PELIFILIP
SKYTOWER BUILDING
246C CALEA FLOREASCA • 15TH FLOOR
014476 - BUCHAREST • 1ST DISTRICT • ROMANIA
PHONE +40 21 527 2000 • FAX +40 21 527 2001
OFFICE@PELIFILIP.COM • WWW.PELIFILIP.COM

DATELE BIOMETRICE, ÎNTRE AVANTAJELE TEHNOLOGIEI ŞI PREOCUPĂRILE PENTRU SECURITATEA PERSOANEI

Extras: *Biometria cumulează tehnologiile care identifică o persoană / autentifică identificarea unei persoane pe baza caracteristicilor fizice sau chiar comportamentale. Dezvoltarea biometriei s-a petrecut în ritm ameţitor, de la tehnologii bazate pe amprenta digitală, la cele bazate pe recunoaşterea irisului, recunoaşterea facială sau chiar a ritmului biologic ori pe caracteristici comportamentale precum trăsături specifice mersului unei persoane. Pentru că suntem în era vitezei şi a simplificării, autentificarea biometrică a devenit din ce în ce mai comună, inclusiv în sistemele de acces în instituţii sau în spaţii publice ori private, dar şi în comerţ.*

Dacă tehnologiile biometrice ne pot facilita viaţa, nu este mai puţin adevarat că ele colectează date care intră în sfera mai largă a datelor personale şi vin cu preocupări pentru securitatea individului.

*În România, procesele legate de date biometrice nu sunt supuse unei reglementări amănunţite sau speciale, iar Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal ("**Autoritatea**") dar şi instanţele de judecată s-au arătat mai degrabă conservatoare în analiza proporţionalităţii utilizării unor tehnologii biometrice. Cu toate acestea, realitatea ne arată că în această materie suntem pe o autostradă cu un singur sens, iar autorităţile cu putere de legiferare şi de decizie trebuie să găsească întotdeauna echilibrul între avantajele tehnologiilor biometrice şi riscurile pe care le presupun.*

1. Colectarea datelor biometrice

Tehnologiile biometrice presupun captarea datelor biometrice ale unei persoane, transformarea lor într-un tipar biometric (*template*), stocarea acestuia într-o bază de date şi, ulterior, verificarea identităţii acelei persoane prin compararea tiparului biometric cu caracteristica corespunzătoare a individului.

Aceste sisteme asigură rapiditatea identificării şi au rata redusă de eşec în identificare. În mod evident, identificarea cu ajutorul unui cititor de amprente este mai rapidă decât cea folosind, spre exemplu, cardul de identitate. În acelaşi timp, întrucât identificarea se face printr-o caracteristică unică a persoanei şi prin eliminarea factorului uman, identificarea este mai sigură.

Totuşi, tehnologiile biometrice şi rezultatele lor în procesul de identificare/ autentificare nu sunt la adăpost de critici. În primul rând, tehnologiile sunt criticate inclusiv din punct de vedere al securităţii întrucât nu exclud riscul furtului de identitate (spre exemplu, prin folosirea amprentelor false realizate din materiale artificiale). Mai mult, există critici legate de caracterul invaziv, agresiv şi inoportun (*intrusive*) al acestor tehnologii care ar depăşi scopul pentru care sunt folosite (de exemplu, conform unor studii, amprentele pot dezvălui alte date sensibile cu privire la persoană, respectiv informaţii privind originea etnică a persoanei).

Se mai invoca şi riscurile de securitate a bazelor de date care conţin date biometrice. Din acest punct de vedere, este de menţionat că pare că există tehnologii mai prietenoase care înlătură acest risc întrucât ar permite identificarea şi autentificarea biometrică a unei persoane fără a conduce la stocarea datelor într-

o bază de date, ci la stocarea lor într-un aparat aflat în controlul acelei persoane (de exemplu, un *smartphone*).

2. Datele biometrice în legislația datelor personale

Conceptul de date biometrice nu este definit sau reglementat în mod expres în Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (”**Legea 677/2001**”); de altfel, el nu este definit nici în Directiva 95/46/EC privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (”**Directiva 95/46/EC**”).

Definiţia rezultă însă din opinia Grupului de Lucru Art. 29 potrivit căreia datele biometrice sunt *„proprietăţi biologice, de comportament, caracteristici psihologice, trăsături sau acţiuni repetate dacă aceste caracteristici sau acţiuni sunt unice pentru un individ, măsurabile, chiar dacă tiparele folosite în practică pentru măsurarea lor presupun un grad de probabilitate (incertitudine)”*[1]

Mai mult, însăşi Legea 677/2001 poate fi considerată prin interpretare că se referă la acest tip de date reglementând categoria datelor *”cu caracter personal având o funcţie de identificare de aplicabilitate generală”* care pot include şi datele biometrice având în vedere că acestea constau în caracteristici ale corpului ce nu pot fi, în general, schimbate şi care pot fi citite de instrumente automate. În plus, datele biometrice sunt menţionate expres printre categoriile de date pentru care obligaţia de notificare rămâne valabilă în Decizia Autorităţii nr. 200/2015 privind stabilirea cazurilor de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea, precum şi pentru modificarea şi abrogarea unor decizii. Aşadar, se poate concluziona că datele biometrice sunt reglementate de legislaţia română, deşi de manieră foarte restrânsă şi prin act cu o natură juridică secundară.

3. Limitele procesarii datelor biometrice conform legislației din Romania

Conform Legii 677/2001, în general, datele cu caracter personal trebui să fie *„adecvate, pertinente şi neexcesive prin raportare la scopul în care sunt colectate şi ulterior prelucrate”*. În plus, datele biometrice pot fi prelucrate exclusiv în baza consimţământului expres al persoanei vizate sau dacă prelucrarea este permisă în mod expres de o prevedere legală.

Cât priveşte caracterul adecvat, pertinent şi neexcesiv, nici legea şi nici reglementările secundare nu oferă linii directoare. Prin aceasta, măsura în care datele colectate sunt adecvate, pertiente şi neexcesive devine subiect de interpretare.

Cu titlu de exemplu, Autoritatea a considerat că un sistem de pontaj ce funcţiona pe bază de cititor de amprente implică o procesare excesiva în raport cu scopul urmărit. Interpretarea Autorităţii a fost îmbrăţişată de instanţa chemată să desfiinţeze interpretarea şi măsurile Autorităţii, instanţa reţinând că *”nu se justifică necesitatea apelării la sistemul de pontare electronică a angajaţilor, pontarea acestora putând fi realizată şi prin alte mijloace […] întrucât amprentarea angajaţilor ar aduce atingere vieţii private a acestora şi s-ar încălca echilibrul între scopul urmărit şi anume monitorizarea prezenţei acestora la locul de muncă şi respectarea drepturilor persoanelor angajate”*[2]. În mod similar, o altă instanţă a constatat că *„sistemul electronic de pontaj cu data biometrice nu este eficient, nefiind justificată necesitatea apelării la acest sistem, câtă vreme pontarea angajaţilor se poate realiza şi prin alte mijloace care să nu aducă atingere vieţii private a angajaţilor”*[3].

Fără a contesta judecata de valoare din deciziile invocate mai sus, faţă de amploarea acestor tehnologii, riscurile dar şi beneficiile lor, efortul de evaluare şi de interpretare al autorităţilor trebuie să fie unul asumat şi constructiv. Vor exista mereu soluţii alternative pentru monitorizarea prezenţei angajaţilor de

---

1 Opinia 4/2007 cu privire la conceptul de date personale;

2 Decizia nr. 155/2016, CA Piteşti, Secţia a II-a de Contencios Administrativ şi Fiscal;

3 Decizia 172/2016 CA Timişoara, Secţia de Contentios Administrativ şi Fiscal;

exemplu, dar tehnologiile biometrice nu vor mai putea fi respinse în orice circumstanţe. În epoca inteligenţei artificiale, analiza măsurii în care o tehnologie nu asigură suficientă protecţie va fi din ce în ce mai necesară.

Din acest punct de vedere, amintim, cum o făceam şi mai sus, că există informaţii cu privire la existenţa unor tehnologii prietenoase care nu permit stocarea datelor biometrice în baze de date ci ştergerea lor imediată odata ce scopul autentificării a fost atins. În mod similar, Grupul de Lucru Art. 29 arată într-una din opiniile sale că criptarea datelor biometrice şi stocarea codului într-o forma în care informaţia nu poate fi folosită pentru a reda datele biometrice în forma iniţială ar trebui să asigure un nivel de securitate adecvat[4]. Autorităţile vor avea nevoie de suportul necesar pentru a evalua argumentele părţilor, a solicita angajamente şi a lua deciziile adecvate.

Cu titlu de exemplu, menţionăm decizia autorităţii pentru protecţia datelor din Franţa care a anunţat în data de 27 Septembrie 2016 că şi-a actualizat doctrina[5] şi a adoptat o decizie cu privire la procesarea datelor biometrice pentru a ţine pasul cu evoluţia tehnologiei. Cu privire la sistemele de acces în spaţiile de lucru pe baza de date biometrice, Autoritatea impune trei obligaţii principale: (i) justificarea folosirii sistemului cu luarea în considerare a măsurii în care pot fi folosite mijloace mai puţin invazive; (ii) demonstrarea faptului că sistemele sunt proiectate pentru a asigura securitatea şi caracterul confidenţial al prelucrării şi (iii) prezentarea de asigurări cu privire la modul de stocare a datelor. În acelaşi timp, adoptarea măsurilor care să micşoreze riscurile de securitate, precum criptarea, este încurajată.

4. Perspectiva

Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date care va intra în vigoare în luna mai a anului 2018 reglementează în mod expres datele biometrice, menţionându-le între categorii de date cu caracter special. Ca regulă, procesarea acestora este posibilă cu consimţământul persoanei vizate, precum şi, în anumite condiţii, în scopul îndeplinirii anumitor obligaţii şi al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forţei de muncă, când prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii. În plus, Statele Membre pot introduce restricţii suplimentare pentru procesarea datelor biometrice.

În considerarea celor de mai sus, intervenţia Autorităţii prin emiterea de proceduri şi linii directoare cu privire la acceptabilitatea procesării datelor biometrice este utilă. Evoluţia tehnologiei este inevitabilă iar autorităţile (de reglementare şi judecătoreşti deopotrivă) nu pot ignora vântul schimbării şi adaptabilitatea accelerată a unui mediu economic competitiv. Ca atare, atât în materie de reglementare cât şi în materie de deliberare în cazuri în care sunt chemate să se pronunţe, autorităţile trebuie să găsească echilibrul invocat în debutul acestui material între utilitatea tehnologiilor de ultimă generaţie şi riscurile lor, astfel încât să protejeze în egală măsură persoana vizată, dar şi interesul economic al operatorilor.

---

4 Opinia 3/2012 a Grupul de Lucru Art. 29 cu privire la dezvoltarile din domeniul tehnologiilor biometrice;

5 http://www.dataguidance.com/france-cnils-new-biometrics-requirements-anticipate-gdpr