CZU: 343.522/.525:343.72:004 **https://doi.org/10.59295/sum8(188)2025_05**

FURTUL DE IDENTITATE: ANATOMIA UNEI INFRACȚIUNI ÎN ERA DIGITALĂ

Serghei BRÎNZA, Vitalie STATI,
Universitatea de Stat din Moldova

Se examinează cele patru elemente constitutive ale infracțiunii prevăzute la art. 260[7] din Codul penal al Republicii Moldova. Sunt identificate obiectul juridic de subgrup și obiectul juridic special al acestei infracțiuni. Pe calea interpretării Legii nr. 195/2024, este caracterizat obiectul imaterial al infracțiunii prevăzute la art. 260[7] din Codul penal al Republicii Moldova. Se stabilește structura și conținutul laturii obiective a acestei infracțiuni. Sunt examinate particularitățile laturii subiective și ale subiectului infracțiunii prevăzute la art. 260[7] din Codul penal al Republicii Moldova. Studiul conține analiza relației dintre această infracțiune și infracțiunile specificate la lit. f) alin. (1) art. 165, art. 167, 168, 177[1], 190, 196, 238, 248, 248[1], 259, 260, 260[8] etc. din Codul penal al Republicii Moldova.

Cuvinte-cheie: *furt de identitate, identitatea unei alte persoane, modul fraudulos, sistem informatic, sistem de telecomunicație, inducerea în eroare, utilizatorul sistemului informatic, date personale.*

IDENTITY THEFT: THE ANATOMY OF AN OFFENSE IN THE DIGITAL AGE

The article examines the four constituent elements of the offense provided by the art. 260[7] of the Criminal Code of the Republic of Moldova. It identifies both the subgroup juridical object and the special juridical object of this offense. Through the interpretation of Law No. 195/2024, the immaterial object of the offense provided by the art. 260[7] of the Criminal Code of the Republic of Moldova is characterized. The structure and content of the objective side of this offense are established. The article also analyses the particularities of the subjective element and the subject provided by the art. 260[7] of the Criminal Code of the Republic of Moldova. The study includes an examination of the relationship between this offense and the offenses provided by the let. f), para. (1), art. 165, art. 167, 168, 177[1], 190, 196, 238, 248, 248[1], 259, 260, 260[8] etc. of the Criminal Code of the Republic of Moldova.

Keywords: *identity theft, another person's identity, fraudulent manner, information system, telecommunication system, deception, user of the information system, personal data.*

Introducere

La începutul anilor 2000, digitalizarea accelerată a societății, impulsionată de extinderea sistemelor informatice și a comunicațiilor electronice, a modificat profund arhitectura interacțiunilor sociale. Activitățile cotidiene – de la cele economice și administrative, până la cele educaționale și personale – au fost reconfigurate prin integrarea tehnologiilor digitale, ceea ce a condus la o expunere sporită a datelor cu caracter personal în mediul informatic. În acest nou cadru, identitatea individuală a devenit vulnerabilă, fiind tot mai des supusă riscurilor de arogare.

Aceste transformări, survenite în conținutul relațiilor sociale, au reclamat instituirea unui mecanism normativ adaptat, concretizat prin reglementări cu destinație specifică.[1] Necesitatea alinierii la o directivă a Uniunii Europene[2] (în continuare – UE) a determinat adoptarea Legii nr. 133 din 08.07.2011 privind

1. A se vedea, de exemplu: Legea cu privire la protecţia datelor cu caracter personal: nr. 17 din 15.02.2007. În: Monitorul Oficial al Republicii Moldova, 2007, nr. 107-111, 468; Hotărârea Guvernului Republicii Moldova privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal: nr. 1123 din 14.12.2010. În: Monitorul Oficial al Republicii Moldova, 2010, nr. 254-256, 1282; Ordinul Centrului Național pentru Protecția Datelor cu Caracter Personal cu privire la aprobarea Regulamentului privind controlul legalității prelucrărilor de date cu caracter personal: nr. 14 din 12.05.2014. În: Monitorul Oficial al Republicii Moldova, 2014, nr. 153-159, 814.

2. A se vedea: Directiva 95/46/CE a Parlamentului European și a Consiliului din 24.10.1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date. [Accesat: 28.08.2025] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:31995L0046

protecţia datelor cu caracter personal[3] (în continuare – Legii nr. 133/2011). Ulterior, adaptarea cadrului normativ la prevederile unui regulament al UE[4] a generat înlocuirea legii în cauză cu alta – Legea nr. 195 din 25.07.2024 privind protecția datelor cu caracter personal[5] (în continuare – Legea nr. 195/2024). Din art. 84 al regulamentului sus-amintit reiese implicit necesitatea de a incrimina fapta de furt de identitate. Această necesitate derivă implicit și din alin. (5) art. 9 al unei directive a UE[6]. De asemenea, în alin. (14) din preambulul la această directivă se menționează, *inter alia*: „Instituirea unor măsuri eficace împotriva furtului de identitate [...] constituie un [...] element important al unei abordări integrate împotriva criminalității informatice [...]" [1].

Raportat la Hotărârea Guvernului Republicii Moldova nr. 1171 din 28.11.2018 pentru aprobarea Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene[7], s-a impus necesitatea protejării prin mijloace de drept penal a valorilor și relațiilor sociale împotriva furtului de identitate. În acest context, prin Legea nr. 136 din 06.06.2024 pentru modificarea unor acte normative[8] (denumită în continuare Legea nr. 136/2024), Codul penal al Republicii Moldova a fost completat cu articolul 260[7], care sancționează o asemenea faptă.

Rezultate obținute și discuții

Art. 260[7] CP RM cuprinde, sub *nomen juris* de furt de identitate, o singură variantă-tip de infracțiune.

A. Obiectul infracţiunii prevăzute la art. 260[7] CP RM

Din chiar titulatura Capitolului XI al părţii speciale a Codului penal putem deduce faptul că *obiectul juridic generic* al infracțiunilor prevăzute în cuprinsul *său, inclusiv* al infracțiunii care este specificată la art. 260[7] CP RM, îl formează relaţiile sociale din domeniul informaticii *şi* al comunicaţiilor electronice.

Infracțiunea, prevăzută la art. 260[7] CP RM, se referă la tipul de infracțiuni informatice care lezează siguranța identității unei alte persoane. Respectiv, *obiectul juridic de subgrup* al acestei infracțiuni îl constituie relațiile sociale cu privire la siguranța identității unei alte persoane.

În cadrul analizei infracțiunii de fals de identitate, prevăzute la art. 177[1] CP RM, am menționat că obiectul juridic special al acesteia îl formează: „relaţiile sociale cu privire la realizarea, în conformitate cu art. 28 din Constituţie, a dreptului la viaţa intimă, familială *şi* privată, sub aspectul încrederii publice acordate constatărilor privind identitatea persoanelor" [2]. Ambele infracțiuni – falsul de identitate și furtul de iden-

3. A se vedea: Legea privind protecţia datelor cu caracter personal: nr. 133 din 08.07.2011. În: Monitorul Oficial al Republicii Moldova, 2011, nr. 170-175, 492.

4. A se vedea: Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27.04.2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE. [Accesat: 28.08.2025] Disponibil: https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX%3A32016R0679

În preambulul la acest regulament, se stabilește, între altele: „Riscul pentru drepturile și libertățile persoanelor fizice [...] poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii [...], în special în cazurile în care [...] prelucrarea poate conduce la [...] furt [...] [al] identității [...]"*; „Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la prejudicii [...] aduse persoanelor fizice, cum ar fi [...] furt [...] de identitate [...]."*

*Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27.04.2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE. [Accesat: 28.08.2025] Disponibil: https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX%3A32016R0679

5. A se vedea: Legea privind protecția datelor cu caracter personal: nr. 195 din 25.07.2024. În: Monitorul Oficial al Republicii Moldova, 2024, nr. 367-369, 574.

6. A se vedea: Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului. [Accesat: 28.08.2025] Disponibil: https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=celex:32013L0040

7. A se vedea: Hotărârea Guvernului Republicii Moldova pentru aprobarea Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene: nr. 1171 din 28.11.2018. În: Monitorul Oficial al Republicii Moldova, 2018, nr. 499-503, 1314.

8. A se vedea: Legea pentru modificarea unor acte normative (modificarea Codului penal și a Codului contravențional): nr. 136 din 06.06.2024. În: Monitorul Oficial al Republicii Moldova, 2024, nr. 245-246, 353.

titate – vizează, într-un fel sau altul, identitatea unei alte persoane. Cu toate acestea, nu putem susține că infracțiunile, prevăzute la art. 177^1 și 260^7 CP RM, au același obiect juridic special. În primul rând, obiectul juridic special al acestor infracțiuni derivă din obiecte juridice generice și obiecte juridice de subgrup diferite. În al doilea rând, diferă conținutul faptelor incriminate în art. 177^1 și 260^7 CP RM, iar aceasta lasă, indubitabil, o amprentă asupra obiectului juridic special al infracțiunilor comparate. Dacă luăm în vedere aceste două criterii, conchidem că *obiectul juridic special* al infracțiunii, prevăzute la art. 260^7 CP RM, îl formează relațiile sociale cu privire la siguranța identității unei alte persoane, sub aspectul asigurării inaccesibilității acestei identități într-o comunicare electronică, în absența consimțământului neviciat al titularului.

Analiza prevederii de la art. 260^7 CP RM indică faptul că identitatea unei alte persoane reprezintă *obiectul imaterial* al infracțiunii specificate la art. 260^7 CP RM. Din interpretarea noțiunii de date cu caracter personal, care este definită în art. 4 al Legii nr. 195/2024, deducem că identitatea unei alte persoane constituie ansamblul de date și caracteristici individuale care permit identificarea distinctă a unei persoane fizice în cadrul relațiilor sociale, fie direct, fie indirect, prin elemente precum: nume și prenume; număr de identificare (IDNP, CNP, ID etc.); date de localizare (adresă, IP); identificator online (username, e-mail); caracteristici personale (fizice, genetice, psihologice, economice, culturale, sociale).

În cazul infracțiunii prevăzute la art. 260^7 CP RM, metoda de inducere în eroare a utilizatorului sistemului informatic, datorită creării unei stări de aparență, este aplicată de către făptuitor cu un scop special: scopul de a determina utilizatorul sistemului informatic să furnizeze date personale în cadrul unei comunicări electronice. De precizat că, în acest caz, datele personale reprezintă obiectul scopului infracțiunii, nu obiectul imaterial al infracțiunii.

Referitor la *victima* infracțiunii prevăzute la art. 260^7 CP RM, în dispoziția acestui articol este specificat titularul identității care este obținută ilegal de către făptuitor, precum și utilizatorul sistemului informatic, care este indus în eroare de către făptuitor. Poate aceeași persoană să cumuleze ambele aceste calități speciale?

Această întrebare are două răspunsuri posibile:

1) o persoană poate fi simultan titular al identității care este obținută ilegal de către făptuitor, și utilizator al sistemului informatic, care este indus în eroare de către făptuitor. În situația descrisă, făptuitorul obține identitatea victimei prin inducerea directă în eroare a acesteia;

2) titularul identității, care este obținută ilegal de către făptuitor, și utilizatorul sistemului informatic, care este indus în eroare de către făptuitor, pot fi persoane distincte. În această situație, făptuitorul obține identitatea primei dintre aceste persoane prin inducerea în eroare a utilizatorului sistemului informatic. În situația examinată, relația dintre un astfel de utilizator și titularul identității, care este obținută ilegal de către făptuitor, poate îmbrăca forme variate: a) prestator de servicii *vs.* consumator; b) cadru didactic *vs.* elev/student; c) funcționar public *vs.* cetățean; d) cadru medical *vs.* pacient; e) funcționar bancar *vs.* client al băncii; f) organizator de concurs/examen *vs.* participant la concurs/examen etc.

În Acordul privind strategia națională de securizare a identității din Australia este formulată următoarea definiție: „Furt de identitate reprezintă însușirea sau asumarea unei identități preexistente (sau a unei părți semnificative a acesteia), cu sau fără consimțământ, indiferent dacă, în cazul unei persoane fizice, aceasta este în viață sau decedată” [3]. În acest context se ridică întrebarea: poate fi obținută identitatea unei persoane decedate în condițiile infracțiunii prevăzute la art. 260^7 CP RM?

Răspunsul afirmativ la această întrebare reiese implicit din Legea nr. 133/2011: „În cazul decesului subiectului datelor cu caracter personal, consimţământul privind prelucrarea datelor sale se acordă, în formă scrisă, de către succesorii acestuia, dacă un astfel de consimţământ nu a fost dat de subiectul datelor cu caracter personal în timpul vieţii” [4] (alin. (4) art. 5); „După decesul subiectului datelor cu caracter personal, datele acestuia se pot utiliza, cu consimţământul succesorilor, în scop de arhivă sau în alte scopuri prevăzute de lege” [4] (alin. (4) art. 11). Această lege va fi substituită la 23.08.2026 prin Legea nr. 195/2024. În legea nouă care nu a intrat încă în vigoare, la lit. d) alin. (2) art. 2, găsim următoarea prevedere relevantă: „Prezenta lege nu se aplică prelucrării datelor cu caracter personal [...] referitoare la persoanele decedate, cu excepția cazului prevăzut la art. 52”. [5] Din art. 53 al Legii nr. 195/2024 reiese că operatorii pot furniza date cu caracter personal referitoare la persoanele decedate doar în măsura în care acestea sunt de interes

public și nu intră în anumite categorii speciale. Mențiuni privind datele cu caracter personal, ce se referă la persoanele decedate, pot fi găsite, de asemenea, într-un act interministerial.[9]

În concluzie, în ipotezele care intră sub incidența normelor extrapenale sus-menționate (care sunt de referință pentru art. 260[7] CP RM), identitatea unei persoane decedate poate fi obținută în condițiile infracțiunii prevăzute de acest articol. În asemenea ipoteze, victimă este doar utilizatorul sistemului informatic, care este indus în eroare de către făptuitor.

O altă întrebare nu mai puțin importantă este: persoana juridică poate fi victimă a infracțiunii prevăzute la art. 260[7] CP RM?

În cadrul analizei infracțiunii prevăzute la art. 177[1] CP RM, am afirmat că „în general, putem vorbi despre identitatea unei persoane juridice. Astfel, spre exemplu, în art. 10 alin. (2) pct. 4) al Legii nr. 124 din 19.05.2022 privind identificarea electronică și serviciile de încredere [...], se recurge la formularea „identitatea [...] persoanei fizice sau juridice" [6]. [...] Cu toate acestea, victimă a infracțiunii, prevăzute la art. 177[1] CP RM, poate fi doar o persoană fizică. [...] Normele din Capitolul V al părții speciale a CP RM protejează nu drepturi subiective în general, ci exclusiv drepturile constituţionale ale cetăţenilor, adică ale persoanelor fizice" [7]. Spre deosebire de infracțiunea prevăzută la art. 177[1] CP RM, cea prevăzută la art. 260[7] CP RM nu face parte dintr-un capitol al legii penale, în care ar fi incriminate fapte îndreptate exclusiv împotriva persoanelor fizice. Mai mult, conform unei definiții formulate de Organizația pentru Cooperare și Dezvoltare Economică (OCDE), „furtul de identitate apare atunci când cineva obține, transmite, deține sau folosește informații personale despre o persoană fizică *sau juridică* (evid. ns.) fără permisiune, cu scopul de a comite fraude sau alte infracțiuni" [8; 9].

Cu toate acestea, din interpretarea art. 260[7] CP RM reiese că identitatea vizată este doar a unei persoane fizice, nu și a unei persoane juridice. Or, conform acestui articol, utilizatorul sistemului informatic este determinat de către făptuitor „să furnizeze date personale în cadrul unei comunicări electronice". [10] Noțiunea de date personale (*alias* date cu caracter personal) este definită în art. 4 al Legii nr. 195/2024, referindu-se la „informații privind o persoană fizică identificată sau identificabilă" [5]. Persoana juridică nu are date personale în sensul art. 260[7] CP RM. Ea are date de identificare (denumire, cod fiscal, sediu etc.), care nu sunt protejate prin regimul juridic al datelor cu caracter personal.

În concluzie, persoana juridică nu poate fi victimă a infracțiunii prevăzute la art. 260[7] CP RM.

B. Latura obiectivă a infracţiunii prevăzute la art. 260[7] CP RM

Înainte de a iniția examinarea acestui element constitutiv, vom scoate în prim plan problema legată de titlul art. 260[7] CP RM. Or, se prezumă că acest titlu ar trebui să reflecte esența juridică a faptei incriminate în art. 260[7] CP RM.

Totuși, în doctrina penală, sunt exprimate puncte de vedere critice privind sintagma „furt de identitate". De exemplu, N. Selavadurai, P. Gillies și R. Islam opinează: „Furtul de identitate nu reprezintă o formă de furt în sensul dreptului penal. În mod tradițional, conceptul de furt din dreptul comun presupune luarea necinstită a bunurilor de la proprietarii de drept, privându-i de folosirea bunurilor care le aparțin" [11]. În același făgaș, G. Zlati relevă: „Noțiunea de furt se dovedește una improprie, fiind de preferat să ne raportăm la noțiunea de uzurpare. Furtul implică o deposedare ce afectează disponibilitatea, în cazul furtului de identitate, de cele mai multe ori, discutăm însă despre obținerea [...] unor informații, fără ca disponibilitatea acestora să fie afectată" [12, p. 596]. Nu în ultimul rând, M. Dobrinoiu argumentează: „Ca noțiune, „furtul de identitate" are o denumire improprie, deoarece identitatea unei persoane nu este de fapt furată, ci mai degrabă preluată (sau asumată, dobândită) în mod ilegal [...]" [13].

Este necesar să remarcăm faptul că, în proiectul inițial care a stat la baza Legii nr. 136/2024, s-a propus ca *nomen juris* pentru infracțiunea analizată să fie „uzurpare de identitate" [14]. Totuși, această opțiune terminologică a fost ulterior abandonată. În ce ne privește, nu considerăm adecvate nici sintagma „furt de identitate", nici sintagma „uzurpare de identitate". Or, după cum decurge din art. 351 CP RM, acțiunea de

9. A se vedea: Ordinul comun al Ministerului Afacerilor Externe şi Integrării Europene, Ministerului Afacerilor Interne, Ministerului Justiţiei, Ministerului Finanţelor şi Ministerului Sănătăţii ale Republicii Moldova cu privire la aprobarea Procedurii de repatriere a cadavrelor: nr. 1293-b-155/296/538/1 din 05.11.2015. În: Monitorul Oficial al Republicii Moldova, 2016, nr. 32-37, 208.

uzurpare implică, în mod necesar, folosirea obiectului uzurpat. În contextul infracțiunii specificate la art. 260[7] CP RM, făptuitorul nu folosește identitatea unei alte persoane, ci doar o obține.

Sintagma „arogarea de identitate” este considerabil mai potrivită, deși nu are încă o consacrare juridică. Sugerând ideea de asumare fără drept a unei identități care nu aparține făptuitorului, sintagma, pe care o sugerăm, este lipsită de carențele conceptuale ce caracterizează cele două sintagme criticabile.

După această digresiune clarificatoare, ne concentrăm acum asupra structurii laturii obiective a infracțiunii prevăzute la art. 260[7] CP RM:

1) fapta prejudiciabilă exprimată în acțiunea de obținere a identității unei alte persoane;

2) modul fraudulos de săvârșire a infracțiunii;

3) mijlocul de săvârșire a infracțiunii: sistemul informatic sau de telecomunicație;

4) metoda de săvârșire a infracțiunii: inducerea în eroare a utilizatorului sistemului informatic datorită creării unei stări de aparență.

Referitor la acțiunea prejudiciabilă analizată, aceasta presupune procesul prin care făptuitorul accede, dobândește sau intră în posesia totală ori parțială a datelor sau caracteristicilor ce formează identitatea unei alte persoane.

Nu oricare obținere a identității unei alte persoane intră sub incidența art. 260[7] CP RM. Pentru a fi calificată în baza acestui articol, acțiunea în cauză trebuie să aibă, desigur, un caracter ilegal. Semnele secundare ale laturii obiective sunt cele care conferă ilegalitate acțiunii descrise în art. 260[7] CP RM.[10]

Primul semn secundar al laturii obiective a infracțiunii, prevăzute la art. 260[7] CP RM, este modul fraudulos de săvârșire a infracțiunii.

Formularea „în mod fraudulos prin intermediul sistemelor informatice sau de telecomunicație cu inducerea în eroare a utilizatorului sistemului informatic datorită creării unei stări de aparență” [10] din dispoziția art. 260[7] CP RM demonstrează că modul fraudulos nu este un semn autosuficient al laturii obiective a infracțiunii prevăzute la art. 260[7] CP RM. Modul fraudulos implică în mod necesar atât aplicarea unui anumit mijloc de săvârșire a infracțiunii (sistemul informatic sau de telecomunicație), cât și recurgerea la o metodă anumită (inducerea în eroare a utilizatorului sistemului informatic datorită creării unei stări de aparență.). Prin urmare, sintagma „mod fraudulos” [10], utilizată în art. 260[7] CP RM, este o formulă-sinteză care presupune, în mod inerent, utilizarea unui astfel de mijloc și a unei astfel de metode. Fără ele, nu se poate vorbi despre o fraudă în contextul infracțiunii prevăzute la art. 260[7] CP RM.

Clarificarea anterioară ne permite acum să examinăm următorul semn secundar al laturii obiective a infracțiunii prevăzute la art. 260[7] CP RM: mijlocul de săvârșire.

Sistemul informatic reprezintă primul mijloc posibil de comitere a acestei infracțiuni. În conformitate cu art. 134[25] CP RM, „prin sistem informatic se înțelege orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură care asigură ori dintre care unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor” [10]. Din această definiție deducem că sistemul informatic reprezintă fie dispozitivul izolat (care poate funcționa autonom, fără a fi conectat la alte dispozitive), fie ansamblul de dispozitive cu comunicație reciprocă sau integrare funcțională, care asigură – în integralitatea lor ori numai în parte – pe calea executării unui program, efectuarea de operațiuni (stocare, analiză, transmitere etc.) asupra datelor, fără o intervenție umană directă.[11]

Al doilea posibil mijloc de comitere a infracțiunii, specificate la art. 260[7] CP RM, este sistemul de telecomunicație.

Trebuie să precizăm că, în Codul penal, termenul de telecomunicație este folosită doar în articolul 260[7]. În alte articole din Codul penal (art. 134[6], 175[1], 177, 220[1], 259, 261[1], 267, 268 și 343), legiuitorul recurge la

10. Sub acest aspect, fapta, incriminată în art. 2607 CP RM, comportă similarități cu infracțiunea prevăzută la art. 226-18 din Codul penal al Republicii Franceze: „colectarea de date cu caracter personal printr-un mijloc fraudulos, neloial sau ilicit”.*

* Codul penal al Republicii Franceze. [Accesat: 28.08.2025] Disponibil: https://codexpenal.just.ro/laws/Cod-Penal-Franta-RO.html

11. Mai multe despre sistemul informatic a se vedea în: BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art. 259 din Codul penal. În: Studia Universitatis Moldaviae (Seria Ştiinţe Sociale), 2022, nr. 8, pp. 77-90. ISSN 1814-3199.

sintagma de comunicații electronice. În această ordine de idei, aducem în atenție un aspect relevant. Astfel, într-o publicație științifică se afirmă: „Noțiunile rețea de *comunicații electronice* și *serviciu de comunicații electronice* sunt definite în art. 2 al Legii nr. 241 din 15.11.2007 a comunicaţiilor electronice[12] (în continuare – Legii nr. 241/2007 – *n.a.*). Din analiza acestor definiții deducem că, prin *comunicații electronice*, trebuie de înțeles: telecomunicaţiile; transmisia prin reţelele utilizate pentru difuzarea programelor audiovizuale; accesul la Internet." [15] Așadar, termenul de telecomunicație și sintagma de comunicații electronice se află într-o relație de tipul „parte – întreg". Din interpretarea Legii nr. 241/2007, dar și a legii, care urmează să o substituie[13], reiese că telecomunicația este procesul de transmitere, recepționare sau schimb de informații la distanță prin mijloace tehnice, cum ar fi undele radio, cablurile, fibrele optice sau alte suporturi electromagnetice. Este o componentă a comunicațiilor electronice, care includ și infrastructura, serviciile digitale și rețelele moderne de transmisie.

Având ca reper această abordare, considerăm că sistem de telecomunicație constituie ansamblul, format din echipamente, rețele și proceduri, care permite transmiterea, recepționarea și procesarea semnalelor sau ale informațiilor la distanță, prin mijloace electromagnetice (cabluri, unde radio, fibre optice etc.). Exemple de sisteme de telecomunicație: rețelele de telefonie mobilă; rețelele de televiziune prin cablu; sistemele de comunicații prin satelit; rețelele de internet prin fibră optică; stațiile radio și radiocomunicațiile etc.

Încheiem analiza semnelor secundare ale laturii obiective a infracțiunii, prevăzute la art. 260^7 CP RM, cu metoda de săvârșire a infracțiunii. Legiuitorul o descrie prin cuvintele „inducerea în eroare a utilizatorului sistemului informatic datorită creării unei stări de aparență" [10].

Cu referire la furtul de identitate în accepțiunea dreptului penal român, G. Zlati face următoarea observație: „Obținerea datelor personale se poate realiza printr-o conduită infracțională tradițională, o conduită infracțională din sfera criminalității informatice ori o conduită ce nu are o natură infracţională *per se*" [12, p. 595]. Accentuăm că opinia în cauză nu corespunde dispoziției din art. 260^7 CP RM. Or, articolul respectiv incriminează nu oricare obținere a identității unei alte persoane, ci doar cea care este săvârșită „în mod fraudulos prin intermediul sistemelor informatice sau de telecomunicație cu inducerea în eroare a utilizatorului sistemului informatic datorită creării unei stări de aparență menite a determina utilizatorul să furnizeze date personale în cadrul unei comunicări electronice" [10]. Iată de ce, spre exemplu, sustragerea de suporturi materiale (stick USB, hard disk extern, CD/DVD, card de memorie, laptop, telefon mobil, router cu funcții de stocare, cameră digitală cu memorie internă etc.), care conțin datele cu caracter personal ale unei alte persoane, nu poate să reprezinte metoda de comitere a infracțiunii prevăzute la art. 260^7 CP RM. Cu atât mai puțin, nu poate să constituie o asemenea metodă o conduită care nu are un caracter ilegal. G. Zlati include în lista unor asemenea conduite „obținerea unor date personale din surse publice (de exemplu, de pe Internet), identificarea unor scurgeri de date personale (*data leaks*, căutarea de documente ce conțin date personale în tomberon), vizualizarea codului PIN introdus de o persoană la tastatura bancomatului etc." [12, p. 596].

A.C. Moise exprimă punctul de vedere, potrivit căruia, în cazul furtului de identitate, obținerea ilegală a identității unei alte persoane se poate realiza „prin intermediul infracţiunii de acces ilegal la un sistem de computer (hacking)" [16]. Într-adevăr, „inducerea în eroare a utilizatorului sistemului informatic datorită creării unei stări de aparență menite a determina utilizatorul să furnizeze date personale în cadrul unei comunicări electronice" [10] se poate regăsi în contextul faptei incriminate în art. 259 CP RM, care prevede răspunderea pentru accesul ilegal la un sistem informatic. Totuși, această posibilitate este limitată de sancțiunile din art. 259 și 260^7 CP RM. Comparând aceste sancțiuni, constatăm că infracțiunea, prevăzută la 260^7 CP RM, poate absorbi accesul ilegal la un sistem informatic în accepțiunea alin. (1) art. 259 CP RM, nu și în accepțiunea alineatelor (2) și (3) din acest articol.

Metoda, descrisă în art. 260^7 CP RM, presupune prezența a două condiții:

a) făptuitorul induce în eroare utilizatorul sistemului informatic;

b) această inducere în eroare se datorează creării unei stări de aparență.

Referitor la prima dintre aceste condiții, este de menționat că „inducerea în eroare implică nu doar pro-

12. A se vedea: Legea comunicaţiilor electronice: nr. 241 din 15.11.2007. În: Monitorul Oficial al Republicii Moldova, 2008, nr. 51-54, 679.

13. A se vedea: Legea comunicațiilor electronice: nr. 72 din 10.04.2025. În: Monitorul Oficial al Republicii Moldova, 2025, nr. 226-228, 266.

fitarea de eroarea victimei. Această condiție este necesară, dar nu și suficientă. O altă condiție, care conferă suficiență conceptului de inducere în eroare, este ca făptuitorul însuși să provoace eroarea victimei” [17, p. 155]. Accentuăm că inducerea în eroare urmează a fi distinsă de menținerea în eroare, adică de „profitarea de eroarea victimei, care nu a fost provocată de către făptuitor” [17, p. 155]. Menținerea în eroare a utilizatorul sistemului informatic nu intră sub incidența art. 260[7] CP RM.

În art. 260[7] CP RM se are în vedere inducerea în eroare a utilizatorului sistemului informatic, care se datorează creării unei stări de aparență. De fapt, această a doua condiție este redundantă și nu ar trebui specificată în dispoziția de incriminare a furtului de identitate. Or, tocmai crearea unei stări de aparență este ceea ce diferențiază inducerea în eroare de menținerea în eroare. În ipoteza inducerii în eroare, reprezentarea falsă a realității devine posibilă prin crearea de către făptuitor a unei stări de aparență, ce denaturează împrejurările obiective și determină victima să acționeze în baza unei imagini distorsionate a faptelor.

Sub influența modului și a mijlocului de săvârșire a infracțiunii, care sunt descrise în art. 260[7] CP RM, metoda de săvârșire a furtului de identitate adoptă anumite forme specifice. Printre aceste forme, în doctrina de specialitate se remarcă: phishing-ul; pharming-ul; spoofing-ul etc.

Prima formă este analizată, de exemplu, de M. Chawki, M.S. Abdel Wahab[14], N. Selavadurai, P. Gillies, R. Islam[15], A. C. Moise[16] și M. Dobrinoiu[17]. Noțiunea de phishing este definită, de asemenea, în Anexa nr. 7 a Hotărârii Băncii Naționale a Moldovei nr. 211 din 23.10.2014 cu privire la aprobarea Instrucțiunii cu privire la raportarea datelor aferente utilizării instrumentelor şi serviciilor de plată (în continuare – HBNM nr. 211/2014): „crearea paginilor de Internet false în vederea captării informației confidențiale ale utilizatorului SADD (adică al sistemului automatizat de deservire la distanță – *n.a.*)” [18].

Din interpretarea definițiilor doctrinare și a celei normative, reiese că phishing-ul reprezintă un procedeu fraudulos ce constă în crearea unei pagini web falsificate, care imită o platformă legitimă, și în transmiterea comunicațiilor electronice aparent autentice, prin care utilizatorul sistemului informatic este indus în eroare și determinat să divulge date cu caracter personal.

O altă formă specifică a metodei de săvârșire a infracțiunii, prevăzute la art. 260[7] CP RM, este pharming-ul. Această formă este examinată, de exemplu, de M. Chawki, M.S. Abdel Wahab[18] și M. Dobrinoiu[19]. Noțiunea de pharming este definită, de asemenea, în Anexa nr. 7 a HBNM nr. 211/2014: „instalarea unui program executabil pe calculatorul utilizatorului SADD, care la accesarea de către acesta a paginilor de Internet îl redirecționează către pagini de Internet false cu scopul de a obține informații confidențiale ale acestuia” [18].

Din interpretarea definițiilor doctrinare și a celor normative, decurge că pharming-ul este un procedeu fraudulos care constă în manipularea sistemului de direcționare a traficului web, prin instalarea programelor executabile în sistemul informatic al utilizatorului indus în eroare de către făptuitor, în scopul redirecționării acestuia către pagini de Internet falsificate, menite să colecteze date cu caracter personal.

Următoarea formă specifică a metodei de săvârșire a infracțiunii, prevăzute la art. 260[7] CP RM, este *spoofing*-ul. Această formă este analizată, de exemplu, de M. Chawki și M.S. Abdel Wahab[20].

14. A se vedea: CHAWKI, Mohamed, ABDEL WAHAB, Mohamed S. Identity Theft in Cyberspace: Issues and Solutions. [Accesat: 28.08.2025] Disponibil: https://www.lex-electronica.org/files/sites/103/11-1_chawki-abdel-wahab.pdf

15. A se vedea: SELVADURAI, Niloufer, GILLIES, Peter, ISLAM, Rizwanul. Theft: Aligning Law and Technology. În: Criminal Law Journal, 2010, vol. 34, is.1, pp. 33-47. ISSN 1740-5580.

16. A se vedea: MOISE, Adrian Cristian. Furtul de identitate săvârșit prin intermediul internetului. [Accesat: 30.08.2025] Disponibil: https://revcurentjur.ro/old/arhiva/attachments_201502/recjurid152_10FR.pdf

17. A se vedea: DOBRINOIU, Maxim. ID Theft in Cyberspace. În: Lex et Scientia International Journal, 2014, Is. XXI, No. 1, pp. 117-120. ISSN 1583-039X.

18. A se vedea: CHAWKI, Mohamed, ABDEL WAHAB, Mohamed S. Identity Theft in Cyberspace: Issues and Solutions. [Accesat: 28.08.2025] Disponibil: https://www.lex-electronica.org/files/sites/103/11-1_chawki-abdel-wahab.pdf

19. A se vedea: DOBRINOIU, Maxim. ID Theft in Cyberspace. În: Lex et Scientia International Journal, 2014, Is. XXI, No. 1, pp. 117-120. ISSN 1583-039X.

20. A se vedea: CHAWKI, Mohamed, ABDEL WAHAB, Mohamed S. Identity Theft in Cyberspace: Issues and Solutions. [Accesat: 28.08.2025] Disponibil: https://www.lex-electronica.org/files/sites/103/11-1_chawki-abdel-wahab.pdf

Noțiunea de spoofing este definită, de asemenea, în Anexa nr. 7 a HBNM nr. 211/2014: „transmiterea mesajelor electronice, de pe adrese false, cu solicitarea expedierii informației confidențiale ale utilizatorului SADD" [18].

Din interpretarea definiției doctrinare și a celei normative, se poate deduce că spoofing-ul constituie un procedeu fraudulos prin care făptuitorul modifică identitatea unei surse de comunicare electronică – precum adresa de e-mail, IP sau domeniu – pentru a simula proveniența legitimă a mesajului, și, astfel, a induce în eroare utilizatorul sistemului informatic, a accesa neautorizat resursele informatice ale acestuia și a obține ilegal date cu caracter personal.

Nu excludem alte forme specifice ale metodei de săvârșire a infracțiunii prevăzute la art. 260^7 CP RM. Esențial este ca acestea să se înscrie în tiparul normativ consacrat în acest articol: „inducerea în eroare a utilizatorului sistemului informatic datorită creării unei stări de aparență" [10].

În contextul examinării laturii obiective a infracțiunii prevăzute la art. 260^7 CP RM, este potrivit să discutăm despre relația dintre această infracțiune și alte infracțiuni.

Astfel, referitor la relația dintre infracțiunile prevăzute la art. 177^1 și 260^7 CP RM, am consemnat anterior că acestea „formează un concurs în ipoteza în care intenția de a săvârși falsul de identitate a apărut după consumarea furtului de identitate. În contrast, urmează a fi aplicat doar art. 177^1 CP RM în cazul în care, în vederea realizării intenției de a comite falsul de identitate, făptuitorul obține identitatea unei alte persoane în mod fraudulos prin intermediul sistemelor informatice sau de telecomunicație cu inducerea în eroare a utilizatorului sistemului informatic datorită creării unei stări de aparență menite a determina utilizatorul să furnizeze date personale în cadrul unei comunicări electronice. Într-un asemenea caz, furtul de identitate își pierde individualitatea, constituind nu altceva decât pregătirea de infracțiunea prevăzută la art. 177^1 CP RM" [7]. Cu acest prilej, se impune sublinierea faptului că relația dintre infracțiunile, prevăzute la art. 177^1 și 260^7 CP RM, este posibilă în cazul în care identitatea unei alte persoane este obținută ilegal prin comiterea furtului de identitate, pentru a fi ulterior falsificată, după care folosită în contextul infracțiunii prevăzute la art. 177^1 CP RM.

O relație similară este posibilă dintre infracțiunea, care este specificată la art. 260^7 CP RM, și alte infracțiuni. Această idee trebuie privită prin prisma următoarei afirmații pe care am făcut-o într-o publicație științifică: „În cazul în care falsul de identitate este săvârșit în contextul unei alte infracțiuni, acesta își pierde individualitatea. În asemenea cazuri, în acord cu regula fixată la art. 118 CP RM, răspunderea se va aplica nu pentru infracțiunea prevăzută la art. 177^1 CP RM, ci pentru una dintre faptele specificate la lit. f) alin. (1) art. 165, art. 167, 168, 190, 196, 238, 248, 248^1 sau altele din Codul penal" [7]. Pe cale de analogie, în cazurile de această natură, distingem două opțiuni de calificare: 1) concursul dintre infracțiunea, care este specificată la art. 260^7 CP RM, și una dintre infracțiunile prevăzute la lit. f) alin. (1) art. 165, art. 167, 168, 190, 196, 238, 248, 248^1 sau altele din Codul penal; 2) infracțiunea prevăzută la lit. f) alin. (1) art. 165, art. 167, 168, 190, 196, 238, 248, 248^1 sau altele din Codul penal (cu precizarea că furtul de identitate constituie pregătirea de o asemenea infracțiune).

În cazul infracțiunii prevăzute la alin. (3) art. 260^8 CP RM, mijlocul de săvârșire a infracțiunii îl constituie, *inter alia*, datele de identificare care permit utilizarea unui instrument de plată fără numerar sau a unui instrument de plată electronică. Nu poate fi exclusă ipoteza în care datele cu caracter personal constituie asemenea date de identificare, iar obținerea acestora se realizează prin comiterea infracțiunii care este specificată la art. 260^7 CP RM. În situația analizată, vom fi în prezența unui concurs de infracțiuni prevăzute la art. 260^7 și alin. (3) art. 260^8 CP RM, dacă intenția de a săvârși ultima dintre aceste infracțiuni survine ulterior consumării furtului de identitate. Alta este soluția de calificare în situația în care furtul de identitate este comis pentru a realiza intenția de a săvârși infracțiunea prevăzută la alin. (3) art. 260^8 CP RM. Într-un asemenea caz, furtul de identitate își pierde autonomia juridico-penală. Drept urmare, în situația analizată, furtul de identitate va constitui o formă de pregătire a infracțiunii prevăzute la alin. (3) art. 260^8 CP RM, fără a genera un concurs de infracțiuni.

Fără a compromite consistența ideatică, prezentăm ca exemplu alin. (1) art. 402.2 din Codul penal al Canadei. Conform acestei norme, furtul de identitate este săvârșit „cu intenția de a [...] folosi [informațiile obținute] pentru a comite o infracțiune gravă care include frauda, înșelăciunea sau falsul ca element al infracțiunii" [19].

Spre deosebire de reglementarea canadiană, art. 260^7 CP RM nu prevede o listă limitativă de infracțiuni care pot fi facilitate prin comiterea furtului de identitate, lăsând astfel deschisă sfera faptelor penale ce pot fi realizate prin utilizarea ilicită a identității unei alte persoane.

Relația dintre infracțiunile, prevăzute la art. 260 și 260^7 CP RM, merită a fi analizată datorită scopului specificat în art. 260 CP RM. Or, scopul infracțiunii de producere, import, comercializare sau punere ilegală la dispoziţie a mijloacelor tehnice sau a produselor program, care este prevăzută de acest articol, este de a săvârși una „dintre infracţiunile prevăzute la art. 237, 259, 260^1-260^3, 260^5-260^7” [10]. În ipoteza în care scopul respectiv se exprimă în săvârșirea infracțiunii prevăzute la art. 260^7 CP RM, putem fi doar în prezența concursului dintre infracțiunile specificate la art. 260 și 260^7 CP RM.

Finalizând examinarea laturii obiective a infracțiunilor prevăzute la art. 260^7 CP RM, menționăm că această infracțiune este formală. Ea se consideră consumată din momentul comiterii faptei prejudiciabile.

C. Latura subiectivă a infracţiunii prevăzute la art. 260^7 CP RM

Infracțiunea analizată poate fi săvârșită doar cu intenție directă. Motivele, care determină săvârșirea infracțiunii specificate la art. 260^7 CP RM, constau în: interesul material; năzuința de a înlesni comiterea altor infracțiuni; răzbunare; năzuința de a obține avantaje nepatrimoniale; teribilism etc.

De precizat că metoda de inducere în eroare a utilizatorului sistemului informatic, datorită creării unei stări de aparență, este aplicată de către făptuitor cu un scop special: scopul de a determina utilizatorul sistemului informatic să furnizeze date personale în cadrul unei comunicări electronice. Accentuăm: scopul, specificat în art. 260^7 CP RM, trebuie să se realizeze până la consumarea infracțiunii prevăzute de acest articol. Or, dacă utilizatorul sistemului informatic (care a fost indus în eroare de către făptuitor) nu-i furnizează acestuia din urmă date personale în cadrul unei comunicări electronice, nu va fi posibil ca făptuitorul să obțină identitatea victimei.

D. Subiectul infracţiunii prevăzute la art. 260^7 CP RM

Subiect al acestei infracțiuni este: 1) persoana fizică responsabilă care la momentul săvârșirii infracțiunii a atins vârsta de 16 ani; 2) persoana juridică (cu excepția autorității publice). Nu este necesar ca subiectul să posede o calitate specială.

Concluzii

Adoptarea Directivei 95/46/CE, a Directivei 2013/40/UE și a Regulamentului (UE) 2016/679 a constituit principala cauză care a determinat completarea Codului penal cu art. 260^7. Obiectul juridic de subgrup al infracțiunii, prevăzute de acest articol, îl formează relațiile sociale cu privire la siguranța identității unei alte persoane. Din acest obiect derivă organic obiectul juridic special al infracțiunii prevăzute la art. 260^7 CP RM: relațiile sociale cu privire la siguranța identității unei alte persoane, sub aspectul asigurării inaccesibilității acestei identități într-o comunicare electronică, în absența consimțământului neviciat al titularului. Identitatea unei alte persoane reprezintă obiectul imaterial al infracțiunii examinate. Victimele infracțiunii, prevăzute la art. 260^7 CP RM, sunt titularul identității care este obținută ilegal de către făptuitor, precum și utilizatorul sistemului informatic, care este indus în eroare de către făptuitor; este posibil ca o persoană să cumuleze ambele aceste calități speciale. Infracțiunea, specificată la acest articol, este formală și se consideră consumată din momentul comiterii faptei prejudiciabile. Latura subiectivă a infracțiunii, prevăzute la art. 260^7 CP RM, se caracterizează prin intenție directă. Subiect al acestora este fie persoana fizică responsabilă care la momentul săvârșirii infracțiunii a atins vârsta de 16 ani, fie persoana juridică (cu excepția autorității publice).

Referințe bibliografice:

1. Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului. [Accesat: 28.08.2025] Disponibil: https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=celex:32013L0040
2. BRÎNZA, S., STATI, V. Falsul de identitate: ce este și când atrage răspunderea penală? În: *Studia Universitatis Moldaviae (Seria Ştiinţe Sociale)*, 2025, nr. 3, pp. 28-38. ISSN 1814-3199.
3. An Agreement to a National Identity Security Strategy. [Accesat: 30.08.2025] Disponibil: https://www.homeaffairs.gov.au/criminal-justice/files/inter-gov-agreement-national-identity-security-strategy.pdf

4. Legea privind protecţia datelor cu caracter personal: nr. 133 din 08.07.2011. În: *Monitorul Oficial al Republicii Moldova*, 2011, nr. 170-175, 492.
5. Legea privind protecția datelor cu caracter personal: nr. 195 din 25.07.2024. În: *Monitorul Oficial al Republicii Moldova*, 2024, nr. 367-369, 574.
6. Legea privind identificarea electronică și serviciile de încredere: nr. 124 din 19.05.2022. În: *Monitorul Oficial al Republicii Moldova*, 2022, nr. 170-176, 317.
7. BRÎNZA, S., STATI, V. Falsul de identitate: ce este și când atrage răspunderea penală? În: *Studia Universitatis Moldaviae (Seria Ştiinţe Sociale)*, 2025, nr. 3, pp. 28-38. ISSN 1814-3199.
8. *Online Identity Theft*. [Accesat: 30.08.2025] Disponibil: https://www.oecd.org/content/dam/oecd/en/publications/reports/2009/03/online-identity-theft_g1gh9f59/9789264056596-en.pdf
9. *OECD Policy Guidance on Online Identity Theft*. [Accesat: 30.08.2025] Disponibil: https://afyonluoglu.org/PublicWebFiles/Reports/PDP/international/2008%20OECD%20Policy%20Guidance%20on%20Online%20Identity%20Theft.pdf
10. Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
11. SELVADURAI, N., GILLIES, P., ISLAM, R. Theft: Aligning Law and Technology. În: *Criminal Law Journal*, 2010, vol. 34, is.1, pp. 33-47. ISSN 1740-5580.
12. ZLATI, G. Tratat de criminalitate informatică. Vol. I. București: Solomon, 2020. 658 p. ISBN 978-606-8892-59-7.
13. DOBRINOIU, M. ID Theft in Cyberspace. În: *Lex et Scientia International Journal*, 2014, Is. XXI, No. 1, pp. 117-120. ISSN 1583-039X.
14. *Proiect. Lege pentru modificarea unor acte normative (modificarea Codului penal și Codului contravențional)*. [Accesat: 30.08.2025] Disponibil: https://justice.gov.md/sites/default/files/document/attachments/proiect_1.pdf
15. STATI, V., FURCULIŢA, D., GUZUN, V. Streaming-ul online, ca expresie a sexualității digitale, în vizorul legii penale a Republicii Moldova. În: *Studia Universitatis Moldaviae (Seria Ştiinţe Sociale)*, 2023, nr. 8, pp. 128-137. ISSN 1814-3199.
16. MOISE, A. C. *Furtul de identitate săvârşit prin intermediul internetului*. [Accesat: 30.08.2025] Disponibil: https://revcurentjur.ro/old/arhiva/attachments_201502/recjurid152_10FR.pdf
17. BRÎNZA, S., STATI, V., STRATAN, A. *Drept penal. Partea specială: Compendiu. Ediția a II-a*. Chișinău: Tipografia Centrală, 2025. 402 p. ISBN 978-5-88554-470-2.
18. Hotărârea Băncii Naționale a Moldovei cu privire la aprobarea Instrucţiunii cu privire la raportarea datelor aferente utilizării instrumentelor şi serviciilor de plată: nr. 211 din 23.10.2014. În: *Monitorul Oficial al Republicii Moldova*, nr. 325-332, 1531.
19. Criminal Code. [Accesat: 28.08.2025] Disponibil: https://laws-lois.justice.gc.ca/eng/acts/c-46/section-402.2.html

Date despre autori:
Serghei BRÎNZA, doctor habilitat în drept, profesor universitar, Facultatea de Drept, Universitatea de Stat din Moldova.
ORCID: 0000-0001-5937-3926
E-mail: brinza.serghei@yahoo.com

Vitalie STATI, doctor în drept, profesor universitar, Facultatea de Drept, Universitatea de Stat din Moldova.
ORCID: 0000-0003-1371-4961
E-mail: vitalie.stati@usm.md

Prezentat: 08.09.2025