SCRISOARE DESCHISĂ

CĂTRE:

- **Ministerul Afacerilor Interne**
- **Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal**
- **Avocatul Poporului**
- **Camera Deputaților - Comisia pentru cercetarea abuzurilor, corupţiei şi pentru petiţii**

Părțile semnatare reprezintă organizații ale drepturilor fundamentale și reprezentanți ai comunității de specialiști în domeniul protecției datelor de pe teritoriul României. Prin această scrisoare deschisă ne exprimăm îngrijorarea cu privire la respectarea principiilor fundamentale ce țin de respectarea vieții private, prin punerea în aplicare a **sistemului de recunoaștere facială** ce urmează a fi achiziționat de Inspectoratul General al Poliției Române prin procedura de achiziție cu numărul CN1014432[1], **formulând totodată mai multe cereri în mod public**.

Atragem atenția asupra obligației autorităților publice de a respecta şi ocroti viaţa intimă, familială şi privată, în temeiul Art. 26 (1) din Constituția României, art 151 din TFUE, art. 8 din COE și art. 71 din Noul Cod Civil - Dreptul la viață privată.

Subliniem faptul că organizațiile semnatare **nu se poziționează împotriva implementării de noi tehnologii** menite să aducă un plus de siguranță locuitorilor României, **susținând în schimb o abordare responsabilă a acestora**, respectând dreptul la viață privată, conform legislației naționale și europene aplicabile.

Considerăm că decizia implimentării unui sistem de monitorizare în masă, care vizează toți locuitorii României, ar fi trebuit luată, conform cerințelor legale, în urma unui proces real și transparent de evaluare a riscurilor, care **să implice atât Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, cât și societatea civilă**. Lipsa acestui proces ne determină să privim cu scepticism atât legalitatea implementării acestui sistem, cât și capacitatea de a-și îndeplini scopul fără a aduce atingeri drepturilor tuturor locuitorilor României.

Redactarea Caietului de sarcini desconsiderând obligațiile privind instituirea unor garanţii adecvate pentru drepturile şi libertăţile persoanelor va avea drept consecință achiziția unui sistem de recunoaștere facială care nu va putea fi folosit în condiții de legalitate. Inspectoratul General al Poliției Române, din subordinea Ministerului Afacerilor Interne, trebuia să facă o analiză de impact **înainte de a demara orice acțiune legată** de prelucrarea datelor cu caracter personal, cum ar fi achiziționarea aplicației software, și să includă criterii fundamentale care să asigure respectarea principiilor “privacy by design” și ”privacy by default”.

1 http://sicap-prod.e-licitatie.ro/pub/notices/c-notice/v2/view/100069755?fbclid=IwAR2R8so4QmYTLdHr1Abfx2FlE0Oecunc04_rbKtdSaF_gaPFReNbJjHHYX4

Toate organizațiile semnatare susțin introducerea unei noi tehnologii privind **creșterea gradului de combatere și elucidare a infracțiunilor,** ce respecta dreptul la viață privată al persoanelor vizate, precum si celelalte criterii prevazute in lege. Subliniem faptul că interoperabilitatea datelor personale trebuie să se bazeze pe transparență și respectarea principiilor colectării datelor cu caracter personal, astfel încât cetățenii să poată avea încredere că datele lor sunt prelucrate corespunzător, fără a exista riscurile unui dezechilibru.

Prin urmare vă solicităm să vă asigurați că ați urmat toți pașii necesari pentru a oferi posibilitatea acestui sistem să devină funcțional, eficacitatea acestuia să fie una optimă, în conformitate cu dispozițiile legale, fără a aduce atingere drepturilor și libertăților persoanelor. Vă solicităm să țineți cont de următoarele noastre propuneri pentru a obține conformitatea soluției tehnice privind implementarea sistemului de recunoaștere facială.

Situația premisă

În urma publicării unui comunicat de presă[2] la începutul acestui an, în data 27.08.2019 a fost publicat în **Sistem informatic colaborativ pentru mediu performant de desfășurare al achizițiilor publice** (SICAP) anunțul cu numărul de participare CN1014432 privind achiziționarea unei **soluții informatice pentru recunoaștere facială + training**, în cadrul proiectului „Dezvoltarea sistemului de identificare și recunoaștere facială (NBIS) și interconectarea acestuia cu autoritățile de aplicare a legii din UE prin intermediul sTESTA", autoritate contractantă fiind **Inspectoratul General al Poliției Române**, din subordinea Ministerului Afacerilor Interne.

Utilizarea sistemelor de recunoaștere facială a făcut subiectul multor controverse pe plan mondial motiv pentru care achiziția unei astfel de tehnologii a atras imediat atenția organizațiilor din România dedicate protecției drepturilor și libertăților persoanelor.

Pentru introducerea unei astfel de tehnologii, considerăm ca este primordial dialogul și consultarea cu părțile interesate, anterior emiterii Caietului de sarcini pentru achiziția sistemului de recunoaștere facială, astfel încât redactarea cerințelor de achizitie să îndeplinească criteriile privind respectarea vieții private.

Întrucât acest dialog nu a avut loc, venim proactiv în sprijinul Autoritatii contractante prin analiza documentației acestei achiziții și am constatat:

- lipsa îndeplinirii cerințelor de ordin tehnic, referitoare la securitatea prelucrărilor de date, obligatorii pentru o funcționare în condițiile legii a unui asemenea sistem.
- lipsa transparenței privind implementarea sistemului în acord cu principiile privind respectarea vieții private
- lipsa de informații privind măsurile de securitate puse în etapa de utilizare a soluției tehnice
- lipsa informațiilor privind modul de exercitare a drepturilor persoanelor vizate
- lipsa unei evaluări prealabile a impactului asupra datelor personale

2 https://www.politiaromana.ro/ro/stiri-si-media/comunicate/proiect-european-implementat-de-politia-romana

- lipsa unei consultări prealabile cu autoritatea națională de supraveghere (ANSPDCP)
- ponderea mică a corectitudinii algoritmului - conform criteriilor de atribuire a contractului menționate în Caietul de sarcini al achiziției, ponderea pentru „Eficacitatea algoritmului de căutare/comparare" este de doar 30%,

Toate aceste aspecte ne întăresc temerile că soluția informatică, așa cum este ea prezentată în Caietul de sarcini, va expune persoanele vizate unui risc iminent de încălcare a dreptului la viață privată.

Am solicitat o serie de **clarificări**[3] Autorității contractante însă răspunsul acesteia ne-a sugerat că în momentul conceperii **Caietului de sarcini**[4] nu au fost urmate etapele obligatorii conform legislației naționale. Subliniem faptul că ignorarea acestor aspecte în momentul conceperii cerințelor Caietului de sarcini, va avea inevitabil **repercusiuni ireversibile asupra persoanelor vizate ce pot fi afectate de sistemul de recunoaștere facială**.

În conformitate cu Art. 32 din Legea nr. 363/2018, precum și Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 174 din 18 octombrie 2018, autoritatea contractantă (Inspectoratul General al Poliției Române) avea obligația:

- realizării unei **evaluări a impactului prelucrărilor de date (DPIA)**;
- **consultarea prealabilă cu Autoritatea Națională de Supraveghere** a Prelucrării Datelor cu Caracter Personal.

Autoritatea contractantă (Inspectoratul General al Poliției Române) nu a putut confirma existența acestei evaluări sau a îndeplinirii acestei obligații.

Conform art. 11 din Legea nr. 363/2018, **adoptarea unei decizii întemeiate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri**, care produce un **efect juridic negativ** pentru persoana vizată sau care o afectează în mod semnificativ **este interzisă**, cu excepţia cazului în care prelucrarea este **reglementată expres de lege**, fiind prevăzute **garanţii adecvate pentru drepturile şi libertăţile persoanei vizate**, inclusiv dreptul de a obţine intervenţia umană din partea operatorului. Autoritatea contractantă nu a indicat existența unei reglementări exprese de lege care să vizeze utilizarea de sisteme de recunoaștere faciala și nici garanţii adecvate pentru drepturile şi libertăţile persoanei vizate.

Am solicitat cerințele Autorității contractante cu privire la funcționalitățile sistemului de recunoaștere facială care vor asigura respectarea prevederilor art. 13 şi art. 16-21 din Legea nr. 363/2018. **Autoritatea contractanta nu a indicat asemenea cerințe în documentația achiziției.**

Conform dispozițiilor art. 25 al Regulamentului General privind Protecţia Datelor (Regulamentul UE 679/2016) prin care se instituie obligativitatea asigurării protecţiei datelor începând cu

3 https://ascpd.ro/wp-content/uploads/2019/09/solicitare.pdf

4 https://ascpd.ro/wp-content/uploads/2019/09/licitatie-recunoastere-faciala.rar

momentul conceperii (“privacy by design”) și pe toata durata de viață a sistemului (“privacy by default”), autoritatea contractantă avea obligația de a institui măsuri tehnice şi organizatorice adecvate încă din momentul elaborării Caietului de sarcini al procedurii în cauză. **Autoritatea contractantă nu a indicat asemenea cerințe cuprinse în documentația achiziției.**

Conform dispozițiilor art. 33 din Legea nr. 363/2018, atunci când discutăm despre utilizarea de noi tehnologii, mecanisme sau proceduri care implică un risc ridicat la adresa drepturilor şi libertăţilor persoanelor vizate, este necesară **consultarea autorității naționale de Supraveghere**. **Autoritatea contractanta nu a indicat existența unei consultări cu autoritatea de supraveghere**.

Conform art. 49 din Legea nr. 363/2018, interoperabilizarea sistemelor de evidenţă a datelor cu caracter personal este posibilă numai cu consultarea prealabilă a autorităţii de supraveghere. **Autoritatea contractantă nu a putut indica existenta unei consultări cu autoritatea de supraveghere.**

Subliniem faptul că Autoritatea contractantă nu a oferit solicitărilor noastre răspunsuri clare și complete așa cum impune legea achizițiilor publice, practic refuzând să ne răspundă, invocând faptul că solicitările noastre nu vizează aspecte de ordin tehnic. Ori, din punctul nostru de vedere, **măsuri tehnice şi organizatorice adecvate** pe care implementarea unui asemenea sistem le implica, vizează tocmai aspecte de ordin tehnic.

Mai mult, Autoritatea contractantă menționează în răspunsul la solicitările de clarificări[5] că „*După finalizarea contractului și semnarea procesului verbal de recepție fără obiecțiuni, înainte de trecerea în producție a sistemului, IGPR va respecta toate normele și prevederile legale în vigoare”*. Din analiza modului de exprimare, înțelegem că IGPR va achiziționa tehnologia de recunoaștere facială fără respectarea cerințelor legale în vigoare, urmând să își asume respectarea legislației în etapa subsecventa de punere în funcțiune. O astfel de abordare ne arată că este foarte puțin probabil ca un sistem funcțional să respecte legislația în vigoare atâta timp cât la momentul achizitiei măsurile tehnice şi organizatorice adecvate impuse de legislația în vigoare au fost omise în momentul întocmirii Caietului de sarcini al achiziției.

Riscurile asociate sistemelor de recunoașterea facială

Câteva dintre riscurile asociate acestui tip de prelucrari:

- **false potriviri** - identificarea eronată a persoanelor;
- **discriminare** - sistemele de recunoaștere facială au o eficiență mult mai redusă în cazul persoanelor BME (Black Male Adult), a femeilor, dar mai ales a copiilor. Aceste erori creează și consolidează categoriile discriminate pe baza genului și rasei, cu efecte negative din punct de vedere social;
- **abuzuri** - fără existența unor reglementări clare privind condițiile de utilizare ale unui asemenea sistem, utilizarea abuzivă a acestuia este foarte probabilă;

[5] https://ascpd.ro/wp-content/uploads/2019/09/Raspunsuri-clarificari-semnat.pdf

- **schimbarea comportamentului** - va determina schimbarea comportamentului persoanelor pentru a se conforma comportamentului general acceptat de societate. Persoanele se vor teme să participe la anumite tipuri de evenimente de teama de a nu fi asociați unei numite categorii de persoane (evenimente sportive, concerte, manifestații publice etc.).

Prevederile legislației europene

În conformitate cu prevederile art. 9 alin. (1) din Directiva 680, operațiunilor de prelucrare automatomată pentru identificarea unică a persoanei fizice, cu generarea unor decizii individuale automatizate care pot genera efecte juridice negative pentru subiecții de date, în vederea combaterii și elucidării cazurilor asociate furtului de identitate, a documentelor pierdute, identificarea suspecților care comit sau intenționează fapte de natură penală (terorism, infracțiune cu violentă etc.) nu le sunt opozabile cerințele Regulamentului general privind protecția datelor (GDPR), în măsura în care datele colectate în scopurile enunțate nu vor fi prelucrate în alte scopuri decât cele care cad sub incidența Regulamentului.

Chiar dacă cerințele Directivei 680 nu au aplicabilitate directă pentru statele membre cum ar fi în cazul GDPR, pentru asigurarea respectării dreptului la viața privată în legătură cu prelucrarea datelor cu caracter personal în sectorul polițienesc aceste trebuințe reprezintă un imperativ.

În acest sens, art. 10 din Directiva 680/2016 stabilește expres și fără drept de interpretare că: **prelucrarea** datelor genetice, prelucrarea datelor biometrice **pentru identificarea unică a unei persoane fizice** [.....] **este autorizată** numai atunci când este strict necesară și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei vizate și numai atunci când **este autorizată de dreptul Uniunii sau de dreptul intern**

Pentru a putea aprecia caracterul conform al acestei achiziții ale IGPR, se impun următoarele întrebări:

- Art. 12-18, cum se vor respecta drepturile persoanelor vizate și în ce măsură vor fi asigurate/restrânse, inclusiv perioada pentru care nu vor fi informați;
- Art. 22, care sunt măsurile organizatorice și tehnice puse în aplicare de către persoana împuternicită, care aparent este de drept privat;
- Art. 24, care este actul normativ care stabilește condițiile de evidență a prelucrărilor de date în special care s-ar referi la: destinatarii datelor, categoriilor de persoane vizate, eventualul transfer către o țară terță, temeiul juridic al prelucrării, termenul limită pentru ștergere a datelor, măsurile generale tehnice de securitate asigurate.
- Art. 27, dacă a fost efectuat impactul asupra protecției datelor cu caracter personal înainte de a prelucra categoria specială de date prin intermediul dezvoltării unei noi tehnologii.
- Art. 28, dacă în prealabil a fost consultată Autoritatea de supraveghere, inclusiv care a fost poziția acesteia pe caz, cu specificarea aspectelor esențiale;
- Art. 36-37, dacă se va efectua transferul către țări terțe și care vor fi situațiile opozabile;
- Art. 41, care este Autoritatea responsabilă de asigurarea protecției datelor cu caracter personal în cazul unor astfel de operațiuni de prelucrare a datelor și care sunt competențele efective ale acesteia.

De menționat că, așa cum opinează CEDO în numeroasele sale hotărâri, simplul fapt al colectării și înregistrării de către o autoritate publică a datelor cu caracter personal ale

unei persoane vizate – reprezintă o ingerință în viața privată, care poate avea loc doar dacă este prevăzută de LEGE și este necesară într-un stat democratic.

Alte aspecte pe care nu pot fi ignorate:

- Conform criteriilor de atribuire a contractului menționate în Caietul de sarcini al achiziției, ponderea pentru „**Eficacitatea algoritmului de căutare/comparare**" este de **doar 30%**, fiind pe aceeași treaptă cu prețul ofertei, restul factorilor de evaluare vizând caracteristici hardware care nu afectează acuratețea funcționarii software-ului de recunoaștere facială;

- De asemenea, un alt aspect ingrijorator este lipsa cerințelor privind demonstrarea **capacității tehnice și profesionale** a ofertantului. Prin urmare, operatorii care vor depune o oferta nu vor trebui să dovedească că dețin **experiență în implementarea unei soluții similare** sau măcar faptul că **personalul** care se va ocupa de instalarea sistemului și/sau instruirea personalului autorității contractante este calificat și deține experiență specifică în astfel de proiecte;

- Conform cerințelor Caietului de sarcini, sistemul de recunoaștere facială va putea efectua căutări/verificări/comparații ale imaginilor faciale din bazele de date ale poliției asociindu-le cu cele provenite de la **CCTV, webcam, telefoane mobile, rețele sociale, camere ATM**. O monitorizare care integrează toate aceste sisteme care colectează date faciale, care poate surprinde persoanele în mediul public, dar și din cel privat, este extrem de invazivă în viața privată a indivizilor. Este o prelucrare disproporționată față de beneficiile teoretice pe care acest sistem le propune, teoretice deoarece aceasta tehnologie este încă în curs de dezvoltare și pentru moment acesta rămâne nesigură.

Exemple privind implementarea sistemelor de recunoaștere facială

1. **Utilizarea de către Poliția South Wales (Marea Britanie) a tehnologiei automate de recunoaștere facială pentru prevenirea infracțiunilor**

Sistemul a fost contestat, iar **judecătorii au decis**[6] că, deși utilizarea unui sistem de recunoaștere facială automată constituie o ingerință în dreptul la viață privată, există o bază legală pentru aceasta, iar garanțiile oferite de poliție privind respectarea drepturilor şi libertăților persoanelor vizate au fost proporționale.

În urma acestei decizii ICO, **autoritatea de supraveghere din Marea Britanie a declarat**[7] că „*Între timp, orice forțe de poliție sau organizații private care utilizează aceste sisteme ar trebui să fie conștiente de faptul că legislația și ghidurile privind protecția datelor încă se aplică*." a declarat ICO.

6 https://www.judiciary.uk/judgments/r-v-the-chief-constable-of-south-wales-police-and-others/

7 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/09/statement-high-court-judgement-frt-south-wales-police/

2. **Utilizarea de către Poliția Metropolitana Londoneza (Marea Britanie) a tehnologiei automate de recunoaștere facială pentru prevenirea infracțiunilor**

Poliția Metropolitană din Londra a testat în perioada august 2016 - iulie 2018 un sistem de recunoaștere facială. Conform **datelor făcute publice de poliția londoneză**[8], în perioada de testare a sistemului au fost declanșate 104 alerte din care 102 s-au dovedit a fi eronate, în timp ce doar două au fost confirmate. Asta înseamnă o rată a falselor potriviri de peste 98 %.

Scenarii de risc asociate achiziției:

- Sistemul nu va putea funcționa din cauza lipsei măsurilor tehnice şi organizatorice adecvate impuse de legislația în vigoare. Cu alte cuvinte, bani aruncați pe fereastră.
- Sistemul nu va funcționa în mod legal, iar toate persoanele care vor fi identificate de acest sistem vor putea contesta în instanță legalitatea acestuia.
- Persoane supuse acestui tip de monitorizare în masa vor face plângere împotriva utilizării acestui sistem invocând încălcarea drepturilor și libertăților acestora;
- Falsele potriviri vor genera neîncrederea românilor în eficacitatea acestui sistem, scăzând astfel și mai mult încrederea în capacitatea Poliției Române de a asigura un grad adecvat de siguranță.

Opinăm că implementarea unui asemenea tip de tehnologie trebuie sa fie ferm reglementat și supus unui control strict pentru a se evita eventuale utilizări abuzive sau care ar avea ca efect încălcarea drepturilor și libertăților persoanelor vizate și totodată scăderea încrederii populației în instituția Poliției Române, al cărei slogan vi-l amintim: „Siguranță și încredere”.

Pentru conformitatea soluției tehnice solicităm analiza următoarele acțiuni propuse:

1. anularea procedurii de achiziție în cauză;
2. identificarea sau elaborarea unui cadru legal care să reglementeze expres un astfel de sistem de monitorizare în masă;
3. efectuarea unei evaluări a impactului prelucrărilor de date pentru acest tip de prelucrare;
4. consultarea societății civile cu privire la utilizarea unui sistem de recunoaștere facială;
5. consultarea autorității cu privire la rezultatul evaluării impactului prelucrărilor pentru a stabili împreuna cu aceasta măsurile corespunzătoare care vor fi instituite pentru protejarea drepturilor, a libertăţilor şi a intereselor legitime ale persoanei vizate;

8 https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/disclosure_2018/april_2018/information-rights-unit---mps-policies-on-automated-facial-recognition-afr-technology

6. redactarea unui nou Caiet de sarcini care să cuprindă cerințe exprese privind măsurile tehnice și organizatorice pe care sistemul trebuie sa le cuprindă încă din momentul conceperii;
7. stabilirea la cel puțin 70% a ponderii criteriului de selectie privind „Eficacitatea algoritmului de căutare/comparare”, acesta fiind de departe cel mai important aspect al acestui sistem;
8. impunerea de criterii de selecție în ceea ce privește demonstrarea capacității tehnice și profesionale prin solicitarea demonstrării existenței unei experiențe similare prin implementarea unui sistem similar și solicitarea de recomandări emise de beneficiari, precum și solicitarea dovezilor privind deținerea unui specialist în data privacy care va asista pe toată perioada de implementare a sistemului și a trainingului personalului autorității contractante.

Semnatari:

Asociația Specialiștilor în Confidențialitate și Protecția Datelor (www.ascpd.ro)

Marius Dumitrescu, Președinte

Asociatia pentru Tehnologie si Internet – ApTI (www.apti.ro)

Bogdan Manolea, Director Executiv

Asociația pentru Protecția Vieții Private (www.privacy.md)

Sergiu Bozianu, Președinte

Asociația pentru Respectarea Drepturilor Omului (www.ardom.ro)

Maria Pop, Președinte