# ÎNCĂLCAREA REGULILOR DE SECURITATE A SISTEMULUI INFORMATIC: ANALIZĂ JURIDICO-PENALĂ

***Maşa ROTARI,***

student, anul IV, Facultatea de Drept, Universitatea de Stat din Moldova

CZU: 343.346.8:004..056.5 E-mail: masharotari11@gmail.com

Într-o eră în care digitalizarea modelează profund societatea modernă, iar activitățile economice și administrative migrează masiv în mediul online, cadrul normativ penal trebuie să țină pasul cu noile forme de criminalitate. Infracțiunile informatice, precum cele comise prin *malware* sau *ransomware*, generează pierderi financiare globale estimate la peste *10 trilioane USD anual* [1].

Criminalitatea informatică a apărut odată cu extinderea utilizării calculatoarelor și rețelelor informatice, generând riscuri majore pentru securitatea digitală. Un exemplu timpuriu îl constituie o fraudă fiscală din 1969 (SUA), în valoare de 620 000 USD, care a evidențiat necesitatea unor reglementări adecvate. În anii ’80, state precum SUA (adoptând modelul „*Computer Fraud and Abuse Act*” din 1986) [2, p.9], Franța și Suedia au promulgat primele legi penale împotriva infracțiunilor informatice. În Republica Moldova, primele reglementări au apărut în 2003, odată cu adoptarea noului Cod penal al Republicii Moldova (articolele 259–261), iar după ratificarea Convenției de la Budapesta în 2009 au fost incriminate interceptarea ilegală, frauda și falsificarea datelor informatice. Instituțional, consolidarea a continuat cu înființarea Agenției Naționale pentru Securitate Cibernetică în februarie 2024. Totuși, numărul cauzelor penale inițiate pentru infracțiuni informatice a scăzut de la 205 în 2022 la 176 în 2023 și doar 16 în 2024, semnalând posibile carențe de aplicare sau eficiență a regimului penal.

Infracțiunea prevăzută de art. 261 din CP RM reglementează încălcarea regulilor de securitate a sistemului informatic. Totuși, analiza critică a acestei norme arată că textul actual este ambiguu și incomplet, afectând atât calificarea juridică, cât și aplicarea coerentă.

În primul rând, folosirea sintagmei „informație computerizată” este depășită. Standardele internaționale, precum *Convenția de la Budapesta* [3], precum și legislația națională (*Legea nr. 20/2009*) [4], utilizează exclusiv termenul „date informatice”. Mai mult, prin adoptarea Rezoluției nr. 43-16 a Adunării Interparlamentare a statelor membre ale CSI, în art. 286 „Accesul ilegal la informația computerizată” din Codul penal model al CSI, sintagma „informația computerizată” a fost substituită prin sintagma „date informatice”, care potrivit notei 1 din același articol, denotă „*orice reprezentare de fapte, informații sau concepte sub o formă adecvată prelucrării într-un sistem informatic*” [5, p.126-127]. Acesta este mai tehnic și mai potrivit pentru a

descrie reprezentarea digitală a informației. Reformularea este imperativă pentru a asigura coerența legislativă.

În al doilea rând, dispoziția enumeră acțiuni ca „colectare”, „păstrare” sau „difuzare”, deși dispoziția art. 261 CP RM fiind una de blanchetă, respectiv în conformitate actele normative extrapenale, putem stabili definițiile sus menționate care deja sunt incluse în definiția legală a „prelucrării datelor” din art. 3 din *Legea nr. 133/2011* ca „*orice operaţiune sau serie de operaţiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea*” [6]. În acest context, venim cu propunerea *de lege ferenda* este ca norma să se refere doar la „încălcarea regulilor de prelucrare a datelor informatice”.

În al treilea rând, referindu-ne la forma de vinovăție manifestată de făptuitor, și anume, în raport cu fapta prejudiciabilă infractorul manifestă intenție (directă sau indirectă) sau imprudență (sine încredere sau neglijență), însă față de urmările prejudiciabile autorul manifestă doar vinovăție sub formă de imprudență, nu este prezentă în toate cazurile prevăzute de norma juridico-penală. Raționamentul celor menționate reiese din dispoziția art. 261 din CP RM care prevede că fapta trebuie să fi „contribuit” la distrugerea, denaturarea sau însușirea datelor. În doctrină, „a contribuit” semnifică participare indirectă la un rezultat prejudiciabil, însă nu stipulează dacă această participare este intenționată și este din imprudență. Concretizăm că, acțiunea de „însușire” presupune, conform *Deciziei nr. 7/RC/2014 a ÎCCJ din România [7]*, intenție directă. Este necesar ca legea să precizeze că această faptă nu poate fi comisă din imprudență.

Astfel, se propune reformularea textului legal pentru a separa clar distrugerea/denaturarea (posibile și din imprudență) de însușire (care implică intenție). În plus, formularea actuală poate conduce la aplicări eronate în practică. Spre exemplu, dacă o persoană acționează imprudent, dar rezultatul constă în însușirea datelor de către un terț, atunci acesta din urmă trebuie sancționat pentru intenție distinctă, nu în cadrul aceleiași norme.

Totodată, în urma cercetării venim cu propune introducerii unei agravante pentru faptele comise de funcționari publici, potrivit *Legii nr. 158/2008*[6], precum și *HG nr. 201/2017* [8], sunt stabilite obligațiile funcționarilor publici în materia securității sistemului informatic.

Prin urmare, propunem reformularea textului normativ al art. 261 CP RM, astfel:

*(1) Încălcarea regulilor de prelucrare a datelor informatice ori a regulilor de protecţie a sistemului informatic prevăzute în conformitate cu statutul informaţiei sau gradul ei de protecţie, dacă această acţiune a contribuit la distrugerea sau denaturarea informației ori la însușirea acesteia de către o persoană terță.*

*(2) Aceleaşi fapte săvârşite de o persoană publică în exercitarea atribuţiilor de serviciu se pedepsesc cu închisoare de la 2 la 4 ani, amendă de la 650 la 1 350 unități*

*convenționale și cu privarea dreptului de a ocupa o funcție publică pe un termen de la 2 la 5 ani.*

Aceste modificări vor consolida caracterul predictibil, proporțional și eficient al normei penale, aliniind-o atât la nevoile reale ale sistemului de justiție, cât și la standardele internaționale de protecție a datelor și securitate cibernetică.

**Referințe:**


1. Dinamica securității cibernetice în Republica Moldova: Răspuns la amenințările complexe, [accesat: 18 februarie 2025]. Disponibil: https://pisa.md/wp-content/uploads/2024/07/Dinamica-securitatii-cibernetice-in-Republica-Moldova-raspuns-la-amenintarile-complexe-1.pdf.
2. МАЗУРОВ В. А., Компьютерные преступления. Классификация и способы противодействия, Москва: Палеотин, 2002.
3. Convenția Consiliului Europei de la Budapesta privind criminalitatea informatică, [accesat: 10 mai 2025]. Disponibil: http://rm.coe.int/1680081561.
4. Lege a Republicii Moldova nr. 20 din 03.02.2009. Publicat în: Monitorul Oficial nr. 11-12 art. 17 din 26-01-2010.
5. STRÎMBEANU, A. Răspunderea penală pentru accesul ilegal la informația computerizată. Teza de doctor, În: USM, Facultatea de Drept, Școala doctorală de științe juridice, 2023
6. Lege a Republicii Moldova nr. 133 din 08.07.2011. Publicat în: Monitorul Oficial nr. 170-175 art. 492 din 14-10-2011.
7. Deciziei a Înaltei Curți de Casație și Justiție nr. 7/RC/2014, [accesat: 14 mai 2025]. Disponibil: https://lege5.ro/Gratuit/gmztoobugy3a/decizia-nr-7-rc-2019-insusirea-bunului-gasit-sau-ajuns-din-eroare-la-faptuitor-art-243-oul-c-pen?utm.
8. Lege al Republicii Moldova nr. 158 din 04.07.2008. Publicat în: MonitorulOficial nr. 230-232 art. 840 din 23.12.2008.
9. Hotărâre de Guvern al Republicii Moldova nr. 201 din 28.03.2017. Publicat în: Monitorul Oficial nr. 109-118 art. 277 din 07-04-2017.


*Recomandat*
***Dorina GUREV**, dr. în d., conf. univ.*