mai grave în domeniul aplicării legii, având în vedere efectele posibile asupra persoanelor vizate, fie juridice, fie de altă natură, care le afectează în mod similar într-un mod semnificativ. În acest context, pare, de asemenea, util să se sublinieze că utilizarea ex post a TRF nu este, în sine, mai sigură, deoarece persoanele pot fi urmărite în timp și în mai multe locuri. Așadar, utilizarea ex post prezintă și riscuri specifice care trebuie evaluate de la caz la caz.[7]

26. După cum a subliniat Agenția pentru Drepturi Fundamentale a UE în raportul său din 2019, „determinarea nivelului necesar de exactitate a software-ului de recunoaștere facială este dificilă: există multe moduri diferite de a evalua și de a aprecia exactitatea, în funcție și de sarcina, scopul și contextul utilizării sale. Dacă tehnologia se aplică în locuri vizitate de milioane de persoane – cum ar fi gările sau aeroporturile –, o proporție relativ mică de erori (de exemplu, 0,01 %)[8] înseamnă totuși că sute de persoane sunt semnalizate greșit. În plus, este posibil ca anumite categorii de persoane să prezinte o probabilitate mai mare de a fi găsite prin corespondență în mod eronat decât altele, după cum se descrie în secțiunea 3. Există diferite moduri de a calcula și de a interpreta ratele de eroare, astfel încât este nevoie de prudență. În plus, în ceea ce privește exactitatea și erorile, întrebările legate de ușurința cu care un sistem poate fi înșelat, de exemplu, cu imagini faciale false (numite „spoofing”), sunt importante în special în scopul aplicării legii.”[9]

27. În acest context, CEPD consideră că este important de reamintit că TRF, indiferent că este utilizată în scopul autentificării sau al identificării, nu oferă un rezultat definitiv, ci se bazează pe probabilitățile ca

[7] Vezi exemplele prezentate în anexa III.
[8] Această rată de exactitate provine din raportul citat și reflectă o rată mult mai bună decât performanța actuală a algoritmilor din aplicațiile TRF.
[9] Tehnologia de recunoaștere facială: considerente privind drepturile fundamentale în contextul aplicării legii, Agenția pentru Drepturi Fundamentale a UE, 21 noiembrie 2019.

două fețe sau imagini ale fețelor să corespundă aceleiași persoane.[10] Acest rezultat este și mai puțin exact atunci când calitatea eșantionului biometric introdus pentru recunoașterea facială este scăzută. Neclaritatea imaginilor de intrare, rezoluția mică a camerei de luat vederi, mișcarea și lumina slabă pot fi factori de calitate scăzută. Alte aspecte cu impact semnificativ asupra rezultatelor sunt prevalența și falsificarea (spoofing), de exemplu, când infractorii încearcă fie să evite să treacă pe lângă camere de luat vederi, fie să înșele TRF. Numeroase studii au evidențiat, de asemenea, că astfel de rezultate statistice obținute prin prelucrare algoritmică pot fi supuse și unor prejudecăți, care rezultă în special din calitatea datelor sursă, precum și din bazele de date de antrenare sau alți factori, cum ar fi alegerea locului de utilizare a tehnologiei. În plus, ar trebui subliniat, de asemenea, impactul tehnologiei de recunoaștere facială asupra altor drepturi fundamentale, cum ar fi respectarea vieții private și de familie, libertatea de exprimare și de informare, libertatea de întrunire și de asociere etc.

28. Prin urmare, este esențial ca fiabilitatea și exactitatea tehnologiei de recunoaștere facială să fie luate în considerare drept criterii pentru evaluarea conformității cu principiile-cheie de protecție a datelor, în conformitate cu articolul 4 din LED, în special în ceea ce privește echitatea și exactitatea.

29. Deși subliniază că datele de înaltă calitate sunt esențiale pentru algoritmi de înaltă calitate, CEPD subliniază și necesitatea ca operatorii de date, ca parte a obligației lor de responsabilitate, să efectueze o evaluare periodică și sistematică a prelucrării algoritmice pentru a asigura în special exactitatea, echitatea și fiabilitatea rezultatului unei astfel de prelucrări a datelor cu caracter personal. Datele cu caracter personal utilizate în scopul evaluării, antrenării și dezvoltării ulterioare a sistemelor bazate pe TRF pot fi prelucrate numai pe baza unui temei legal suficient și în conformitate cu principiile comune de protecție a datelor.

3 CADRUL JURIDIC APLICABIL

30. Utilizarea tehnologiilor de recunoaștere facială este legată în mod intrinsec de prelucrarea datelor cu caracter personal, inclusiv a categoriilor speciale de date. În plus, are un impact direct sau indirect asupra unei serii de drepturi fundamentale, consacrate în Carta drepturilor fundamentale a UE. Acest lucru este deosebit de relevant în domeniul aplicării legii și al justiției penale. Prin urmare, orice utilizare a tehnologiilor de recunoaștere facială ar trebui efectuată în strictă conformitate cu cadrul juridic aplicabil.

31. Următoarele informații sunt destinate să fie utilizate pentru a fi luate în considerare la evaluarea viitoarelor măsuri legislative și administrative, precum și la punerea în aplicare a legislației existente în fiecare caz în parte care implică TRF. Relevanța cerințelor respective variază în funcție de situația specifică. Întrucât nu se pot prevedea toate situațiile viitoare, se consideră că informațiile oferă doar sprijin și nu trebuie interpretate ca o enumerare exhaustivă.

3.1 Cadrul juridic general – Carta drepturilor fundamentale a UE și Convenția Europeană a Drepturilor Omului (CEDO)

[10] Această probabilitate se numește „scor de încredere”.

3.1.1 Aplicabilitatea cartei

32. Carta drepturilor fundamentale a UE (denumită în continuare „Carta”) se adresează instituțiilor, organelor, oficiilor și agențiilor Uniunii, precum și statelor membre atunci când pun în aplicare dreptul Uniunii.

33. Reglementarea prelucrării datelor biometrice în scopul aplicării legii în conformitate cu articolul 1 alineatul (1) din LED pune, în mod inevitabil, problema respectării drepturilor fundamentale, în special a respectării vieții private și a secretului comunicațiilor în temeiul articolului 7 din Cartă și a dreptului la protecția datelor cu caracter personal în temeiul articolului 8 din Cartă.

34. Colectarea și analiza înregistrărilor video ale persoanelor fizice, inclusiv ale fețelor acestora, implică prelucrarea de date cu caracter personal. Atunci când se prelucrează din punct de vedere tehnic imaginea, prelucrarea acoperă și datele biometrice. Prelucrarea tehnică a datelor referitoare la fața unei persoane fizice în raport cu timpul și locul permite formularea unor concluzii cu privire la viața privată a persoanelor relevante. Aceste concluzii se pot referi la originea rasială sau etnică, sănătate, religie, obiceiurile din viața de zi cu zi, locurile de reședință permanente sau temporare, deplasările zilnice sau de altă natură, activitățile desfășurate, relațiile sociale ale acelor persoane și la mediile sociale frecventate de acestea. Gama largă de informații care pot fi dezvăluite prin aplicarea TRF arată în mod clar impactul posibil asupra dreptului la protecția datelor cu caracter personal prevăzut la articolul 8 din Cartă, dar și asupra dreptului la viață privată prevăzut la articolul 7 din Cartă.

35. În astfel de circumstanțe, nu este de neconceput nici faptul că colectarea, analiza și prelucrarea ulterioară a datelor biometrice (faciale) în cauză ar putea avea un efect asupra modului în care oamenii se simt liberi să acționeze, chiar dacă acțiunile respective s-ar încadra pe deplin în limitele unei societăți libere și deschise. Acestea ar putea avea implicații grave și asupra exercitării drepturilor lor fundamentale, de exemplu dreptul la libertatea de gândire, de conștiință și de religie, libertatea de exprimare, libertatea de întrunire pașnică și libertatea de asociere în temeiul articolelor 1, 10, 11 și 12 din Cartă. Această prelucrare implică și alte riscuri, de exemplu riscul de utilizare abuzivă a informațiilor cu caracter personal colectate de autoritățile relevante ca urmare a accesării și utilizării ilicite a datelor cu caracter personal, a încălcării securității etc. Riscurile depind adesea de prelucrare și de circumstanțele acesteia, cum ar fi riscul de accesare și utilizare ilicită de către funcționarii poliției sau de către alte părți neautorizate. Unele riscuri sunt însă pur și simplu inerente naturii unice a datelor biometrice. Spre deosebire de o adresă sau de un număr de telefon, este imposibil ca o persoană vizată să-și schimbe caracteristicile unice, cum ar fi fața sau irisul. În cazul accesului neautorizat sau al publicării accidentale a datelor biometrice, acest lucru ar duce la compromiterea datelor în utilizarea lor ca parole sau chei de criptare sau ar putea fi folosit pentru alte activități de supraveghere neautorizate în detrimentul persoanei vizate.

3.1.2 Atingerea adusă drepturilor prevăzute în Cartă

36. Prelucrarea datelor biometrice în toate situațiile constituie în sine o atingere gravă adusă drepturilor. Aceasta nu depinde de rezultat, de exemplu un rezultat pozitiv al punerii în corespondență. Prelucrarea constituie o interferență chiar și dacă modelul biometric este șters imediat după ce punerea în corespondență cu o bază de date a poliției nu a avut un rezultat pozitiv.

37. Interferența cu drepturile fundamentale ale persoanelor vizate poate proveni dintr-un act legislativ care fie urmărește, fie are ca efect restrângerea dreptului fundamental respectiv[11]. Aceasta poate

[11] CJUE, C-219/91 – Ter Voort, Rec., 1992, p. I-05485, punctul 36; CJUE, C-200/96 – Metronome, Rec., 1998, p. I-1953, punctul 28.

rezulta și dintr-un act al unei autorități publice cu același scop sau efect sau chiar al unei entități private abilitate prin lege să exercite competențe de autoritate publică și competențe publice.

38. O măsură legislativă care servește drept temei legal pentru prelucrarea datelor cu caracter personal aduce atingere în mod direct drepturilor garantate prin articolele 7 și 8 din Cartă[12].

39. Utilizarea datelor biometrice și a TRF în special afectează, în multe cazuri, și dreptul la demnitate umană, garantat prin articolul 1 din Cartă. Demnitatea umană impune ca persoanele să nu fie tratate ca simple obiecte. TRF calculează caracteristici existențiale și foarte personale, și anume trăsăturile faciale, într-o formă prelucrabilă automat, cu scopul de a o utiliza ca plăcuță de înmatriculare umană sau drept carte de identitate, transformând astfel fața într-un obiect.

40. O asemenea prelucrare poate să aducă atingere și altor drepturi fundamentale, cum ar fi drepturile prevăzute la articolele 10, 11 și 12 din Cartă, în măsura în care efectele disuasive fie sunt intenționate prin supravegherea video relevantă de către autoritățile de aplicare a legii, fie rezultă din aceasta.

41. În plus, riscurile potențiale generate de utilizarea tehnologiilor de recunoaștere facială de către autoritățile de aplicare a legii în ceea ce privește dreptul la un proces echitabil și prezumția de nevinovăție în temeiul articolelor 47 și 48 din Cartă ar trebui, de asemenea, luate în considerare cu atenție. Rezultatul aplicării TRF, de exemplu, o corespondență, poate nu numai să ducă la desfășurarea unor activități polițienești suplimentare în cazul persoanei în cauză, ci și să constituie o probă decisivă în cadrul procedurilor judiciare. Deficiențele TRF, cum ar fi posibila prejudecată, discriminare sau identificare greșită („rezultat fals pozitiv”), pot duce, așadar, la implicații grave și asupra procedurilor penale. În plus, în cadrul evaluării dovezilor, rezultatul aplicării TRF poate fi favorizat, chiar dacă există dovezi contradictorii („prejudecată legată de automatizare”).

3.1.3 Justificarea interferenței

42. În conformitate cu articolul 52 alineatul (1) din Cartă, orice restrângere a exercitării drepturilor și libertăților fundamentale trebuie să fie prevăzută de lege și să respecte substanța acestor drepturi și libertăți. Prin respectarea principiului proporționalității, pot fi impuse restrângeri numai dacă sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniunea Europeană sau necesității protejării drepturilor și libertăților celorlalți.

3.1.3.1 Prevăzut de lege

43. Articolul 52 alineatul (1) din Cartă stabilește cerința unui temei juridic specific. Acest temei juridic trebuie să fie formulat suficient de clar pentru a da cetățenilor indicii adecvate despre condițiile și circumstanțele în care autoritățile sunt împuternicite să recurgă la orice măsuri de colectare a datelor și de supraveghere secretă[13]. Acesta trebuie să indice cu claritate rezonabilă domeniul de aplicare și modalitatea de exercitare a puterii discreționare relevante conferite autorităților publice, astfel încât să asigure persoanelor nivelul minim de protecție la care au dreptul în temeiul statului de drept într-o societate democratică[14]. În plus, legalitatea necesită garanții adecvate pentru a asigura în special respectarea dreptului unei persoane prevăzut la articolul 8 din Cartă. Aceste principii se aplică și prelucrării datelor cu caracter personal în scopul evaluării, antrenării și dezvoltării ulterioare a sistemelor bazate pe TRF.

44. Având în vedere că datele biometrice, când sunt prelucrate în scopul identificării unice a unei persoane fizice, constituie categorii speciale de date enumerate la articolul 10 din LED, diferitele aplicații ale TRF

[12] CJUE, C-594/12, punctul 36; CJUE, C-291/12, punctul 23 și următoarele.
[13] CEDO, Shimovolos împotriva Rusiei, § 68; Vukota-Bojić împotriva Elveției.
[14] CEDO, Piechowicz împotriva Poloniei, § 212.

ar necesita, în majoritatea cazurilor, o lege specifică, care să descrie cu precizie aplicarea și condițiile de utilizare ale acesteia. Aceasta include în special tipurile de infracțiuni și, după caz, pragul adecvat de gravitate a acestor infracțiuni, pentru a exclude, printre altele, în mod eficace infracțiunile minore.[15]

3.1.3.2 Substanța dreptului fundamental la viață privată și a dreptului la protecția datelor cu caracter personal prevăzute la articolele 7 și 8 din Cartă

45. Restrângerile drepturilor fundamentale iminente pentru fiecare situație trebuie să asigure totuși respectarea substanței drepturilor în cauză. Substanța se referă la esența însăși a dreptului fundamental relevant[16]. Demnitatea umană trebuie, de asemenea, respectată, chiar și atunci când un drept este restrâns[17].

46. Indiciile unei posibile încălcări a nucleului inviolabil sunt următoarele:

- o dispoziție care impune restrângeri indiferent de comportamentul individual al unei persoane sau de circumstanțele excepționale[18];
- recurgerea la instanțe nu este posibilă sau este împiedicată[19];
- înainte de o restrângere drastică, circumstanțele persoanei în cauză nu sunt luate în considerare[20];
- în ceea ce privește drepturile prevăzute la articolele 7 și 8 din Cartă: pe lângă o colectare amplă de metadate referitoare la comunicații, cunoașterea conținutului comunicațiilor electronice ar putea încălca substanța acestor drepturi[21];
- în ceea ce privește drepturile prevăzute la articolele 7, 8 și 11 din Cartă: legislația care prevede ca furnizorii de acces la servicii de comunicații publice online și furnizorii de servicii de găzduire să păstreze, în mod general și nediferențiat, printre altele, date cu caracter personal referitoare la aceste servicii[22];
- în ceea ce privește drepturile prevăzute la articolul 8 din Cartă: lipsa principiilor de bază ale protecției și securității datelor ar putea să încalce și substanța dreptului[23].

3.1.3.3 Scopul legitim

47. După cum s-a explicat deja la punctul 3.1.3., restrângerile drepturilor fundamentale trebuie să răspundă efectiv obiectivelor de interes general recunoscute de Uniunea Europeană sau să răspundă necesității protejării drepturilor și libertăților celorlalți.

48. Recunoscute de Uniune sunt atât obiectivele menționate la articolul 3 din Tratatul privind Uniunea Europeană, cât și alte interese protejate prin dispoziții specifice ale tratatelor[24], și anume – printre altele – un spațiu de libertate, securitate și justiție, prevenirea și combaterea criminalității. În relațiile sale cu lumea întreagă, Uniunea ar trebui să contribuie la pace și securitate și la apărarea drepturilor omului.

---

[15] Vezi, de exemplu, hotărârile CJUE în cauzele C-817/19, Ligue des droits humains, punctul 151, și C-207/16, Ministerio Fiscal, punctul 56.
[16] CJUE, C-279/09, Rec., 2010, p. I-13849, punctul 60.
[17] Explicații cu privire la Carta drepturilor fundamentale, titlul I, Explicație cu privire la articolul 1, JO C 303, 14.12.2007, p. 17-35.
[18] CJUE, C-601/15, punctul 52.
[19] CJUE, C-400/10, Rec., 2010, p. I-08965, punctul 55.
[20] CJUE, C-408/03, Rec., 2006, p. I-02647, punctul 68.
[21] CJUE, C-203/15, Tele2 Sverige, punctul 101 cu trimitere la CJUE, C-293/12 și C-594/12, punctul 39.
[22] CJUE, C-512/18, La Quadrature du Net, punctul 209 și următoarele.
[23] CJUE, C-594/12, punctul 40.
[24] Explicații cu privire la Carta drepturilor fundamentale, titlul I, Explicație cu privire la articolul 52, JO C 303, 14.12.2007, p. 17-35.

49. Necesitatea de a proteja drepturile și libertățile celorlalți se referă la drepturile persoanelor protejate de legislația Uniunii Europene sau a statelor sale membre. Evaluarea trebuie efectuată cu scopul de a reconcilia cerințele de apărare a drepturilor respective și de a asigura un echilibru just între acestea[25].

3.1.3.4 Testul necesității și al proporționalității

50. În cazul în care sunt în discuție atingeri aduse drepturilor fundamentale, marja de apreciere a legiuitorului național și a legiuitorului Uniunii se poate dovedi limitată. Asta depinde de o serie de factori, inclusiv de domeniul vizat, de natura dreptului în cauză garantat de Cartă, de natura și gravitatea atingerii aduse, precum și de obiectivul urmărit prin interferență[26]. Măsurile legislative trebuie să fie adecvate pentru realizarea obiectivelor legitime urmărite de legislația în cauză. În plus, măsura nu trebuie să depășească limitele a ceea ce este adecvat și necesar pentru a realiza aceste obiective[27]. Un obiectiv de interes general – oricât de important ar fi – nu justifică, în sine, restrângerea unui drept fundamental[28].

51. Potrivit jurisprudenței constante a CJUE, derogările și restrângerile în ceea ce privește protecția datelor cu caracter personal trebuie să se aplice numai în măsura în care acest lucru este strict necesar[29]. Aceasta înseamnă și că nu sunt disponibile mijloace mai puțin intruzive pentru realizarea scopului. Trebuie identificate și evaluate cu atenție alternative posibile, de exemplu – în funcție de scopul dat – suplimentarea personalului, activități polițienești mai frecvente sau iluminat stradal suplimentar. Măsurile legislative trebuie să diferențieze și să țintească persoanele vizate de acestea, ținând seama de obiectivul urmărit, de exemplu, combaterea infracțiunilor grave. Dacă acoperă toate persoanele la modul general, fără o asemenea diferențiere, limitare sau excepție, acest lucru intensifică atingerea adusă drepturilor[30]. De asemenea, se aduce o atingere gravă drepturilor dacă prelucrarea datelor acoperă o parte semnificativă a populației[31].

52. Protecția datelor cu caracter personal care rezultă din obligația explicită prevăzută la articolul 8 alineatul (1) din cartă este deosebit de importantă pentru dreptul la respectarea vieții private consacrat la articolul 7 din Cartă[32]. Legislația trebuie să stabilească norme clare și precise care să reglementeze domeniul de aplicare și aplicarea măsurii în cauză și să impună garanții astfel încât persoanele ale căror date au fost prelucrate să aibă suficiente garanții care să permită protejarea eficientă a datelor cu caracter personal împotriva riscului de abuz și împotriva oricărei accesări sau utilizări ilicite a datelor respective[33]. Necesitatea unor astfel de garanții este cu atât mai mare în cazul în care datele cu caracter personal sunt supuse unei prelucrări automate și când există un risc

[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31-32.
[26] CJUE, C-594/12, punctul 47 cu următoarele surse: vezi, prin analogie, în ceea ce privește articolul 8 din CEDO, CEDO, S. și Marper împotriva Regatului Unit [GC], nr. 30562/04 și 30566/04, § 102, CEDO 2008-V.
[27] CJUE, C-594/12, punctul 46 cu următoarele surse: cauza C-343/09, Afton Chemical, EU:C:2010:419, punctul 45; Volker und Markus Schecke și Eifert, EU:C:2010:662, punctul 74; cauzele C-581/10 și C-629/10, Nelson și alții, EU:C:2012:657, punctul 71; cauza C-283/11, Sky Österreich, EU:C:2013:28, punctul 50; și cauza C-101/12, Schaible, EU:C:2013:661, punctul 29.
[28] CJUE, C-594/12, punctul 51.
[29] CJUE, C-594/12, punctul 52, cu următoarele surse: cauza C-473/12, IPI, EU:C:2013:715, punctul 39 și jurisprudența citată.
[30] CJUE, C-594/12, punctul 57.
[31] CJUE, C-594/12, punctul 56.
[32] CJUE, C-594/12, punctul 53.
[33] CJUE, C-594/12, punctul 54, cu următoarele surse: vezi, prin analogie, în ceea ce privește articolul 8 din CEDO, CEDO, Liberty și alții împotriva Regatului Unit, 1 iulie 2008, nr. 58243/00, § 62 și 63; Rotaru împotriva României, § 57-59, și S. și Marper împotriva Regatului Unit, § 99.

semnificativ de acces ilicit la date[34]. În plus, autorizarea internă sau externă, de exemplu judiciară, a implementării TRF poate contribui, de asemenea, ca garanție și se poate dovedi necesară în anumite cazuri de atingeri grave aduse drepturilor.[35]

53. Normele stabilite trebuie să fie adaptate situației specifice, de exemplu cantitatea de date prelucrate, natura datelor[36]și riscul de acces ilicit la date. În acest scop sunt necesare norme care să servească, în special, la reglementarea protecției și a securității datelor în cauză într-o manieră clară și strictă, pentru a asigura integritatea și confidențialitatea deplină a acestora[37].

54. În ceea ce privește relația dintre operator și persoana împuternicită de către operator, nu ar trebui să se permită ca persoanele împuternicite de operator să aibă în vedere numai considerente economice când stabilesc nivelul de securitate pe care îl aplică datelor cu caracter personal; acest lucru ar putea pune în pericol un nivel de protecție suficient de ridicat[38].

55. Un act legislativ trebuie să prevadă condiții materiale și procedurale, precum și criterii obiective, prin care să se stabilească limitele accesului autorităților competente la date și ale utilizării ulterioare a acestora. În scopul prevenirii, depistării sau urmăririi penale, infracțiunile în cauză ar trebui să fie considerate suficient de grave pentru a justifica amploarea și gravitatea acestor atingeri aduse drepturilor fundamentale consacrate, de exemplu, la articolele 7 și 8 din Cartă[39].

56. Datele trebuie să fie prelucrate într-un mod care să asigure aplicabilitatea și efectul normelor UE de protecție a datelor, în special a celor prevăzute la articolul 8 din Cartă, care prevede că respectarea cerințelor de protecție și securitate se supune controlului unei autorități independente. Locul geografic unde se realizează prelucrarea poate fi relevant într-o astfel de situație[40].

57. În ceea ce privește diferitele etape ale prelucrării datelor cu caracter personal, ar trebui făcută o distincție între categoriile de date pe baza utilității lor posibile în scopul realizării obiectivului urmărit sau în funcție de persoanele vizate[41]. Stabilirea condițiilor de prelucrare, de exemplu, stabilirea perioadei de păstrare, trebuie să se bazeze pe criterii obiective pentru a asigura că atingerea drepturilor este limitată la ceea ce este strict necesar[42].

58. În funcție de fiecare situație în parte, evaluarea necesității și a proporționalității trebuie să identifice și să ia în considerare toate implicațiile care intră în domeniul de aplicare al altor drepturi fundamentale, cum ar fi demnitatea umană în temeiul articolului 1 din Cartă, libertatea de gândire, de conștiință și de religie în temeiul articolului 10 din Cartă, libertatea de exprimare în temeiul articolului 11 din Cartă, precum și libertatea de întrunire și de asociere în temeiul articolului 12 din Cartă.

59. În plus, trebuie luat în considerare, ca o chestiune de gravitate, faptul că, dacă datele sunt prelucrate în mod sistematic fără ca persoanele vizate să aibă cunoștință de acest lucru, există probabilitatea să

[34] CJUE - C-594/12, punctul 55, cu următoarele surse: vezi, prin analogie, în ceea ce privește articolul 8 din CEDO, S. și Marper împotriva Regatului Unit, § 103, și M. K. împotriva Franței, 18 aprilie 2013, nr. 19522/09, § 35.
[35] CEDO, Szabó și Vissy împotriva Ungariei, § 73-77.
[36] Vezi și cerințele sporite privind măsurile tehnice și organizatorice în cazul prelucrării categoriilor speciale de date, articolul 29 alineatul (1) din LED.
[37] CJUE, C-594/12, punctul 66.
[38] CJUE, C-594/12, punctul 67.
[39] CJUE, C-594/12, punctele 60 și 61.
[40] CJUE, C-594/12, punctul 68.
[41] CJUE, C-594/12, punctul 63.
[42] CJUE, C-594/12, punctul 64.

se genereze o concepție generală de supraveghere constantă[43]. Acest lucru poate duce la efecte disuasive în ceea ce privește unele sau toate drepturile fundamentale în cauză.

60. Pentru a facilita și a operaționaliza evaluarea necesității și a proporționalității în cadrul măsurilor legislative legate de recunoașterea facială în domeniul aplicării legii, legiuitorii naționali și legiuitorul Uniunii ar putea profita de instrumentele practice disponibile, concepute în mod special pentru această sarcină. S-ar putea folosi, în special, setul de instrumente privind necesitatea și proporționalitatea[44] furnizat de Autoritatea Europeană pentru Protecția Datelor.

3.1.3.5 Articolul 52 alineatul (3), articolul 53 din Cartă (nivelul de protecție, de asemenea în raport cu cel al CEDO)

61. Potrivit articolului 52 alineatul (3) și articolului 53 din Cartă, înțelesul și întinderea drepturilor prevăzute în Cartă care corespund drepturilor garantate prin CEDO trebuie să fie aceleași cu cele prevăzute de CEDO. Deși în special pentru articolul 7 din Cartă se poate găsi un echivalent în CEDO, acest lucru nu este valabil pentru articolul 8 din Cartă[45]. Articolul 52 alineatul (3) din Cartă nu împiedică dreptul Uniunii să confere o protecție mai largă. Întrucât CEDO nu constituie un instrument juridic care a fost încorporat în mod formal în dreptul Uniunii, legislația Uniunii trebuie să se realizeze din perspectiva drepturilor fundamentale prevăzute în Cartă[46].

62. Conform articolului 8 din CEDO, nu este admis amestecul unei autorități publice în exercitarea acestui drept la respectarea vieții private și de familie, decât atunci când 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.

63. CEDO stabilește și standarde în ceea ce privește modul în care pot fi aplicate restrângerile. O cerință de bază, pe lângă statul de drept, este previzibilitatea. Pentru a îndeplini această cerință a previzibilității, legislația trebuie să aibă prevederi suficient de clare pentru a da oamenilor indicii adecvate în ceea ce privește circumstanțele și condițiile în care autoritățile sunt împuternicite să recurgă la asemenea măsuri[47]. Această cerință este recunoscută de CJUE și de dreptul UE în domeniul protecției datelor (vezi secțiunea 3.2.1.1).

64. Specificând mai detaliat drepturile prevăzute la articolul 8 din CEDO, dispozițiile Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal[48] trebuie, de asemenea, respectate pe deplin. Trebuie considerat totuși că aceste dispoziții reprezintă doar un standard minim, având în vedere prevalența dreptului Uniunii.

3.2 Cadrul juridic specific – Directiva privind protecția datelor în materie de aplicare a legii

[43] CJUE, C-594/12, punctul 37.
[44] Autoritatea Europeană pentru Protecția Datelor: Ghid de evaluare a necesității unor măsuri care limitează dreptul fundamental la protecția datelor cu caracter personal (11.4.2017); Autoritatea Europeană pentru Protecția Datelor: „Orientările AEPD privind evaluarea proporționalității măsurilor care limitează drepturile fundamentale la viața privată și la protecția datelor cu caracter personal (19.12.2019).
[45] CJUE, C-203/15, Tele2 Sverige, punctul 129.
[46] CJUE, C-311/18, punctul 99.
[47] Curtea Europeană a Drepturilor Omului, Hotărârea din 3.4.2007, Copland împotriva Regatului Unit, cererea nr. 62617/00, § 46.
[48] Seria de tratate ale Consiliului Europei nr. 108.

65. Un anumit cadru privind utilizarea tehnologiei de recunoaștere facială este prevăzut în LED. În primul rând, articolul 3 punctul 13 din LED definește termenul „date biometrice”[49]. Pentru detalii, vezi secțiunea 2.1 de mai sus. În al doilea rând, articolul 8 alineatul (2) clarifică faptul că, pentru ca orice prelucrare să fie legală, aceasta trebuie – pe lângă faptul că este necesară în scopurile menționate la articolul 1 alineatul (1) din LED – să fie reglementată în dreptul intern care precizează cel puțin obiectivele prelucrării, datele cu caracter personal care urmează să fie prelucrate și scopul prelucrării. Alte dispoziții cu relevanță specială în ceea ce privește datele biometrice sunt articolele 10 și 11 din LED. Articolul 10 trebuie citit în coroborare cu articolul 8 din LED[50]. Principiile pentru prelucrarea datelor cu caracter personal prevăzute la articolul 4 din LED ar trebui respectate întotdeauna, iar orice evaluare a unei eventuale prelucrări biometrice prin tehnologie de recunoaștere facială ar trebui să aibă la bază aceste principii.

3.2.1 Prelucrarea categoriilor speciale de date în scopul aplicării legii

66. Conform articolului 10 din LED, prelucrarea categoriilor speciale de date, cum ar fi datele biometrice, este autorizată numai când este strict necesară și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei vizate. În plus, este permisă numai când este autorizată de dreptul Uniunii sau de dreptul intern, când este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice sau când prelucrarea respectivă se referă la date care sunt făcute publice în mod manifest de persoana vizată. Această clauză generală evidențiază sensibilitatea prelucrării categoriilor speciale de date.

3.2.1.1 Autorizată de dreptul Uniunii sau de dreptul intern

67. În ceea ce privește tipul necesar de măsură legislativă, considerentul 33 din LED prevede că „[a]tunci când prezenta directivă face trimitere la dreptul intern, la un temei juridic sau la o măsură legislativă, aceasta nu necesită neapărat un act legislativ adoptat de către un parlament, fără a aduce atingere cerințelor care decurg din ordinea constituțională a statului membru în cauză”.[51]

68. Potrivit articolului 52 alineatul (1) din Cartă, orice restrângere a exercitării drepturilor și libertăților recunoscute prin Cartă trebuie să fie „prevăzută de lege”. Această mențiune este conformă cu expresia „prevăzut de lege” de la articolul 8 alineatul (2) din CEDO, care înseamnă nu numai respectarea legislației aplicabile, ci se referă și la calitatea legislației respective, fără a aduce atingere naturii actului, impunând ca acesta să fie compatibil cu statul de drept.

69. Considerentul 33 din LED prevede, de asemenea, că „[c]u toate acestea, dreptul intern, temeiul juridic sau măsura legislativă în cauză ar trebui să fie clare și precise, iar aplicarea să fie previzibilă destinatarilor, în conformitate cu jurisprudența Curții de Justiție și a Curții Europene a Drepturilor Omului. Dreptul intern care reglementează prelucrarea datelor cu caracter personal din domeniul de aplicare al prezentei directive ar trebui să precizeze cel puțin obiectivele, datele cu caracter personal care urmează a fi prelucrate, scopurile prelucrării și procedurile de păstrare a integrității și a confidențialității datelor cu caracter personal și procedurile de distrugere a acestora”.

[49] Articolul 3 punctul 13 din LED: „«date biometrice» înseamnă date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a respectivei persoane fizice, cum ar fi imaginile faciale sau datele dactiloscopice”.

[50] WP258, Aviz cu privire la unele aspecte esențiale ale Directivei privind aplicarea legii (UE 2016/680), p. 7.

[51] Tipul de măsuri legislative luate în considerare trebuie să fie conforme cu dreptul Uniunii sau cu dreptul intern. În funcție de gradul de atingere adusă drepturilor prin restricționare, ar putea fi necesară o anumită măsură legislativă la nivel național, ținând seama de nivelul normei.

70. Dreptul intern trebuie să aibă prevederi suficient de clare pentru a oferi persoanelor vizate indicii adecvate în ceea ce privește circumstanțele și condițiile în care operatorii sunt împuterniciți să recurgă la orice astfel de măsuri. Printre acestea se numără condiții prealabile posibile pentru prelucrare, cum ar fi tipuri specifice de dovezi, precum și necesitatea unei autorizări judiciare sau interne. Legislația respectivă poate fi neutră din punct de vedere tehnologic, în măsura în care riscurile și caracteristicile specifice ale prelucrării datelor cu caracter personal de către sistemele bazate pe TRF sunt abordate în mod suficient. În conformitate cu LED și cu jurisprudența Curții de Justiție a Uniunii Europene (CJUE) și a Curții Europene a Drepturilor Omului (CEDO), este într-adevăr esențial ca măsurile legislative, care urmăresc să ofere un temei juridic pentru o măsură de recunoaștere facială, să fie previzibile pentru persoanele vizate.

71. O măsură legislativă nu poate fi invocată ca lege care autorizează prelucrarea datelor biometrice prin intermediul tehnologiei de recunoaștere facială în scopul aplicării legii, dacă este o simplă transpunere a clauzei generale prevăzute la articolul 10 din LED.

72. Pe lângă datele biometrice, articolul 10 din LED reglementează prelucrarea altor categorii speciale de date, cum ar fi orientarea sexuală, opiniile politice și confesiunea religioasă, acoperind astfel o gamă largă de prelucrări. În plus, o astfel de dispoziție nu ar conține cerințe specifice care să indice circumstanțele și condițiile în care autoritățile de aplicare a legii ar fi împuternicite să recurgă la utilizarea tehnologiei de recunoaștere facială. Din cauza trimiterii la alte tipuri de date și a necesității explicite a unor garanții speciale fără specificații suplimentare, dispoziția națională de transpunere a articolului 10 din LED în dreptul intern – cu o formulare la fel de generală și abstractă – nu poate fi invocată ca temei legal pentru prelucrarea datelor biometrice care implică recunoașterea facială, deoarece ar fi lipsită de precizie și de previzibilitate. În conformitate cu articolul 28 alineatul (2) sau cu articolul 46 alineatul (1) litera (c) din LED, înainte ca legiuitorul să creeze un nou temei juridic pentru orice formă de prelucrare a datelor biometrice care utilizează recunoașterea facială, ar trebui consultată autoritatea națională de supraveghere a protecției datelor.

3.2.1.2 Strict necesară

73. Prelucrarea poate fi considerată „strict necesară” numai dacă atingerea adusă protecției datelor cu caracter personal și restrângerile acesteia sunt limitate la ceea ce este absolut necesar[52]. Adăugarea termenului „strict” înseamnă că legiuitorul a intenționat ca prelucrarea categoriilor speciale de date să aibă loc numai în condiții chiar mai stricte decât condițiile de necesitate (vezi mai sus, punctul 3.1.3.4). Această cerință trebuie interpretată ca fiind indispensabilă. Aceasta limitează marja de apreciere permisă autorității de aplicare a legii în cadrul testului necesității la un minimum absolut. În conformitate cu jurisprudența constantă a CJUE, condiția de „strictă necesitate” este strâns legată și de cerința unor criterii obiective pentru a defini circumstanțele și condițiile în care poate fi efectuată prelucrarea, excluzând astfel orice prelucrare cu caracter general sau sistematic[53].

3.2.1.3 Făcute publice în mod manifest

74. Atunci când se evaluează dacă prelucrarea se referă la date care sunt făcute publice în mod manifest de către o persoană vizată, ar trebui reamintit că o fotografie ca atare nu se consideră în mod sistematic că ar constitui date biometrice[54]. Prin urmare, faptul că o fotografie a fost făcută publică în

[52] Jurisprudența constantă privind dreptul fundamental la respectarea vieții private, vezi CJUE, cauza C-73/07, punctul 56 (Satakunnan Markkinapörssi și Satamedia); CJUE, cauzele C-92/09 și C-93/09, punctul 77 (Schecke și Eifert); CJUE, C-594/12, punctul 52 (drepturi digitale); CJUE, cauza C-362/14, punctul 92 (Schrems).
[53] CJUE, cauza C-623/17, punctul 78.
[54] Vezi considerentul 51 din RGPD: „[p]relucrarea fotografiilor nu ar trebui să fie considerată în mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, întrucât fotografiile intră sub incidența

mod manifest de către persoana vizată nu implică faptul că datele biometrice conexe, care pot fi extrase din fotografie prin mijloace tehnice specifice, se consideră că au fost făcute publice în mod manifest.

75. În ceea ce privește datele cu caracter personal în general, pentru ca datele biometrice să fie considerate ca fiind făcute publice în mod manifest de către persoana vizată, aceasta trebuie să fi făcut în mod deliberat modelul biometric (și nu doar o imagine facială) liber accesibil și public printr-o sursă deschisă. Dacă un terț divulgă datele biometrice, nu se poate considera că datele au fost făcute publice în mod manifest de către persoana vizată.

76. În plus, nu este suficientă interpretarea comportamentului unei persoane vizate pentru a considera că datele biometrice au fost făcute publice în mod manifest. De exemplu, în cazul rețelelor sociale sau al platformelor online, CEPD consideră că faptul că persoana vizată nu a declanșat sau nu a setat caracteristici de confidențialitate specifice nu este suficient pentru a considera că persoana vizată a făcut publice în mod manifest datele sale cu caracter personal și că aceste date (de exemplu, fotografii) pot fi prelucrate în modele biometrice și utilizate în scopuri de identificare fără consimțământul persoanei vizate. La un nivel mai general, setările implicite ale unui serviciu, de exemplu, punerea la dispoziția publicului a unor modele sau absența posibilității de alegere, de exemplu atunci când modelele sunt făcute publice fără ca utilizatorul să poată modifica această setare, nu ar trebui în niciun caz interpretate ca date făcute publice în mod manifest.

3.2.2 Procesul decizional individual automatizat, inclusiv crearea de profiluri

77. Articolul 11 alineatul (1) din LED prevede obligația statelor membre de a interzice, în general, deciziile întemeiate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produc un efect juridic negativ pentru persoana vizată sau care o afectează în mod semnificativ. Ca derogare de la această interdicție generală, o astfel de prelucrare poate fi posibilă numai dacă 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. Aceasta poate fi utilizată numai în mod restrictiv. Acest prag se aplică pentru categoriile obișnuite (adică nu speciale) de date cu caracter personal. Se aplică un prag și mai mare și o utilizare mai restrictivă pentru derogarea prevăzută la articolul 11 alineatul (2) din LED. Acesta subliniază din nou că deciziile menționate la alineatul (1) nu se întemeiază pe categoriile speciale de date, adică, în special, pe date biometrice în scopul identificării unice a unei persoane fizice. Poate fi prevăzută o derogare numai dacă au fost instituite măsuri corespunzătoare pentru protejarea drepturilor și a libertăților persoanei vizate, precum și a intereselor legitime ale persoanei fizice în cauză. Această derogare trebuie interpretată în plus față de dispozițiile articolului 10 din LED și ținând seama de acestea.

78. În funcție de sistemul bazat pe TRF, chiar și intervenția umană care evaluează rezultatele TRF poate să nu ofere neapărat o garanție suficientă în sine pentru respectarea drepturilor persoanelor și, în special, a dreptului la protecția datelor cu caracter personal, având în vedere posibilele prejudecăți și erori care pot rezulta din prelucrarea în sine. În plus, intervenția umană poate fi considerată o garanție doar dacă persoana care intervine poate contesta în mod critic rezultatele TRF în timpul intervenției umane. Este esențial să se permită persoanei respective să înțeleagă sistemul bazat pe TRF și limitele acestuia, precum și să interpreteze în mod corespunzător rezultatele acestuia. De asemenea, este necesar să se stabilească un loc de muncă și o organizație care să contracareze efectele prejudecății legate de

definiției datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice ”.

automatizare și care să evite încurajarea acceptării necritice a rezultatelor, de exemplu prin presiunea timpului, proceduri greoaie, efecte negative potențiale asupra carierei etc.

79. Potrivit articolului 11 alineatul (3) din LED, 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, cum ar fi datele biometrice. Conform articolului 3 punctul 4 din LED, „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 a preconiza aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, localizarea sau deplasările respectivei persoane fizice. Atunci când se analizează dacă sunt prevăzute măsuri corespunzătoare pentru protejarea drepturilor și a libertăților persoanei vizate, precum și a intereselor legitime ale persoanei fizice în cauză, trebuie să se țină seama de faptul că utilizarea TRF poate duce la crearea de profiluri, în funcție de modul și scopul pentru care se aplică TRF. În orice caz, în conformitate cu dreptul Uniunii și cu articolul 11 alineatul (3) din LED, este interzisă crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza categoriilor speciale de date cu caracter personal.

3.2.3 Categorii de persoane vizate

80. Articolul 6 din LED se referă la necesitatea de a face distincție între diferitele categorii de persoane vizate. Această distincție trebuie făcută după caz și în măsura posibilului. Aceasta trebuie să se manifeste în modul în care sunt prelucrate datele. Din exemplele prezentate la articolul 6 din LED se poate deduce că, de regulă, prelucrarea datelor cu caracter personal trebuie să îndeplinească criteriile de necesitate și proporționalitate și în ceea ce privește categoria de persoane vizate[55]. În plus, se poate deduce că, în ceea ce privește persoanele vizate pentru care nu există nicio dovadă de natură să sugereze că comportamentul lor ar putea avea o legătură, chiar indirectă sau îndepărtată, cu scopul legitim în conformitate cu LED, cel mai probabil nu există nicio justificare pentru a aduce atingere drepturilor[56]. Dacă nu se aplică sau nu este posibilă nicio distincție în conformitate cu articolul 6 din LED, derogarea de la regula prevăzută la articolul 6 din LED trebuie luată în considerare în mod riguros în evaluarea necesității și proporționalității atingerii aduse drepturilor. Distincția între diferitele categorii de persoane vizate apare ca o cerință esențială atunci când este vorba de prelucrarea datelor cu caracter personal care implică recunoașterea facială, având în vedere și posibilele rezultate fals pozitive sau fals negative, care pot avea un impact semnificativ pentru persoanele vizate, precum și în cursul unei investigații.

81. După cum s-a spus, la punerea în aplicare a dreptului Uniunii, trebuie respectate dispozițiile Cartei drepturilor fundamentale a Uniunii Europene, vezi articolul 52 din Cartă. Cadrul și criteriile pe care le oferă LED trebuie deci interpretate ținând seama de Cartă. Actele legislative ale UE și ale statelor sale membre nu trebuie să se situeze sub această măsură și trebuie să asigure efectul deplin al Cartei.

3.2.4 Drepturile persoanei vizate

82. CEPD a oferit deja îndrumări privind drepturile persoanelor vizate în temeiul RGPD în diferite aspecte[57]. LED prevede drepturi similare ale persoanelor vizate, iar îndrumări generale în acest sens au fost furnizate într-un aviz al Grupului de lucru instituit prin articolul 29, care a fost aprobat de CEPD[58]. În

[55] Vezi și CJUE, C-594/12, punctele 56 - 59.
[56] Vezi și CJUE, C-594/12, punctul 58.
[57] Vezi de exemplu, Ghidul CEPD 1/2022 privind drepturile persoanei vizate – dreptul de acces și Ghidul CEPD 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video.
[58] WP258, Aviz cu privire la unele aspecte esențiale ale Directivei privind aplicarea legii (UE 2016/680).

anumite situații, LED permite anumite restrângeri ale acestor drepturi. Parametrii pentru aceste restrângeri vor fi detaliați în secțiunea 3.2.4.6. „Restrângeri legitime ale drepturilor persoanei vizate”.

83. Deși toate drepturile persoanei vizate, enumerate în capitolul III din LED, se aplică, în mod firesc, și prelucrării datelor cu caracter personal prin intermediul tehnologiei de recunoaștere facială (TRF), următorul capitol se va concentra asupra unora dintre drepturile și aspectele care ar putea prezenta un interes deosebit în ceea ce privește primirea de îndrumări. În plus, în acest capitol și în analiza pe care o cuprinde se menționează că prelucrarea prin TRF în cauză trebuie să respecte cerințele legale descrise în capitolul anterior.

84. Având în vedere natura prelucrării datelor cu caracter personal prin intermediul TRF (prelucrarea categoriilor speciale de date cu caracter personal, adesea fără nicio interacțiune aparentă cu persoana vizată), operatorul trebuie să analizeze cu atenție modul în care îndeplinește (sau dacă poate să îndeplinească) cerințele prevăzute în LED înainte de a lansa orice prelucrare prin TRF. În special, analizând cu atenție:

- cine sunt persoanele vizate [adesea mai multe decât cea (cele) care reprezintă ținta principală în scopul prelucrării],
- modul în care persoanele vizate sunt informate cu privire la prelucrarea prin TRF (vezi secțiunea 3.2.4.1),
- modul în care persoanele vizate își pot exercita drepturile (în acest caz, atât drepturile de informare și de acces, cât și drepturile de rectificare sau de restricționare pot fi deosebit de greu de respectat în cazul în care TRF se folosește la toate verificările, cu excepția verificării unu la unu în contact direct cu persoana vizată).

3.2.4.1 Aducerea la cunoștința persoanelor vizate a drepturilor și a informațiilor într-o formă concisă, inteligibilă și ușor accesibilă

85. Tehnologia de recunoaștere facială creează provocări în ceea ce privește asigurarea faptului că persoanele vizate sunt informate cu privire la prelucrarea datelor lor biometrice. În cazul în care o autoritate de aplicare a legii analizează prin TRF materiale video care provin de la un terț sau sunt furnizate de un terț, este deosebit de dificil ca autoritatea de aplicare a legii respectivă să notifice persoana vizată în momentul colectării (de exemplu, printr-o indicație la fața locului) deoarece există puține posibilități pentru a face acest lucru și, de cele mai multe ori, niciuna. Orice material video care nu este relevant pentru investigație (sau în scopul prelucrării) ar trebui întotdeauna eliminat sau anonimizat (de exemplu, prin estomparea fără capacitatea retroactivă de recuperare a datelor (blurarea)) înainte de efectuarea oricărei prelucrări a datelor biometrice, pentru a se evita riscul de a nu fi respectat principiul reducerii la minimum prevăzut la articolul 4 alineatul (1) litera (e) din LED și de a nu fi îndeplinite obligațiile de informare prevăzute la articolul 13 alineatul (2) din LED. Este responsabilitatea operatorului să evalueze ce informații ar fi importante pentru persoana vizată în exercitarea drepturilor sale și să se asigure că sunt furnizate informațiile necesare. Exercitarea efectivă a drepturilor persoanei vizate depinde de îndeplinirea de către operator a obligațiilor sale de informare.

86. Articolul 13 alineatul (1) din LED stipulează informațiile minime care trebuie furnizate persoanei vizate în general. Aceste informații pot fi furnizate prin intermediul site-ului operatorului, în format tipărit (de exemplu, o broșură disponibilă la cerere) sau prin alte surse ușor de accesat pentru persoana vizată. Operatorul de date trebuie, în orice caz, să se asigure că informațiile sunt furnizate în mod eficient în legătură cu cel puțin următoarele elemente:

- identitatea și datele de contact ale operatorului, inclusiv ale responsabilului cu protecția datelor;
- scopul prelucrării și faptul că este vorba de o prelucrare prin TRF;
- dreptul de a depune o plângere în fața unei autorități de supraveghere și datele de contact ale acesteia;
- dreptul de a solicita acces la datele cu caracter personal și rectificarea sau ștergerea lor, precum și restricționarea prelucrării datelor cu caracter personal.

87. În plus, în anumite cazuri, astfel cum sunt definite în dreptul intern care ar trebui să fie în conformitate cu articolul 13 alineatul (2) din LED[59], ca de exemplu prelucrarea prin TRF, următoarele informații trebuie furnizate direct persoanei vizate:

- temeiul legal al prelucrării;
- informații despre locul în care datele cu caracter personal au fost colectate fără știrea persoanei vizate;
- perioada pentru care vor fi stocate datele cu caracter personal sau, dacă nu este posibil, criteriile utilizate pentru a stabili respectiva perioadă;
- dacă este cazul, categoriile de destinatari ai datelor cu caracter personal (inclusiv țări terțe sau organizații internaționale).

88. Deși articolul 13 alineatul (1) din LED face referire la informații generale puse la dispoziția publicului, articolul 13 alineatul (2) din LED se referă la informațiile suplimentare care trebuie furnizate unei anumite persoane vizate în anumite cazuri, de exemplu în situația în care datele sunt colectate direct de la persoana vizată sau indirect, fără știrea persoanei vizate[60]. Nu există o definiție clară a ceea ce se înțelege prin formularea „în anumite cazuri" de la articolul 13 alineatul (2) din LED. Cu toate acestea, se referă la situațiile în care persoanele vizate trebuie informate cu privire la prelucrarea care le vizează în mod specific și să primească informații adecvate pentru a-și exercita efectiv drepturile. CEPD consideră că, atunci când se evaluează dacă există un „anumit caz", trebuie luați în considerare mai mulți factori, inclusiv dacă datele cu caracter personal sunt colectate fără știrea persoanei vizate, deoarece aceasta ar fi singura modalitate de a permite persoanelor vizate să-și exercite în mod efectiv drepturile. Alte exemple de „anumite cazuri" ar putea fi cele în care datele cu caracter personal sunt prelucrate ulterior în cadrul unei proceduri internaționale de cooperare în materie penală sau în situația în care datele cu caracter personal sunt prelucrate în cadrul unor operațiuni sub acoperire, astfel cum se specifică în dreptul intern. În plus, din considerentul 38 din LED rezultă că, în cazul în care procesul decizional se bazează exclusiv pe TRF, atunci persoanele vizate trebuie să fie informate cu privire la caracteristicile procesului decizional automatizat. Acest lucru ar indica și că acesta este un anumit caz în care persoanei vizate ar trebui să i se furnizeze informații suplimentare conform articolului 13 alineatul (2) din LED[61].

[59] De exemplu, articolul 56 alineatul (1) din Legea federală privind protecția datelor din Germania, care, printre altele, precizează ce informații trebuie furnizate persoanelor vizate în cadrul operațiunilor sub acoperire.
[60] WP258, Aviz cu privire la unele aspecte esențiale ale Directivei privind aplicarea legii (UE 2016/680), p. 17-18.
[61] Observați cu atenție diferența dintre formularea „pune la dispoziția persoanelor vizate" de la articolul 13 alineatul (1) din LED și formularea „comunică persoanei vizate" de la articolul 13 alineatul (2) din LED. La articolul 13 alineatul (2) din LED, operatorul trebuie să se asigure că informațiile ajung la persoana vizată, în cazul în care informațiile publicate pe un site nu vor fi suficiente.

89. În cele din urmă, ar trebui remarcat faptul că, în conformitate cu articolul 13 alineatul (3) din LED, statele membre pot adopta măsuri legislative care restricționează obligația de a furniza informații în anumite cazuri și pentru anumite obiective. Acest lucru se aplică în măsura în care și atâta timp cât o astfel de măsură constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei vizate.

3.2.4.2 Dreptul de acces

90. În general, persoana vizată are dreptul de a primi o confirmare pozitivă sau negativă a oricărei prelucrări a datelor sale cu caracter personal și, în cazul în care răspunsul este pozitiv, accesul la datele cu caracter personal ca atare, plus informații suplimentare, astfel cum sunt enumerate la articolul 14 din LED. În cazul TRF, atunci când datele biometrice sunt stocate și legate de o identitate și prin date alfanumerice, acest lucru ar trebui să permită autorității competente să confirme o cerere de acces pe baza unei căutări după aceste date alfanumerice și fără a lansa nicio prelucrare suplimentară a datelor biometrice ale altor persoane (de exemplu, prin căutarea cu TRF într-o bază de date). Trebuie respectat principiul reducerii la minimum a datelor și nu ar trebui stocate mai multe date decât cele necesare în ceea ce privește scopul prelucrării.

3.2.4.3 Dreptul la rectificarea datelor cu caracter personal

91. Deoarece TRF nu asigură exactitatea absolută, este deosebit de important ca operatorii să fie vigilenți în ceea ce privește cererile de rectificare a datelor cu caracter personal. Acest lucru poate fi valabil și atunci când o persoană vizată, pe baza TRF, a fost încadrată într-o categorie inexactă, de exemplu, a fost clasificată în mod eronat în categoria suspecților pe baza unei presupuneri inițiale privind modul de acțiune dintr-o înregistrare video. Riscurile pentru persoanele vizate sunt deosebit de grave dacă astfel de date inexacte sunt stocate într-o bază de date a poliției și/sau sunt partajate cu alte entități. Operatorul trebuie să corecteze datele stocate și sistemele bazate pe tehnologia de recunoaștere facială în consecință, vezi considerentul 47 din LED.

3.2.4.4 Dreptul la ștergerea datelor

92. În majoritatea circumstanțelor – în cazul în care nu este utilizată pentru verificarea unu la unu/autentificare – tehnologia de recunoaștere facială va echivala cu prelucrarea unui număr mare de date biometrice ale persoanelor vizate. Prin urmare, este important ca operatorul să analizeze în prealabil unde se situează limitele scopului și necesității sale, pentru ca o cerere de ștergere a datelor în conformitate cu articolul 16 din LED să poată fi tratată fără întârzieri nejustificate (deoarece operatorul trebuie, printre altele, să șteargă datele cu caracter personal care sunt prelucrate dincolo de ceea ce permite legislația aplicabilă în conformitate cu articolele 4, 8 și 10 din LED).

3.2.4.5 Dreptul la restricționare

93. În cazul în care exactitatea datelor este contestată de persoana vizată, iar exactitatea datelor nu poate fi stabilită (sau când datele cu caracter personal trebuie păstrate în scopul unor dovezi viitoare), operatorul are o obligație de a restricționa datele cu caracter personal ale persoanei vizate respective, în conformitate cu articolul 16 din LED. Acest aspect devine deosebit de important când este vorba despre tehnologia de recunoaștere facială [bazată pe algoritm(i) și care, prin urmare, nu prezintă niciodată un rezultat definitiv] în situațiile în care sunt colectate cantități mari de date, iar exactitatea și calitatea identificării pot varia. În cazul materialelor video de slabă calitate (de exemplu, de la locul săvârșirii unei infracțiuni), riscul de rezultate fals pozitive crește. În plus, dacă imaginile faciale dintr-o listă de supraveghere nu sunt actualizate regulat, și acest lucru va mări riscul de rezultate fals pozitive sau fals negative. În anumite cazuri, în care datele nu pot fi șterse deoarece există motive întemeiate să se considere că ștergerea datelor ar putea afecta interesele legitime ale persoanei vizate, datele ar trebui, în schimb, să fie restricționate și prelucrate doar în scopul care a împiedicat ștergerea lor (vezi considerentul 47 din LED).

3.2.4.6 Restrângeri legitime ale drepturilor persoanei vizate

94. În ceea ce privește obligațiile de informare ale operatorului și dreptul de acces al persoanelor vizate, restrângerile sunt permise numai în măsura în care sunt prevăzute de lege care, la rândul său, trebuie să constituie o măsură necesară și proporțională într-o societate democratică, ținându-se seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice în cauză [vezi articolul 13 alineatele (3) și (4), articolul 15 și articolul 16 alineatul (4) din LED]. Atunci când se utilizează TRF în scopul aplicării legii, se poate preconiza că aceasta va fi utilizată în circumstanțe în care ar fi dăunător pentru scopul urmărit să fie informată persoana vizată sau să se permită accesul la date. Acest lucru ar fi valabil, de exemplu, pentru investigarea unei infracțiuni de către o autoritate polițienească sau pentru a proteja securitatea națională sau siguranța publică.

95. Dreptul de acces nu înseamnă în mod automat acces la toate informațiile, de exemplu, într-o cauză penală în care apar date cu caracter personal ale unei persoane. Un exemplu viabil de situație în care pot fi permise restrângeri ale dreptului ar putea fi în timpul unei anchete penale.

3.2.4.7 Exercitarea drepturilor prin intermediul autorității de supraveghere

96. În cazurile în care există restrângeri legitime ale exercitării drepturilor în conformitate cu capitolul III din LED, persoana vizată poate solicita autorității pentru protecția datelor să exercite drepturile în numele său, verificând legalitatea prelucrării efectuate de operator. Operatorului îi revine sarcina de a informa persoana vizată cu privire la posibilitatea de a-și exercita drepturile în acest mod [vezi articolul 17 din LED și articolul 46 alineatul (1) litera (g) din LED]. În ceea ce privește tehnologia de recunoaștere facială, acest lucru înseamnă că operatorul trebuie să se asigure că sunt instituite măsuri adecvate pentru ca o astfel de cerere să poată fi tratată, de exemplu, permițând căutarea materialelor înregistrate, cu condiția ca persoana vizată să furnizeze informații suficiente pentru a localiza datele cu caracter personal ale acesteia.

3.2.5 Alte cerințe legale și garanții

3.2.5.1 Articolul 27 – Evaluarea impactului asupra protecției datelor

97. Efectuarea unei evaluări a impactului asupra protecției datelor (EIPD) înainte de utilizarea TRF este o cerință obligatorie, deoarece tipul de prelucrare, în special care implică utilizarea de noi tehnologii, și ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, este susceptibil să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice. Având în vedere că utilizarea tehnologiei de recunoaștere facială implică prelucrarea automată sistematică a categoriilor speciale de date, se poate presupune că, în astfel de cazuri, operatorul ar avea, de regulă, obligația de a efectua o EIPD. Evaluarea în cauză ar trebui să conțină cel puțin o descriere generală a operațiunilor de prelucrare preconizate, o evaluare a necesității și a proporționalității operațiunilor de prelucrare în raport cu scopurile, o evaluare a riscurilor la adresa drepturilor și libertăților persoanelor vizate, măsurile preconizate în vederea abordării riscurilor, garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea. CEPD recomandă publicarea rezultatelor acestor evaluări sau cel puțin a principalelor lor constatări și concluzii, ca măsură de consolidare a încrederii și a transparenței[62].

3.2.5.2 Articolul 28 – Consultarea prealabilă a autorității de supraveghere

98. În conformitate cu articolul 28 din LED, operatorul sau persoana împuternicită de operator trebuie să consulte autoritatea de supraveghere înainte de prelucrare, în cazul în care: (a) o evaluare a impactului asupra protecției datelor indică faptul că prelucrarea ar genera un risc ridicat în absența măsurilor

[62] Pentru mai multe informații, vezi WP 248 rev. 01 Orientări privind evaluarea impactului asupra protecției datelor (DPIA) și modul în care se determină dacă prelucrarea este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679.

luate de operator pentru atenuarea riscului sau (b) tipul de prelucrare, în special în cazul în care se utilizează noi tehnologii, mecanisme sau proceduri, implică un risc ridicat la adresa drepturilor și libertăților persoanelor vizate. După cum s-a explicat deja în secțiunea 2.3. din ghid, CEPD consideră că cele mai multe cazuri de implementare și utilizare a tehnologiei de recunoaștere facială prezintă un risc ridicat intrinsec pentru drepturile și libertățile persoanelor vizate. Prin urmare, pe lângă evaluarea impactului asupra protecției datelor, autoritatea care implementează TRF ar trebui să consulte autoritatea de supraveghere competentă, înainte de implementarea sistemului.

3.2.5.3 Articolul 29 – Securitatea prelucrării

99. Natura unică a datelor biometrice face imposibilă modificarea lor de către persoana vizată, în cazul în care acestea sunt compromise, de exemplu, ca urmare a unei încălcări a securității datelor. Prin urmare, autoritatea competentă, care implementează și/sau utilizează TRF, ar trebui să acorde o atenție deosebită securității prelucrării, în conformitate cu articolul 29 din LED. În special, autoritatea de aplicare a legii ar trebui să se asigure că sistemul respectă standardele relevante și să pună în aplicare măsuri de protecție a modelelor biometrice[63]. Această obligație este și mai relevantă dacă autoritatea de aplicare a legii utilizează un furnizor de servicii terț (persoană împuternicită de operator).

3.2.5.4 Articolul 20 – Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

100. Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, în conformitate cu articolul 20 din LED, urmărește să asigure că principiile și garanțiile privind protecția datelor, cum ar fi reducerea la minimum a datelor și limitarea stocării, sunt integrate în tehnologie prin măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, chiar înainte de începerea prelucrării datelor cu caracter personal și vor fi aplicate pe parcursul întregului său ciclu de viață. Având în vedere riscul ridicat inerent pentru drepturile și libertățile persoanelor fizice, alegerea unor astfel de măsuri nu ar trebui să se întemeieze doar pe considerente economice[64], ci ar trebui, în schimb, să se străduiască să pună în aplicare tehnologiile de vârf în materie de protecție a datelor. În aceeași ordine de idei, dacă o autoritate de aplicare a legii intenționează să aplice și să utilizeze TRF de la furnizori externi, aceasta trebuie să se asigure, de exemplu prin procedura de achiziții, că sunt implementate numai TRF bazate pe principiile asigurării protecției datelor începând cu momentul conceperii și în mod implicit[65]. Acest lucru implică și faptul că transparența privind funcționarea TRF nu este limitată de invocarea secretelor comerciale sau a drepturilor de proprietate intelectuală.

3.2.5.5 Articolul 25 – Înregistrarea

101. LED stipulează diferite metode prin care operatorul sau persoana împuternicită de operator să demonstreze legalitatea prelucrării și să garanteze integritatea și securitatea datelor. În acest sens, înregistrările în sistem reprezintă un instrument foarte util și o garanție importantă pentru verificarea legalității prelucrării, atât la nivel intern (adică monitorizare proprie), cât și de către autoritățile de supraveghere externe, cum ar fi autoritățile pentru protecția datelor. În temeiul articolului 25 din LED, se înregistrează cel puțin următoarele operațiuni de prelucrare în cadrul sistemelor de prelucrare automată: colectarea, modificarea, consultarea, divulgarea inclusiv transferurile, combinarea și

[63] Vezi de exemplu: ISO/IEC 24745 Securitatea informației, securitatea cibernetică și protecția vieții private – Protecția informațiilor biometrice.
[64] Vezi considerentul 53 din LED.
[65] Pentru mai multe informații, vezi Orientările CEPD privind asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

ștergerea. În plus, înregistrările consultărilor și ale divulgărilor ar trebui să facă posibilă determinarea motivelor, a datei și a momentului acestor operațiuni și, în măsura în care este posibil, identificarea persoanei care a consultat sau a divulgat date cu caracter personal și identitatea destinatarilor acestor date cu caracter personal. Mai mult, în contextul sistemelor de recunoaștere facială, se recomandă înregistrarea următoarelor operațiuni de prelucrare suplimentare (parțial în afara articolului 25 din LED):

- modificările bazei de date de referință (adăugare, ștergere sau actualizare). Înregistrarea ar trebui să păstreze o copie a imaginii relevante (adăugate, șterse sau actualizate), atunci când nu se poate verifica în alt mod legalitatea sau rezultatul operațiunilor de prelucrare;

- încercările de identificare sau de verificare, inclusiv rezultatul și scorul de încredere. Ar trebui aplicat principiul reducerii stricte la minimum, astfel încât în înregistrări să se păstreze doar identificatorul imaginii din baza de date de referință, în loc să se stocheze imaginea de referință. Înregistrarea datelor biometrice de intrare ar trebui evitată, cu excepția cazului în care este necesară (de exemplu, doar în cazurile de corespondență);

- identitatea utilizatorului care a solicitat încercarea de identificare sau de verificare;

- orice date cu caracter personal stocate în înregistrările din sisteme sunt supuse unor limitări stricte ale scopului (de exemplu, audituri) și nu ar trebui să fie utilizate în alte scopuri (de exemplu, pentru a putea efectua în continuare recunoașterea/verificarea, inclusiv a unei imagini care a fost ștearsă din bazele de date de referință). Ar trebui aplicate măsuri de securitate pentru a asigura integritatea înregistrărilor, în timp ce sistemele de monitorizare automată pentru detectarea utilizării abuzive a înregistrărilor sunt foarte recomandate. Pentru înregistrările în baza de date de referință, măsurile de securitate ar trebui să fie echivalente cu baza de date de referință, în cazul stocării imaginilor faciale. De asemenea, ar trebui implementate procese automate de asigurare a respectării perioadei de păstrare a datelor pentru înregistrări.

3.2.5.6 Articolul 4 alineatul (4) – Responsabilitate

102. Operatorul trebuie să fie în măsură să demonstreze conformitatea prelucrării cu principiile prevăzute la articolul 4 alineatele (1)-(3), vezi articolul 4 alineatul (4) din LED. În acest sens, este esențială o documentare sistematică și actualizată a sistemului (inclusiv actualizări, modernizări și antrenare algoritmică), a măsurilor tehnice și organizatorice (inclusiv monitorizarea performanței sistemului și potențiala intervenție umană) și a prelucrării datelor cu caracter personal. Pentru a demonstra legalitatea prelucrării, un element deosebit de important este înregistrarea în conformitate cu articolul 25 din LED (vezi secțiunea 3.2.5.5). Principiul responsabilității nu se referă numai la sistem și la prelucrare, ci și la documentarea garanțiilor procedurale, cum ar fi evaluările necesității și proporționalității, evaluările impactului asupra protecției datelor, precum și consultările interne (de exemplu, aprobarea de către conducere a proiectului sau deciziile interne privind valorile scorului de încredere) și consultările externe (de exemplu, autoritatea pentru protecția datelor). Anexa II conține o serie de elemente în acest sens.

3.2.5.7 Articolul 47 – Supravegherea eficientă

103. Supravegherea eficientă de către autoritățile competente pentru protecția datelor este una dintre cele mai importante garanții pentru drepturile și libertățile fundamentale ale persoanelor afectate de utilizarea TRF. În același timp, asigurarea resurselor umane, tehnice și financiare, precum și a sediilor și a infrastructurii necesare fiecărei autorități pentru protecția datelor reprezintă o condiție esențială

pentru îndeplinirea cu eficacitate a sarcinilor și exercitarea competențelor acestora[66]. Chiar mai importante decât numărul de membri ai personalului disponibili sunt competențele experților, care ar trebui să acopere o gamă foarte largă de aspecte – de la anchetele penale și cooperarea polițienească până la analiza volumelor mari de date și inteligența artificială. Prin urmare, statele membre ar trebui să se asigure că resursele autorităților de supraveghere sunt adecvate și suficiente pentru a le permite să-și îndeplinească mandatul de a proteja drepturile persoanelor vizate și să urmărească îndeaproape orice evoluție în acest sens.[67]

4 CONCLUZIE

104. Utilizarea tehnologiilor de recunoaștere facială este legată în mod intrinsec de prelucrarea unor cantități semnificative de date cu caracter personal, inclusiv a categoriilor speciale de date. Fața și, în general, datele biometrice sunt legate în mod permanent și irevocabil de identitatea unei persoane. Prin urmare, utilizarea recunoașterii faciale are un impact direct sau indirect asupra unei serii de drepturi și libertăți fundamentale consacrate în Carta drepturilor fundamentale a UE, care pot merge dincolo de protecția vieții private și a datelor, cum ar fi demnitatea umană, libertatea de circulație, libertatea de întrunire și altele. Acest lucru este deosebit de relevant în domeniul aplicării legii și al justiției penale.

105. CEPD înțelege nevoia autorităților de aplicare a legii de a beneficia de cele mai bune instrumente posibile pentru a identifica rapid autorii actelor de terorism și ai altor infracțiuni grave. Totuși, aceste instrumente ar trebui utilizate în strictă conformitate cu cadrul juridic aplicabil și numai în cazurile în care îndeplinesc cerințele de necesitate și proporționalitate, astfel cum se prevede la articolul 52 alineatul (1) din Cartă. În plus, deși tehnologiile moderne pot fi o parte a soluției, ele nu reprezintă în niciun caz o soluție simplă garantată.

106. Există anumite cazuri de utilizare a tehnologiilor de recunoaștere facială care prezintă riscuri inacceptabil de mari pentru persoane și societate („linii roșii”). Din aceste motive, CEPD și AEPD au solicitat interzicerea generală a acestora[68].

107. În special, identificarea biometrică de la distanță a persoanelor în spații accesibile publicului prezintă un risc mare de intruziune în viața privată a persoanelor și nu își are locul într-o societate democratică, deoarece, prin natura sa, implică o supraveghere în masă. În aceeași ordine de idei, CEPD consideră că sistemele de recunoaștere facială sprijinite de IA care clasifică indivizii pe baza datelor lor biometrice în grupuri în funcție de originea etnică, de gen, precum și de orientarea politică sau sexuală nu sunt compatibile cu carta. În plus, CEPD este convins că utilizarea recunoașterii faciale sau a unor tehnologii similare pentru a deduce emoțiile unei persoane fizice este extrem de nedorită și ar trebui interzisă, eventual cu puține excepții justificate corespunzător. Mai mult, CEPD consideră că prelucrarea datelor cu caracter personal într-un context de aplicare a legii care s-ar baza pe o bază de date populată prin colectarea de date cu caracter personal în masă și în mod generalizat, de exemplu prin extragerea („scraping”) fotografiilor și a imaginilor faciale accesibile online, în special a celor puse la dispoziție prin

[66] Vezi comunicarea Comisiei intitulată „Primul raport referitor la aplicarea și funcționarea Directivei (UE) 2016/680 privind protecția datelor în materie de aplicare a legii («LED»)”, COM(2022)0364, secțiunea 3.4.1.

[67] Vezi Contribuția CEPD la evaluarea de către Comisia Europeană a Directivei privind protecția datelor în materie de aplicare a legii (LED) în temeiul articolului 62, punctul 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

[68] Vezi Avizul comun CEPD-AEPD 5/2021 privind propunerea de regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

intermediul rețelelor sociale, nu ar îndeplini, ca atare, cerința de strictă necesitate prevăzută de dreptul Uniunii.

5 ANEXE

Anexa I: Model de sprijin

Anexa II: Îndrumări practice pentru gestionarea proiectelor care implică TRF în cadrul autorităților de aplicare a legii

Anexa III: Exemple practice

ANEXA I – MODEL PENTRU DESCRIEREA SCENARIILOR

(Cu casete de informații pentru aspectele tratate în cadrul scenariului)

Descrierea prelucrării:

- Descrierea prelucrării, contextul (legătura cu infracțiunea), scopul

Sursa informațiilor:

- Tipuri de persoane vizate: ☐ toți cetățenii ☐ condamnați ☐ suspecți ☐ copii ☐ alte persoane vizate vulnerabile
- Sursa imaginii: ☐ spații accesibile publicului ☐ internet ☐ entitate privată ☐ alte persoane fizice ☐ altele .....
- Legătura cu infracțiunea: ☐ Temporală directă ☐ Nu este temporală directă ☐ Geografică directă ☐ Nu este geografică directă ☐ Nu este necesară
- Modul de colectare a informațiilor: ☐ la distanță ☐ într-o cabină sau într-un mediu controlat
- Context – afectează alte drepturi fundamentale:
  ☐ Nu
  Da, și anume ☐ libertatea de întrunire
  ☐ libertatea de exprimare
  ☐ diverse:.....
- Posibilități pentru surse suplimentare de informații despre persoana vizată:
  ☐ document de identitate☐ utilizarea telefonului public ☐ plăcuța de înmatriculare a vehiculului
  ☐ altele .....

Baza de date de referință (cu care se compară informațiile colectate):

- Specificitate: ☐ baze de date cu scop general ☐ baze de date specifice legate de domeniul criminalității
- Descrierea modului în care au fost populate aceste baze de date de referință (și temeiul juridic)
- Schimbarea scopului bazei de date (de exemplu, securitatea proprietății private a fost obiectivul principal): ☐ DA ☐ NU

Algoritm:

- Tip de prelucrare: ☐ verificare unu la unu (autentificare) ☐ identificare realizată prin compararea mai multor serii de date
- Considerente privind exactitatea
- Garanții tehnice

Rezultat:

- Impact ☐ Direct (de exemplu, persoana vizată poate fi arestată, interogată, comportament discriminatoriu)

  ☐ Indirect (se utilizează pentru modele statistice, nu există acțiuni în justiție cu consecințe grave împotriva persoanelor vizate)

- Decizie automatizată: ☐ DA ☐ NU
- Durata stocării

Analiza juridică:

- Analiza necesității și proporționalității – scopul/gravitatea infracțiunii/numărul de persoane neimplicate, dar afectate de prelucrare
- Tipul de informare prealabilă a persoanei vizate: ☐ La intrarea în zona specifică

  ☐ Pe site-ul autorității de aplicare a legii în general

  ☐ Pe site-ul autorității de aplicare a legii pentru prelucrarea specifică

  ☐ Altele .....
- Cadrul juridic aplicabil:

  ☐ LED transpusă în mare parte în dreptul intern

  ☐ Dreptul intern general pentru utilizarea datelor biometrice de către autoritățile de aplicare a legii

  ☐ Legislația internă specifică pentru această prelucrare (recunoaștere facială) pentru autoritatea competentă respectivă

  ☐ Legislația internă specifică pentru această prelucrare (decizie automatizată)

Concluzie:

Considerente generale cu privire la probabilitatea ca prelucrarea descrisă să fie compatibilă cu dreptul Uniunii (și unele sugestii cu privire la condițiile prealabile legale)

ANEXA II – ÎNDRUMĂRI PRACTICE PENTRU GESTIONAREA PROIECTELOR CARE IMPLICĂ TEHNOLOGIA DE RECUNOAȘTERE FACIALĂ ÎN CADRUL AUTORITĂȚILOR DE APLICARE A LEGII

Prezenta anexă oferă unele îndrumări practice suplimentare pentru autoritățile de aplicare a legii („AAL") care planifică să inițieze un proiect care implică tehnologia de recunoaștere facială („TRF"). Aceasta oferă mai multe informații despre măsurile organizatorice și tehnice care trebuie luate în considerare în timpul implementării proiectului și nu trebuie considerată o listă exhaustivă de etape/măsuri care trebuie urmate/luate. De asemenea, trebuie interpretată în coroborare cu Ghidul CEPD 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video[69], precum și cu orice regulament al UE/SEE și cu orientările CEPD privind utilizarea inteligenței artificiale.

Prezenta anexă oferă îndrumări bazate pe ipoteza că autoritățile de aplicare a legii vor achiziționa TRF (sub formă de produse gata de utilizare). Dacă autoritățile de aplicare a legii planifică să dezvolte (să antreneze ulterior) TRF, atunci se aplică cerințe suplimentare pentru selectarea seturilor de date necesare pentru antrenare, validare și testare care urmează să fie utilizate în timpul dezvoltării, precum și a rolurilor/măsurilor pentru mediul de dezvoltare. În mod similar, un produs gata de utilizare poate necesita ajustări suplimentare pentru utilizarea preconizată, iar în acest caz trebuie îndeplinite cerințele menționate mai sus pentru selectarea seturilor de date de testare, validare și antrenare.

Faptul că aparțin aceleiași autorități de aplicare a legii nu oferă acces deplin la datele biometrice. Ca și celelalte categorii de date cu caracter personal, datele biometrice colectate pentru un anumit scop de aplicare a legii pe baza unui temei juridic specific nu pot fi utilizate fără un temei legal adecvat pentru un scop diferit de aplicare a legii [articolul 4 alineatul (2) din Directiva (UE) 2016/680 (LED)]. De asemenea, dezvoltarea/antrenarea unui instrument bazat pe TRF este considerată un scop diferit și ar trebui evaluat dacă este necesară și proporțională prelucrarea datelor biometrice pentru a măsura performanța tehnologiei/a antrena tehnologia, astfel încât să se evite impactul performanțelor scăzute asupra persoanelor vizate, ținând seama de scopul inițial al prelucrării.

1. ROLURI ȘI RESPONSABILITĂȚI

Atunci când o autoritate de aplicare a legii utilizează TRF pentru îndeplinirea sarcinilor sale care intră în domeniul de aplicare al LED (prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor etc., conform articolului 3 din LED), aceasta poate fi considerată operator pentru tehnologiile în cauză. Totuși, autoritățile de aplicare a legii sunt formate din mai multe unități/departamente care pot fi implicate în această prelucrare, fie prin definirea procesului de aplicare a TRF, fie prin aplicarea acesteia în practică. Având în vedere particularitățile acestei tehnologii, ar putea fi necesar ca diferite unități să fie implicate fie pentru a sprijini măsurarea performanței sale, fie pentru a o antrena în continuare.

În cadrul unui proiect care implică TRF există mai multe părți interesate[70] din cadrul autorității de aplicare a legii care ar trebui poate implicate:

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[70] Următoarele roluri indică diferitele părți interesate și responsabilitățile acestora în cadrul unui proiect care implică TRF. Deși limbajul utilizat pentru a descrie rolurile din această anexă nu este imperativ, fiecare autoritate

- personalul de conducere de nivel superior – pentru a aproba proiectul după punerea în balanță a riscurilor și a beneficiilor potențiale;
- responsabilul cu protecția datelor și/sau departamentul juridic al autorității de aplicare a legii – pentru a contribui la evaluarea legalității implementării unui anumit proiect care implică TRF; pentru a contribui la efectuarea EIPD; pentru a asigura respectarea și exercitarea drepturilor persoanelor vizate;
- responsabilul de proces – care acționează în calitate de unitate specifică în cadrul autorității de aplicare a legii competente pentru a dezvolta proiectul și care decide detaliile proiectului care implică TRF, inclusiv cerințele de performanță a sistemului; care decide cu privire la indicatorul de echitate adecvat; care stabilește scorul de încredere[71]; care stabilește praguri acceptabile pentru prejudecăți; care identifică riscurile potențiale pe care proiectul care implică TRF le prezintă la adresa drepturilor și libertăților persoanelor [prin consultarea și cu responsabilul cu protecția datelor și cu departamentul de IT și inteligență artificială și/sau de știință a datelor (vezi mai jos)] și le prezintă personalului de conducere de nivel superior. Responsabilul de proces se va consulta și cu administratorul bazei de date de referință, înainte de a decide cu privire la detaliile proiectului care implică TRF, pentru a înțelege atât scopul utilizării bazei de date de referință, cât și detaliile tehnice ale acesteia. În cazul reantrenării unei TRF achiziționate, responsabilul de proces va fi responsabil și pentru selectarea setului de date de antrenare. În calitate de unitate însărcinată cu dezvoltarea și stabilirea detaliilor proiectului, responsabilul de proces este responsabil pentru efectuarea EIPD;
- departamentul de IT și inteligență artificială și/sau de știință a datelor – pentru a contribui la efectuarea unei EIPD; pentru a explica indicatorii disponibili pentru măsurarea performanței sistemului, a echității[72] și a prejudecăților posibile; pentru a implementa tehnologia și garanțiile tehnice, cu scopul de a preveni accesul neautorizat la datele colectate, atacurile cibernetice etc. În cazul reantrenării unei TRF achiziționate, departamentul de IT și inteligență artificială și/sau de știință a datelor va antrena sistemul, pe baza setului de date de antrenare furnizat de responsabilul de proces. Acest departament va fi responsabil și pentru stabilirea măsurilor de atenuare a riscurilor identificate în comun de responsabilii de proces (de exemplu, riscurile specifice IA, cum ar fi atacurile prin deducție a modelelor);
- utilizatorii finali (cum ar fi funcționarii poliției de pe teren sau din laboratoarele de criminalistică) – pentru a efectua o comparație cu baza de date; pentru a revizui în mod critic rezultatele, ținând seama de dovezile anterioare și pentru a oferi feedback responsabilului de proces în ceea ce privește rezultatele fals pozitive și indicii de posibilă discriminare;
- administratorul bazei de date de referință – unitatea specifică din cadrul autorității de aplicare a legii competente responsabilă pentru dezvoltarea și gestionarea bazei de date de referință, adică a bazei de date cu care vor fi comparate imaginile, inclusiv pentru ștergerea imaginilor faciale după perioada de păstrare definită. Această bază de date poate fi creată în mod specific pentru proiectul avut în vedere care implică TRF sau poate exista în prealabil, în scopuri compatibile. Administratorul bazei de date de referință este responsabil de definirea momentului și a circumstanțelor în care pot fi stocate imaginile faciale, precum și de stabilirea cerințelor de păstrare a datelor (în funcție de timp sau de alte criterii).

---

de aplicare a legii trebuie să definească și să atribuie roluri similare în funcție de organizarea sa. Se poate întâmpla ca o unitate să acumuleze mai multe roluri, de exemplu, responsabil de proces și administrator al bazei de date de referință sau responsabil de proces și departamentul de IT și inteligență artificială și/sau de știință a datelor (în cazul în care unitatea responsabilului de proces deține toate cunoștințele tehnice necesare).

[71] Scorul de încredere reprezintă nivelul de încredere al predicției (corespondență), sub forma unei probabilități. De exemplu, prin compararea a două modele, se obține un scor de încredere de 90 % că acestea aparțin aceleiași persoane. Scorul de încredere este diferit de performanța TRF, însă afectează performanța. Cu cât pragul de încredere este mai mare , cu atât sunt mai puține rezultate fals pozitive și mai multe rezultate fals negative în rezultatele TRF.

[72] Echitatea poate fi definită ca lipsa discriminării injuste și ilicite, de exemplu prejudecățile rasiale și de gen.

Întrucât cele mai multe cazuri de implementare și utilizare a TRF prezintă un risc ridicat intrinsec pentru drepturile și libertățile persoanelor vizate, autoritatea de supraveghere a protecției datelor ar trebui să fie implicată și în contextul consultării prealabile prevăzute la articolul 28 din LED.

2. INIȚIERE/ÎNAINTE DE ACHIZIȚIONAREA SISTEMULUI BAZAT PE TRF

Responsabilul de proces din cadrul unei autorități de aplicare a legii ar trebui mai întâi să înțeleagă clar procesul (procesele) care urmărește (urmăresc) utilizarea TRF (cazul/cazurile de utilizare) și să se asigure că există un temei legal pentru a justifica respectivul caz de utilizare preconizată. Pe această bază, responsabilul de proces trebuie:

- să descrie în mod formal cazul de utilizare. Trebuie să se descrie problema care trebuie soluționată și modul în care TRF va oferi o soluție, precum și prezentarea generală a procesului (sarcinii) în care TRF va fi aplicată. În acest sens, autoritatea de aplicare a legii trebuie să documenteze cel puțin[73]:
  - categoriile de date cu caracter personal înregistrate în cadrul procesului;
  - obiectivele și scopurile concrete în care va fi utilizată TRF, inclusiv consecințele potențiale pentru persoana vizată după stabilirea unei corespondențe;
  - când și cum vor fi colectate imaginile faciale (inclusiv informații despre contextul acestei colectări, de exemplu, la poarta aeroportului, materiale video de la camerele de securitate din fața unui magazin unde s-a comis o infracțiune etc. și categoriile de persoane vizate ale căror date biometrice vor fi prelucrate);
  - baza de date cu care vor fi comparate imaginile (baza de date de referință), precum și informațiile despre modul în care a fost creată, mărimea ei și calitatea datelor biometrice pe care le conține;
  - actorii din cadrul autorității de aplicare a legii care vor fi autorizați să utilizeze sistemul TRF și să acționeze în consecință în contextul aplicării legii (profilurile și drepturile de acces ale acestora trebuie definite de către responsabilul de proces);
  - perioada de păstrare preconizată pentru datele de intrare sau momentul care va determina sfârșitul acestei perioade (cum ar fi încheierea sau încetarea procedurilor penale în conformitate cu dreptul procedural național pentru care au fost colectate inițial), precum și orice acțiune ulterioară (ștergerea acestor date, anonimizarea și utilizarea în scopuri statistice sau de cercetare etc.);
  - implementarea înregistrării și accesibilitatea înregistrărilor și a evidențelor păstrate;
  - indicatorii de performanță (de exemplu, exactitate, precizie, rapel, scor F1) și pragurile minime acceptabile ale acestora;[74]
  - o estimare a numărului de persoane care vor fi supuse TRF și în ce perioadă de timp/cu ce ocazie;

[73] În anexa I este prezentată o listă de elemente care ajută operatorul să descrie un caz de utilizare a TRF.

[74] Există diferiți indicatori pentru a evalua performanța unui sistem bazat pe TRF. Fiecare indicator oferă o imagine diferită a rezultatelor sistemului, iar succesul său în furnizarea unei imagini adecvate a performanțelor bune sau slabe ale sistemului bazat pe TRF depinde de cazul de utilizare a TRF. Dacă se pune accentul pe obținerea unor procentaje ridicate de punere corectă în corespondență a unei fețe, s-ar putea utiliza indicatori precum precizia și rapelul. Totuși, acești indicatori nu măsoară cât de bine gestionează TRF exemplele negative (câte corespondențe incorecte au fost stabilite de sistem). Responsabilul de proces, sprijinit de departamentul de IT și inteligență artificială și/sau de știință a datelor, ar trebui să fie în măsură să stabilească cerințele de performanță și să le exprime prin indicatorul cel mai potrivit în funcție de cazul de utilizare a TRF.

- să efectueze o evaluare a necesității și a proporționalității[75]. Faptul că această tehnologie există nu ar trebui să fie factorul care determină aplicarea sa. Responsabilul de proces trebuie să evalueze mai întâi dacă există un temei legal adecvat pentru prelucrarea preconizată. În acest scop, trebuie să se consulte responsabilul cu protecția datelor și serviciul juridic. Ceea ce determină implementarea TRF ar trebui să fie faptul că aceasta este o soluție necesară și proporțională pentru o problemă definită în mod specific de autoritatea de aplicare a legii. Acest lucru trebuie evaluat în funcție de scopul/gravitatea infracțiunii/numărul de persoane care nu sunt implicate, dar sunt afectate de sistemul bazat pe TRF. Pentru evaluarea legalității, trebuie luate în considerare cel puțin următoarele aspecte: LED[76], RGPD,[77] [78] orice cadru juridic existent privind IA[79] și toate orientările de însoțire furnizate de autoritățile de supraveghere a protecției datelor (cum ar fi Ghidul CEPD 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video[80]). Aceste acte legislative ale UE ar trebui coroborate întotdeauna cu cerințele naționale aplicabile, în special în domeniul dreptului procesual penal. Evaluarea proporționalității ar trebui să identifice drepturile fundamentale ale persoanelor vizate care pot fi afectate (dincolo de protecția vieții private și a datelor). De asemenea, ar trebui să descrie și să ia în considerare orice limite (sau lipsa limitelor) impuse în cazul de utilizare pentru sistemul bazat pe TRF. De exemplu, dacă sistemul va funcționa continuu sau temporar și dacă va fi limitat la o zonă geografică.
- să efectueze o evaluare a impactului asupra protecției datelor (EIPD) [81]. Trebuie efectuată o EIPD deoarece implementarea TRF în domeniul aplicării legii este predispusă să genereze un risc mare pentru drepturile și libertățile persoanelor[82]. EIPD trebuie să conțină în special: o descriere generală a operațiunilor de prelucrare preconizate[83], o evaluare a riscurilor pentru drepturile și

[75] Pentru a ține seama de principiul necesității, se pot lua în considerare măsuri suplimentare în ceea ce privește adaptarea și utilizarea sistemului, astfel încât descrierea cazului de utilizare poate fi, de asemenea, ușor modificată în timpul evaluării necesității și proporționalității.

[76] 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.

[77] 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.

[78] În cazurile în care pentru un proiect științific care vizează cercetarea utilizării TRF ar trebui să se prelucreze date cu caracter personal, dar această prelucrare nu ar intra sub incidența articolului 4 alineatul (3) din LED, în general s-ar aplica RGPD [articolul 9 alineatul (2) din LED]. În cazul proiectelor-pilot care ar fi urmate de operațiuni de aplicare a legii, LED s-ar aplica în continuare.

[79] De exemplu, există o propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI DE STABILIRE A UNOR NORME ARMONIZATE PRIVIND INTELIGENȚA ARTIFICIALĂ (LEGEA PRIVIND INTELIGENȚA ARTIFICIALĂ) ȘI DE MODIFICARE A ANUMITOR ACTE LEGISLATIVE ALE UNIUNII, care însă nu este încă stabilită ca regulament.

[80] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[81] Orientări suplimentare privind EIPD pot fi găsite în documentul intitulat „Ghid privind evaluarea impactului asupra protecției datelor (DPIA) și modul în care se determină dacă prelucrarea este «susceptibilă să genereze un risc ridicat» în sensul Regulamentului 2016/679, WP 248 rev. 01, disponibil la adresa: https://ec.europa.eu/newsroom/article29/items/611236 și în setul de instrumente al AEPD intitulat Responsabilitatea pe teren, partea II, disponibil la adresa: https://edps.europa.eu/node/4582_en

[82] TRF, în funcție de cazul de utilizare, poate intra sub incidența următoarelor criterii care declanșează prelucrarea cu risc ridicat (din Ghidul privind EIPD, WP 248 rev. 01): monitorizarea sistematică, datele prelucrate pe scară largă, corelarea sau combinarea seturilor de date, utilizarea inovatoare sau aplicarea unor soluții tehnologice sau organizaționale noi.

[83] Descrierea prelucrării, precum și evaluarea necesității și a proporționalității, astfel cum au fost deja descrise în etapele de mai sus, fac parte tot din EIPD, în afară de evaluarea riscurilor. Dacă este necesar, în EIPD se va furniza o descriere mai detaliată a fluxurilor de date cu caracter personal.

libertățile persoanelor vizate[84], măsurile preconizate pentru a răspunde la aceste riscuri, garanțiile, măsurile de securitate și mecanismele de asigurare a protecției datelor cu caracter personal și de demonstrare a conformității. EIPD este un proces continuu, prin urmare, trebuie adăugate orice elemente noi ale prelucrării, iar evaluarea riscurilor ar trebui actualizată în fiecare etapă a proiectului;

- să obțină aprobarea personalului de conducere de nivel superior, explicând riscurile pentru drepturile și libertățile persoanelor vizate (rezultate din cazul de utilizare și din tehnologie) și planurile respective de tratare a riscurilor;

3. ÎN TIMPUL ACHIZIȚIEI ȘI ÎNAINTE DE IMPLEMENTAREA TRF

- să decidă criteriile de selectare a TRF (algoritmul). Responsabilul de proces ar trebui să decidă criteriile de selectare a unui algoritm, cu ajutorul departamentului de IT și inteligență artificială și/sau de știință a datelor. În practică, acestea ar include indicatorii de echitate și performanță stabiliți în descrierea cazului de utilizare. Aceste criterii trebuie să includă și informații referitoare la datele cu care a fost antrenat algoritmul. Seturile de date de antrenare, testare și validare trebuie să includă în mod suficient eșantioane ale tuturor caracteristicilor persoanelor vizate care urmează să fie supuse TRF (luând în considerare, de exemplu, vârsta, genul și rasa), pentru a reduce prejudecățile. Furnizorul TRF trebuie să furnizeze informații și indicatori privind seturile de date de antrenare, testare și validare a TRF și să descrie măsurile luate pentru a măsura și a atenua potențialele discriminări și prejudecăți ilicite. Responsabilul de proces, când este posibil, trebuie să verifice dacă a existat un temei legal pentru ca furnizorul să utilizeze acest set de date în scopul antrenării algoritmilor (pe baza informațiilor pe care furnizorul le va pune la dispoziție). De asemenea, responsabilul de proces trebuie să se asigure că furnizorul TRF aplică standarde de securitate legate de datele biometrice, cum ar fi ISO/IEC 24745, care oferă orientări pentru protecția informațiilor biometrice în conformitate cu diferite cerințe privind confidențialitatea, integritatea și posibilitatea de reînnoire/de revocare în timpul stocării și transmisiei, precum și cu cerințe și orientări pentru gestionarea și prelucrarea securizată și cu respectarea vieții private a informațiilor biometrice;

- să reantreneze algoritmul (dacă este necesar). Responsabilul de proces trebuie să se asigure că ajustarea sistemului bazat pe TRF pentru obținerea unei exactități mai mari înainte de utilizarea acestuia face parte, de asemenea, din serviciile achiziționate. În cazul în care este necesară o antrenare suplimentară a sistemului bazat pe TRF achiziționat pentru a respecta indicatorii de exactitate, responsabilul de proces, pe lângă luarea deciziei de reantrenare, trebuie să decidă, cu ajutorul departamentului de IT și inteligență artificială și/sau de știință a datelor, asupra setului de date adecvat și reprezentativ care trebuie utilizat și să verifice legalitatea acestei utilizări pentru date;
- să stabilească garanțiile adecvate pentru a răspunde la riscurile legate de securitate, de prejudecăți și de performanță scăzută. Aceasta include stabilirea unui proces de monitorizare a TRF după începerea utilizării (înregistrare și feedback pentru exactitatea și echitatea rezultatelor). În plus, se asigură că riscurile specifice anumitor sisteme de învățare automată și TRF [de exemplu, manipularea datelor („data poisoning”), exemple contradictorii, inversarea modelului, deducție de tip „white box”] sunt identificate, măsurate și atenuate. De asemenea, responsabilul de proces

[84] Analiza riscurilor pentru persoanele vizate ar trebui să includă riscurile legate de locul în care se află imaginile faciale care urmează să fie comparate (local/la distanță), riscurile legate de persoanele împuternicite de către operatori/subcontractanți, precum și riscurile specifice învățării automate atunci când aceasta este aplicată [de exemplu, manipularea datelor („data poisoning”), exemple contradictorii].

trebuie să stabilească garanții adecvate pentru a se asigura că vor fi respectate cerințele de păstrare a datelor pentru datele biometrice incluse în setul de date pentru reantrenare;

- să documenteze sistemul bazat pe TRF. Aceasta trebuie să includă o descriere generală a sistemului bazat pe TRF, o descriere detaliată a elementelor sistemului bazat pe TRF și a procesului de instituire a acestuia, informații detaliate despre monitorizarea, funcționarea și controlul asupra sistemului bazat pe TRF, precum și o descriere detaliată a riscurilor acestuia și a măsurilor de atenuare a riscurilor. Elementele incluse în această documentație vor include elementele principale ale descrierii sistemului bazat pe TRF din etapele anterioare (vezi mai sus), însă acestea vor fi consolidate cu informații referitoare la monitorizarea performanței și la aplicarea modificărilor în sistem, inclusiv a oricăror actualizări ale versiunilor și/sau reantrenări;
- să creeze manuale de utilizare, explicând tehnologia și cazurile de utilizare. Acestea trebuie să explice clar toate scenariile și condițiile prealabile în care va fi utilizată TRF;
- să formeze utilizatorii finali cu privire la modul de utilizare a tehnologiei. Astfel de cursuri de formare trebuie să explice capacitățile și limitările tehnologiei, pentru ca utilizatorii să înțeleagă circumstanțele în care este necesar să o aplice și cazurile în care poate fi inexactă. Aceste cursuri de formare vor contribui și la atenuarea riscurilor legate de lipsa verificării/analizei critice a rezultatului algoritmului;
- să consulte autoritatea de supraveghere a protecției datelor, în conformitate cu articolul 28 alineatul (1) litera (b) din LED; să furnizeze informații în conformitate cu articolul 13 din LED, pentru a informa persoanele vizate cu privire la prelucrare și la drepturile lor. Aceste notificări trebuie să se adreseze persoanelor vizate într-un limbaj adecvat, pentru ca acestea să înțeleagă prelucrarea, și să le explice elementele de bază ale tehnologiei, inclusiv ratele de exactitate, seturile de date de antrenare și măsurile luate pentru a evita discriminarea și exactitatea scăzută a algoritmului;

4. RECOMANDĂRI DUPĂ IMPLEMENTAREA TRF

- să asigure intervenția umană și supravegherea rezultatelor. Să nu adopte niciodată o măsură referitoare la o persoană numai pe baza rezultatului TRF (acest lucru ar implica o încălcare a articolului 11 din LED – procesul decizional individual automatizat, care are efecte juridice sau alte efecte similare asupra persoanei vizate). Să se asigure că un funcționar al autorității de aplicare a legii examinează rezultatele TRF. De asemenea, să se asigure că utilizatorii din cadrul autorității de aplicare a legii evită prejudecățile legate de automatizare, investigând informațiile contradictorii și contestând în mod critic rezultatele tehnologiei. În acest scop, formarea continuă și sensibilizarea utilizatorilor finali sunt importante, însă personalul de conducere de nivel superior trebuie să se asigure că există resurse umane adecvate pentru a efectua o supraveghere eficace. Acest lucru implică acordarea de suficient timp fiecărui agent pentru a contesta în mod critic rezultatele tehnologiei. Să înregistreze, să măsoare și să evalueze măsura în care supravegherea umană modifică decizia inițială a TRF;
- să monitorizeze și să abordeze deriva modelului TRF (degradarea performanței) după ce modelul se află în producție;
- să stabilească un proces de reevaluare a riscurilor și a măsurilor de securitate în mod periodic și de fiecare dată când tehnologia sau cazul de utilizare suferă modificări;
- să documenteze orice modificare adusă sistemului pe parcursul întregului său ciclu de viață (de exemplu, modernizări, reantrenare);
- să stabilească un proces, precum și capacitățile tehnice conexe pentru a răspunde cererilor de acces formulate de persoanele vizate. Capacitatea tehnică pentru extragerea datelor, în cazul în care este necesar să fie furnizate persoanelor vizate, trebuie să existe înainte de formularea oricărei cereri;

- să se asigure că există proceduri pentru cazurile de încălcare a securității datelor. În cazul în care se produce o încălcare a securității datelor cu caracter personal, care implică date biometrice, este probabil ca riscurile să fie mari. În acest caz, toți utilizatorii implicați trebuie să cunoască procedurile relevante care trebuie urmate, responsabilul cu protecția datelor trebuie informat imediat, iar persoanele vizate ar trebui informate.

ANEXA III – EXEMPLE PRACTICE

Există multe contexte practice și scopuri diferite de utilizare a recunoașterii faciale, cum ar fi în medii controlate, precum punctele de trecere a frontierei, verificarea încrucișată cu date din bazele de date ale autorităților polițienești sau cu date cu caracter personal făcute publice în mod manifest de către persoana vizată, imagini în timp real de la camerele de luat vederi (recunoaștere facială în timp real) etc. Prin urmare, riscurile pentru protecția datelor cu caracter personal și a altor drepturi și libertăți fundamentale variază semnificativ în diferitele cazuri de utilizare. Pentru a facilita evaluarea necesității și a proporționalității, care ar trebui să preceadă decizia privind implementarea posibilă a recunoașterii faciale, orientările actuale oferă o listă neexhaustivă a aplicărilor posibile a TRF în domeniul aplicării legii.

Scenariile prezentate și evaluate se bazează pe situații **ipotetice** și sunt menite să ilustreze anumite utilizări concrete ale TRF și să ofere asistență pentru examinarea de la caz la caz, precum și să stabilească un cadru general. Acestea nu aspiră să fie exhaustive și nu aduc atingere niciunei proceduri în curs sau viitoare desfășurate de o autoritate națională de supraveghere cu privire la proiectarea, experimentarea sau implementarea tehnologiilor de recunoaștere facială. Prezentarea acestor scenarii ar trebui să servească doar în scopul de a exemplifica orientările, care sunt furnizate deja în prezentul document, pentru responsabilii de elaborarea politicilor, legiuitori și autoritățile de aplicare a legii, atunci când se concepe și se planifică implementarea tehnologiilor de recunoaștere facială pentru a asigura respectarea deplină a acquis-ului UE în domeniul protecției datelor cu caracter personal. În acest context, ar trebui ținut seama că, chiar și în situații similare de utilizare a TRF, prezența sau absența anumitor elemente poate duce la un rezultat diferit al evaluării necesității și proporționalității.

1 SCENARIUL 1

1.1. Descriere

Un sistem automatizat de control la frontieră care permite trecerea automatizată a frontierei prin autentificarea imaginii biometrice stocate în documentul de călătorie electronic al cetățenilor UE și al altor călători care trec prin punctul de trecere a frontierei și prin stabilirea faptului că pasagerul respectiv este titularul legitim al documentului.

Această verificare/autentificare implică doar recunoașterea facială unu la unu și se desfășoară în mediu controlat (de exemplu, la porțile electronice ale aeroportului). Datele biometrice ale călătorului care trece prin punctul de trecere a frontierei sunt colectate atunci când i se solicită în mod explicit să privească în camera de luat vederi de la poarta electronică și sunt comparate cu cele din documentul prezentat (pașaport, carte de identitate etc.) care este eliberat în conformitate cu cerințe tehnice specifice.

În același timp, deși prelucrarea în astfel de cazuri nu intră, în principiu, în domeniul de aplicare al LED, rezultatul verificării poate fi utilizat și pentru punerea în corespondență a datelor (alfanumerice) ale persoanei respective cu bazele de date în materie de aplicare a legii ca parte a controlului la frontieră și, prin urmare, poate implica acțiuni cu efecte juridice semnificative pentru persoana vizată, de exemplu arestarea conform unei semnalări în SIS. În anumite circumstanțe specifice, datele biometrice pot fi utilizate și pentru a căuta corespondențe în bazele de date în materie de aplicare a legii (în acest caz, s-ar efectua o identificare realizată prin compararea mai multor serii de date în această etapă).

Rezultatul prelucrării imaginilor biometrice are un impact direct asupra persoanei vizate: numai în cazul unei verificări cu succes, aceasta permite trecerea prin punctul de trecere a frontierei. În cazul în

care nu s-a putut realiza identificarea, polițiștii de frontieră trebuie să efectueze o a doua verificare pentru a se asigura că persoana vizată este diferită de cea prezentată în documentul de identificare.

În cazul în care se identifică o semnalare în SIS sau națională, polițiștii de frontieră trebuie să efectueze o a doua verificare și verificările suplimentare necesare și apoi să ia orice măsuri necesare, de exemplu să aresteze persoana respectivă, să informeze autoritățile în cauză.

Sursa informațiilor:

- Tipuri de persoane vizate: ☒ toate persoanele care trec frontierele
- Sursa imaginii: ☒ altele (documentul de identitate)
- Legătura cu infracțiunea: ☒ Nu este necesar
- Modul de colectare a informațiilor: ☒ într-o cabină sau într-un mediu controlat
- Context – afectează alte drepturi fundamentale: Da, și anume: ☒ dreptul la liberă circulație ☒ dreptul de azil

Baza de date de referință (cu care se compară informațiile colectate):

- Specificitate: ☒ baze de date specifice legate de controlul la frontiere

Algoritm:

- Tipul de verificare: ☒ verificare unu la unu (autentificare)

Rezultat:

- Impact☒ Direct (persoanei vizate i se permite sau i se refuză intrarea)
- Decizie automatizată:☒ Da

1.2. Cadrul juridic aplicabil

Din 2004, conform Regulamentului (CE) nr. 2252/2004 al Consiliului[85], pașapoartele și alte documente de călătorie eliberate de statele membre trebuie să conțină o fotografie facială biometrică stocată pe un cip electronic integrat în document.

Codul frontierelor Schengen[86] stabilește cerințele pentru verificările persoanelor la frontierele externe. Pentru cetățenii UE și pentru alte persoane care beneficiază de dreptul la liberă circulație în temeiul dreptului Uniunii, verificările minime ar trebui să constea într-o verificare a documentelor lor de călătorie, prin utilizarea, după caz, a unor dispozitive tehnice. Codul frontierelor Schengen a fost modificat ulterior prin Regulamentul (UE) 2017/2225[87], care a introdus, printre altele, definiții pentru „porțile electronice”, „sistemul automatizat de control la frontiere” și „sistemul de self-service”, precum și posibilitatea de prelucrare a datelor biometrice pentru efectuarea verificărilor la frontiere.

Prin urmare, s-ar putea presupune că există un temei legal clar și previzibil care autorizează această formă de prelucrare a datelor cu caracter personal. În plus, cadrul juridic este adoptat la nivelul Uniunii și este direct aplicabil statelor membre.

1.3. Necesitatea și proporționalitatea – scopul/gravitatea infracțiunii

Verificarea identității cetățenilor UE în cadrul unui control automatizat la frontiere, utilizând imaginea biometrică a acestora, este un element al controalelor la frontierele externe ale UE. În consecință, este

[85] REGULAMENTUL (CE) nr. 2252/2004 AL CONSILIULUI din 13 decembrie 2004 privind standardele pentru elementele de securitate și elementele biometrice integrate în pașapoarte și în documente de călătorie emise de statele membre.

[86] REGULAMENTUL (UE) 2016/399 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 9 martie 2006 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen).

[87] Regulamentul (UE) 2017/2225 al Parlamentului European și al Consiliului din 30 noiembrie 2017 de modificare a Regulamentului (UE) 2016/399 în ceea ce privește utilizarea Sistemului de intrare/ieșire.

legată direct de securitatea frontierelor și servește unui obiectiv de interes general recunoscut de Uniune. În plus, porțile de control automatizat la frontiere contribuie la accelerarea procesării pasagerilor și reduc riscul de erori umane. Mai mult, domeniul de aplicare, amploarea și intensitatea atingerii aduse drepturilor în acest scenariu sunt mult mai limitate față de alte forme de recunoaștere facială. Cu toate acestea, prelucrarea datelor biometrice creează riscuri suplimentare pentru persoanele vizate, care trebuie soluționate și atenuate în mod corespunzător de către autoritatea competentă care implementează și utilizează TRF.

1.4. Concluzie

Verificarea identității cetățenilor UE în contextul unui control automatizat la frontiere este o măsură necesară și proporțională, atâta timp cât există garanții adecvate, în special aplicarea principiilor limitării scopului, al calității datelor, al transparenței și un nivel ridicat de securitate.

2 SCENARIUL 2

2.1. Descriere

Un sistem de identificare a victimelor răpirii de copii este stabilit de autoritatea de aplicare a legii. Un funcționar autorizat al poliției poate efectua o comparare a datelor biometrice ale unui copil, suspectat că ar fi răpit, cu o bază de date a victimelor răpirii de copii, în condiții stricte, în scopul unic de a identifica minorii care ar putea corespunde descrierii copilului dispărut pentru care s-a deschis o investigare și s-a emis semnalarea.

Prelucrarea în cauză ar consta în compararea feței sau a imaginii unei persoane, care poate corespunde descrierii unui copil dispărut, cu imaginile stocate în baza de date. Această prelucrare ar avea loc în anumite cazuri, și nu în mod sistematic.

Baza de date cu care se va efectua compararea este populată cu fotografii ale copiilor dispăruți pentru care s-a raportat o suspiciune de răpire de copii, o amenințare la adresa vieții sau a integrității fizice a copilului și s-a deschis o investigație în cadrul unei autorități judiciare și pentru care s-a emis o semnalare privind răpirea de copii. Datele sunt colectate în cadrul procedurilor stabilite de către autoritatea competentă de aplicare a legii, adică de către funcționarii poliției autorizați să efectueze misiuni judiciare de poliție. Categoriile de date cu caracter personal înregistrate sunt următoarele:

- identitate, poreclă, pseudonim, filiație, naționalitate, adrese, adrese de e-mail, numere de telefon;
- data și locul nașterii:
- informații privind filiația;
- fotografie cu caracteristici tehnice care permite utilizarea unui dispozitiv de recunoaștere facială și alte fotografii.

Rezultatele comparării trebuie, de asemenea, să fie revizuite și verificate de un funcționar autorizat, pentru a corobora dovezile anterioare cu rezultatul comparării și pentru a exclude orice rezultate fals pozitive posibile.

Fotografiile și datele cu caracter personal ale copiilor pot fi păstrate numai pe durata semnalării și trebuie șterse imediat după încheierea sau încetarea procedurii penale, în conformitate cu procedurile naționale pentru care au fost introduse în baza de date.

Deși perioada de păstrare a datelor biometrice în baza de date poate fi preconizată pentru o perioadă relativ lungă și definită în conformitate cu dreptul intern, exercitarea drepturilor persoanelor vizate și, în special, a dreptului la rectificare și ștergere oferă o garanție suplimentară pentru a limita atingerea adusă dreptului la protecția datelor cu caracter personal al persoanelor vizate în cauză.

Sursa informațiilor:

- Tipuri de persoane vizate: ☒ Copii
- Sursa imaginii ☒ altele: nepredefinită, victimă presupusă a răpirii de copii
- Legătura cu infracțiunea ☒ Nu este temporală directă ☒ Nu este geografică directă
- Modul de colectare a informațiilor: ☒ într-o cabină sau într-un mediu controlat
- Context: afectează alte drepturi fundamentale ☒ Da, și anume: ☒ diverse

Baza de date de referință (cu care se compară informațiile colectate):

- Specificitate ☒ bază de date specifică

Algoritm:

- Tipul de verificare: ☒ identificare realizată prin compararea mai multor serii de date

Rezultat:

- Impact☒ Direct
- Decizie automatizată: ☒ NU, revizuire obligatorie de către un funcționar autorizat

Analiza juridică:

- Cadrul juridic aplicabil: ☒ Legislația internă specifică pentru această prelucrare (recunoaștere facială)

2.2. Cadrul juridic aplicabil

Dreptul intern prevede un cadru juridic specific de instituire a bazei de date, care stabilește scopurile prelucrării, precum și criteriile pentru popularea, accesarea și utilizarea bazei de date. Măsurile legislative necesare pentru punerea sa în aplicare prevăd și stabilirea unei perioade de păstrare, precum și trimiterea la principiile aplicabile ale integrității și confidențialității. Măsurile legislative prevăd, de asemenea, modalitățile de furnizare a informațiilor către persoana vizată și, în acest caz, către titularul (titularii) răspunderii părintești, precum și modalitățile de exercitare a drepturilor persoanei vizate și posibila restrângere, dacă este cazul. În timpul elaborării propunerii pentru măsura legislativă respectivă, autoritatea națională de supraveghere trebuia să fie consultată.

2.3. Necesitatea și proporționalitatea - scopul/gravitatea infracțiunii/numărul de persoane neimplicate, dar afectate de prelucrare

Condiții și garanții pentru prelucrare

Compararea bazată pe recunoașterea facială poate fi efectuată de un funcționar autorizat numai în ultimă instanță, dacă nu sunt disponibile alte mijloace mai puțin intruzive și dacă este strict necesar, de exemplu, când există îndoieli cu privire la autenticitatea documentului de identitate al copilului minor care călătorește și/sau după ce au fost analizate dovezile anterioare și materialele colectate care indică o posibilă corespondență cu descrierea unui copil dispărut pentru care se efectuează o investigare.

O garanție suplimentară este oferită și prin revizuirea și verificarea obligatorie a comparării bazate pe recunoașterea facială de către un funcționar autorizat, pentru a corobora dovezile anterioare cu rezultatul comparării și pentru a exclude orice rezultate fals pozitive posibile.

Obiectivul urmărit

Crearea bazei de date servește unor obiective importante de interes public general, în special prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea pedepselor și protecția drepturilor și libertăților altor persoane. Crearea bazei de date și prelucrarea prevăzută par să contribuie la identificarea copiilor care sunt victime ale răpirii și, prin urmare, pot fi considerate o măsură adecvată de sprijin pentru obiectivul legitim de investigare și urmărire penală a acestor infracțiuni.

Scopul și popularea bazei de date

Scopurile prelucrării sunt definite în mod clar prin lege, iar baza de date se utilizează numai în scopul identificării copiilor dispăruți pentru care a fost raportată o suspiciune de răpire de copii și s-a deschis o investigație sub supravegherea unei autorități judiciare și pentru care a fost emisă o semnalare privind răpirea de copii. Condițiile stabilite prin lege pentru popularea bazei de date vizează limitarea strictă a numărului de persoane vizate și de date cu caracter personal care urmează să fie incluse în baza de date. Titularul răspunderii părintești asupra copilului trebuie informat cu privire la prelucrarea efectuată și la condițiile de exercitare a drepturilor copilului în ceea ce privește prelucrarea biometrică preconizată în scopul identificării sau cu privire la datele cu caracter personal ale copilului stocate în baza de date.

2.4. Concluzie

Având în vedere necesitatea și proporționalitatea prelucrării preconizate, precum și interesul superior al copilului în efectuarea acestei prelucrări a datelor cu caracter personal și cu condiția existenței unor garanții suficiente pentru a asigura în special exercitarea drepturilor persoanelor vizate – ținând seama îndeosebi de faptul că urmează să fie prelucrate date ale copiilor, această aplicare a prelucrării prin recunoaștere facială poate fi considerată ca fiind probabil compatibilă cu dreptul Uniunii.

În plus, având în vedere tipul de prelucrare și tehnologia utilizată, care implică un risc ridicat pentru drepturile și libertățile persoanei vizate în cauză, CEPD consideră că elaborarea unei propuneri de măsură legislativă care urmează să fie adoptată de un parlament național sau a unei măsuri de reglementare bazate pe o astfel de măsură legislativă, care se referă la prelucrarea preconizată, trebuie să includă o consultare prealabilă a autorității de supraveghere pentru a asigura consecvența și conformitatea cu cadrul juridic aplicabil, vezi articolul 28 alineatul (2) din LED.

3 SCENARIUL 3

3.1. Descriere

În cursul intervențiilor autorităților polițienești în timpul revoltelor și în cursul investigărilor ulterioare, o serie de persoane au fost identificate ca suspecte, de exemplu în urma unor investigări anterioare care au utilizat acoperirea prin TVCI sau martori. Fotografiile acestor suspecți sunt comparate cu fotografiile persoanelor care au fost înregistrate pe dispozitive TVCI sau dispozitive mobile la locul săvârșirii unei infracțiuni sau în zonele înconjurătoare.

Pentru a obține dovezi mai detaliate privind persoanele suspectate că au participat la revoltele din jurul unei demonstrații, autoritățile polițienești creează o bază de date formată din materiale sub

formă de imagini, cu o legătură locală și temporală slabă cu revoltele. Baza de date include înregistrări private încărcate pentru autoritățile polițienești de către cetățeni, materiale de la TVCI ale mijloacelor de transport în comun, materiale de supraveghere video deținute de autoritățile polițienești și materiale publicate de mass-media, fără nicio limitare sau protecție specifică. Manifestarea unui comportament infracțional grav nu este o condiție prealabilă pentru colectarea fișierelor în baza de date. Prin urmare, materiale cu persoanele care nu au fost implicate în revolte – un procent considerabil din populația locală care a trecut întâmplător pe acolo în momentul demonstrației sau a participat la demonstrație, dar nu și la revolte – sunt stocate în baza de date. Aceasta este formată din mii de fișiere video și imagine.

Cu ajutorul unui software de recunoaștere facială, toate fețele care apar în aceste fișiere sunt atribuite unor identificatori faciali unici. Fețele suspecților sunt apoi comparate automat cu acești identificatori faciali. Baza de date formată din toate modelele biometrice din miile de fișiere video și imagini este stocată până la încheierea tuturor investigărilor posibile. Rezultatele pozitive ale punerii în corespondență sunt analizate de către funcționarii responsabili, care decid apoi cu privire la acțiunile ulterioare. Acestea pot include asocierea fișierului găsit în baza de date cu dosarul penal al persoanei respective, precum și măsuri suplimentare, cum ar fi interogarea sau arestarea persoanei respective.

Legislația internă cuprinde o dispoziție generală potrivit căreia prelucrarea datelor biometrice în scopul identificării unice a unei persoane fizice este admisibilă dacă este strict necesară și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei în cauză.

Sursa informațiilor:

- Tipuri de persoane vizate: ☒ toate persoanele
- Sursa imaginii: ☒ spații accesibile publicului ☒ entitate privată ☒ alte persoane ☒ altele: mass-media
- Legătura cu infracțiunea: ☒ Nu este neapărat o legătură geografică sau temporală directă
- Modul de colectare a informațiilor: ☒ la distanță
- Context – afectează alte drepturi fundamentale: Da, și anume ☒ contextul libertății de întrunire
- Surse suplimentare de informații disponibile despre persoana vizată: ☒ altele: nu sunt excluse (de exemplu utilizarea ATM-urilor sau magazinele în care a intrat), deoarece nu se poate exercita niciun control asupra motivelor din imagini

Baza de date de referință (cu care se compară informațiile colectate):

- Specificitate: ☒ baze de date specifice legate de domeniul criminalității

Algoritm:

- Tipul de prelucrare: ☒ identificare realizată prin compararea mai multor serii de date

Rezultat:

- Impact: ☒ Direct (de exemplu, persoana vizată poate fi arestată, interogată)
- Decizie automatizată: ☒ NU
- Durata de stocare: până la încheierea tuturor investigărilor posibile

Analiza juridică:

- Tipul de informare prealabilă a persoanei vizate: ☒ Pe site-ul autorității de aplicare a legii în general
- Cadrul juridic aplicabil: ☒ LED transpusă în mare parte în dreptul intern ☒ Dreptul intern general pentru utilizarea datelor biometrice de către autoritățile de aplicare a legii

3.2. Cadrul juridic aplicabil

După cum s-a clarificat mai sus, temeiurile legale care nu fac decât să repete clauza generală prevăzută la articolul 10 din LED nu au prevederi suficient de clare pentru a da persoanelor fizice indicii adecvate în ceea ce privește condițiile și circumstanțele în care autoritățile de aplicare a legii sunt împuternicite să utilizeze înregistrările TVCI din spațiile publice pentru a crea un model biometric al feței lor și pentru a-l compara cu bazele de date ale autorităților polițienești, cu alte înregistrări TVCI disponibile sau cu înregistrări private etc. Prin urmare, cadrul juridic stabilit în acest scenariu nu îndeplinește cerințele minime pentru a servi ca temei legal.

3.3. Necesitatea și proporționalitatea

În acest exemplu, prelucrarea ridică numeroase probleme în temeiul principiilor necesității și proporționalității, din mai multe motive.

Persoanele nu sunt suspectate de săvârșirea unei infracțiuni grave. Manifestarea unui comportament infracțional grav nu este o condiție prealabilă pentru utilizarea fișierelor din baza de date care conțin materialele sub formă de imagini. De asemenea, o legătură temporală și geografică directă cu infracțiunea nu este o condiție prealabilă pentru utilizarea fișierelor din baza de date. Acest lucru duce la stocarea de materiale referitoare la un procent semnificativ al populației locale într-o bază de date biometrice pentru o durată care poate fi de mai mulți ani, până la încheierea tuturor investigărilor.

Baza de date de la locul săvârșirii unei infracțiuni nu se limitează la imaginile care îndeplinesc cerințele de proporționalitate, ceea ce duce la o cantitate nelimitată de imagini care trebuie comparate. Acest lucru contravine principiului reducerii la minimum a datelor. O cantitate mai mică de imagini ar permite, de asemenea, să se ia în considerare utilizarea altor mijloace decât algoritmii și mai puțin intruzive, de exemplu, a așa-numitelor persoane „super recognizers”.[88]

Întrucât exemplul este extras din contextul unui protest, este, de asemenea, probabil ca imaginile să dezvăluie opiniile politice ale participanților la demonstrație, fiind a doua categorie specială de date care ar putea fi afectate în acest scenariu. În acest scenariu nu este clar cum poate fi împiedicată colectarea acestor date și cu ce garanții. În plus, atunci când persoanele vizate află că participarea lor la o demonstrație a dus la introducerea lor într-o bază de date biometrice a autorităților polițienești, acest lucru poate avea efecte disuasive grave asupra exercitării viitoare de către acestea a dreptului lor la întrunire.

Modelele biometrice din baza de date pot fi comparate și între ele. Acest lucru permite autorităților polițienești nu numai să caute o anumită persoană în toate materialele lor, ci și să recreeze modelul de comportament al unei persoane pe o perioadă de mai multe zile. De asemenea, autoritățile polițienești pot colecta informații suplimentare despre persoane, cum ar fi contactele sociale și implicarea politică.

Atingerea adusă drepturilor este intensificată și mai mult de faptul că datele sunt prelucrate fără știrea persoanelor vizate.

Având în vedere că oamenii fac tot timpul fotografii și materiale video și că inclusiv acoperirea prin TVCI omniprezentă poate fi analizată biometric, acest lucru poate duce la efecte disuasive grave.

[88] Adică persoane cu o capacitate extraordinară de recunoaștere a fețelor. Vezi și: „Face Recognition by Metropolitan Police Super-Recognisers”, 26 februarie 2016, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

Utilizarea extensivă a fotografiilor și a materialelor video private, inclusiv utilizarea abuzivă potențială, cum ar fi denunțarea, este un alt motiv de îngrijorare. Întrucât utilizarea abuzivă, precum denunțarea, este un risc inerent și procedurilor penale în general, riscul este considerabil mai mare în ceea ce privește scalabilitatea datelor prelucrate și numărul persoanelor implicate, deoarece persoanele ar putea încărca și materiale referitoare la o anumită persoană sau la un grup de persoane pe care le antipatizează. Solicitările autorităților polițienești de a încărca fotografii și materiale video ar putea duce la praguri foarte scăzute pentru ca persoanele să furnizeze materiale, mai ales că acest lucru ar putea fi efectuat în mod anonim sau, cel puțin, fără a fi necesar ca o persoană să se prezinte și să se identifice la o secție de poliție.

3.4. Concluzie

În acest exemplu, nu există nicio dispoziție specifică care ar putea servi ca temei legal. Cu toate acestea, chiar dacă ar exista un temei legal suficient, cerințele de necesitate și proporționalitate nu ar fi îndeplinite, ceea ce ar duce la o atingere disproporționată adusă drepturilor persoanei vizate la respectarea vieții private și la protecția datelor cu caracter personal prevăzute de Cartă.

4 SCENARIUL 4

4.1. Descriere

Autoritățile polițienești pun în aplicare o modalitate de identificare prin TRF retrospectivă a persoanelor suspectate că au comis o infracțiune gravă surprinse de camerele de supraveghere video. Un funcționar al poliției selectează manual imaginea (imaginile) cu suspecții din materialul video care a fost colectat de la locul săvârșirii infracțiunii sau din altă parte în cadrul unei investigații preliminare și apoi trimite imaginea (imaginile) către departamentul de criminalistică. Departamentul de criminalistică utilizează TRF pentru a pune în corespondență această (aceste) imagine (imagini) cu fotografiile unor persoane pe care autoritățile polițienești le-au colectat anterior într-o bază de date (o așa-numită bază de date descriptivă formată din suspecți și foști condamnați). Pentru această procedură, baza de date descriptivă este analizată temporar și într-un mediu izolat cu ajutorul TRF pentru a putea efectua procesul de punere în corespondență. Pentru a reduce la minimum atingerea adusă drepturilor și intereselor persoanelor găsite prin corespondență, un număr foarte limitat de angajați din cadrul departamentului de criminalistică au permisiunea de a efectua procedura efectivă de punere în corespondență, accesul la date este limitat la acei funcționari cărora li s-a încredințat dosarul respectiv, iar un control manual al rezultatelor este efectuat înainte de a transmite orice rezultat funcționarului care efectuează investigarea. Datele biometrice nu sunt transmise în afara mediului controlat și izolat. Doar rezultatul și imaginea (și nu modelul biometric) sunt utilizate ulterior în cadrul investigării. Angajații primesc o formare specifică referitoare la normele și procedurile pentru această prelucrare, iar toate prelucrările de date cu caracter personal și de date biometrice sunt specificate suficient în dreptul intern.

Sursa informațiilor:

- Tipuri de persoane vizate: ☒ suspecți identificați din înregistrările camerelor de supraveghere video
- Sursa imaginii: ☒ spații accesibile publicului ☒ internet
- Legătura cu infracțiunea: ☒ Temporală directă
  ☒ Geografică directă
- Modul de colectare a informațiilor: ☒ la distanță

- Context – afectează alte drepturi fundamentale: Da, și anume: ☒ Libertatea de întrunire ☒ Libertatea de exprimare ☒ diverse: __

Baza de date de referință (cu care se compară informațiile colectate):

- Specificitate: ☒ baze de date specifice legate de domeniul criminalității

Algoritm:

- Tipul de prelucrare: ☒ identificare realizată prin compararea mai multor serii de date

Rezultat:

- Impact: ☒ Direct (de exemplu, persoana vizată este arestată, interogată)
- Decizie automatizată: ☒ NU

Analiza juridică:

- Cadrul juridic aplicabil: ☒ Legislația internă specifică pentru această prelucrare (recunoaștere facială) pentru autoritatea competentă respectivă

4.2. Cadrul juridic aplicabil

În acest scenariu, în dreptul intern se specifică că datele biometrice pot fi utilizate pentru efectuarea analizelor criminalistice când este strict necesar pentru realizarea scopului de identificare a persoanelor suspectate că au săvârșit o infracțiune gravă prin punerea în corespondență a imaginilor din baza de date descriptivă. Dreptul intern precizează datele care pot fi prelucrate, precum și procedurile de păstrare a integrității și a confidențialității datelor cu caracter personal și procedurile de distrugere a acestora, oferind astfel garanții suficiente împotriva riscului de abuz și de acțiuni arbitrare.

4.3. Necesitatea și proporționalitatea

Utilizarea recunoașterii faciale este în mod clar mai eficientă din punct de vedere al timpului decât punerea manuală în corespondență la nivel criminalistic. Selectarea manuală a imaginilor în prealabil limitează atingerile aduse drepturilor față de compararea tuturor materialelor video cu o bază de date și, prin urmare, diferențiază și vizează doar persoanele care intră sub incidența obiectivului, și anume combaterea infracțiunilor grave. Totuși este important să se analizeze dacă respectiva punere în corespondență poate fi efectuată manual într-un interval de timp rezonabil, în funcție de cazul avut în vedere. Impactul asupra drepturilor la viață privată și la protecția datelor se diminuează dacă un număr restrâns de persoane au acces la tehnologie și la datele cu caracter personal, precum și dacă modelele biometrice nu sunt stocate sau nu sunt folosite ulterior în cadrul investigării. Controlul manual al rezultatului înseamnă și reducerea riscului de rezultate fals pozitive.

4.4. Concluzie

Este important ca legislația națională să ofere un temei legal adecvat pentru prelucrarea datelor biometrice, precum și pentru baza de date națională cu care are loc punerea în corespondență. În acest scenariu au fost puse în aplicare mai multe măsuri pentru a limita atingerea adusă drepturilor de protecție a datelor, de exemplu condițiile de utilizare a TRF precizate în temeiul legal, numărul de persoane care au acces la tehnologie și la datele biometrice, controalele manuale etc. TRF îmbunătățește în mod semnificativ eficiența activității de investigare a departamentului criminalistic al autorităților polițienești, se bazează pe o legislație care permite autorităților polițienești să prelucreze date biometrice când este absolut necesar și, prin urmare, în aceste perimetre poate fi considerată o atingere legală adusă drepturilor persoanei.

5 SCENARIUL 5

5.1. Descriere

Identificarea biometrică la distanță este atunci când identitățile persoanelor sunt stabilite prin identificatori biometrici (imagine facială, mers, iris etc.) la distanță, într-un spațiu public și în mod continuu sau neîntrerupt, prin compararea acestora cu datele (biometrice) stocate într-o bază de date[89]. Identificarea biometrică la distanță se efectuează în timp real, în cazul în care colectarea materialelor sub formă de imagini, compararea și identificarea au loc fără întârzieri semnificative.

Înainte de fiecare implementare a identificării biometrice la distanță în timp real, poliția întocmește o listă de supraveghere a subiecților de interes în cadrul unei investigări. Aceasta este populată cu imagini faciale ale persoanelor. Pe baza informațiilor operative care sugerează că persoanele se vor afla într-o anumită zonă, de exemplu un centru comercial sau o piață publică, autoritățile polițienești decid când, unde și cât timp implementează identificarea biometrică la distanță.

În ziua acțiunii, se amplasează o furgonetă a poliției pe teren ca centru de comandă, cu un funcționar al poliției cu rang înalt la bord. Furgoneta conține monitoare care afișează înregistrări de la camerele de supraveghere video amplasate în apropiere, fie instalate ad-hoc, fie prin conectarea la fluxurile video ale camerelor de supraveghere deja instalate. Pe măsură ce pietonii trec prin fața camerelor de supraveghere, tehnologia izolează imaginile faciale, le convertește într-un model biometric și le compară cu modelele biometrice ale persoanelor aflate pe lista de supraveghere.

Dacă se detectează o corespondență potențială între lista de supraveghere și persoanele care trec prin fața camerelor de supraveghere, se transmite o semnalare funcționarilor din furgonetă, care apoi îi informează pe funcționarii de la fața locului dacă semnalarea este pozitivă, de exemplu, printr-un dispozitiv radio. Funcționarul de la fața locului decide apoi dacă intervine, dacă se apropie sau dacă, în cele din urmă, arestează persoana în cauză. Măsurile luate de funcționarul de pe teren sunt înregistrate. În cazul unui control discret, informațiile colectate (de exemplu, cine însoțește persoana, ce poartă persoana și locul spre care se îndreaptă) sunt stocate.

Legislația internă menționată cuprinde o dispoziție generală potrivit căreia prelucrarea datelor biometrice în scopul identificării unice a unei persoane fizice este admisibilă dacă este strict necesară și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei în cauză.

Sursa informațiilor:

- Tipuri de persoane vizate: ☒ toate persoanele
- Sursa imaginii: ☒ spații accesibile publicului
- Legătura cu infracțiunea: ☒ Nu este neapărat o legătură geografică sau temporală directă
- Modul de colectare a informațiilor: ☒ la distanță
- Context – afectează alte drepturi fundamentale: Da, și anume:☒ Libertatea de întrunire☒ Libertate de exprimare☒ diverse
- Surse suplimentare de informații disponibile despre persoana vizată:
  ☒ altele: nu sunt excluse (de exemplu utilizarea ATM-urilor sau magazinele în care a intrat)

Baza de date de referință (cu care se compară informațiile colectate):

- Specificitate: ☒ baze de date specifice legate de domeniul criminalității

Algoritm:

- Tipul de prelucrare: ☒ identificare realizată prin compararea mai multor serii de date

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Rezultat:

- Impact: ☒ Direct (de exemplu, persoana vizată este arestată, interogată)
- Decizie automatizată: ☒ NU
- Durata de stocare: până la încheierea tuturor investigărilor posibile

Analiza juridică:

- Tipul de informare prealabilă a persoanei vizate: ☒ Pe site-ul autorității de aplicare a legii în general
- Cadrul juridic aplicabil: ☒ LED transpusă în mare parte în dreptul intern ☒ Dreptul intern general pentru utilizarea datelor biometrice de către autoritățile de aplicare a legii

5.2. Cadrul juridic aplicabil

Temeiurile legale care nu fac decât să repete clauza generală prevăzută la articolul 10 din LED nu au prevederi suficient de clare pentru a oferi persoanelor fizice indicii adecvate în ceea ce privește condițiile și circumstanțele în care autoritățile de aplicare a legii sunt împuternicite să utilizeze înregistrările TVCI din spațiile publice pentru a crea un model biometric al feței lor și pentru a-l compara cu bazele de date ale autorităților polițienești. Prin urmare, cadrul juridic stabilit în acest scenariu nu îndeplinește cerințele minime pentru a servi ca temei legal.[90]

5.3. Necesitatea și proporționalitatea

Cu cât atingerea adusă drepturilor este mai profundă, cu atât mai ridicat este standardul în ceea ce privește necesitatea și proporționalitatea. Identificarea biometrică la distanță în spațiile publice are mai multe implicații asupra drepturilor fundamentale.

Scenariile presupun monitorizarea tuturor trecătorilor din spațiul public respectiv. Așadar, identificarea biometrică la distanță afectează grav așteptările rezonabile ale cetățenilor de a fi anonimi în spațiile publice[91]. Aceasta este o condiție prealabilă pentru multe fațete ale procesului democratic, precum decizia de a se alătura unei asociații civice, de a participa la adunări și de a întâlni persoane din toate mediile sociale și culturale, de a participa la un protest politic și de a vizita locuri de orice fel. Noțiunea de anonimat în spațiile publice este esențială pentru colectarea și schimbul liber de informații și idei. Acesta menține pluralismul de opinie, libertatea de întrunire pașnică și libertatea de asociere, precum și protecția minorităților și sprijină principiile separării puterilor și echilibrului puterilor. Subminarea noțiunii de anonimat în spațiile publice poate avea un efect disuasiv grav asupra cetățenilor. Aceștia se pot abține de la anumite comportamente care se încadrează pe deplin în limitele unei societăți libere și deschise. Acest lucru ar afecta interesul public, deoarece pentru o societate democratică sunt necesare autodeterminarea și participarea cetățenilor săi la procesul democratic.

În cazul în care se aplică o astfel de tehnologie, simplul fapt de a merge pe stradă, la metrou sau la brutărie în zona afectată va duce la colectarea de date cu caracter personal, inclusiv date biometrice, de către autoritățile de aplicare a legii și, în primul scenariu, și la punerea în corespondență cu bazele

[90] În cazurile în care un proiect științific care vizează cercetarea utilizării TRF ar trebui să prelucreze date cu caracter personal, dar această prelucrare nu ar intra sub incidența articolului 4 alineatul (3) din LED sau în domeniul de aplicare al dreptului Uniunii, s-ar aplica RGPD. În cazul proiectelor-pilot care ar fi urmate de operațiuni de aplicare a legii, LED s-ar aplica în continuare.

[91] Răspunsul CEPD adresat deputaților în Parlamentul European referitor la aplicația de recunoaștere facială dezvoltată de Clearview AI, 10 iunie 2020, ref.: OUT2020-0052.

de date ale autorităților polițienești. O situație în care același lucru s-ar realiza prin prelevarea amprentelor digitale ar fi în mod clar disproporționată.

Numărul de persoane vizate afectate este extrem de mare, deoarece este afectată orice persoană care trece prin zona publică respectivă. În plus, scenariile ar implica prelucrarea automată în masă a datelor biometrice și, de asemenea, o punere masivă în corespondență a datelor biometrice cu bazele de date ale autorităților polițienești.

În jurisprudența europeană, supravegherea în masă este interzisă (de exemplu, în cauza S. și Marper împotriva Regatului Unit, CEDO a considerat că păstrarea generalizată a datelor biometrice reprezintă o „atingere disproporționată" adusă dreptului la viață privată deoarece nu poate fi considerată „necesară într-o societate democratică").

Identificarea biometrică la distanță este atât de predispusă la supravegherea în masă, încât nu există mijloace fiabile de restricționare. Aceasta este în esență diferită de supravegherea video ca atare, deoarece utilizarea posibilă a înregistrărilor video fără identificare biometrică este deja o atingere puternică adusă drepturilor, dar totodată limitată, în timp ce, dacă se aplică TRF, sistemul de supraveghere video deja larg răspândit ca sursă principală de date va suferi o schimbare a calității. În plus, în special în ceea ce privește efectele disuasive implicate, eventualele restricții în aplicarea instalațiilor de supraveghere video deja existente nu vor fi vizibile și, prin urmare, nu vor beneficia de încrederea publicului.

Identificarea biometrică la distanță de către autoritățile polițienești îi tratează pe toți ca suspecți potențiali. Într-un stat de drept, se presupune însă că cetățenii sunt cinstiți până când poate fi dovedit comportamentul necorespunzător. Acest principiu este reflectat parțial și în LED, care subliniază necesitatea de a face distincție, în măsura posibilului, între tratamentul aplicat condamnaților penal sau suspecților, pentru care autoritățile de aplicare a legii trebuie să aibă „*motive serioase să [...] creadă că au săvârșit sau că urmează să săvârșească o infracțiune*" [articolul 6 litera (a) din LED], și cel aplicat persoanelor care nu sunt condamnate sau suspectate de activități infracționale.

Prin folosirea unei tehnologii capabile să identifice în mod unic o singură persoană, să urmărească și să analizeze locul unde se află aceasta și mișcările acesteia, aplicată în punctele nodale de transport sau în spațiile publice, autoritățile de aplicare a legii vor avea acces la cele mai sensibile informații despre o persoană (chiar și preferințele sexuale, religia, problemele de sănătate). Odată cu aceasta apare un risc imens de acces și de utilizare ilicită a datelor.

Instalarea unui sistem care permite descoperirea esenței comportamentului și a caracteristicilor persoanei duce la efecte disuasive puternice. Asta îi face pe cetățeni să se îndoiască dacă să participe sau nu la o anumită manifestații, ceea ce dăunează procesului democratic. De asemenea, întâlnirea și faptul de a fi văzut în public cu un anumit prieten cunoscut ca având probleme cu autoritățile polițienești sau care se comportă într-un mod unic ar putea fi considerate critice, deoarece toate acestea ar duce la atragerea algoritmului sistemului și, prin urmare, a autorităților de aplicare a legii.

Persoanele vizate vulnerabile, de exemplu copiii, sunt imposibil de protejat. În plus, sunt afectate persoanele care au un interes profesional – și adesea o obligație legală corespunzătoare – de a păstra confidențialitatea contactelor lor, de exemplu jurnaliștii, avocații și clerul. Acest lucru ar putea duce, de exemplu, la dezvăluirea sursei și a jurnalistului sau a faptului că o persoană consultă un avocat al apărării în materie penală. Această problemă nu se aplică doar pentru locurile publice aleatorii, unde se întâlnesc, de exemplu, jurnaliștii și sursele lor, ci, bineînțeles, și pentru spațiile publice necesare pentru a aborda și a avea acces la instituții sau profesioniști în această privință.

În plus, disconfortul creat cetățenilor de TRF îi poate determina să-și schimbe comportamentul, să evite locurile în care este implementată TRF și, astfel, să se retragă din viața socială și de la evenimentele culturale. În funcție de amploarea implementării TRF, impactul asupra cetățenilor poate fi atât de semnificativ încât să le afecteze capacitatea de a trăi o viață demnă[92].

Prin urmare, există o mare probabilitate de a afecta esența – nucleul intangibil – al dreptului la protecția datelor cu caracter personal. Indicii solide (vezi secțiunea 3.1.3.2 din ghid) sunt în special următoarele: pe scară largă, caracteristicile biologice unice ale persoanelor sunt prelucrate automat de către autoritățile de aplicare a legii cu ajutorul unor algoritmi care se bazează pe plauzibilitate, cu o explicabilitate limitată a rezultatelor. Dreptul la viață privată și dreptul la protecția datelor sunt restrânse indiferent de comportamentul individual al persoanei sau de circumstanțele care o privesc. Din punct de vedere statistic, aproape toate persoanele vizate afectate de această atingere adusă drepturilor sunt oameni care respectă legea. Există doar posibilități limitate de a furniza informații persoanei vizate. În majoritatea cazurilor, utilizarea căilor de atac va fi posibilă numai ulterior.

Dependența de un sistem bazat pe plauzibilitate și cu o explicabilitate limitată poate duce la diminuarea răspunderii și la lipsa căilor de atac și poate încuraja neglijența.

Odată ce un astfel de sistem, care poate fi aplicat și pentru camerele TVCI existente, este aplicat, cu foarte puține eforturi și fără a fi vizibil pentru oameni, el poate fi utilizat în mod abuziv și poate avea capacitatea de a întocmi în moc sistematic și rapid liste de persoane în funcție de originea etnică, sex, religie etc. Principiul prelucrării datelor cu caracter personal în funcție de criterii prestabilite, cum ar fi locul unde se află o persoană și traseul parcurs, este utilizat deja[93] și predispune la discriminare.

În funcție de sensibilitatea, expresivitatea și cantitatea datelor prelucrate, sistemele pentru recunoaștere facială la distanță în locuri accesibile publicului sunt predispuse la a fi utilizate în mod abuziv, cu efecte negative pentru oamenii respectivi. De asemenea, aceste date pot fi colectate cu ușurință și utilizate în mod abuziv pentru a pune presiune asupra actorilor-cheie în cadrul principiului echilibrului puterilor, cum ar fi opoziția politică, funcționari și jurnaliști.

În cele din urmă, sistemele bazate pe TRF tind să încorporeze prejudecăți puternice în ceea ce privește rasa și genul: rezultatele fals pozitive afectează în mod disproporționat persoanele de culoare și femeile[94], ceea ce duce la discriminare. Măsurile polițienești adoptate în urma unui rezultat fals pozitiv, cum ar fi perchezițiile și arestările, stigmatizează și mai mult aceste grupuri.

5.4. Concluzie

Scenariile menționate anterior privind prelucrarea la distanță a datelor biometrice în spații publice în scopuri de identificare nu asigură un echilibru just între interesele private și cele publice concurente, constituind astfel o atingere disproporționată adusă drepturilor persoanei vizate în temeiul articolelor 7 și 8 din Cartă.

---

92 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, pagina 20.

93 Vezi articolul 6 din 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 și articolul 33 din 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.

94 https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

6 SCENARIUL 6

6.1. Descriere

O entitate privată furnizează o aplicație în care imaginile faciale sunt extrase de pe internet pentru a crea o bază de date. Utilizatorul, de exemplu autoritățile polițienești, poate apoi să încarce o fotografie și, utilizând identificarea biometrică, aplicația va încerca să o pună în corespondență cu imaginile faciale sau cu modelele biometrice din baza sa de date.

Un departament de poliție local efectuează o investigare cu privire la o infracțiune surprinsă pe suport video, în care mai mulți potențiali martori și suspecți nu pot fi identificați prin punerea în corespondență a informațiilor colectate cu bazele de date interne sau cu informații operative. Pe baza informațiilor colectate, persoanele nu sunt înregistrate în nicio bază de date existentă a autorităților polițienești. Autoritățile polițienești decid să utilizeze un instrument precum cel descris mai sus, care este furnizat de o companie privată, pentru a identifica persoanele prin identificare biometrică.

Sursa informațiilor:

- Tipuri de persoane vizate: ☒ toți cetățenii (martori) ☒ condamnați ☒ suspecți
- Sursa imaginii: ☒ Înregistrări video dintr-un loc public sau colectate din altă parte în cadrul unei investigații preliminare
- Legătura cu infracțiunea: ☒ Nu este necesar
- Modul de colectare a informațiilor: ☒ la distanță
- Context – afectează alte drepturi fundamentale: Da, și anume:☒ Libertatea de întrunire☒ Libertate de exprimare☒ __ diverse:

Baza de date de referință (cu care se compară informațiile colectate):

- Specificitate: ☒ baze de date cu scop general populate de pe internet

Algoritm:

- Tipul de prelucrare: ☒ identificare realizată prin compararea mai multor serii de date

Rezultat:

- Impact ☒ Direct (de exemplu, persoana vizată este arestată, interogată, comportament discriminatoriu)
- Decizie automatizată: ☒ NU

Analiza juridică:

- Tipul de informare prealabilă a persoanei vizate: ☒ Nu

6.2. Cadrul juridic aplicabil

Atunci când o entitate privată furnizează un serviciu care include prelucrarea datelor cu caracter personal pentru care stabilește scopul și mijloacele (în acest caz, extragerea de imagini de pe internet pentru a crea o bază de date), această entitate privată trebuie să aibă un temei legal pentru această prelucrare. În plus, autoritatea de aplicare a legii care decide să utilizeze acest serviciu în scopurile sale trebuie să aibă un temei legal pentru prelucrarea pentru care stabilește scopurile și mijloacele. Pentru ca autoritatea de aplicare a legii să poată prelucra date biometrice trebuie să existe un cadru juridic care să specifice obiectivul, datele cu caracter personal care urmează să fie prelucrate, scopurile prelucrării și procedurile de păstrare a integrității și a confidențialității datelor cu caracter personal, precum și procedurile de distrugere a acestora.

Acest scenariu implică colectarea în masă a datelor cu caracter personal de la persoane care nu cunosc faptul că datele lor sunt colectate. O astfel de prelucrare ar putea fi legală numai în circumstanțe cu totul excepționale. În funcție de locul în care este situată baza de date, utilizarea unui astfel de serviciu poate implica transferul de date cu caracter personal și/sau de categorii speciale de date cu caracter personal în afara Uniunii Europene (de către autoritățile polițienești, de exemplu, „trimițând" imaginea facială din materialul video de supraveghere sau colectată în alt mod), ceea ce necesită, așadar, condiții specifice pentru acest transfer, vezi articolul 39 din LED.

Nu există norme specifice în acest scenariu care să permită prelucrarea de către autoritatea de aplicare a legii.

6.3. Necesitatea și proporționalitatea

Utilizarea serviciului de către autoritatea de aplicare a legii înseamnă că datele cu caracter personal sunt partajate cu o entitate privată care utilizează o bază de date în care datele cu caracter personal sunt colectate într-un mod nelimitat și în masă. Nu există nicio legătură între datele cu caracter personal colectate și obiectivul urmărit de autoritatea de aplicare a legii. Partajarea datelor de către autoritatea de aplicare a legii cu entitatea privată înseamnă, de asemenea, o lipsă de control din partea autorității asupra datelor prelucrate de entitatea privată și o mare dificultate pentru persoanele vizate de a-și exercita drepturile, deoarece acestea nu vor avea cunoștință de faptul că datele lor sunt prelucrate în acest mod. Acest lucru stabilește un standard foarte înalt pentru situațiile în care ar putea avea loc o astfel de prelucrare. Este discutabil dacă vreun obiectiv ar îndeplini cerințele prevăzute în directivă, deoarece orice derogări de la drepturile la viața privată și la protecția datelor și orice restrângeri ale acestor drepturi se aplică numai când este strict necesar. Interesul general legat de eficacitatea în combaterea infracțiunilor grave nu poate, în sine, să justifice prelucrarea atunci când cantități atât de mari de date sunt colectate în mod nediferențiat. Prin urmare, această prelucrare nu ar îndeplini cerințele de necesitate și de proporționalitate.

6.4. Concluzie

Lipsa unor norme clare, precise și previzibile care să îndeplinească cerințele prevăzute la articolele 4 și 10 din directivă, precum și lipsa dovezilor că această prelucrare este strict necesară pentru atingerea obiectivelor preconizate conduc la concluzia că utilizarea acestei aplicații nu ar îndeplini cerințele de necesitate și de proporționalitate și ar însemna o atingere disproporționată adusă drepturilor persoanelor vizate la respectarea vieții private și la protecția datelor cu caracter personal prevăzute de cartă.