GRUPUL DE LUCRU „ARTICOLUL 29” PENTRU PROTECŢIA DATELOR

00720/12/RO

WP193

Avizul 3/2012 privind progresele înregistrate de tehnologiile biometrice

Adoptat la 27 aprilie 2012

Rezumat

Sistemele biometrice sunt strâns legate de o persoană, întrucât acestea pot utiliza o anumită caracteristică unică a unei persoane în scopul identificării și/sau al autentificării. Datele biometrice ale unei persoane pot fi șterse sau modificate, în timp ce sursa din care au fost preluate acestea nu poate fi, în general, nici modificată, nici ștearsă.

Datele biometrice sunt utilizate cu succes și eficiență în cercetarea științifică, reprezintă un element-cheie al științei criminalistice și constituie un element valoros pentru sistemele de control al accesului. Acestea pot contribui la sporirea nivelului de securitate și pot face procedurile de identificare și autentificare mai ușoare, mai rapide și mai accesibile. În trecut, utilizarea acestei tehnologii era costisitoare și, ca urmare a acestei constrângeri economice, impactul său asupra dreptului persoanelor la protecția datelor era limitat. În ultimii ani, situația s-a schimbat semnificativ. Analiza ADN-ului a devenit mai rapidă și accesibilă aproape tuturor. Progresul tehnologic a determinat ieftinirea spațiului de stocare și a puterii de calcul, ceea ce a permis crearea de albume de fotografii online și de rețele de socializare cu miliarde de fotografii. Cititoarele de amprente și dispozitivele de supraveghere video au devenit necostisitoare. Dezvoltarea acestor tehnologii a contribuit la ieftinirea multor operațiuni, la soluționarea multor cauze de infracțiuni și la sporirea fiabilității sistemelor de control al accesului, însă a generat, de asemenea, noi amenințări pentru drepturile fundamentale. Discriminarea genetică a devenit o problemă reală. Furtul de identitate nu mai este o amenințare doar la nivel teoretic.

În timp ce alte noi tehnologii care vizează populații numeroase și care au stârnit de curând îngrijorare cu privire la protecția datelor nu se concentrează neapărat asupra stabilirii unei legături directe cu o anumită persoană – sau crearea acestei legături necesită un efort considerabil – datele biometrice, prin însăși natura lor, sunt legate în mod direct de o persoană. Acest fapt nu este întotdeauna un avantaj și implică mai multe neajunsuri. De exemplu, dotarea sistemelor de supraveghere video și a telefoanelor inteligente (smartphone) cu sisteme de recunoaștere facială care au drept suport bazele de date ale rețelelor de socializare ar putea însemna sfârșitul anonimatului și al circulației nelocalizate a persoanelor. Pe de altă parte, cititoarele de amprente, cititoarele modelelor de vene sau doar un zâmbet în fața unei camere video ar putea înlocui cardurile, codurile, parolele și semnăturile.

Prezentul aviz abordează aceste progrese și alte astfel de evoluții recente pentru a spori gradul de sensibilizare, atât a persoanelor vizate, cât și a organelor legislative. Aceste inovații tehnice, prezentate adesea ca tehnologii care nu fac decât să îmbunătățească experiența utilizatorului și să faciliteze utilizarea aplicațiilor, ar putea conduce la pierderea treptată a vieții private dacă nu se pun în aplicare măsuri de protecție adecvate. Prin urmare, prezentul aviz identifică măsuri tehnice și organizatorice care vizează diminuarea riscurilor la adresa protecției datelor și a vieții private și care pot contribui la prevenirea impactului negativ asupra vieții private a cetățenilor europeni și asupra dreptului fundamental al acestora la protecția datelor cu caracter personal.

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL

constituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

având în vedere articolul 29 și articolul 30 alineatul (1) litera (a) și alineatul (3) din directivă,

având în vedere regulamentul său de procedură,

ADOPTĂ PREZENTUL AVIZ:

1. Domeniul de aplicare a avizului

În Documentul de lucru din 2003 privind datele biometrice (WP80), Grupul de lucru „Articolul 29" („în continuare, grupul de lucru") a analizat aspectele legate de protecția datelor cu privire la utilizarea tehnologiilor viitoare, capabile să citească și să prelucreze electronic datele biometrice. În anii trecuți, această tehnologie a fost utilizată la scară largă atât în sectorul public, cât și în sectorul privat, apărând o serie de servicii noi. Tehnologiile biometrice, care necesitau altădată resurse financiare și informatice semnificative, au devenit mult mai ieftine și mai rapide. Utilizarea cititoarelor de amprente este acum un fapt obișnuit. De exemplu, unele laptopuri includ un cititor de amprentă pentru controlul biometric al accesului. Progresele înregistrate în analiza ADN-ului fac ca rezultatele să fie disponibile în câteva minute. Unele dintre tehnologiile create recent, cum ar fi recunoașterea modelului venelor sau recunoașterea facială, au ajuns deja la maturitate și sunt utilizate la tot pasul în viața noastră de zi cu zi. Tehnologiile biometrice sunt strâns legate de anumite caracteristici ale unei persoane și unele dintre ele pot fi utilizate pentru a divulga date sensibile. În plus, multe dintre aceste tehnologii permit urmărirea, localizarea și stabilirea profilelor persoanelor în mod automat și, prin urmare, au un impact potențial ridicat asupra vieții private și asupra dreptului persoanelor la protejarea datelor lor cu caracter personal. Impactul lor este cu atât mai mare cu cât astfel de tehnologii sunt în plină dezvoltare. Este probabil ca fiecare persoană să fie înscrisă în unul sau mai multe sisteme biometrice.

Prezentul aviz își propune să prezinte un cadru revizuit și actualizat de orientări și recomandări generale armonizate cu privire la punerea în aplicare a principiilor referitoare la viața privată și la protecția datelor în aplicațiile biometrice. Avizul se adresează autorităților legislative europene și naționale, industriei sistemelor biometrice și utilizatorilor acestor tehnologii.

2. Definiții

Problema tehnologiilor biometrice nu este nouă, aceasta fiind deja abordată în diferite avize ale grupului de lucru. Această secțiune urmărește să prezinte definițiile relevante și informații actualizate atunci când este necesar.

Date biometrice: Conform celor arătate de grupul de lucru în avizul 4/2007 (WP136), datele biometrice pot fi definite după cum urmează:

„proprietăți biologice, aspecte comportamentale, caracteristici fiziologice, trăsături vitale sau acțiuni repetate, atât trăsăturile cât și/sau acțiunile fiind caracteristice persoanei și fiind măsurabile, chiar dacă modelele utilizate în practică pentru măsurarea din punct de vedere tehnic a acestora implică un anumit grad de probabilitate."

Datele biometrice modifică în mod irevocabil relația dintre corp și identitate, întrucât, pe baza acestor date, caracteristicile corpului uman pot fi „citite" de un dispozitiv și pot fi folosite ulterior.

Datele biometrice pot fi stocate și prelucrate sub diferite forme. Uneori, datele biometrice colectate de la o persoană sunt stocate și prelucrate într-o formă brută, care permite recunoașterea sursei din care au provenit, fără alte informații speciale, de exemplu fotografia unui chip, fotografia unei amprente sau o înregistrare vocală. Alteori, informațiile biometrice brute colectate sunt prelucrate astfel încât doar anumite caracteristici și/sau trăsături sunt extrase și salvate ca model biometric.

Sursă de date biometrice: Sursele de date biometrice sunt foarte variate și includ aspecte fizice, fiziologice, comportamentale sau psihologice ale unei persoane. Conform avizului 4/2007 (WP136):

„sursele din care se obțin datele biometrice (de exemplu, probele de țesut uman) nu constituie în ele însele date biometrice,însă pot fi utilizate pentru a obține date biometrice (prin extragerea de informații din acestea)."

Astfel cum se arată în WP80, există două categorii principale de tehnici biometrice:

- în primul rând, există tehnici bazate pe caracteristici fizice și **fiziologice,** care măsoară caracteristicile fizice și fiziologice ale unei persoane și care includ: verificarea amprentelor digitale, analiza imaginii degetului, recunoașterea irisului, analiza retinei, recunoașterea facială, modelul conturului mâinii, recunoașterea formei urechilor, detectarea mirosului corporal, recunoașterea vocală, analiza tiparului ADN, analiza porilor sudoripari etc.;
- în al doilea rând, există tehnici bazate pe aspecte **comportamentale**, care evaluează comportamentul unei persoane, incluzând verificarea semnăturii olografe, analiza modului de tastare, analiza mersului, modul de a merge sau de a se mișca, tipare comportamentale care indică gânduri din subconștient, precum faptul de a minți etc.

Trebuie menționate, de asemenea, o serie de tehnici de natură **psihologică**, aflate în curs de dezvoltare, care se referă la măsurarea reacțiilor la situații concrete sau la teste specifice, pentru includerea într-un anumit profil psihologic.

Model biometric: Din forma brută a datelor biometrice se pot extrage caracteristici cheie (de exemplu, măsurători faciale în baza unei imagini), iar acestea pot fi stocate pentru a fi prelucrate ulterior, nemaifiind necesară stocarea datelor brute. Acesta reprezintă modelul biometric al datelor. Definirea dimensiunilor modelului (cantitatea de informații) constituie un aspect esențial. Pe de o parte, modelul trebuie să fie suficient de cuprinzător pentru a fi sigur (pentru a evita suprapunerile dintre diferite date biometrice sau substituțiile de identitate) și, pe de altă parte, acesta nu trebuie să fie prea larg, astfel încât să se evite riscul reconstrucției datelor biometrice. Generarea modelului trebuie să fie un proces unidirecțional,

în sensul că nu trebuie să existe posibilitatea recreării datelor biometrice brute pe baza modelului.

Sisteme biometrice: Conform WP80, sistemele biometrice sunt:

> *„aplicații care utilizează tehnologii biometrice, care permit identificarea automată și/sau autentificarea/verificarea unei persoane. Aplicațiile de autentificare/verificare sunt utilizate adesea pentru diverse activități în domenii complet diferite, în scopuri diferite și sub autoritatea unei game diferite de entități."*

Datorită evoluțiilor tehnice recente, în prezent utilizarea sistemelor biometrice în scopuri de clasificare/segregare este, de asemenea, posibilă.

Riscurile pe care le implică sistemele biometrice provin din însăși natura datelor biometrice prelucrate. Prin urmare, o definiție mai generală ar fi următoarea: un sistem care extrage și prelucrează ulterior datele biometrice.

Prelucrarea datelor biometrice în cadrul unui sistem biometric implică, de obicei, diferite procese precum înregistrarea, stocarea, compararea și identificarea:

- Înregistrarea datelor biometrice: Cuprinde toate procesele desfășurate în cadrul unui sistem biometric cu scopul de a extrage datele biometrice dintr-o sursă de date biometrice și de a lega datele respective de o persoană. Cantitatea și calitatea datelor necesare în timpul înregistrării trebuie să fie suficiente pentru a permite identificarea, autentificarea, clasificarea sau verificarea exactă a persoanei, fără înregistrarea unei cantități excesive de date. Cantitatea de date extrase dintr-o sursă biometrică în timpul etapei de înregistrare trebuie să fie adaptată scopului prelucrării și nivelului de performanță a sistemului biometric.

Etapa de înregistrare reprezintă, de obicei, primul contact al unei persoane cu un anumit sistem biometric. În majoritatea cazurilor, înregistrarea necesită participarea persoanei (de exemplu, în cazul prelevării amprentelor), prin urmare, aceasta poate constitui o oportunitate adecvată de a oferi informații și o notificare privind prelucrarea corectă a datelor cu caracter personal. Cu toate acestea, persoanele pot fi înscrise fără știrea sau consimțământul lor (de exemplu, sistemele CCTV cu funcție de recunoaștere facială încorporată). Acuratețea și securitatea procesului de înregistrare sunt esențiale pentru performanța întregului sistem. O persoană se poate înregistra din nou într-un sistem biometric pentru a-și actualiza datele biometrice înregistrate.

- Stocarea datelor biometrice: Datele obținute în timpul etapei de înregistrare pot fi stocate la nivel local în centrul de operațiuni în care a avut loc înregistrarea (de exemplu, într-un cititor) pentru a fi utilizate ulterior, sau pe un dispozitiv aflat asupra persoanei (de exemplu, un card inteligent) sau pot fi trimise și stocate într-o bază de date centralizată, accesibilă pentru unul sau mai multe sisteme biometrice.

- Compararea datelor biometrice: Acesta constituie procesul de comparare a datelor sau a modelului biometric (colectat în etapa de înregistrare) cu datele sau modelul biometric obținut dintr-o probă nouă, în scopul identificării, al verificării/autentificării sau al clasificării.

Identificarea biometrică: Identificarea unei persoane cu ajutorul unui sistem biometric este, de obicei, procesul prin care se compară datele biometrice ale unei persoane (colectate în

momentul identificării) cu o serie de modele biometrice stocate într-o bază de date (mai precis, un proces de comparare a unei serii de date cu mai multe serii de date).

Verificare/autentificare biometrică: Verificarea unei persoane cu ajutorul unui sistem biometric este, în general, procesul de comparare a datelor biometrice ale unei persoane (obținute în momentul verificării) cu un singur model biometric stocat într-un dispozitiv (mai exact, un proces de comparare unu-la-unu).

Clasificare/segregare biometrică: Clasificarea/segregarea unei persoane cu ajutorul unui sistem biometric este, de obicei, procesul prin care se stabilește dacă datele biometrice ale unei persoane aparțin unui grup cu caracteristici predefinite, în scopul întreprinderii unei anumite acțiuni. În acest caz, nu este important ca persoana să fie identificată sau verificată, ci ca aceasta să fie inclusă în mod automat într-o anumită categorie. De exemplu, un afișaj publicitar poate prezenta diferite reclame în funcție de persoana care îl privește, pe baza criteriilor de vârstă sau sex.

Biometria multimodală: Aceasta poate fi definită ca o combinație între diferite tehnologii biometrice menită să crească acuratețea sau performanța sistemului (aceasta mai este numită și biometrie pe mai multe niveluri). Sistemele biometrice utilizează două sau mai multe trăsături/modalități biometrice ale aceleiași persoane în procesul de comparare. Astfel de sisteme pot lucra în diferite moduri, fie prin colectarea diverselor date biometrice cu ajutorul unor senzori diferiți, fie prin colectarea de unități multiple ale acelorași date biometrice. Unele studii includ în această categorie și sistemele care efectuează citiri multiple ale acelorași date biometrice sau cele care utilizează algoritmi multipli pentru extragerea de caracteristici din aceeași probă biometrică. Exemple de sisteme biometrice multimodale sunt pașapoartele electronice la nivelul UE și *US-VISIT Biometric Identification Services* (Servicii de identificare biometrică) în Statele Unite.

Acuratețea: Atunci când se utilizează sistemele biometrice, este dificil să se obțină rezultate 100% fără erori. Aceasta se poate datora diferențelor de mediu în momentul colectării datelor (lumină, temperatură etc.) sau diferențelor dintre echipamentele utilizate (camere video, dispozitive de scanare etc.). Cele mai utilizate instrumente convenționale de măsurare a performanței sunt rata de acceptare falsă (False Accept Rate - FAR) și rata de respingere falsă (False Reject Rate - FRR), acestea putând fi adaptate la sistemul utilizat:

- rata de acceptare falsă este probabilitatea ca un sistem biometric să identifice în mod incorect o persoană sau să nu respingă un impostor. Aceasta măsoară procentajul de date nevalide care sunt acceptate în mod eronat, fiind cunoscută, de asemenea, sub numele de rată fals pozitivă („false positive rate”).

- rata de respingere falsă este probabilitatea ca un sistem să respingă în mod eronat date valide. Respingerea falsă are loc atunci când nu se stabilește corespondența între o persoană și propriul său model biometric existent. Aceasta este cunoscută, de asemenea, sub numele de rată fals negativă („false negative rate”).

Dacă sistemul este reglat și setat în mod corespunzător, erorile critice ale sistemelor biometrice pot fi reduse până la nivelul acceptat pentru utilizarea operațională prin micșorarea riscului de analiză eronată. Un sistem perfect are valoarea zero pentru FAR și FRR, însă, de obicei, acestea sunt corelate negativ. Atunci când crește FAR, scade nivelul FRR.

Este important să se țină seama de scopul prelucrării, de FAR, FRR și de mărimea populației atunci când se evaluează dacă acuratețea unui anumit sistem biometric este acceptabilă sau nu. În plus, în evaluarea acurateței unui sistem biometric, trebuie să se țină seama și de capacitatea de a detecta o mostră vie. De exemplu, amprentele digitale pot fi copiate și utilizate pentru a crea degete false. Un cititor de amprente nu trebuie să poată efectua o identificare pozitivă într-o astfel de situație.

3. Analiza juridică

Cadrul juridic relevant este constituit de Directiva privind protecția datelor (95/46/CE). Grupul de lucru a afirmat deja în WP80 că datele biometrice sunt, în majoritatea cazurilor, date cu caracter personal. Prin urmare, datele pot fi prelucrate numai dacă există un temei legal și dacă prelucrarea este adecvată, relevantă și nu este excesivă față de scopurile în care acestea sunt colectate și/sau prelucrate ulterior.

Scopul

O condiție prealabilă pentru utilizarea biometriei este definirea clară a scopului în care sunt colectate și prelucrate datele biometrice, având în vedere riscurile pentru protecția drepturilor și libertăților fundamentale ale persoanelor.

Datele biometrice pot fi colectate, de exemplu, pentru a asigura sau spori securitatea sistemelor de prelucrare prin aplicarea de măsuri adecvate pentru protecția datelor cu caracter personal împotriva accesării nepermise. În principiu, se pot implementa măsuri de securitate adecvate, bazate pe trăsăturile biometrice ale persoanelor însărcinate cu prelucrarea datelor, pentru a asigura un nivel de securitate corespunzător riscurilor aferente prelucrării și naturii datelor cu caracter personal care trebuie protejate. Cu toate acestea, trebuie să se aibă în vedere că utilizarea biometriei în sine nu asigură o securitate sporită, deoarece multe date biometrice pot fi obținute fără știrea persoanei vizate. Cu cât nivelul de securitate urmărit este mai înalt, cu atât mai puține date biometrice izolate vor putea apărea în acest scop.

Principiul limitării scopului trebuie să fie respectat, alături de celelalte principii referitoare la protecția datelor; trebuie să se țină seama, în special, de principiul proporționalității, al necesității și al reducerii la minim a datelor atunci când se definesc diferitele scopuri ale unei aplicații. Atunci când este posibil, persoana vizată trebuie să aibă posibilitatea de a alege între mai multe scopuri ale unei aplicații cu funcții multiple, în special dacă una sau mai multe dintre funcții presupune prelucrarea datelor biometrice.

Exemplu:
Utilizarea dispozitivelor electronice care efectuează proceduri de autentificare specifice pe baza datelor biometrice a fost recomandată în legătură cu măsurile de securitate necesare pentru:

- prelucrarea datelor cu caracter personal obținute de operatorii de telefonie în timpul activităților de ascultare a convorbirilor autorizate de către instanță;
- accesul la datele referitoare la trafic (și la datele referitoare la locație) colectate din ordinul instanței de către furnizorii de servicii publice de comunicații electronice sau de către o rețea publică de comunicații, precum și accesul în unitățile relevante în care sunt prelucrate aceste date;

- colectarea și stocarea datelor genetice și a probelor biologice.

Fotografiile de pe internet, din rețelele de socializare, din aplicațiile online de gestionare sau transmitere a fotografiilor nu pot fi prelucrate ulterior în vederea extragerii de modele biometrice sau a înregistrării acestora într-un sistem biometric cu scopul de a recunoaşte în mod automat persoanele din fotografii (recunoaştere facială), fără să existe un temei legal (de exemplu, consimțământul) pentru acest scop. Dacă există un temei legal pentru acest scop secundar, prelucrarea trebuie să fie, în plus, adecvată, relevantă și să nu fie excesivă în raport cu scopul respectiv. Chiar dacă o persoană furnizoare de date a acceptat ca fotografiile în care apare să fie prelucrate pentru ca aceasta să fie identificată în mod automat într-un album de fotografii online cu algoritm de recunoaștere facială, prelucrarea trebuie să fie realizată cu respectarea caracterului personal al datelor: datele biometrice care nu mai sunt necesare după atașarea la fotografii a numelui, a numelui de utilizator sau a altui text cerut de persoana vizată trebuie să fie șterse. Crearea unei baze de date biometrice permanentă nu este necesară *a priori* pentru acest scop.

Proporţionalitatea

Utilizarea biometriei ridică problema proporționalității fiecărei categorii de date prelucrate în lumina scopului în care sunt prelucrate acestea. Având în vedere faptul că datele biometrice pot fi utilizate numai dacă sunt adecvate, relevante și neexcesive, trebuie să se evalueze cu exactitate necesitatea și proporționalitatea datelor prelucrate și să se analizeze dacă scopul urmărit ar putea fi atins într-un mod mai puțin intruziv.

În evaluarea proporționalității unui sistem biometric dat, trebuie să se analizeze mai întâi dacă sistemul este necesar pentru satisfacerea necesității identificate, mai precis dacă principalul criteriu luat în considerare este satisfacerea necesității respective și nu faptul că sistemul biometric este cel mai la îndemână sau cel mai eficient din punct de vedere al costurilor. În al doilea rând, trebuie să se analizeze dacă sistemul poate fi eficient în ceea ce privește îndeplinirea scopului urmărit prin considerarea caracteristicilor specifice ale tehnologiei biometrice care urmează a fi utilizată[1]. În al treilea rând, trebuie să se evalueze dacă detrimentul produs vieții private a persoanelor vizate este proporțional cu beneficiile anticipate. Dacă beneficiile sunt relativ mici, precum creșterea facilității de utilizare sau o ușoară scădere a costurilor, detrimentul produs vieții private nu este justificat. Cel de-al patrulea aspect care trebuie luat în considerare în evaluarea oportunității introducerii unui sistem biometric este dacă există o altă modalitate mai puțin intruzivă pentru viața privată prin care ar putea să se atingă scopul urmărit[2].

[1] Biometria este folosită fie în scop de verificare, fie în scop de identificare: un identificator biometric ar putea fi considerat adecvat din punct de vedere tehnic pentru unul dintre scopuri și neadecvat pentru celălalt (de exemplu, tehnologiile caracterizate de o rată scăzută de respingere falsă ar trebui să fie preferate în sisteme destinate identificării persoanelor în aplicarea legii).

[2] De exemplu, cardurile inteligente sau alte metode care nu colectează sau centralizează informații biometrice în scop de autentificare.

Exemplu:
Într-un club de sănătate şi fitness, se instalează un sistem biometric centralizat bazat pe colectarea amprentelor digitale, cu scopul de permite accesul la sălile de fitness şi la alte servicii aferente numai clienţilor care au plătit taxa corespunzătoare.
Pentru funcţionarea acestui sistem, este necesar să se stocheze amprentele tuturor clienţilor şi ale membrilor personalului. Această aplicaţie biometrică pare disproporţionată în raport cu necesitatea de a controla accesul în club şi de a gestiona clienţii plătitori. Se pot imagina cu uşurinţă alte mijloace, precum o simplă listă de verificare sau etichete RFID sau un card magnetic, care nu necesită prelucrarea datelor biometrice şi care sunt la fel de practice şi de eficiente.

Grupul de lucru avertizează în legătură cu riscurile implicate de utilizarea datelor biometrice în scopul identificării în cadrul unor baze de date centralizate extinse, având în vedere consecinţele potenţial negative asupra persoanelor vizate.

Trebuie să se ţină seama de impactul major al acestor sisteme asupra demnităţii umane a persoanelor vizate şi de implicaţiile lor asupra drepturilor fundamentale. În lumina Convenţiei europene pentru apărarea drepturilor omului şi a libertăţilor fundamentale, precum şi a jurisprudenţei Curţii Europene a Drepturilor Omului privind articolul 8 din convenţie, grupul de lucru arată că orice încălcare a dreptului la protecţia datelor este permisă numai cu condiţia să respecte legea şi să fie necesară, într-o societate democratică, pentru protejarea unui interes public important[3].

Pentru a asigura respectarea acestor condiţii, este necesar să se precizeze scopul urmărit de sistem şi să se evalueze proporţionalitatea datelor care urmează să fie introduse în sistem în raport cu scopul respectiv.

Pentru aceasta, operatorul trebuie să stabilească dacă prelucrarea, mecanismele de prelucrare, categoriile de date care urmează a fi colectate şi prelucrate şi transferul informaţiilor din baza de date sunt necesare şi indispensabile. Măsurile de securitate adoptate trebuie să fie adecvate şi eficiente. Operatorul trebuie să aibă în vedere drepturile de care beneficiază persoanele ale căror date personale sunt colectate şi să se asigure că aplicaţia conţine un mecanism adecvat pentru exercitarea acestor drepturi.

Exemplu:
Utilizarea datelor biometrice în scopul identificării. Sistemele care analizează chipul unei persoane, precum şi cele care analizează ADN-ul unei persoane, pot contribui în mod foarte eficient la lupta împotriva infracţiunilor şi pot dezvălui identitatea unei persoane necunoscute, suspectate de săvârşirea unei infracţiuni grave. Cu toate acestea, utilizarea acestor sisteme la scară largă determină efecte secundare importante. În cazul recunoaşterii faciale, unde datele biometrice pot fi colectate cu uşurinţă, fără cunoştinţa persoanei vizate, utilizarea la scară largă ar însemna sfârşitul anonimatului în spaţiile publice şi ar permite localizarea constantă a persoanelor. În cazul datelor referitoare la ADN, utilizarea acestei tehnologii implică riscul ca datele sensibile privind sănătatea unei persoane să fie divulgate.

[3] A se vedea Curtea de Justiţie a Uniunii Europene, Hotărârea din 20 mai 2003 în cauzele comune C-465/00, C-138/01 şi C-139/01 (Rechnungshof c. Österreichischer Rundfunk şi alţii), Curtea Europeană a Drepturilor Omului, Hotărârea din 4 decembrie 2008, cererile nr. 30562/04 şi 30566/04 (S. şi Marper c. Regatul Unit) şi Hotărârea din 19 iulie 2011, cererile nr. 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 şi 64027/09 (Goggins şi alţii c. Regatul Unit).

Acuratețea

Datele biometrice prelucrate trebuie să fie exacte și relevante în raport cu scopul în care sunt colectate. Datele trebuie să fie exacte atât în momentul înregistrării, cât și în momentul în care se stabilește legătura între persoană și datele biometrice. Acuratețea datelor în momentul înregistrării este importantă, de asemenea, pentru prevenirea uzurpării de identitate.

Datele biometrice sunt unice și cele mai multe dintre acestea generează un model sau o imagine unică. Dacă sunt utilizate la scară largă, în special pentru o parte substanțială dintr-o populație, datele biometrice pot fi considerate un identificator cu aplicabilitate generală în sensul Directivei 95/46/CE. În acest caz, s-ar aplica dispozițiile articolului 8 alineatul (7) din Directiva 95/46/CE, iar statele membre ar trebui să determine condițiile în care se efectuează prelucrarea.

Reducerea la minim a datelor

O dificultate specifică poate rezulta din faptul că datele biometrice conțin adesea mai multe informații decât este necesar pentru funcția de comparare. Principiul reducerii la minim a datelor trebuie să fie pus în aplicare de către operatorul de date. În primul rând, aceasta înseamnă că numai informațiile cerute, și nu toate informațiile disponibile, ar trebui să fie prelucrate, transmise sau stocate. În al doilea rând, operatorul de date ar trebui să se asigure că protecția datelor este promovată de însăși configurația predefinită și că nu mai este necesar să ia măsuri specifice în acest sens.

Perioada de reținere

Operatorul trebuie să stabilească o perioadă de reținere pentru datele biometrice, care nu trebuie să fie mai lungă decât este necesar pentru scopul în care acestea au fost colectate sau în care sunt prelucrate în continuare. Operatorul trebuie să se asigure că datele sau profilele rezultate din datele biometrice sunt șterse definitiv după scurgerea perioadei de timp justificate.

Trebuie să se facă o diferență clară între datele cu caracter personal de natură generală, care pot fi necesare pentru o perioadă mai lungă de timp, și datele biometrice care nu mai sunt utile, de exemplu, atunci când persoana vizată nu mai are acces la o anumită zonă.

Exemplu:
Un angajator a pus în funcțiune un sistem biometric pentru a controla accesul la o zonă cu acces restricționat. Atribuțiile unui angajat nu-i mai cer să acceseze zona respectivă (de exemplu, își schimbă locul de muncă sau responsabilitățile). În acest caz, datele sale biometrice trebuie să fie șterse, întrucât scopul în care au fost colectate nu mai este valabil.

3.1. Temeiul legal

Prelucrarea datelor biometrice trebuie să se bazeze pe unul dintre temeiurile legale menționate la articolul 7 din Directiva 95/46/CE.

3.1.1. Consimțământul, articolul 7 alineatul (a)

Primul temei legal, menționat la articolul 7 litera (a), este constituit de acordarea consimțământului de către persoana vizată. Conform Directivei privind protecția datelor, articolul 2 litera (h), consimțământul trebuie să fie o manifestare de voință liberă, specifică și

informată a persoanei vizate. Trebuie să fie clar că un astfel de consimțământ nu poate fi obținut în mod liber prin acceptarea obligatorie a unor termeni și condiții generale sau prin opțiunea de neparticipare. În plus, consimțământul trebuie să fie revocabil. În această privință, în avizul său privind definiția consimțământului, grupul de lucru subliniază diferite aspecte importante ale acestei noțiuni: validitatea consimțământului, dreptul persoanelor de a-și retrage consimțământul; consimțământul acordat înainte de începerea prelucrării; cerințe privind calitatea și accesibilitatea informațiilor[4].

În multe cazuri de prelucrare a datelor biometrice, în lipsa unei alternative valabile, precum o parolă sau un card magnetic, consimțământul nu poate fi considerat liber exprimat. De exemplu, un sistem a cărui utilizare ar descuraja persoanele vizate (de exemplu, deoarece necesită prea mult timp sau este prea complicată) nu poate fi considerat o alternativă valabilă, prin urmare, acesta nu ar determina un consimțământ valabil.

Exemplu:
În lipsa altor temeiuri legale alternative, un sistem biometric de autentificare poate fi utilizat pentru a controla accesul la un club video numai dacă clienții sunt liberi să decidă dacă doresc sau nu să utilizeze sistemul respectiv. Aceasta înseamnă că proprietarul clubului trebuie să le pună la dispoziție mecanisme alternative, mai puțin intruzive pentru viața privată. Un astfel de sistem permite unui client care nu dorește sau nu poate să se supună amprentării din cauza unor circumstanțe personale să nu își acorde consimțământul. Simplul fapt că o persoană are de ales între furnizarea datelor sale biometrice și neutilizarea unui serviciu arată clar că acordarea consimțământului nu a fost liberă și aceasta nu poate fi considerată temei legitim.

Într-o grădiniță, se instalează un scanner de modele de vene, pentru a verifica dacă fiecare adult care intră (părinți și membri ai personalului) are sau nu drept de acces. Pentru funcționarea acestui sistem, este necesară stocarea amprentelor tuturor părinților și membrilor personalului. Consimțământul ar fi un temei legal contestabil, în special pentru angajați, întrucât aceștia nu ar avea posibilitatea reală de a refuza utilizarea unui astfel de sistem. De asemenea, aceasta ar reprezenta o situație problematică pentru părinți, de vreme ce nu există o metodă alternativă de a intra în grădiniță.

Deși există prezumția că dezechilibrul tipic dintre angajator și angajat poate afecta caracterul liber al consimțământului, grupul de lucru nu exclude acest tip de consimțământ „*cu condiția să existe suficiente garanții privind exprimarea cu adevărat liberă a consimțământului*”[5].

Prin urmare, în contextul relației angajat-angajator, consimțământul trebuie să fie pus sub semnul întrebării și justificat în mod corespunzător. În loc să încerce să obțină consimțământul angajaților, angajatorii ar putea să cerceteze dacă este cu adevărat necesar să utilizeze datele biometrice ale angajaților într-un scop legitim și să evalueze această necesitate în raport cu drepturile și libertățile fundamentale ale angajaților. În situațiile în care necesitatea utilizării datelor biometrice poate fi demonstrată în mod corespunzător, temeiul legal al prelucrării ar putea fi reprezentat de interesul legitim al operatorului, astfel cum este definit la articolul 7 litera (f) din Directiva 95/46/CE. Angajatorul trebuie să caute întotdeauna metoda cea mai puțin intruzivă, prin alegerea unui proces care nu implică prelucrarea datelor biometrice, dacă acest lucru este posibil.

4 WP 187, Avizul 15/2011 privind definiția consimțământului.

5 WP 187, Avizul 15/2011 privind definiția consimțământului.

Cu toate acestea, astfel cum se arată în secțiunea 3.1.3, pot exista situații în care introducerea unui sistem biometric poate fi în interesul legitim al operatorului. În aceste situații, consimțământul nu este necesar.

Consimțământul este valabil numai atunci când se furnizează informații suficiente cu privire la utilizarea datelor biometrice. Având în vedere faptul că datele biometrice pot fi utilizate ca identificator unic și universal, furnizarea de informații clare și ușor accesibile privind modul în care sunt utilizate datele specifice trebuie să fie considerată ca absolut necesară pentru garantarea unei prelucrări corecte. Prin urmare, această cerință este esențială pentru un consimțământ valabil în utilizarea datelor biometrice.

Exemple:
Pentru a obține un consimțământ valabil în vederea instalării unui sistem de control al accesului pe bază de amprente digitale, persoanele vizate trebuie să fie informate dacă sistemul biometric creează sau nu un model unic recunoscut de sistemul respectiv. Dacă se utilizează un algoritm care generează același model biometric în diferite sisteme biometrice, persoana vizată trebuie să știe că poate fi recunoscută în cadrul mai multor sisteme biometrice diferite.

O persoană își încarcă fotografia într-un album de fotografii pe internet. Înregistrarea fotografiei într-un sistem biometric necesită consimțământul explicit al persoanei respective, bazat pe informații complete privind utilizarea datelor biometrice, durata și scopul prelucrării acestora.

Consimțământul poate fi retras în orice moment, prin urmare, operatorii de date trebuie să implementeze mijloace tehnice care pot elimina datele biometrice din sistem. Astfel, un sistem biometric introdus pe baza consimțământului trebuie să poată șterge în mod eficient toate legăturile de identitate pe care le-a creat.

3.1.2. Contractul, articolul 7 litera (b)

Prelucrarea datelor biometrice poate fi necesară pentru executarea unui contract la care subiectul datelor este parte sau în vederea luării unor măsuri, la cererea acestuia, înainte de încheierea contractului. Trebuie precizat, totuși, că această dispoziție se aplică, în general, numai atunci când se furnizează servicii pur biometrice. Acest temei legal nu poate fi utilizat pentru a înregistra o persoană într-un sistem biometric. Dacă acest serviciu poate fi separat de serviciul principal, contractul privind serviciul principal nu poate conferi legitimitate prelucrării datelor biometrice. Datele cu caracter personal nu sunt bunuri care pot fi solicitate în schimbul prestării unui serviciu, prin urmare, contractele care prevăd acest lucru sau contractele care oferă un serviciu numai cu condiția ca o persoană să accepte să i se prelucreze datele biometrice pentru un alt serviciu nu pot constitui un temei legal pentru prelucrarea datelor respective.

Exemple:
a) Doi frați depun mostre de păr la un laborator în vederea efectuării unui test ADN deoarece doresc să afle dacă sunt într-adevăr frați. Contractul încheiat cu laboratorul pentru efectuarea acestui test constituie un temei legal suficient pentru înregistrarea și prelucrarea datelor biometrice.

b) O persoană încarcă o fotografie într-un album foto din cadrul unei rețele de socializare pentru a le-o arăta prietenilor săi. În cazul în care contractul (condițiile de utilizare) prevede că utilizarea serviciului presupune înregistrarea utilizatorului într-un sistem biometric, această prevedere nu reprezintă un temei leal suficient pentru înregistrare.

3.1.3. Obligația legală, articolul 7 litera (c)

Un alt temei legal pentru prelucrarea datelor cu caracter personal este situația în care prelucrarea este necesară pentru îndeplinirea unei obligații legale care îi revine operatorului. Această dispoziție se aplică, de exemplu, în unele țări, la emiterea și/sau utilizarea pașapoartelor[6] și a vizelor[7].

3.1.4. Interesul legitim al operatorului de date, articolul 7 litera (f)

Conform articolului 7 din Directiva 95/46/CE, prelucrarea datelor biometrice cu caracter personal poate fi justificată, de asemenea, atunci când este „necesară pentru realizarea interesului legitim urmărit de operator sau de către unul sau mai mulți terți, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate".

Aceasta înseamnă că există situații în care utilizarea sistemelor biometrice este în interesul legitim al operatorului de date. Cu toate acestea, interesul operatorului constituie temei legitim numai dacă acesta poate demonstra că interesul său primează în mod obiectiv față de dreptul persoanelor vizate de a nu fi înregistrate într-un sistem biometric. De exemplu, atunci când trebuie să se asigure securitatea unor zone cu grad înalt de risc printr-un mecanism care poate verifica cu precizie dacă persoanele au acces la zonele respective, utilizarea unui sistem biometric poate fi în interesul legitim al operatorului. În exemplul oferit mai jos, privind un sistem biometric de control al accesului la un laborator, operatorul nu poate pune la dispoziția angajatului un mecanism alternativ fără a afecta în mod direct securitatea zonei cu acces restricționat deoarece nu există măsuri alternative mai puțin invazive care să poată asigura un nivel adecvat de securitate pentru aceste zone. Prin urmare, este în interesul său legitim să instaleze sistemul și să înregistreze un număr limitat de angajați, consimțământul acestora nemaifiind necesar. Totuși, în cazul în care interesul legitim al operatorului constituie un temei legal valid pentru prelucrare, toate celelalte principii privind protecția datelor se aplică, ca întotdeauna, în special principiul proporționalității și cel al reducerii la minim a datelor.

---

6 Amprentele au fost integrate în pașapoarte în conformitate cu Regulamentul nr. 2252/2004 al Consiliului UE din 13 decembrie 2004 și în permisele de ședere în conformitate cu Regulamentul nr. 1030/2002 al Consiliului UE din 13 iunie 2002.

7 Înregistrarea identificatorilor biometrici în Sistemul de informații privind vizele (VIS) este reglementată de Regulamentul (CE) nr. 767/2008 l din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS). A se vedea, de asemenea, Avizul nr. 3/2007 privind Propunerea de Regulament al Parlamentului European și al Consiliului de modificare a Instrucțiunilor consulare comune privind vizele adresate misiunilor diplomatice și oficiilor consulare în legătură cu introducerea biometriei, inclusiv a dispozițiilor privind organizarea primirii și prelucrării cererilor de viză [COM(2006)269 final] WP134; Avizul nr. 2/2005 referitor la Propunerea de Regulament al Parlamentului European și al Consiliului privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (COM (2004) 835 final) WP 110; Avizul 7/2004 privind includerea de elemente biometrice în permisele de ședere și vize, având în vedere instituirea sistemului european de informații privind vizele (VIS) WP 96.

Exemplu:
Într-o întreprindere care cercetează virusuri periculoase, securitatea unui laborator este asigurată cu ajutorul unor uși care se deschid numai după scanarea și recunoașterea amprentei și a irisului. Prin această măsură, se urmărește să se asigure că numai persoanele care cunosc riscurile și procedurile specifice și în care întreprinderea are încredere vin în contact cu aceste materiale periculoase. Interesul legitim al întreprinderii de a asigura că numai persoanele relevante pot intra în zona cu acces restricționat, cu scopul de a garanta reducerea semnificativă a riscurilor de securitate asociate cu accesul la zona respectivă, primează asupra dorinței persoanelor ca datele lor biometrice să nu fie prelucrate.

De regulă, utilizarea biometriei pentru satisfacerea unor cerințe generale de securitate a bunurilor și persoanelor nu poate fi privită ca interes legitim care primează asupra intereselor sau drepturilor și libertăților fundamentale ale subiectului datelor. Dimpotrivă, prelucrarea datelor biometrice poate fi justificată numai ca instrument necesar pentru asigurarea securității bunurilor și/sau a persoanelor, în cazul în care există dovezi bazate pe circumstanțe obiective și justificate prin documente cu privire la existența concretă a unui risc considerabil. În acest scop, operatorul trebuie să dovedească că există circumstanțe specifice care prezintă un risc concret considerabil, pe care operatorul trebuie să-l evalueze cu atenție specială. Pentru a respecta principiul proporționalității, în astfel de situații cu un grad înalt de risc, operatorul are obligația să verifice dacă există măsuri alternative care ar putea fi la fel de eficiente, însă mai puțin intruzive în raport cu obiectivele urmărite, și să aleagă aceste alternative.
Existența circumstanțelor menționate trebuie, de asemenea, să fie verificată cu regularitate. Pe baza rezultatului verificării, operațiunile de prelucrare de date care nu mai sunt justificate trebuie să fie sistate sau suspendate.

3.2. Operatorul de date și persoana împuternicită de către operator

Directiva 95/46/CE impune anumite obligații pentru operatorii de date cu privire la prelucrarea datelor cu caracter personal. În contextul biometriei, diferite tipuri de entități pot fi operatori de date, de exemplu angajatori, autorități de aplicare a legii sau autorități în domeniul migrației.

Grupul de lucru reamintește orientările oferite în avizul său privind conceptul de „operator” și cel de „persoană împuternicită de către operator”[8], care conține clarificări efective privind modul de interpretare a acestor definiții cheie din directivă.

3.3. Prelucrarea automată (articolul 15 din directivă)

Atunci când se utilizează sisteme bazate pe prelucrarea datelor biometrice, trebuie să se acorde o atenție specială consecințelor discriminatorii potențiale asupra persoanelor respinse de sistem. În plus, pentru a proteja dreptul persoanei de a nu fi supusă unei măsuri care o afectează numai din cauza prelucrării automate a datelor, trebuie să se introducă măsuri de protecție adecvate, precum intervenții umane, remedii sau mecanisme care permit subiectului datelor să-și exprime punctul de vedere.

Conform articolului 15 din Directiva 95/46/CE „*statele membre recunosc fiecărei persoane dreptul de a nu face obiectul unei decizii care să producă efecte juridice asupra sa ori să o afecteze în mod semnificativ și care să fie întemeiată numai pe prelucrarea automatizată a*

[8] WP169, Avizul nr. 1/2010 privind conceptele de „operator” și „persoană împuternicită de către operator”.

datelor destinată să evalueze anumite aspecte ale personalității sale, cum ar fi randamentul profesional, credibilitatea, încrederea pe care o prezintă, conduita etc."

3.4. Transparența și informarea persoanelor vizate

Conform principiului prelucrării corecte, persoanele vizate trebuie să fie informate cu privire la colectarea și/sau utilizarea datelor lor biometrice (articolul 6 din Directiva 95/46/CE). Orice sistem care colectează astfel de date fără cunoștința persoanei vizate trebuie să fie evitat.

Operatorul de date trebuie să asigure că persoanele vizate sunt informate în mod corespunzător cu privire la elementele cheie ale prelucrării, în conformitate cu articolul 10 din Directiva privind protecția datelor, precum identitatea operatorului, scopurile prelucrării, tipul de date, durata prelucrării, dreptul persoanelor vizate de a accesa, rectifica sau retrage datele, dreptul de a-și retrage consimțământul și informații cu privire la destinatarii sau categoriile de destinatari ai datelor. Dată fiind obligația operatorului sistemului biometric de a informa persoanele vizate, nu trebuie să se colecteze datele biometrice ale unei persoane fără cunoștința acesteia.

3.5. Dreptul de a accesa datele biometrice

Subiecții datelor au dreptul de a obține de la operatorii de date accesul la datele lor, inclusiv, de regulă, la datele biometrice proprii. Aceștia au, de asemenea, dreptul de a accesa potențialele profile bazate pe astfel de date biometrice. Dacă operatorul trebuie să verifice identitatea persoanelor vizate pentru a le permite accesul, este esențial ca accesul să le fie acordat fără prelucrarea unor date cu caracter personal suplimentare.

3.6. Securitatea datelor

Operatorii de date trebuie să pună în aplicare măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii accidentale, modificării, divulgării sau accesului neautorizat și împotriva tuturor celorlalte forme ilegale de prelucrare[9].

Trebuie să se asigure o securitate corespunzătoare pentru datele colectate și stocate. Proiectanții sistemelor trebuie să se consulte cu experți în securitate pentru a asigura că vulnerabilitățile de securitate sunt soluționate în mod corespunzător, în special dacă sistemele existente sunt transferate pe internet.

3.7. Măsuri de protecție pentru persoanele cu nevoi speciale

Utilizarea biometriei ar putea avea un impact semnificativ asupra demnității, vieții private și dreptului la protecția datelor ale persoanelor vulnerabile precum copiii, persoanele în vârstă și persoanele care sunt incapabile, din punct de vedere fizic, să efectueze cu succes procesul de înregistrare. Având în vedere consecințele potențial defavorabile asupra persoanelor în cauză, este necesar să se îndeplinească cerințe mai stricte în procesul de evaluare a impactului oricărei măsuri care afectează demnitatea umană, mai precis prin analizarea necesității și a proporționalității măsurii, precum și a posibilităților persoanei de a-și exercita dreptul privind protecția datelor, pentru ca măsura respectivă să fie considerată admisibilă. Trebuie să se introducă măsuri de protecție adecvate împotriva riscului de stigmatizare sau discriminare a unor astfel de persoane, fie din cauza vârstei acestora, fie din cauza incapacității de a se înregistra.

---

[9] Articolul 17 alineatul (1) din Directiva 95/46/CE.

În ceea ce privește introducerea unei obligații legale generalizate de colectare a identificatorilor biometrici pentru aceste grupuri, în special pentru copiii cu vârste mici și pentru persoanele în vârstă, la controalele de frontieră în scop de identificare, grupul de lucru a considerat necesar ca „*pentru demnitatea persoanei și asigurarea fiabilității procedurii, colectarea și prelucrarea amprentelor să fie restrânsă în cazul copiilor și al persoanelor în vârstă, iar limita de vârstă să fie conformă cu limitele de vârstă în vigoare pentru alte baze de date biometrice importante din UE (în special Eurodac)*”[10].

În orice caz, trebuie să se introducă măsuri de protecție specifice (de exemplu, proceduri subsidiare adecvate) pentru a se asigura respectul pentru demnitatea umană și libertățile fundamentale ale oricărei persoane incapabile să efectueze cu succes procesul de înregistrare, evitând astfel împovărarea acestor persoane cu imperfecțiunile sistemului tehnic[11].

3.8. Date sensibile

Unele date biometrice ar putea fi considerate sensibile în sensul articolului 8 din Directiva 95/46/EC, în special, datele referitoare la originea rasială sau etnică sau datele referitoare la sănătate. De exemplu, ADN-ul unei persoane include adesea informații despre sănătatea acesteia sau poate indica originea rasială sau etnică. În acest caz, datele privind ADN-ul reprezintă date sensibile și este necesar să se aplice măsurile speciale de protecție prevăzute la articolul 8, pe lângă principiile generale de protecție a datelor din directivă. Pentru a evalua caracterul sensibil al datelor prelucrate de un sistem biometric, trebuie să se țină seama, de asemenea, de contextul prelucrării[12].

3.9. Rolul autorităților naționale de protecție a datelor

Având în vedere gradul din ce în ce mai mare de standardizare a tehnologiilor biometrice în vederea interoperabilității, se știe că stocarea centralizată a datelor biometrice sporește atât riscul utilizării datelor biometrice ca element de interconectare a multiplelor baze de date (ceea ce poate conduce la crearea de profile detaliate ale unei persoane), cât și riscurile specifice asociate cu reutilizarea acestor date în scopuri incompatibile, în special în eventualitatea accesului neautorizat.

Grupul de lucru recomandă ca sistemele care utilizează datele biometrice ca element de interconectare a mai multor baze de date să fie prevăzute cu măsuri de protecție suplimentare, deoarece este probabil ca acest tip de prelucrare să prezinte riscuri specifice la adresa drepturilor și libertăților subiecților datelor (articolul 20 din Directiva 95/46/CE). Pentru a asigura măsuri de protecție adecvate, în special, pentru a diminua riscurile pentru subiecții datelor, operatorul ar trebui să consulte autoritatea națională competentă pentru protecția datelor înainte de introducerea unor astfel de măsuri.

---

[10] WP134 – Avizul nr. 3/2007 cu privire la Propunerea de Regulament al Parlamentului European și al Consiliului de modificare a Instrucțiunilor consulare comune privind vizele pentru misiuni diplomatice și posturi consulare relativ la introducerea biometriei, inclusiv dispoziții referitoare la organizarea primirii și prelucrării cererilor de viză [COM(2006)269 final].

[11] Conform WP134 – Avizul nr. 3/2007, p. 8.

[12] Conform WP 29 Recomandări privind categoriile speciale de date („date sensibile”) Domeniile de referință (2011)444105 - 20/04/2011.

4. Evoluții și tendințe noi ale tehnologiei, scenarii noi

4.1. Introducere

Tehnologiile biometrice sunt utilizate de multă vreme, în principal de către autoritățile guvernamentale, însă situația s-a schimbat în prezent, entitățile comerciale jucând un rol major în utilizarea acestor tehnologii și dezvoltarea de produse noi.

Unul dintre factorii care au determinat această schimbare este evoluția tehnologică, astfel încât sistemele biometrice care funcționau în mod corespunzător numai în condiții controlate au fost îmbunătățite și pot fi utilizate în prezent la scară largă în diverse medii. Din această cauză, biometria înlocuiește sau completează, în unele cazuri, metodele convenționale de identificare, în special cele bazate pe factori multipli de identificare, necesare pentru sistemele puternice de autentificare. Tehnologiile biometrice sunt folosite din ce în ce mai mult, de asemenea, în aplicații care pot identifica o persoană rapid și comod, însă cu un nivel mai scăzut de acuratețe.

În plus, utilizarea tehnologiilor biometrice a depășit treptat domeniul său de aplicare inițial – identificarea și autentificarea – extinzându-se la analiza comportamentală, supraveghere și prevenirea fraudelor.

Progresele realizate în domeniul tehnologiilor și rețelelor informatice au determinat, de asemenea, apariția unei așa-numite a doua generație de tehnologii biometrice, bazate pe utilizarea izolată a trăsăturilor comportamentale și psihologice sau în combinație cu alte sisteme clasice, formând sisteme multimodale. Pentru o imagine completă, trebuie menționată tendința de a utiliza biometria în inteligența ambientală și calculul ubicuu.

4.2. Tendințe noi în biometrie

Există o serie de tehnologii biometrice care pot fi considerate mature, având mai multe aplicații în aplicarea legii, guvernarea electronică și sistemele comerciale. O listă neexhaustivă ar cuprinde amprentele digitale, geometria mâinii, scanarea irisului și unele tipuri de recunoaștere facială. Sunt în curs de apariție, de asemenea, unele tehnologii biometrice care analizează caracteristici ale corpului. Unele dintre acestea sunt noi, însă altele sunt tehnologii biometrice tradiționale care evoluează datorită noilor capacități de procesare.

Noile sisteme sunt caracterizate, în general, de utilizarea caracteristicilor corporale, care permit clasificarea/identificarea persoanelor, precum și de colectarea datelor la distanță. Datele obținute sunt utilizate pentru crearea de profile, supravegherea la distanță și pentru funcții mai complexe precum inteligența ambientală.

Progresele au devenit posibile datorită dezvoltării constante a senzorilor care permit colectarea de caracteristici fiziologice noi, precum și datorită noilor metode de prelucrare a datelor biometrice tradiționale.

Trebuie menționată, de asemenea, utilizarea așa numitei biometrii ușoare, caracterizată prin utilizarea unor trăsături comune, care nu sunt adecvate pentru a distinge sau a identifica fără dubiu o persoană, însă care permit creșterea performanței altor sisteme de identificare.

Un alt element esențial al noilor sisteme biometrice este capacitatea de a colecta informații la distanță sau în mișcare, fără să fie necesară cooperarea sau de vreo acțiune din partea persoanei vizate. Deși această tehnologie nu este dezvoltată pe deplin, se depun eforturi semnificative în acest sens, în special în scopul aplicării legii.

Un progres rapid s-a înregistrat în ceea ce privește utilizarea sistemelor multimodale, care folosesc diferite date biometrice în mod simultan sau mai multe citiri/unități ale acelorași date biometrice care pot fi adaptate în vederea optimizării securității/facilității de utilizare a sistemelor biometrice. Aceasta poate reduce rata de acceptare falsă, poate îmbunătăți rezultatele unui sistem de recunoaștere sau poate facilita colectarea datelor unei populații mai numeroase, compensând caracterul neuniversal al unei surse de date biometrice prin combinarea sa cu o altă sursă.

Sistemele biometrice sunt utilizate din ce în ce mai mult, atât de instituțiile publice, cât și de entitățile private; în mod tradițional, datele biometrice sunt utilizate adesea în sectorul public pentru aplicarea legii; în domeniul financiar, bancar și al e-sănătate, biometria este din ce în ce mai utilizată, precum și în alte sectoare precum educația, vânzarea cu amănuntul și telecomunicațiile. Această evoluție este stimulată de noile proprietăți derivate din convergența/fuziunea tehnologiilor existente. Un exemplu în acest sens este utilizarea sistemelor CCTV care permit atât colectarea, cât și analiza datelor biometrice și a trăsăturilor comportamentale umane.

Aspectele prezentate anterior pot fi privite și ca o modificare a tendințelor în domeniul sistemelor biometrice, de la identificare la recunoaștere ușoară, cu alte cuvinte, de la identificare la detectarea comportamentului sau a nevoilor specifice ale persoanelor. Aceasta deschide, de asemenea, calea către utilizări foarte diferite față de asigurarea securității la scară largă: securitatea personală, jocurile video și vânzarea cu amănuntul vor beneficia de pe urma acestei interacțiuni sporite între om și mașină, care permite mai mult decât identificarea sau clasificarea unei persoane.

4.3. Impactul asupra vieții private și protecției datelor

Încă de la începutul implementării acestora, sistemele biometrice au dat naștere la îngrijorări în mai multe domenii, inclusiv în ceea ce privește viața privată și protecția datelor, acest fapt influențând cu siguranță acceptarea lor socială și alimentând controversele privind legalitatea, limitele utilizării, măsurile de protecție și garanțiile necesare pentru a diminua riscurile identificate.

În general, reticența față de sistemele biometrice a fost și este legată încă de protecția drepturilor persoanelor. Totuși, noile sisteme și îmbunătățirile aduse celor existente provoacă din nou preocupare. Aceasta se referă la posibilitatea colectării, stocării și prelucrării clandestine a datelor, precum și la colectarea de material conținând informații foarte sensibile, invadându-se astfel spațiul cel mai intim al persoanei.

Denaturarea funcțiilor a reprezentat un motiv de preocupare important încă de la prima utilizare a tehnologiilor și sistemelor biometrice; chiar dacă acesta este un risc bine cunoscut și pentru care s-a încercat găsirea de soluții în biometria tradițională, este evident că potențialul tehnic mai ridicat al noilor sisteme informatice antrenează riscul ca datele să fie utilizate contrar scopului lor original.

Tehnicile clandestine permit identificarea persoanelor fără cunoștința acestora, ceea ce reprezintă o amenințare importantă pentru viața privată și o breșă în controlul asupra datelor cu caracter personal. Acest fapt are efecte grave asupra capacității persoanelor de a-și exercita dreptul la consimțământul liber exprimat sau, pur și simplu, de a obține informații privind prelucrarea datelor lor. În plus, unele sisteme pot colecta în secret informații referitoare la stări emoționale sau la caracteristici ale corpului și pot dezvălui informații legate de starea de sănătate, ceea ce presupune o prelucrare neproporțională a datelor, precum și o prelucrare a datelor sensibile în sensul articolului 8 din Directiva 95/46/CE.

Având în vedere faptul că tehnologiile biometrice nu pot asigura acurateţe în proporţie de 100%, există întotdeauna un risc implicit legat de identificarea incorectă. Aceste situaţii de fals pozitiv conduc la decizii ce afectează drepturile persoanelor. Furtul de identitate bazat pe utilizarea de surse biometrice copiate sau furate poate produce pagube importante. Spre deosebire de alte sisteme de identificare, în acest caz persoana nu poate primi pur şi simplu o nouă identificare doar pentru că aceasta este compromisă.

În contextul luării de decizii automate sau al anticipării comportamentului sau a preferinţelor într-o anumită situaţie, trebuie să se menţioneze, de asemenea, crearea de profile. Unele date biometrice pot divulga informaţii fizice despre o persoană. Acestea pot fi utilizate pentru identificare şi pentru crearea de profile, însă poate conduce, în egală măsură, la discriminare, la stigmatizare sau la confruntarea nedorită cu informaţii neaşteptate/nedorite.

4.4. Prezentarea sistemelor şi tehnologiilor biometrice specifice

4.4.1. Modelul venelor şi utilizări combinate

Două tehnologii principale aflate în uz sunt bazate pe recunoaşterea modelului venelor: recunoaşterea venelor din palmă şi recunoaşterea venelor din deget, ambele tehnici fiind utilizate în prezent la scară largă, în special în Japonia.

Din punct de vedere tehnic, recunoaşterea modelului venelor se bazează pe tiparul venelor, citit cu ajutorul unei camere video cu infraroşu, atunci când degetul sau mâna sunt expuse la o lumină infraroşie la mică distanţă. Imaginea obţinută este prelucrată pentru a pune în evidenţă caracteristicile modelului venelor, rezultând, după prelucrare, într-o imagine a reţelei vasculare. Principalul avantaj al acestei tehnologii este faptul că nicio persoană nu lasă o urmă a caracteristicii sale biometrice[13], deoarece nu este necesar să „atingă" cititorul. În acelaşi timp, este dificil ca aceste date biometrice să fie colectate fără consimţământul persoanei vizate. În final, această tehnică poate fi, de asemenea, utilizată pentru a detecta dacă proba prezentată sistemului este vie, observându-se dacă sângele curge sau nu.

Recunoaşterea modelului venelor poate fi utilizată pentru aplicaţii de acces logic şi acces fizic la diferite locaţii. Producătorii oferă posibilitatea de a include senzorul în alte produse, în special în scop bancar.

Riscurile în materie de protecţie a datelor asociate cu utilizarea sistemelor de recunoaştere a modelului venelor sunt prezentate în continuare:

- Acurateţe: nivelul de performanţă a modelului venelor este înalt, această tehnologie fiind considerată o alternativă viabilă la recunoaşterea amprentelor. Recunoaşterea modelului venelor prezintă, de asemenea, o rată scăzută a „eşecului de înregistrare" ("Failure to Enrol Rate" – FER), deoarece nu este afectată de deteriorarea degetului sau a mâinii. Aceste tehnologii nu au fost încă experimentate/utilizate pe o populaţie numeroasă (în Japonia, acest model este comparat cu modelul stocat pe un card inteligent). În unele cazuri, această tehnologie poate fi afectată, de asemenea, de condiţii climatice care influenţează sistemul vascular (căldură, presiune etc.).

[13] Unii autori afirmă că tehnologiile asociate cu recunoaşterea venelor pot indica boli precum hipertensiunea sau anomaliile vasculare.

- Impact: impactul sistemelor de recunoaștere a modelului venelor asupra protecției datelor este limitat, deoarece acest tip de date biometrice nu se colectează ușor, iar utilizarea lor este limitată în prezent la aplicații din sectorul privat.

- Consimțământ și transparență: având în vedere faptul că datele referitoare la modelul venelor pot fi colectate numai cu ajutorul luminii și al camerelor video cu raze infraroșii la mică distanță, se poate considera că persoana are cunoștință de prelucrarea datelor sale și își dă consimțământul atunci când își așează degetul sau mâna în fața cititorului. Cu toate acestea, la fel ca în orice sistem biometric, această presupunere poate să nu funcționeze în anumite situații, de exemplu atunci când persoana vizată este un angajat al operatorului de date.

- Alt scop (alte scopuri) al (ale) prelucrării: în prezent, datele referitoare la modelul venelor prezintă riscuri limitate în ceea ce privește utilizarea lor în alte scopuri. Riscurile pot crește dacă acest tip de prelucrare se generalizează și dacă practicile de *spoofing* (uzurpare de date personale) devin mai ușor de aplicat.

- Stabilirea de legături: datele referitoare la modelul venelor nu oferă informații care pot fi legate de alte date, cu excepția datelor referitoare la modelul venelor rezultate dintr-o altă prelucrare.

- Urmărirea/crearea de profile: riscurile privind urmărirea/crearea de profile care derivă din utilizarea datelor privind modelul venelor sunt limitate, atât timp cât acest tip de date biometrice nu sunt folosite la scară largă, de exemplu într-o bază de date centralizată pentru cardurile de plăți.

- Prelucrarea datelor sensibile: singurele date sensibile care ar putea rezulta din modelul venelor se referă la starea de sănătate, însă, până în prezent, nu s-a realizat nicio evaluare oficială în acest sens.

- Revocabilitate: datele referitoare la modelul venelor par foarte stabile în timp, însă această afirmație trebuie să fie confirmată pe cale experimentală (sistemele de recunoaștere a modelului venelor sunt prea recente pentru a obține rezultate confirmate). Datele referitoare la modelul venelor ar trebui să fie considerate, prin urmare, irevocabile.

- Protecție *anti-spoofing*: *spoofing*-ul în materie de date privind modelul venelor nu a fost cercetat încă pe larg, însă un studiu recent a arătat că spoofing-ul poate fi aplicat unui cititor de vene din palmă[14]. Principala dificultate în spoofing-ul datelor privind modelul venelor este reprezentată de colectarea unei mostre din datele biometrice respective.

4.4.2. Amprentele și utilizările combinate

Recunoașterea amprentelor constituie unul dintre sistemele biometrice cele mai vechi, cele mai studiate și cele mai utilizate. Identificarea cu ajutorul amprentelor este folosită de mai mult de 100 de ani în aplicarea legii în scop de verificare și de identificare. Aceasta se bazează pe faptul că fiecare persoană are amprente unice, prezentând caracteristici specifice,

[14] A se vedea: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf.

care pot fi măsurate cu scopul de a se decide dacă o amprentă prelevată se potrivește cu o probă înregistrată.

Înregistrarea necesită prezența fizică a persoanei și, în funcție de utilizarea dorită, implicarea unui personal calificat pentru a asigura o bună calitate a datelor. Colectarea amprentelor nu este o sarcină neînsemnată. Acuratețea la comparare va depinde de calitatea imaginii, în raport cu tehnica imaginii. Tehnicile pot varia: se pot amprenta unul, două, până la zece degete, prin apăsare sau ușoară rotire. În funcție de sistem, amprentele pot fi utilizate numai pentru verificare (1:1) sau pentru identificare și compararea cu anumite urme (1: n). Cu toate acestea, astfel cum au arătat unele studii, o parte din populație nu poate fi înregistrată din diferite motive, ceea ce ridică o problemă care necesită existența unor proceduri subsidiare adecvate, în special pentru sistemele mari, pentru a nu lipsi persoanele de anumite drepturi de care dispun acestea.

Deși, în principiu, nu este o metodă foarte invazivă, amprentarea poate fi percepută astfel, deoarece este asociată cu ideea negativă de a fi tratat ca suspect, din cauza utilizării sale frecvente în procedurile de aplicare a legii.

Amprentele prezintă diferite caracteristici care pot fi utilizate pentru verificare/identificare, deși analiza detaliilor este încă tehnica cea mai utilizată. Dezvoltarea unor tehnici noi (de exemplu, scanere de înaltă rezoluție) permite utilizarea altor caracteristici. Au fost dezvoltate, de asemenea, tehnici de identificare care permit utilizarea de baze de date mari în scop de identificare.

În acest sens, cele mai avansate sisteme sunt așa-numitele sisteme automate de identificare a amprentelor (*automated fingerprint identification systems* – AFIS), folosite în aplicarea legii, care pot fi utilizate pentru a face schimb de date prin căutarea în diferite depozite de date la nivel transfrontaliere. Schimbul de date implică probleme legate de faptul că locațiile, formatele și nivelurile de calitate sunt diferite.

La nivelul UE, exemple de AFIS sunt Eurodac și Visa Information System (Sistemul de informații privind vizele), care, conform așteptărilor, se vor număra printre cele mai mari baze de date din lume, având în vedere că vor fi stocate în aceste sisteme aproximativ 70 de milioane de amprente. În avizele sale anterioare, grupul de lucru a ridicat câteva probleme legate de utilizarea bazelor de date la scară largă, ținând seama de necesitatea de a asigura proporționalitatea. Trebuie să se soluționeze, în special, problemele de fiabilitate referitoare la cazurile de fals pozitiv și fals negativ, controlul efectiv al accesului la bazele de date și problemele legate de utilizarea amprentelor prelevate de la copii și de la persoanele în vârstă.

Tiparele sunt utilizate în mod frecvent în sistemele biometrice bazate pe amprentare și sunt considerate, de regulă, de către furnizorii de sisteme, drept o modalitate de protecție a persoanei. Cu toate acestea, în funcție de sistemul/algoritmul utilizat pentru crearea tiparului, există riscuri potențiale legate de posibilitatea de a lega tiparele de alte baze de date pentru amprente în vederea identificării persoanelor.

Practicile care urmăresc sustragerea de la recunoașterea amprentelor de către sistem prin utilizarea unor degete artificiale sau a unor amprente fabricate din materiale artificiale și care permit furtul de identitate constituie, de asemenea, un aspect important. Există diferite soluții pentru a reduce vulnerabilitatea acestor sisteme, cum ar fi detectarea probelor vii, recunoașterea amprentelor de la mai multe degete și utilizarea unei supravegheri umane corespunzătoare pentru procesele de înregistrare și identificare/verificare.

Există motive de preocupare, în materie de protecție a datelor, asociate cu utilizarea amprentelor, descrise pe scurt în continuare:

- Acuratețe: cu toate că amprentele au un grad înalt de acuratețe, acesta poate fi afectat de limitările legate de informații – calitatea scăzută a datelor sau procesul de colectare neconsecvent – sau reprezentare – caracteristicile selectate sau calitatea algoritmilor de extragere. Aceasta poate conduce la situații de respingere falsă sau de potrivire falsă.

- Impact: ireversibilitatea procesului poate reduce posibilitatea persoanelor vizate de a-și exercita drepturile sau de a schimba decizii bazate pe o identificare falsă. Datorită încrederii în acuratețea amprentelor, erorile posibile pot fi mai greu de rectificat, ceea ce poate avea consecințe importante pentru persoanele implicate. Trebuie să se țină seama de acest fapt atunci când se evaluează proporționalitatea prelucrării în raport cu decizia specifică care urmează a fi luată pe baza amprentelor. Trebuie menționat, de asemenea, că lipsa de măsuri de securitate poate conduce la furtul de identitate, care poate avea un impact puternic asupra persoanei vizate.

- Stabilirea de legături: amprentele pot fi utilizate în mod necorespunzător deoarece datele pot fi legate cu alte baze de date. Posibilitatea de a stabili legături cu alte baze de date poate antrena utilizări care nu sunt compatibile cu scopurile originale. Există unele tehnici, precum biometria convertibilă sau codificarea biometrică, care pot fi utilizate pentru a reduce riscul.

- Prelucrarea datelor sensibile: conform unor studii, amprentele pot dezvălui informații privind originea etnică a persoanei[15].

- Alt scop (alte scopuri) ale prelucrării: Stocarea centralizată a datelor, în special în baze de date de mari dimensiuni, implică riscuri cu privire la securitatea datelor, stabilirea de legături și denaturarea funcțiilor. În lipsa unor măsuri de protecție, aceasta permite utilizarea amprentelor în alte scopuri decât cele care justificau inițial prelucrarea.

- Consimțământ și transparență: consimțământul este un aspect esențial în utilizarea amprentelor pentru alte scopuri decât aplicarea legii. Amprentele pot fi copiate cu ușurință din imprimate existente sau chiar din fotografii, fără cunoștința persoanei vizate. Alte aspecte referitoare la consimțământ sunt cele legate de obținerea consimțământului copiilor și de rolul părinților în acest sens (de exemplu, pentru amprentarea în școli), precum și de valabilitatea consimțământului pentru prelevarea amprentelor în contextul relațiilor angajat-angajator.

- Revocabilitate: datele referitoare la amprente sunt foarte stabile în timp și trebuie considerate irevocabile. Un tipar de amprentă poate fi revocat în anumite condiții.

- Protecție anti-spoofing: amprentele pot fi colectate cu ușurință datorită numeroaselor urme de amprente pe care le lasă o persoană în jurul său. În plus, amprentele false pot trece nedetectate de multe sisteme și senzori, în special de sistemele care nu includ măsuri de protecție specifice anti-spoofing. Succesul unui atac depinde în mare măsură de tipul de senzor (optic, capacitiv etc.) și de materialul utilizat de atacator.

[15] http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm and http://www.crime-scene-investigator.net/fingerprintpatterns.html

Exemplu:
Un spital utilizează amprentele dintr-o bază de date centralizată pentru a autentifica pacienții în secția de radioterapie, pentru a asigura astfel că fiecare pacient primește tratamentul corect. Se preferă utilizarea amprentelor și nu a modelului venelor, deoarece tratamentul afectează sistemul vascular. În plus, se utilizează o bază de date centralizată deoarece, din cauza stării pacienților (vârstă, patologie), insignele s-ar putea pierde, ceea ce ar bloca accesul la tratament. În acest caz, utilizarea amprentelor pare să fie o soluție adecvată.

4.4.3. Recunoașterea facială și utilizări combinate

Chipul, ca și amprentele, a fost utilizat adesea ca sursă de date biometrice timp de mulți ani. În prezent, chipul este utilizat pentru a stabili nu numai identitatea unei persoane, ci și caracteristici fiziologice și psihologice, precum originea etnică, emoțiile și starea de bine. Posibilitatea de a extrage toate aceste date dintr-o imagine și faptul că o fotografie poate fi făcută de la o oarecare distanță, fără cunoștința persoanei vizate, arată că există numeroase probleme în materie de protecție a datelor asociate cu aceste tehnologii.

Recunoașterea facială, ca mijloc de identificare și verificare, nu a rămas neutilizată de către autoritățile de aplicare a legii, alte autorități publice și entitățile private. De mulți ani, fotografiile apar pe pașapoarte, permise de conducere, cărți naționale de identitate, precum și ca fotografii de identitate judiciară. Nu este un lucru neobișnuit ca fotografia titularului să apară pe o legitimație pentru controlul accesului sau din cadrul unei organizații. În mod tipic, fotografiile sunt făcute sub o lumină specifică și reprezintă persoana din față sau din profil. Acest set de imagini controlate constituia, în mod natural, o bază adecvată pentru a începe prelucrarea și recunoașterea automată a persoanelor. Această utilizare a fost depășită, iar tehnologia actuală face posibilă identificarea pe baza unor imagini care implică o serie de camere video, diferite unghiuri și condiții de lumină. În același timp, există o cantitate imensă de imagini disponibile în mod public pe internet, cum ar fi cele încărcate pe site-urile rețelelor de socializare sau în alte galerii foto cu acces public. Riscurile nu se limitează la fotografiile tradiționale, întrucât recunoașterea facială poate fi aplicată cu succes videoclipurilor difuzate în timp real. Atunci când adaugă noi capacități de prelucrare unui sistem existent (de exemplu, introducerea funcției de recunoaștere facială într-un sistem CCTV), operatorii de date trebuie să recunoască faptul că, astfel, se modifică scopul sau scopurile specificate ale sistemului original și trebuie să reevalueze impactul modificării asupra vieții private.

Riscurile în materie de protecție a datelor asociate cu utilizarea sistemelor de recunoaștere facială sunt prezentate în continuare:

- Acuratețe: în cazul în care calitatea imaginilor nu poate fi garantată, există riscul de compromitere a acurateței. Dacă chipul nu este complet reprezentat (de exemplu, este umbrit de păr sau de o pălărie), este evident că o clasificare sau comparare vor implica un grad înalt de eroare. Diferențele de atitudine și lumină rămân o provocare importantă pentru recunoașterea facială deoarece afectează într-o mare măsură acuratețea.

- Impact: impactul specific al unui anumit sistem de recunoaștere facială asupra protecției datelor depinde de scopul acestuia și de contextul specific. Un sistem de clasificare care urmărește cuantificarea vizitatorilor unei atracții turistice, fără a dispune de capacități de înregistrare, va avea un impact diferit asupra protecției datelor față de un sistem care vizează supravegherea secretă de către autoritățile de aplicare a legii, cu scopul de a identifica potențialii infractori.

- Consimțământ și transparență: un risc pentru protecția datelor care nu apare la multe alte tipuri de prelucrare a datelor biometrice este legat de faptul că imaginile pot fi captate și prelucrate din mai multe unghiuri, în diferite condiții de mediu și fără cunoștința persoanei vizate. În avizul 15/2011 privind definiția consimțământului, grupul de lucru a subliniat faptul că acordarea consimțământului poate constitui un temei legal pentru prelucrare numai în cazul în care este vorba despre consimțământul „informat". Dacă persoana vizată nu are cunoștință de prelucrarea imaginilor în scopul recunoașterii faciale, dispoziția nu se aplică. Chiar dacă persoana vizată știe de existența unei camere video, este posibil ca, vizual, să nu poată face diferența între un sistem CCTV live sau care înregistrează și un aparat care face fotografii pentru un sistem de recunoaștere facială.

- Alt scop (alte scopuri) al (ale) prelucrării: după captarea, legală sau ilegală, a imaginilor digitale, acestea pot fi transmise sau copiate cu ușurință pentru a fi prelucrate în alte sisteme decât cele pentru care erau destinate inițial. Acest fapt este evident în rețelele de socializare, unde utilizatorii își încarcă fotografiile personale pentru a le împărtăși cu familia, prietenii sau colegii. Odată introduse pe platforma media, imaginile pot fi refolosite chiar de platforma respectivă în mai multe scopuri, fiind posibil ca unele dintre aceste scopuri să fi fost incluse în platformă după captarea și/sau încărcarea imaginii.

- Stabilirea de legături: există multe servicii online care permit utilizatorilor să încarce o imagine, aceasta urmând a fi inclusă în profilul utilizatorului. Se poate utiliza recunoașterea facială pentru a stabili legături între profilele asociate diferitelor servicii online (prin fotografia inclusă în profil), dar și între lumea reală și cea virtuală. Nu este deloc imposibil să faci o fotografie pe stradă unei persoane și să-i stabilești identitatea în timp real, căutând printre fotografiile din profilele publice. Unele servicii terțe pot, de asemenea, să se servească de fotografiile din profile și de alte fotografii disponibile în mod public pentru a crea colecții imense de imagini, care permit asocierea unei identități din lumea reală cu o astfel de imagine.

- Urmărire/Creare de profile: un sistem de identificare poate fi utilizat și în cazul în care nu se cunoaște identitatea reală a unei persoane. Un sistem de recunoaștere facială dintr-un complex comercial sau dintr-o altă locație publică similară poate fi utilizat pentru a urmări rutele și obiceiurile cumpărătorilor. Unul dintre scopuri poate fi gestionarea eficientă a aglomerației sau amplasarea produselor, pentru a spori confortul clienților. Totuși, posibilitatea de a urmări sau de a localiza o anumită persoană antrenează posibilitatea de a crea profile și de a oferi publicitate specializată sau alte servicii specifice.

- Prelucrarea datelor sensibile: astfel cum s-a menționat anterior, prelucrarea datelor biometrice poate fi utilizată pentru a afla date sensibile, în special date cu indicii vizuale precum rasa, originea etnică sau o anumită afecțiune medicală.

- Revocabilitate: o persoană își poate schimba cu ușurință înfățișarea (cu ajutorul bărbii, al ochelarilor, al unei pălării), ceea ce poate fi suficient pentru a păcăli sistemele de recunoaștere facială, în special atunci când acestea funcționează într-un mediu necontrolat. Cu toate acestea, principalele trăsături faciale ale unei persoane sunt

stabile în timp, iar sistemele își pot îmbunătăți capacitatea de recunoaștere prin colectarea și asocierea diferitelor „înfățișări” cunoscute ale unei persoane.

- Protecție anti-spoofing: există multe sisteme de recunoaștere facială vulnerabile la spoofing, însă producătorii încearcă să sporească măsurile de protecție cu ajutorul unor tehnici precum imaginile 3D sau înregistrarea video. Totuși, majoritatea sistemelor de bază utilizate în cadrul aplicațiilor publice nu includ astfel de măsuri de protecție.

Exemplu:
Un exemplu imaginar extrem ar fi un sistem de supraveghere de nouă generație, instalat într-un centru comercial, care poate să recunoască persoane, să urmărească mișcările în mod automat, să facă diferența între expresiile faciale precum zâmbetul sau mânia. Acesta ar putea recunoaște clienții obișnuiți care intră în parcarea auto din cadrul complexului și ar putea să-i conducă spre anumite locuri de parcare. Atunci când clienții intră în complexul comercial, sistemul ar putea să le identifice hainele pentru a le sugera ce magazine ar putea vizita, în funcție de ofertele curente ale magazinelor, de istoricul cumpărăturilor persoanei respective sau de o serie de indicatori anticipați. Se poate introduce publicitatea personalizată în vitrinele magazinelor sau interzicerea automată a accesului în anumite magazine, restaurante sau alte locații. Hoții de mașini ar putea fi identificați și urmăriți chiar înainte de a atinge vreo mașină. Dacă este necesar, vehicule aeriene teleghidate (drone), dotate cu camere video și alți senzori, ar putea urmări suspecții până la eliminarea sau confirmarea suspiciunii. Obiectele ascunse sub îmbrăcăminte (cuțite sau obiecte furate) ar putea fi detectate. Această tehnologie nu este bazată numai pe sisteme biometrice noi, ci combină și prelucrează informații care sunt deja furnizate, alături de alte date, de către o serie de alte sisteme.

O aplicație similară a fost proiectată în cadrul proiectului INDECT (*Intelligent information system supporting observation, searching and detection for security of citizens in urban environment* - sistem inteligent de informații de observare, căutare și detectare pentru securitatea cetățenilor din mediul urban), în care tehnologiile sunt combinate pentru a lupta împotriva potențialelor acte de terorism și infracțiuni, înainte ca acestea să aibă loc. Grupul de lucru subliniază că o astfel de utilizare a datelor biometrice ar necesita un temei legal adecvat și considerații stricte privind necesitatea și proporționalitatea acestor măsuri.

4.4.4. Recunoașterea vocală și utilizări combinate

Pe lângă utilizarea recunoașterii vocale ca dată biometrică în scop de identificare, o utilizare relativ frecventă presupune identificarea anumitor caracteristici ale tiparului vocal pentru a clasifica vorbitorul. Un astfel de exemplu ar fi analizarea răspunsurilor unei persoane în cadrul unei conversații telefonice cu scopul de a identifica tiparele de accent și neregularitățile de vorbire, pentru a identifica potențialele cazuri de fraudă.

Producătorii au declarat că, după implementarea acestei tehnologii, societățile de servicii financiare și-au sporit rata de detectare a fraudelor și au introdus servicii mai rapide pentru a mulțumi clienții reali.

În cazul unui sistem de clasificare, riscurile privind protecția datelor sunt ușor diferite față de sistemele de identificare biometrică, prin faptul că nu ar trebui să existe o etapă de înregistrare și nu este necesară stocarea pe termen lung a unui model biometric. Cu toate acestea, dacă o conversație telefonică este înregistrată, astfel cum se întâmplă de obicei în instituțiile

financiare, trebuie să se introducă măsuri adecvate de control pentru a asigura securitatea acestor date.

- Acuratețe: unul dintre riscurile în materie de protecție a datelor asociate cu un astfel de sistem se referă la ratele de detecție, în special cazurile de fals pozitiv și fals negativ, mai precis motivul pentru care multe persoane sunt identificate în mod eronat ca având intenții de fraudă, iar multe acțiuni frauduloase nu sunt detectate. Deși este posibil ca un sistem de clasificare să tolereze rate de eroare mai mari decât cele de verificare sau identificare, trebuie să existe măsuri adecvate pentru a soluționa în mod oportun cazurile care pot fi clasificate în mod eronat.

- Consimțământ și transparență: în cazul acestor tehnologii, se pot adopta abordări care respectă viața privată – de exemplu, se pot lua măsuri privind verificarea caracterului adecvat al conversațiilor și privind informarea persoanelor vizate despre acțiunea desfășurată. Într-un studiu de caz, unele persoane au fost considerate neeligibile pentru că nu vorbeau limba engleză ca limbă maternă, pentru că aveau deficiențe de auz sau cognitive sau pentru că nu aveau acces la telefon. Solicitanții au fost liberi să refuze participarea la convorbire și să ofere informații în mod tradițional, ca și persoanele care nu au dorit sau nu au fost capabile să participe la acest sistem, fără a fi dezavantajați.

- Alt scop (alte scopuri) al prelucrării: cu toate că, în cele mai multe cazuri, implementarea acestei tehnologii necesită modificări specifice ale infrastructurii, în prezent, atât sectorul public, cât și cel privat își consolidează infrastructura IT pentru a include tehnologii precum Voice over IP, prin urmare, această tehnologie poate fi mai ușor integrată, fără a ține seama de obligațiile operatorului în materie de protecție a datelor.

- Revocabilitate: cu toate că o persoană își poate modifica vocea în mod deliberat, tiparele de voce sunt destul de stabile și pot fi eficiente pentru identificarea unei persoane, în special dacă aceasta nu este informată (și, prin urmare, nu tinde să-și modifice vocea).

- Protecția anti-spoofing: spoofing-ul poate fi aplicat sistemelor de recunoaștere vocală, prin utilizarea de voci înregistrate. Tehnicile anti-spoofing includ întrebări/răspunsuri privind informații contextuale (vorbitorului i se cere să indice data curentă sau să repete cuvinte rare).

4.4.5. ADN

Îmbunătățirile aduse dispozitivelor utilizate pentru secvențierea și compararea ADN-ului, precum și disponibilitatea echipamentului necesar pentru analiza ADN-ului la prețuri accesibile fac necesară revenirea asupra unor afirmații din documentul de lucru anterior referitor la datele biometrice (WP80).

Una dintre schimbările majore aduse de tehnologiile de creare de profile ADN este reducerea timpului necesar pentru operațiunile de secvențiere și comparare a ADN-ului. Progresele permanente realizate de-a lungul anilor de către cercetători și dezvoltatorii de biotehnologii au redus timpul necesar pentru generarea unui profil ADN de la câteva zile la câteva ore sau chiar mai puțin de o oră.

Inițierea unei piețe de servicii online bazate pe ADN reprezintă o amenințare pentru drepturile persoanelor la protecția datelor cu caracter personal, în special atunci când serviciul respectiv

implică transferul de probe și date biometrice între diferite țări (inclusiv țări din afara UE), operatori de date multipli și lipsa unor măsuri adecvate pentru prelucrarea de date genetice sau referitoare la sănătatea persoanelor vizate.

Este foarte probabil ca, în viitorul apropiat, să existe posibilitatea de a se crea profile ADN și de a se compara probe de ADN în timp real (sau aproape real), cu ajutorul unor dispozitive portabile, iar acesta va reprezenta punctul de plecare pentru dezvoltarea de sisteme biometrice de identificare/autentificare pe baza ADN-ului, care prezintă un grad mai înalt de acuratețe comparativ cu autentificarea pe baza amprentelor, a recunoașterii vocale sau faciale.

Îmbunătățirile aduse generării de profile ADN reflectă, de asemenea, interesul din ce în ce mai mare al guvernelor, judecătorilor și autorităților de aplicare a legii pentru biotehnologiile utilizate în cercetarea penală. Datorită fiabilității potrivirii ADN-ului și a faptului că probele ADN pot fi colectate fără cunoștința persoanei vizate, mai multe state membre au creat în timp sau au introdus inițiative de a crea bănci de date centralizate conținând profilele ADN ale persoanelor condamnate, precum și probele descoperite la locul faptei.

În mai 2005, șapte state membre UE au semnat acordul cunoscut sub numele de „Tratatul de la Prüm", cu scopul de a îmbunătăți cooperarea în cadrul anchetelor penale transfrontaliere și în domeniul justiției prin schimbul de informații. Acordul pune noi baze de cooperare, oferind semnatarilor anumite drepturi de acces la bazele de date ADN naționale, numai în contextul urmăririi penale, precum și la date referitoare la amprente, date cu și fără caracter personal și informații privind înmatricularea vehiculelor. Ulterior, alte state membre au aderat la tratat, elementele principale ale acestuia fiind incluse în Decizia 2008/615/JAI a Consiliului.

În acest cadru juridic, mai multe state membre ale UE dețin sau vor deține în viitorul apropiat o bancă de date națională funcțională conținând profilele ADN ale persoanelor condamnate și probe de la locul faptei, ceea ce dă naștere la preocupări cu privire la această prelucrare specifică a datelor.

Una dintre problemele majore legate de crearea băncilor de date ADN constă în faptul că datele genetice derivate din probele ADN (loci) pot dezvălui – nu imediat, în etapa de colectare – informații asociate cu starea de sănătate, predispoziția pentru contractarea unor boli sau originea etnică. Din acest motiv, crearea de baze de date ADN prezintă un risc semnificativ pentru demnitatea umană și drepturile fundamentale. Acest risc a fost analizat în Rezoluția 2009/C 296/01 a Consiliului. Există dispoziții specifice privind limitarea analizei ADN la zonele cromozomiale fără caracteristici genetice, prin utilizarea unui set specific de markeri ADN care, conform datelor cunoscute, nu oferă informații referitoare la caracteristici ereditare specifice [acesta este cunoscut sub denumirea ESS – „European Standard Set" (setul european de referință)].

Cu toate acestea, având în vedere posibilitatea ca unul dintre markerii extrași și introduși într-o bază de date ADN națională să dezvăluie, în viitor, caracteristici ereditare sau alte informații sensibile, trebuie să se acorde o atenție constantă progreselor înregistrate în domeniul biologiei, cu consecința ca, într-o astfel de situație, unele dintre informațiile din baza de date să fie șterse imediat. În plus, având în vedere că bazele de date ADN conțin profilele persoanelor condamnate, analiza statistică a datelor trebuie să fie limitată strict, pentru a se evita crearea de profile bazate pe criterii de gen sau rasiale.

În ceea ce privește bazele de date ADN pentru uzul poliției și al justiției penale, Curtea Europeană a Drepturilor Omului a hotărât să se facă o distincție clară între prelucrarea datelor

cu caracter personal și profilele genetice ale suspecților și ale persoanelor condamnate pentru săvârșirea unei infracțiuni[16].

Există, de asemenea, un risc potențial ca analiza ADN-ului să fie utilizată pentru a identifica membri de familie sau rude legate de infracțiuni nesoluționate sau persoane condamnate, deoarece profilele ADN pot fi căutate în baza de date pe baza unor seturi parțiale de markeri sau caractere de înlocuire. Această funcție ridică probleme privind implicațiile urmăririi informațiilor derivate dintr-o căutare pe criterii familiale.

Trebuie precizat, de asemenea, că există riscuri specifice asociate cu utilizarea seturilor de date din genom în contextul cercetării. Grupul de lucru consideră că accesul la probe și la date ar trebui să fie limitat strict la cercetători și ar trebui permis exclusiv în scopuri de cercetare; în plus, este necesar să se clarifice circumstanțele în care datele și rezultatele cercetării ar trebui să fie dezvăluite persoanelor (ținând seama, de asemenea, de dreptul lor de a nu ști) sau să fie incluse în evidențele medicale.

Riscurile în materie de protecție a datelor asociate cu utilizarea ADN-ului ca dată biometrică sunt prezentate în continuare:

- Acuratețe: chiar dacă ADN-ul prezintă un grad foarte înalt de acuratețe, trebuie să se țină seama de faptul că aceasta depinde de numărul de markeri (loci) analizați. Sistemele de testare ar trebui să asigure cel mai înalt grad de acuratețe.

- Impact: utilizarea ADN-ului poate fi privită ca foarte intruzivă pentru persoanele vizate. Datele genetice pot dezvălui informații sensibile. Analiza statistică a datelor poate fi utilizată, de asemenea, pentru crearea de profile și poate avea efecte discriminatorii asupra persoanelor vizate.

- Alt scop/alte scopuri al (ale) prelucrării: noile tehnologii permit, în prezent, schimbul de cantități din ce în ce mai mari de date. Din acest motiv, trebuie să se stabilească clar cine poate avea acces la informațiile dintr-o bază de date ADN. Căutarea pe criterii familiale și identificarea rasială pot fi considerate noi tehnologii care nu corespund scopului original al prelucrării în bazele de date ADN disponibile în prezent.

- Consimțământ și transparență: în prezent, se oferă servicii de efectuare a analizei ADN a unor probe biologice trimise prin serviciile poștale (de exemplu, salivă), rezultatele acesteia urmând să fie comunicate prin internet. Verificarea insuficientă a identității poate permite persoanelor sau entităților să trimită probe ale altor persoane și să obțină astfel date sensibile cu caracter personal ale persoanelor respective.

- Stabilirea de legături: având în vedere cantitatea și varietatea informațiilor care pot rezulta din secvențierea ADN-ului, există un potențial crescut ca acesta să fie folosit în mod incorect, deoarece datele extrase pot fi legate cu ușurință de alte baze de date, ceea ce permite generarea profilului persoanei. Căutarea pe criterii familiale permite, de asemenea, crearea de legături cu rudele.

- Prelucrarea datelor sensibile: ADN-ul poate furniza informații referitoare la starea de sănătate, predispoziția de a contracta anumite boli sau originea etnică a unei persoane. Prin urmare, este extrem de important să se aplice principiul reducerii la minim a

[16] CEDO, Hotărârea din 4.12.2008, S. și Marper c. UK (cererile nr. 30562/04 și 30566/04), în special punctul 125.

datelor atunci când se aleg markerii (loci) relevanți. Datele ADN pot fi extrase din multe mostre pentru o perioadă lungă de timp, prin urmare, este recomandabil ca accesul la mostre să fie limitat strict la utilizatorii autorizați și pentru utilizări autorizate.

- Revocabilitate: ADN-ul este irevocabil.

- Protecție anti-spoofing: *a priori*, este foarte dificil ca ADN-ul să fie afectat de spoofing; cu toate acestea, în multe cazuri, nu este dificil să se obțină probe de ADN de la o persoană (de exemplu, fire de păr) fără cunoștința acesteia.

4.4.6. Biometria semnăturii

Biometria semnăturii poate fi considerată un exemplu de utilizare nouă a tehnologiilor biometrice tradiționale. Aceasta constă în tehnici biometrice bazate pe trăsături comportamentale care măsoară comportamentul unei persoane astfel cum este exprimat acesta de dinamica semnăturii olografe. În timp ce recunoașterea tradițională a semnăturii se bazează pe analiza caracteristicilor statice sau geometrice ale imaginii vizuale a semnăturii (aspectul semnăturii), biometria semnăturii se referă, în schimb, la analiza caracteristicilor dinamice ale semnăturii (modul în care a fost făcută semnătura), aceste tehnici fiind cunoscute adesea sub denumirea de „semnătură dinamică”.

Caracteristicile dinamice tipice măsurate de un sistem biometric de autentificare a semnăturii (cum ar fi o tabletă grafică) sunt gradul de presiune, unghiul de scriere, rapiditatea și accelerația stiloului, formarea literelor, direcția liniilor din semnătură și alte trăsături dinamice unice. Utilizarea și importanța acestor caracteristici variază de la comerciant la comerciant și sunt colectate folosind dispozitive sensibile la contact. Unele dispozitive de recunoaștere a semnăturii pot efectua verificarea prin combinarea analizei caracteristicilor statice (imaginea vizuală) și dinamice (presiunea, unghiul, rapiditatea etc.) ale unei semnături.

Riscurile în materie de protecție a datelor asociate cu utilizarea biometriei semnăturii sunt prezentate în continuare:

- Acuratețe: este posibil ca aceeași persoană să nu semneze întotdeauna în același mod, prin urmare ar putea întâmpina probleme atât în cadrul procesului de înregistrare, cât și atunci când i se verifică identitatea.

- Impact: datele biometrice referitoare la caracteristici comportamentale precum semnătura pot să nu rămână unice în timp și pot fi modificate de persoana vizată. Semnătura poate suferi modificări, de asemenea, din motive fiziologice, ceea ce împiedică verificarea, fiind necesare proceduri alternative pentru verificarea identității persoanelor.

- Anti-spoofing: în timp ce imaginea grafică a semnăturii tradiționale poate fi copiată și falsificată cu ușurință de o persoană cu experiență în acest sens, prin fotocopiere sau cu ajutorul programelor de grafică pe calculator, o semnătură dinamică este mai sigură deoarece, în procesul de verificare, se analizează, de asemenea, caracteristicile dinamice, care sunt complexe și unice scrierii de mână a unei persoane.

5. Orientări generale, recomandări specifice pe sectoare și măsuri tehnice și organizatorice

Introducerea unui sistem biometric necesită cooperarea mai multor actori:

- producătorii: proiectează și testează senzorii biometrici și definesc performanța tehnologiilor biometrice;
- integratorii: proiectează produsul final care va fi vândut clienților; aleg tehnologia biometrică și definesc, în parte, scopurile sistemului (prin alegerea clienților cărora li se adresează sistemul);
- revânzătorii: comercializează produsul final clienților; informează, în general, clienții cu privire la performanța, riscurile și, eventual, cadrul juridic;
- instalatorii: instalează produsul la sediul clientului;
- clienții: aleg să achiziționeze un sistem biometric; definesc scopul și mijloacele prelucrării și sunt, prin urmare, operatori de date;
- persoanele vizate: furnizează datele biometrice utilizate de sistem.

Unii actori îndeplinesc unul sau mai multe dintre rolurile enumerate mai sus. Fiecare dintre aceștia are responsabilitatea de a asigura o utilizare a sistemelor biometrice care respectă viața privată: de exemplu, instalatorul poate să nu implementeze o măsură de securitate definită de integrator.

5.1. Principii generale

În ceea ce privește datele biometrice, securitatea trebuie să constituie o preocupare primordială deoarece datele biometrice sunt irevocabile: prin urmare, o breșă în securitatea datelor biometrice afectează utilizarea viitoare sigură a datelor biometrice ca identificatori și dreptul la protecția datelor al persoanelor, pentru care nu este posibil să se reducă efectele provocate de producerea breșei.

Riscurile cresc odată cu numărul aplicațiilor care utilizează astfel de date (în special, riscurile de apariție a breșelor și de denaturare a funcțiilor). Cu cât se utilizează mai multe date biometrice, cu atât mai probabil este furtul de date biometrice.

Grupul de lucru recunoaște tendința actuală de a permite accesarea de la distanță a sistemelor biometrice, de exemplu interfețe furnizate pe internet. Această tendință generează o nouă serie de probleme de securitate, multe dintre ele fiind binecunoscute în industria IT. Instalarea unui astfel de sistem ar trebui să presupună implicarea unor specialiști în securitate din domeniul IT, încă din faza de proiectare.

Grupul de lucru recomandă un nivel înalt de protecție tehnică pentru prelucrarea datelor biometrice, utilizând cele mai recente posibilități tehnice. În această privință, grupul de lucru recomandă respectarea standardelor industriale privind protejarea sistemelor în care se prelucrează date biometrice.

5.2. Respectarea vieții private în conceperea sistemelor

Acest concept („Privacy by design”)se referă la integrarea în mod proactiv a principiilor privind respectarea vieții private în tehnologia concepută.

În ceea ce privește sistemele biometrice, acest concept influențează întregul lanț valoric al sistemelor:

- producătorii ar trebui să implementeze principiile privind respectarea vieții private în conceperea sistemelor atunci când proiectează tehnologii și senzori noi: aceasta poate

presupune ștergerea automată a datelor brute după generarea modelului sau utilizarea codificării în stocarea datelor biometrice (fie într-o bază de date centralizată, fie pe un card inteligent). De asemenea, producătorii ar trebui să se concentreze asupra dezvoltării de tehnologii biometrice care respectă viața privată a persoanelor;

- integratorii și revânzătorii ar trebui să implementeze, de asemenea, principiile privind respectarea vieții private încă din momentul conceperii, atunci când definesc produsul final care va fi comercializat, alegând tehnologii care nu afectează viața privată și adăugând produsului final măsuri de securitate suplimentare precum descentralizarea bazei de date;
- clienții (viitorii operatori de date) ar trebui să aplice principiile privind respectarea vieții private încă din momentul conceperii sistemelor biometrice,atunci când solicită un anumit sistem biometric sau atunci când definesc caracteristicile tehnice ale sistemului. În acest caz, producătorii și integratorii ar trebui să ofere produse cu un anumit grad de flexibilitate, pentru a se respecta principiile proporționalității, limitării scopului, minimizării datelor și securității.

Aceste principii au fost deja implementate cu succes în unele dispozitive biometrice: unii producători au inclus într-un cititor biometric specific funcții de codificare, comutatoare anti-pulling și anti-tamper pentru a împiedica accesul neautorizat la datele biometrice.

Grupul de lucru recomandă ca sistemele biometrice să fie proiectate în conformitate cu „ciclurile de viață al dezvoltării" oficiale, care includ următoarele etape:

1. Specificarea cerințelor pe baza unei analize a riscurilor și/sau a unei evaluări specifice a impactului asupra vieții private.
2. Descrierea și justificarea modului în care proiectul îndeplinește cerințele.
3. Validarea, pe baza testelor de funcționare și de securitate.
4. Verificarea conformității proiectului final cu dispozițiile cadrului de reglementare.

Grupul de lucru încurajează stabilirea de sisteme de certificare, care ar putea asigura aplicarea principiilor privind respectarea vieții private încă din momentul conceperii și ar completa informațiile operatorilor de date cu privire la riscurile în materie de protecție a datelor asociate cu sistemele biometrice.

5.3. Cadrul evaluării impactului asupra vieții private

5.3.1. Principii generale

Evaluarea impactului asupra vieții private este un proces în cadrul căruia o entitate efectuează o analiză a riscurilor asociate cu prelucrarea datelor cu caracter personal și stabilește măsuri suplimentare menite să reducă aceste riscuri. De exemplu, în ceea ce privește tehnologia RFID, grupul de lucru a stabilit că entitatea care definește aplicația este răspunzătoare de realizarea evaluării impactului asupra vieții private. Această entitate poate fi operatorul de date sau furnizorul care proiectează aplicația RFID.

Având în vedere riscurile specifice asociate cu utilizarea datelor biometrice, grupul de lucru recomandă ca entitatea care definește scopul și funcționarea dispozitivului să efectueze evaluarea impactului asupra vieții private ca parte integrantă a fazei de proiectare a sistemelor care utilizează acest tip de date. Această entitate poate fi producătorul, integratorul sau clientul final.

Evaluarea impactului asupra vieții private ar trebui să țină seama de:

- natura informațiilor colectate;
- scopul colectării informațiilor;

- acuratețea sistemului, presupunând că potrivirea/nepotrivirea unui model biometric poate determina luarea de decizii importante pentru persoana vizată;
- temeiul legal și respectarea prevederilor legale; este consimțământul necesar?
- accesul la dispozitiv și schimbul intern și extern de informații în cadrul entității operator de date, care necesită proceduri și tehnici de securitate în vederea protejării datelor cu caracter personal împotriva accesului neautorizat;
- măsurile mai puțin invazive pentru viața privată care au fost deja luate. Există o alternativă la introducerea dispozitivului biometric (precum solicitarea prezentării cărții de identitate)?
- deciziile luate cu privire la perioada de reținere și ștergerea datelor. Care este perioada de timp relevantă? Sunt toate datele colectate pentru aceeași perioadă de timp? Există un mecanism automat de decizie și un proces subsidiar adecvat?
- drepturile persoanelor vizate.

Evaluarea impactului asupra vieții private nu ar trebui să se concentreze numai pe identificarea riscurilor, ci ar trebui să prevadă, de asemenea, măsuri adecvate de protecție a datelor și să precizeze modul în care operatorul de date a identificat soluții adecvate pentru reducerea riscurilor referitoare la protecția datelor, prezentate în secțiunea anterioară.

În cazul în care evaluarea impactului a fost realizată de către producător sau de către integrator, introducerea sistemului biometric poate necesita o evaluare suplimentară, care să ia în considerare particularitățile operatorului de date. De exemplu, în situația în care un sistem biometric este integrat în sistemul informatic al clientului, acesta ar trebui să realizeze o evaluare suplimentară a impactului asupra vieții private cu privire la propriile proceduri și măsuri de securitate IT.

5.3.2. Specificitatea datelor biometrice

Datele biometrice necesită o atenție specifică, deoarece acestea identifică în mod neechivoc o persoană utilizând caracteristicile sale comportamentale sau fiziologice unice.

Din acest motiv, evaluarea impactului asupra vieții private ar trebui să analizeze modul în care următoarele trei riscuri pot fi evitate sau limitate în mod substanțial de sistemul în cauză.

Primul risc îl reprezintă uzurparea identității, în special în cazul identificării sau al autentificării. Dispozitivul biometric ar trebui să nu se lase păcălit de un atac spoofing și să se asigure că persoana care încearcă să efectueze potrivirea este, într-adevăr, persoana înregistrată în sistem. Această amenințare pare mai puțin semnificativă în cazul datelor care nu pot fi colectate fără cunoștința persoanei vizate, precum modelul venelor[17]. În schimb aceasta constituie, cu siguranță, o preocupare majoră pentru dispozitivele bazate pe amprente și recunoașterea facială. Amprentele se pot lăsa oriunde, prin simpla atingere a unui obiect. Chipul, de asemenea, poate fi surprins într-o fotografie fără cunoștința persoanei vizate.

[17] Chiar dacă este dificil să se anticipeze tipurile de atacuri asupra tehnologiei bazate pe modelul venelor care vor fi posibile în anii următori, în cazul în care această tehnologie își lărgește aria de utilizare.

Cel de-al doilea risc îl reprezintă devierea scopului, fie de către operatorul de date însuși, fie de către un terț, inclusiv autoritățile de aplicare a legii. Acest risc frecvent privind datele cu caracter personal devine esențial atunci când este vorba despre datele biometrice. Producătorii ar trebui să ia toate măsurile de securitate pentru a evita orice utilizare neadecvată a datelor și pentru a asigura că datele care nu mai sunt necesare pentru prelucrare sunt șterse fără întârziere.

Ca și în cazul altor date, datele biometrice sau sursele datelor biometrice, prelucrate sau stocate în mod legitim, nu pot fi prelucrate sau înregistrate de către operator în alt scop decât dacă există un nou temei legal pentru noua prelucrare a datelor.

Cel de-al treilea risc este breșa în securitatea datelor, care necesită măsuri speciale în contextul datelor biometrice, în funcție de tipul de date care au fost compromise. Dacă se utilizează un sistem care creează date biometrice pe baza unui algoritm care transformă un model biometric într-un anumit cod și dacă algoritmul sau datele biometrice sunt furate sau compromise, acestea trebuie să fie înlocuite. Atunci când o breșă de securitate determină pierderea unor date biometrice identificate direct, care sunt foarte apropiate de sursa datelor biometrice, precum fotografii ale chipului unei persoane sau amprente, persoana respectivă trebuie să primească o notificare detaliată pentru a putea să se apere într-o potențială situație viitoare în care datele biometrice compromise pot fi folosite ca probă împotriva acesteia.

5.4. Măsuri tehnice și organizatorice

Datorită naturii acestora, prelucrarea datelor biometrice necesită acțiuni și măsuri de precauție tehnice și organizatorice speciale pentru a se preveni efectele negative asupra persoanei vizate în eventualitatea producerii unei breșe de securitate – în special, din cauza riscurilor rezultate din acțiuni ilegale prin care se urmărește „reconstruirea" unei caracteristici biometrice pe baza unui model de referință, stabilirea de legături cu diferite baze de date sau „utilizarea" în continuare a datelor fără cunoștința persoanei vizate, în scopuri incompatibile cu cele inițiale și/sau a posibilității ca unele date biometrice să fie utilizate pentru a se extrage informații rasiale sau medicale cu privire la persoanele vizate.

5.4.1. Măsuri tehnice

- *Utilizarea modelelor biometrice*

Datele biometrice ar trebui să fie stocate sub formă de modele biometrice, atunci când există această posibilitate.

Modelul ar trebui să fie extras printr-o metodă specifică sistemului biometric respectiv, care nu este utilizată de alți operatori deținători de sisteme similare, pentru a garanta că o persoană poate fi identificată numai în cadrul sistemelor biometrice care au un temei legal pentru prelucrare.

- *Stocarea pe dispozitive personale sau stocarea centralizată*

Atunci când prelucrarea datelor biometrice este permisă, se preferă să se evite stocarea centralizată a informațiilor biometrice cu caracter personal.

În special în scop de verificare, grupul de lucru consideră că este recomandabil ca sistemele biometrice să se bazeze pe citirea datelor biometrice stocate sub formă de modele criptate pe dispozitive de stocare deținute exclusiv de către persoanele vizate relevante (de exemplu, carduri inteligente sau dispozitive similare). Caracteristicile biometrice pot fi comparate cu modelul (modelele) stocat(e) pe card și/sau dispozitiv cu ajutorul procedurilor standard de comparare implementate direct pe cardul și/sau dispozitivul în cauză, iar crearea unei baze de

date care include informații biometrice ar trebui să fie evitată, în general și dacă este posibil. Într-adevăr, în cazul în care cardul și/sau dispozitivul este pierdut sau rătăcit, există, în prezent, riscuri limitate ca informațiile biometrice respective să fie utilizate în mod fraudulos. Pentru a reduce riscul furtului de identitate, dispozitivele ar trebui să stocheze date limitate de identificare privind subiectul datelor.

Cu toate acestea, în scopuri specifice și pentru necesități obiective, bazele de date centralizate conținând informații și/sau modele biometrice pot fi considerate admisibile. Sistemul biometric utilizat și măsurile de securitate selectate ar trebui să limiteze riscurile menționate și să garanteze că reutilizarea în alte scopuri a datelor biometrice în cauză este imposibilă sau, cel puțin, detectabilă. Ar trebui să se utilizeze mecanisme bazate pe tehnologiile de codificare pentru a preveni citirea, copierea, modificarea sau scoaterea neautorizată a datelor biometrice.

Atunci când datele biometrice sunt stocate pe un dispozitiv pe care subiectul datelor îl controlează din punct de vedere fizic, ar trebui să se utilizeze o cheie de criptare specifică pentru dispozitivele de citire, ca o măsură de protecție eficientă a datelor împotriva accesului neautorizat. În plus, sistemele descentralizate asigură datelor biometrice un nivel de protecție mai înalt prin însăși natura acestora, deoarece subiectul datelor deține controlul fizic asupra datelor sale și nu există niciun element care poate fi vizat sau exploatat.

Grupul de lucru subliniază, de asemenea, că ideea de bază de date centralizată acoperă o gamă largă de aplicații tehnice, de la stocarea în cadrul cititorului până la o bază de date găzduită de o rețea.

- *Înnoirea și revocabilitatea*

Având în vedere faptul că sursa datelor biometrice nu se poate schimba, sistemele biometrice care au ca scop stabilirea unei legături de identitate trebuie să fie proiectate astfel încât procesul de înregistrare și de prelucrare a datelor biometrice să permită extragerea de modele biometrice multiple și independente din aceeași sursă, pentru a exista posibilitatea înlocuirii acestora în eventualitatea unei breșe de securitate sau a progreselor tehnice.

Sistemele biometrice ar trebui concepute astfel încât să existe posibilitatea revocării legăturii de identitate, fie în vederea înnoirii acesteia, fie a ștergerii sale definitive, de exemplu în cazul în care consimțământul este retras[18].

- *Forma criptată*

În ceea ce privește securitatea, ar trebui să se adopte măsuri corespunzătoare pentru protejarea datelor stocate și prelucrate de sistemul biometric: datele biometrice trebuie să fie stocate întotdeauna sub formă criptată. Trebuie să se stabilească un cadru de gestionare care să garanteze că toate cheile de decriptare sunt accesibile numai persoanelor relevante.

Având în vedere utilizarea la scară largă a bazelor de date publice și private care conțin informații biometrice și interoperabilitatea crescândă a diferitelor sisteme care utilizează date

[18] De exemplu, tehnologia TURBINE, menită să protejeze modelul biometric prin transformarea criptografică a informațiilor referitoare la amprentă într-o cheie neconvertibilă care permite potrivirea prin comparare bit-cu-bit. Datele biometrice transformate sunt considerate ireversibile, nemaiputându-se reveni la probele și modelele biometrice originale. În plus, pentru a spori încrederea utilizatorului, această cheie este, de asemenea, revocabilă, însemnând că o nouă cheie independentă poate fi generată pentru a recrea identități biometrice. A se vedea, de asemenea: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf

biometrice, ar trebui să se prefere tehnologiile specifice sau formatele de date care fac imposibile interconectările bazelor de date biometrice și divulgările neautorizate de date.

- *Anti-spoofing*

Pentru a menține fiabilitatea unui sistem biometric și a preveni uzurparea de identitate, producătorul trebuie să implementeze sisteme care urmăresc să stabilească dacă datele biometrice sunt autentice și sunt încă legate de o persoană fizică. În ceea ce privește recunoașterea facială, este esențial să se asigure că chipul este cel real și nu, de exemplu, o fotografie atașată în locul capului unui impostor.

- *Criptarea și decriptarea biometrică*

Criptarea biometrică este o tehnică care utilizează caracteristici biometrice în cadrul algoritmului de criptare/decriptare. În acest caz, un fragment din datele biometrice este utilizat, în general, ca o cheie de criptare a unui identificator necesar pentru serviciu.

Acest sistem prezintă multiple avantaje[19]. În sistem nu se stochează identificatorul sau datele biometrice, ci numai rezultatul identificatorului criptat odată cu datele biometrice. În plus, datele cu caracter personal sunt revocabile, deoarece este posibil să se creeze un alt identificator care poate fi protejat, de asemenea, prin criptare biometrică. În final, sistemul este mai sigur și mai ușor de utilizat pentru persoana vizată, nemaifiind necesar ca aceasta să trebuiască să memoreze parole lungi și complexe.

Totuși, abordarea criptografică presupune o problemă dificilă, deoarece criptarea și decriptarea nu tolerează modificarea cheii, în timp ce datele biometrice determină diferite modele, care pot da naștere la modificări în cheia extrasă. Prin urmare, sistemul trebuie să fie capabil să calculeze aceeași cheie din date biometrice ușor diferite, fără ca rata de acceptare falsă să crească.

Grupul de lucru este de acord cu faptul că tehnologia de criptare biometrică este un domeniu de cercetare fertil și care a devenit suficient de matur pentru a fi inclus în politici publice mai largi, pentru dezvoltarea de prototipuri și pentru analiza aplicațiilor.

- *Mecanisme automate de ștergere a datelor*

Pentru a preveni stocarea informațiilor biometrice pentru o perioadă mai lungă decât este necesar în scopul pentru care au fost colectate și prelucrate ulterior, trebuie să se implementeze mecanisme automate corespunzătoare de ștergere a datelor, inclusiv în cazul în care perioada de reține poate fi prelungită în mod legal, asigurându-se astfel ștergerea oportună a datelor cu caracter personal care nu mai sunt necesare pentru funcționarea sistemului biometric.

Atunci când se utilizează stocarea integrată pe cititor, producătorii pot implementa, de asemenea, stocarea modelelor biometrice pe memorii volatile, care garantează că datele vor fi șterse atunci când se întrerupe alimentarea cititorului. Prin urmare, bazele de date biometrice nu mai există atunci când cititorul este vândut sau dezinstalat. Se pot utiliza, de asemenea, comutatoare anti-extragere pentru a șterge în mod automat datele în cazul în care cineva încearcă să fure cititorul.

- *Baze de date biometrice de mari dimensiuni și baze de date „cu legături slabe”*

Unele țări utilizează baze de date biometrice mari în special în două scopuri: pentru cercetarea penală și pentru securizarea eliberării documentelor de identitate (pașapoarte, cărți de

[19] http://www.ipc.on.ca/images/resources/bio-encryp.pdf.

identitate, permise de conducere). Bazele de date utilizate în cercetarea penală conțin, în general, informații despre infractori și suspecți și sunt concepute în vederea identificării unei persoane pe baza datelor biometrice. În schimb, bazele de date utilizate pentru combaterea uzurpării de identitate includ datele biometrice ale întregii populații și ar trebui să fie utilizate numai pentru a autentifica persoana (de exemplu, dacă o persoană și-a pierdut documentele de identitate sau a distrus cipul de securitate al pașaportului, în care sunt stocate datele biometrice).

Atunci când o bază de date centrală este utilizată în scopul combaterii uzurpării de identitate, grupul de lucru consideră că ar trebui să se implementeze măsuri tehnice pentru a se evita denaturarea scopului. În primul rând, principiul reducerii la minim a datelor impune colectarea exclusivă a datelor necesare pentru autentificarea persoanei. De exemplu, conform cercetărilor, compararea amprentelor de la două degete este suficient de precisă pentru a autentifica o persoană.

În plus, operatorii de date pot utiliza baze de date „cu legături slabe”, în care identitatea unei persoane nu este legată de un singur set de date biometrice, ci, mai degrabă, de un grup de astfel de seturi. Modul de concepere a bazei de date ar trebui să garanteze autentificarea persoanei cu un grad foarte ridicat de probabilitate (de exemplu, un procentaj de 99,9% este suficient pentru a descuraja impostorii) și să asigure că baza de date nu poate fi folosită pentru identificare (deoarece un set de date biometrice corespunde unui număr mare de persoane).

Grupul de lucru susține utilizarea acestui tip de sisteme atunci când se utilizează baze de date biometrice de mari dimensiuni în scopul combaterii uzurpării de identitate.

Exemplu: măsuri tehnice pentru sistemele de autentificare
Sursa datelor biometrice este unică și poate fi asociată subiectului datelor pe întreaga durată a vieții acestuia. Dacă aceasta este utilizată ca fundament al sistemelor de autentificare, trebuie să se aibă în vedere că sursa de date biometrice nu poate fi schimbată, în timp ce, în cadrul tehnicilor obișnuite de autentificare care necesită, în general, „cunoașterea sau deținerea” unui mijloc de legitimare (de exemplu, cunoașterea numelui de utilizator, a unei parole), este întotdeauna posibil ca mijlocul respectiv să fie modificat. Prin urmare, sistemele care utilizează autentificarea biometrică trebuie să fie echipate cu măsuri de protecție speciale pentru a proteja legătura dintre datele biometrice și alte date referitoare la identitatea persoanei vizate:
- Datele referitoare la modele nu trebuie să fie stocate la nivel centralizat, deoarece securitatea stocării datelor biometrice este esențială pentru securitatea generală a sistemului biometric. Ar trebui să se prefere stocarea distribuită (de exemplu, pe un card inteligent). În acest caz, atât sursa datelor, cât și modelul se află în posesia subiectului datelor.
- Stocarea și transmiterea datelor biometrice trebuie să fie protejate împotriva interceptării, divulgării neautorizate și modificării prin utilizarea unor tehnologii de criptare adecvate.
- Unele tipuri de date biometrice nu sunt secrete (de exemplu, chipul) și nu pot fi blocate sau schimbate în urma breșelor de securitate, a divulgării sau a cazurilor de utilizare clandestină. Prin urmare, autentificarea ar trebui să fie combinată cu alte mijloace de verificare care pot fi blocate sau schimbate.

5.4.2. Măsuri organizatorice

Pentru a garanta protecția datelor, este necesar să se planifice și să se pună în aplicare măsuri organizatorice. De exemplu, operatorul de date trebuie să stabilească o procedură clară privind persoanele care pot accesa informațiile din sistem, tipul de acces (parțial sau integral) și motivele accesării. Trebuie să se poată asigura trasabilitatea tuturor acțiunilor.

Grupul de lucru constată că externalizarea serviciului către furnizorii externi este posibilă, inclusiv pentru cererile de viză [secțiunile 13 și 43 din Regulamentul (CE) nr. 810/2009 din 13 iulie 2009 privind instituirea unui Cod comunitar de vize], și devine din ce în ce mai răspândită, din cauza utilizării din ce în ce mai frecvente a stocării dematerializate.

În această situație, operatorul de date trebuie să stabilească o politică detaliată privind modul de verificare a contractanților, de exemplu prin efectuarea de inspecții inopinate, și să solicite garanții cu privire la angajați, procedura referitoare la drepturile individuale etc.

Adoptat la Bruxelles, la 27 aprilie 2012

Pentru grupul de lucru
Președintele
Jacob KOHNSTAMM