CZU: 342.7:004.8

PROTECȚIA DREPTURILOR ȘI LIBERTĂȚILOR FUNDAMENTALE ALE OMULUI ÎN PROCESUL UTILIZĂRII TEHNOLOGIEI RECUNOAȘTERII FACIALE

Nicolae VASILIȘIN,
doctorand, asistent universitar,
Catedra „Activitate specială de investigații și anticorupție"
a Academiei „Ștefan cel Mare" a MAI
ORCID: 0000-0002-8840-8750

Rezumat

Recunoașterea facială este un subiect discutat în contradictoriu, iar pe măsura dezvoltării continue a capacităților tehnologice, ascunde în aparență și unele realități sensibile privind viața privată a omului prin prisma siguranței informațiilor colectate despre persoană/e.

Cuvinte-cheie: drepturile omului, recunoaștere facială, inteligență artificială, tehnologie, sistem, software, activitate specială de investigații, măsuri speciale de investigații.

Summary

Facial recognition is a subject discussed in contradiction, and according to the continuous development of technological capabilities, it apparently hides some sensitive realities regarding the private life of the person through the prism of the security of the information collected about the person/s.

Keywords: human rights, facial recognition, artificial intelligence, technology, system, software, special investigative activity, special investigative measures.

Dezvoltarea elementelor tehnice de recunoaștere facială a început în jumătatea a doua a secolului XX, fiind o formă de aplicație computerizată. Progresul tehnologic, în majoritatea cazurilor, a devenit un proces mult mai rapid comparativ cu cel de reglementare juridică care, fiind mai lent, nu poate oferi încă un cadru adecvat de garanții pentru om în protejarea sigură a datelor personale.

Aspectul criminologic al recunoașterii faciale a fost studiat și explicat în numeroase lucrări ale cercetătorilor străini și autohtoni, iar titularul lucrării „Bazele științifice, pregătirea și efectuarea prezentării spre recunoaș-

tere", Iurie Bulai, a reliefat că, în Republica Moldova, ar fi binevenită introducerea unui sistem de recunoaștere facială care ar facilita recunoașterea operativă a persoanei [1, p. 43].

Recunoașterea facială este o modalitate de a identifica sau de a confirma identitatea unui individ prin intermediul tehnologiei, folosindu-se fața acestuia prin compararea informațiilor cu o bază de date cu fețe cunoscute pentru a găsi o potrivire. Sistemul de recunoaștere facială (Sistemul FRS) poate fi utilizat pentru a identifica persoane în fotografii, în video filmări sau în timp real.

Principalii pași ai recunoașterii faciale sunt:

- **detectarea feței** – identificarea feței persoanei într-o imagine sau în mulțime;

- **analiza feței** – identificarea reperelor faciale (punctelor nodale) prin măsurarea algoritmică a distanței dintre ochi și a distanței dintre frunte și bărbie, care are ca rezultat crearea semnăturii faciale;

- **conversia unei imagini în date** – fiecare punct nodal devine un număr în baza de date a aplicației după analiză, iar fiecare persoană își obține propria amprentă facială;

- **matching** – găsirea unei potriviri a amprentei faciale comparată cu alte amprente faciale din baza de date.

Tehnologia de recunoaștere facială (în *continuare* TRF) identifică o potrivire pentru trăsăturile faciale exacte și returnează utilizatorului rezultatul potrivit.

Principalele beneficii ai utilizării recunoașterii faciale sunt:

- **consolidarea măsurilor de securitate** (*de exemplu, aeroporturile folosesc recunoașterea facială pentru a verifica potrivirile amprentei faciale fizice cu cea din documentul prezentat, precum și pentru a identifica infractorii și potențialele amenințări la adresa pasagerilor*);
- **ajutor la identificarea persoanelor dispărute și care nu sunt în stare să comunice informații utile despre sine** (*una dintre utilizările recunoașterii faciale este de a prezice modul în care o persoană poate arăta câțiva ani mai târziu*);
- **procesarea mai rapidă pentru a asigura verificarea imediată a unei persoane** (*verificarea non-evazivă a identității*);
- **automatizarea identificării** (*elimină identificarea manuală și crește precizia acestui proces*);
- **reducerea fraudelor**;
- **detectarea posibilelor maladii genetice**, etc.

Tehnologia recunoașterii faciale atrage și un șir de riscuri, cum ar fi:

- **protecția drepturilor și libertăților omului** (*utilizarea recunoaș-*

terii faciale pentru determinarea culorii pielii, credinței religioase sau de altă natură, sexului, originii rasiale a unei persoane, vârstei, stării de sănătate sau statutului social ar trebui interzise pentru a evita discriminarea);

• **confidențialitatea și protecția datelor** (*datele biometrice care identifică persoana nu sunt protejate și pot fi diseminate de către utilizatorii TRF*);

• **acces liber și necontrolat** (*persoanele juridice și cele fizice pot utiliza TRF în medii necontrolate, iar tehnologiile care pot identifica emoțiile și pot fi utilizate pentru a detecta trăsăturile de personalitate, emotivitatea sau starea de sănătate mintală a unei persoane ar trebui interzise, inclusiv din cauza prezentării riscurilor în domenii precum angajarea, accesul la asigurări și la educație*);

• **abuz jurisdicțional** (*țările lumii au jurisdicție diferită, iar legislația lor nu poate garanta înlăturarea tuturor pericolelor de abuz a accesării și prelucrării datelor fețelor noastre care se regăsesc pe diferite platforme online*);

• **lipsă de siguranță** (*utilizarea TRF pe scară largă va atrage consecințe ireversibile, iar înlăturarea lor va fi dificilă, fapt care impune și interzicerea pentru unii utilizatori a acestor posibilități tehnice*);

• **libertate de gândire, conștiință, religie ori de exprimare sau de mișcare** (*utilizarea TRF pentru a monitoriza adunările cultelor, minorităților etnice sau religioase ori pentru a monitoriza protestele anti-guvernamentale sau pentru controlul traversării frontierei*);

• **egalitate și nediscriminare** (*utilizarea TRF pe baza unor algoritmi părtinitori pentru a alege cine este eligibil să beneficieze de un serviciu sau un produs*);

• **viață privată** (*afectarea unor drepturi și libertăți ale omului prin utilizarea TRF în spații publice în scop de supraveghere și control*), etc.

Tehnologiile informaționale, care cuprind TRF, trebuie să se dezvolte în armonie cu respectarea drepturilor și libertăților omului, având la bază protecția datelor cu caracter personal, iar dincolo de interesul economic (profit) al companiilor ce dezvoltă aceste tehnologii urmează ca acestea să livreze produse bazate pe transparență, încredere și lipsă de influență.

Așadar, puține tehnologii stârnesc atât de multe controverse în lume precum recunoașterea facială, deoarece eficacitatea ei depinde și de reglementarea detaliată a folosirii acestei tehnologii.

John Frank, vicepreședinte al afacerilor guvernamentale pentru Uniunea Europeană din cadrul Microsoft, în interviul acordat în 2019 pentru HotNews.ro, a menționat că Europa trebuie să reglementeze în detaliu folosirea tehnologiei de recunoaștere facială, fiindcă în condiții de laborator rezultatele obținute sunt foarte bune, dar nu la fel și pe teren, iar de aici decurg mai multe probleme [2].

Potrivit intervievatului menționat, tehnologia recunoașterii faciale încă este departe de perfecțiune, iar implementarea acesteia pe scară largă, îndeosebi în statele cu regimuri represive, trezește mai multe îndoieli.

Astfel, TRF este folosită pe scară largă în China, iar în marele orașe chineze în baza datelor fixate de camerele de supraveghere sunt amendate persoanele ce traversează strada în locuri nepermise, fiindu-le deduse în mod automat din cont amenzile aplicate, iar din cauza celebrului „credit social" milioane de oameni nu au mai avut dreptul să cumpere bilete de avion sau de tren. Modelul chinez al creditului social pare ciudat, iar o supraveghere continuă a tuturor este cu totul inacceptabilă pentru occidentali, care consideră că supravegherea ar trebui să fie țintită în privința celor ce se află în conflict cu legea pentru a nu face ingerință în drepturile și libertățile omului.

Tehnologia recunoașterii faciale este folosită în India pentru a găsi copii dispăruți, iar în mai multe aeroporturi ale lumii această tehnologie este folosită la îmbarcarea pasagerilor. Această tehnologie poate fi folosită și pentru detectarea unor boli, în special când primele semne indică schimbări în aspectul feței [ibidem 2].

Prin urmare, oamenii devin tot mai obișnuiți cu sistemele extinse de supraveghere publică de stil CCTV (televiziune cu circuit închis), ce de regulă sunt utilizate în zonele în care este nevoie de monitorizare (*aeroporturi, bănci, magazine, spitale, școli, instituții cu regim inclusiv militare, restaurante și baruri, alte zone unde este necesar de asigurat securitatea*), însă această supraveghere video generează tot mai multe dezbateri privind echilibrarea utilizării sale cu dreptul persoanelor la viața privată, chiar și atunci când se află în public.

În Republica Moldova, în ultimul deceniu, supravegherea publică de stil CCTV a luat amploare, iar cadrul normativ ce asigură protecția datelor cu caracter personal colectate prin intermediul supravegherii video este Legea nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal. Cu toate acestea, legea menționată nu reglementează relațiile juridice specifice ce apar în procesul instalării, utilizării și gestionării mijloacelor de supraveghere video, efectuate în totalitate sau în parte prin mijloace automatizate, precum și prin alte mijloace tehnice, iar acest fapt impune adoptarea unei astfel de legi pentru asigurarea protecției dreptului persoanei fizice la inviolabilitatea vieții intime, familiale și private.

Tehnologia de recunoaștere facială se află în legătură reciprocă cu supravegherea video prin care se obțin imagini despre persoană/e, care apoi pot fi prelucrate și potrivite datelor biometrice ce identifică persoana aflată în baza de date a fețelor cunoscute ori aflată în sistemele de informații naționale și/sau globale.

Aşadar, pentru a identifica cu exactitate persoanele sau expresiile faciale, recunoaşterea facială foloseşte fotografii sau videoclipuri pentru a distinge diferite trăsături faciale, cum ar fi ochii, nasul şi gura, ale diferitor persoane şi le potriveşte caracteristicilor din bazele de date care conţin informaţii similare. TRF este una răspândită şi se găseşte inclusiv în telefoanele inteligente, care în foarte multe situaţii folosesc de la autentificarea până la aplicarea filtrelor fotografice pe Facebook sau Instagram. Totodată, această tehnologie necesită mai multă transparenţă, iar posibilităţile ei tehnice urmează a fi valorificate nu în detrimentul, ci în beneficiul omului.

Tehnologia de recunoaştere facială este parte a inteligenţei artificiale, iar prin urmare, necesită şi o reglementare normativă pentru a anticipa şi a exclude utilizarea acestei oportunităţi în contradictoriu cu normele de apărare a drepturilor şi libertăţilor omului.

Luând în consideraţie că recunoaşterea facială este o tehnologie probabilistică care poate recunoaşte automat indivizii pe baza feţei lor pentru a le autentifica sau identifica, deducem că TRF se încadrează în categoria mai largă a tehnologiei biometrice ce include toate procesele automate utilizate pentru recunoaşterea unui individ prin cuantificarea caracteristicilor fizice, fiziologice sau comportamentale (*amprente digitale, structura irisului, voce, mers, modele ale vaselor de sânge, etc*). Totodată, recunoaşterea facială este o funcţionalitatea *software* care poate fi implementată în cadrul sistemelor existente (*baze de date de imagini, sisteme de supraveghere, etc.*).

Trebuie să recunoaştem că nu toate statele îşi pot crea şi dezvolta propriile tehnologii de recunoaştere facială, iar în legătură cu acest fapt, majoritatea ţărilor au recurs la procurarea licenţei *software* propuse pe piaţa globală, produs care nu asigură garanţii necesare de protejare a vieţii private şi a datelor personale colectate prin intermediul conexiunii la Internet.

Astfel, compania americană „Clearview AI" este un furnizor *software* de recunoaştere facială care dispune de o bază de date de peste 20 de miliarde de imagini colectate de pe Internet, inclusiv aplicaţii de social media [3], conectate la *software*-ul realizat. Un număr impunător de agenţii guvernamentale de aplicare a legii, inclusiv organizaţii neguvernamentale din Statele Unite ale Americii, din Uniunea Europeană **şi** din alte ţări, au procurat *software*-ul de recunoaştere facială de la compania menţionată, însă nu şi-au asigurat aplicarea mecanismelor de prelucrare şi păstrare confidenţială a datelor stocate în sistemul centralizat de date – sistem administrat, întreţinut şi dezvoltat de către Clearview AI. Aplicând *software*-ul menţionat, mai mulţi utilizatori au admis un şir de încălcări ale legislaţiei, adică n-au asigurat confidenţialitatea păstrării şi nediseminării datelor prelucrate, inclusiv ale celor ce rezultau din investigaţiile efectuate în SUA şi în alte ţări, iar în-

călcarea regulilor și reglementărilor privind prelucrarea datelor cu caracter personal a avut ca impact aplicarea sancțiunilor unor utilizatori.

Amenda administrativă în valoare aproximativă de 250 000 de euro aplicată în cauza Autorității Suedeze pentru protecția vieții private (IMY) contra Autorității de Poliție din aceeași țară, pentru folosirea de către polițiști, în perioada 2019-2020, a recunoașterii faciale Clearview Al, în scopul identificării persoanelor, fără autorizația respectivă [4], precum și amenda administrativă în valoare aproximativă de 20 000 de euro aplicată de către IMY unei municipalități pentru permiterea procesării datelor biometrice într-o școală din Suedia [5], sunt doar unele cazuri ce demonstrează repetat necesitatea aplicării mecanismelor legale în operațiunile de prelucrare a datelor cu caracter personal și nu în ultimul rând necesitatea asigurării confidențialității datelor prelucrate care nu trebuiau diseminate persoanelor neautorizate.

Așadar, putem constata că practicile aplicate de către unele companii de furnizare a *software* și a componentelor de mentenanță cuprind un șir de dificultăți privind confidențialitatea datelor colectate, prelucrate, stocate și păstrate în procesul utilizării inteligenței artificiale, componenta căreia este tehnologia recunoașterii faciale. De aceea, la procurarea licenței *software* și a componentelor de mentenanță, furnizorul și beneficiarul urmează reciproc să-și asume angajamentul de responsabilitate privind riscurile și limitele legale de aplicare a posibilităților inteligenței artificiale, excluzând ingerința neautorizată în viața privată a omului.

Deși, nu există încă o normă dedicată nemijlocit inteligenței artificiale, care ar cuprinde și condițiile de utilizare a TRF, la 14 iunie 2023 Parlamentul European a adoptat poziția de negociere pe baza căreia vor începe discuții cu țările UE cu privire la reglementarea normativă a inteligenței artificiale (Legea privind inteligența artificială). Astfel, Uniunea Europeană își dorește elaborarea și aplicarea în spațiul acestei comunități a normelor armonizate privind inteligența artificială, care să funcționeze în conformitate cu valorile, drepturile fundamentale și principiile UE [6].

În spațiul Uniunii Europene deja funcționează sisteme de recunoaștere facială, la nivel de programe-pilot sau cu amploare mai mare, iar unele țări sunt în proces de implementare a astfel de proiecte.

Chiar dacă țările din spațiul UE au reglementat la nivel național utilizarea sistemelor de recunoaștere facială, Comisia Europeană și-a expus poziția privind adoptarea actelor legislative pentru o abordare europeană coordonată a implicațiilor umane și etice ale inteligenței artificiale, iar pentru a nu depăși limitele legii, UE va introduce reguli stricte pentru întărirea reglementărilor actuale care protejează viața privată și datele personale [7].

Potrivit Liniilor directorii 05/2022 privind utilizarea tehnologiei de recunoaștere facială în domeniul aplicări legii, adoptată la 26 aprilie 2023 de către Comitetul European pentru protecția datelor [8], utilizarea tehnologiei de recunoaștere facială este interdependentă de prelucrarea datelor cu caracter personal, iar prin urmare are un impact direct sau indirect asupra drepturilor fundamentale ale omului. Utilizarea TRF are o relevanță deosebită în domeniul de aplicare a legii și a justiției. Prin urmare, orice utilizare a tehnologiilor de recunoaștere facială ar trebui efectuată în strictă conformitate cu cadrul legal aplicabil.

Republica Moldova nu are o normă dedicată nemijlocit recunoașterii faciale, iar posibilitatea aplicării acestei tehnologii nu este interzisă în condițiile respectării Convenției nr. 108 pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal, adoptată de Consiliul Europei la 28 ianuarie 1981 [9], și a Legii nr. 133 din 08 iulie 2001 privind protecția datelor cu caracter personal [10].

Totodată, în R. Moldova recunoașterea facială este aplicată de către Poliția de Frontieră în condițiile reglementate prin Hotărârea Guvernului nr. 834 din 07.07.2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră [11], iar în corespundere cu Regulamentul privind eliberarea actelor de identitate și evidența locuitorilor Republicii Moldova [12], Agenția Servicii Publice deține Registrul de stat al populației în care sunt stocate imaginile faciale și amprentele digitale ale populației odată cu perfectarea documentelor de identitate.

Pentru realizarea Planului de acțiuni privind liberalizarea regimului de vize, semnat la 12 iunie 2014 [13], responsabilitatea de implementare, dezvoltare și asigurare a utilizării Sistemului de recunoaștere facială (Sistemul FRS) i-a revenit Întreprinderii de Stat „Centrul Resurselor Informaționale de Stat „Registru" (ÎS CRIS „Registru") care, prin Hotărârea Guvernului nr. 314 din 22.05.2017, a fost reorganizată prin transformare în Agenția Servicii Publice (ASP). Prin urmare, ASP i-au fost acordate drepturi exclusive privind prestarea unor anumite servicii informaționale și elaborarea produselor *software*, inclusiv de importanță statală.

Pe parcursul anilor 2016-2017, de către ÎS CRIS „Registru, în cadrul activităților aferente valorificării suportului bugetar oferit pentru implementarea Matricei de politici în domeniul liberalizării regimului de vize, a fost achiziționat pentru implementare Sistemul FRS, iar Ministerul Afacerilor Interne este printre beneficiarii utilizării *software* de recunoaștere facială.

Obiectivul Sistemului FRS constă în asigurarea unui management al datelor biometrice deținute în resursele informaționale de stat și departamentale din Republica Moldova, iar în scopul de a extinde posibilitățile de

identificare a persoanelor aflate pe teritoriul Republicii Moldova sau care traversează frontiera acesteia, sistemul menționat a fost pilotat, pentru început, la patru puncte de trecere a frontierei de stat, cu următoarele posibilități tehnice:

– prelevarea datelor biometrice de la persoanele fizice (*captarea fotografică*);

– citirea datelor biometrice din actul de identitate biometric;

– verificarea (1:1) datelor biometrice prelevate conform datelor biometrice din actul de identitate biometric;

– autentificarea (1:1) persoanei fizice după datele biometrice prelevate conform datelor biometrice din Registrul de Stat al Populației (*cu indicarea suplimentară a IDNP*);

– identificarea persoanei fizice după datele biometrice prelevate conform datelor biometrice din Registrul de Stat al Populației (1:N) – în cazul persoanelor fără acte sau care trezesc dubii;

– verificarea persoanelor fizice după datele biometrice prelevate conform masivelor interne de la Inspectoratul General al Poliției de Frontieră (*lista neagră*).

Succesele, dar și insuccesele acestui proiect-pilot nu sunt cunoscute publicului larg, iar pentru efectuarea unei analize privind impactul asupra drepturilor și libertăților omului în rezultatul aplicării tehnologiei de recunoaștere facială este nevoie de o transparență și o reglementare clară a utilizării TRF în Republica Moldova.

De asemenea, utilizarea posibilităților TRF de către unele bănci din Moldova, care impun cerințe clienților săi la accesarea unor date ce-i vizează, cum ar fi CVV (*a celor 3 cifre de pe verso cardului bancar*) numai cu condiția acceptării biometriei (*aplicația* „maib biometrie"), pare a fi nu doar ciudată din lipsa de transparență, dar și inexplicabilă din punct de vedere normativ. Or, în lipsa unui cadru legal, persoana nu poate fi supusă unor restricții nejustificate, iar aplicarea unor mecanisme de colectare și prelucrare a datelor personale nu este admisibilă fără acordul și cunoștința persoanei, cu excepția condițiilor în care sunt autorizate prin lege unele ingerințe echilibrate în drepturile și libertățile omului.

Cu siguranță, aplicarea tehnologiei de recunoaștere facială este importantă în procesul efectuării activității speciale de investigații, în special în cadrul efectuării măsurilor speciale de investigații, iar utilizarea acestei tehnologii se încadrează perfect în reglementarea Codului de procedură penală (în *continuare* CPP), secțiunea a 5-a [14] și în reglementarea Legii nr. 59 din 29.03.2012 privind activitatea specială de investigații (în *continuare* Legea privind ASI) [15], cu modificările și completările efectuate [16].

Procedura de autorizare a măsurilor speciale de investigații (în *continuare* MSI), prevăzută în CPP și în Legea privind ASI, asigură mecanismul de control din partea statului privind respectarea dreptului omului în procesul efectuării MSI, în realizarea cărora se fac uz de sisteme informaționale, care cuprind programe de colectare, analiză și sistematizare a informațiilor, ușor adaptabile pentru recunoașterea facială. Prin urmare, utilizarea posibilităților TRF va asigura operativitatea de reacționare a autorităților de aplicare a legii cu atribuții de prevenire și de combatere a infracțiunilor.

Orice persană are dreptul la respectarea vieții sale private și de familie, iar amestecul unei autorități publice în exercitarea acestui drept este permis numai dacă este prevăzut de lege și numai când este necesar pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei, ori protejarea drepturilor și libertăților altora [17, art. 8]. Pentru respectarea acestei reglementări din Convenția Europeană a Drepturilor Omului, Republica Moldova urmează să-și revadă cadrul normativ național și/sau în lipsa unor reglementări să elaboreze acte normative clare cu privire la mecanismele și condițiile de utilizare a inteligenței artificiale, în limitele prevăzute de lege.

Referințe bibliografice

1. Bulai Iu. *Bazele* științifice, *pregătirea* și *efectuarea prezentării spre recunoaștere. Teză de doctor* în *drept.* Chișinău, 2015, p. 43.

2. Barza V., HotNews.ro „Interviu John Frank, Microsoft, despre riscurile tehnologiei de recunoaștere facială: În Europa trebuie creat un cadru de reglementare care să excludă posibilitatea instalării unui sistem atotputernic de supraveghere", publicat 1 octombrie 2019.

3. en.wikipedia.org. Clerview Al – companie americană de recunoaștere facială.

4. DPA suedeză: Poliția a folosit ilegal aplicația de recunoaștere facială, edpb.europa.eu, 12.02.2021.

5. DPA suedeză a amendat o municipalitate cu 200 000 SEK (aproximativ 20 000 de euro) pentru utilizarea tehnologiei de recunoaștere facială pentru a monitoriza prezența elevilor la școală, edpb.europa.eu, 22.08.2019.

6. Propunere de Regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială) și modificarea anumitor acte legislative ale Uniunii, Bruxelles, 21.4.2021, COM (2021) 206 final, 2021/0106 (COD).

7. Cartea Albă Inteligența artificială – O abordare europeană axată pe excelență și încredere, Bruxelles, 19.2.2020, COM/2020/65 final/2.

8. Linii directorii 05/2022 privind utilizarea tehnologiei de recunoaștere facială în domeniul aplicări legii, versiunea 2.0, adoptată la 26 aprilie 2023 de către Comitetul European pentru protecția datelor.

9. Convenția nr. 108 pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal, adoptată de Consiliul Europei la 28 ianuarie 1981.

10. Legea nr. 133 din 08 iulie 2001 privind protecția datelor cu caracter personal, publicată la 14.10.2011 în Monitorul Oficial nr. 170-175, art.492.

11. Hotărârea Guvernului nr. 834 din 07.07.2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră, publicat la 15.07.2008 în Monitorul Oficial nr. 125-126, art.841.

12. Hotărârea Guvernului nr. 125 din 18.02.2013 pentru aprobarea Regulamentului privind eliberarea actelor de identitate și evidența locuitorilor Republicii Moldova, publicată la 22.02.2013 în Monitorul Oficial nr. 36-40 art.171.

13. Hotărârea Guvernului nr. 526 din 03.07.2014 pentru aprobarea Acordului de finanțare dintre Guvernul Republicii Moldova și Uniunea Europeană privind suportul în implementarea Planului de acțiuni privind liberalizarea regimului de vize, semnat la 12 iunie 2014, publicat la 11.07.2014 în Monitorul Oficial nr. 178-184 art.570.

14. Codul de procedură penală al Republicii Moldova nr. 122 din 14.03.2003, publicat la 07.06.2003 în Monitorul Oficial nr. 104-110 art. 447 și republicat în MO, 2013, nr. 248-251, art. 699.

15. Legea Republicii Moldova nr. 59 din 29.03.2012 privind activitatea specială de investigații, publicată la 08.06.2012 în Monitorul Oficial nr. 113-118 art.373.

16. Legea nr. 286 din 05.10.2023 pentru modificarea unor acte normative (privind activitatea specială de investigații), publicată la 28.11.2023 în Monitorul Oficial nr. 452-454 art.772.

17. Convenția pentru Apărarea Drepturilor Omului și a Libertăților Fundamentale/ Convenția Europeană a Drepturilor Omului, adoptată de Consiliul Europei la 4 noiembrie 1950 la Roma, în vigoare din 3 septembrie 1953.