

ÎNCĂLCAREA REGULILOR DE SECURITATE A SISTEMULUI INFORMATIC: INFRAȚIUNE CONTRA CONFIDENȚIALITĂȚII ȘI INTEGRITĂȚII SISTEMULUI INFORMATIC

VIOLATION OF COMPUTER SECURITY RULES: CRIME AGAINST THE CONFIDENTIALITY AND INTEGRITY OF THE COMPUTER SYSTEM

CZU: 343.346.8:343.45:004.056.53

<https://doi.org/10.59295/spd2025j.04>

Ludmila DUMNEANU

ORCID: 0000-0002-0195-8267

E-mail: bpap.lspinu@gmail.com

Universitatea de Stat din Moldova, Chișinău, Republica Moldova

Summary. *The international community unanimously considers the Council of Europe Convention on Cybercrime, signed in Budapest on November 23, 2001, to be the economic cornerstone among international legal regulations in the field of preventing and combating cybercrime, as it aims to become a global legal instrument, having been ratified and signed by an increasing number of states from various parts of the world. However, the legal world has not intervened through legislative measures regarding the examined field, and the area of information technology is continuously evolving, requiring special attention, particularly by highlighting the obstacles in the prevention and combat process.*

Keywords: *cybercrime, computer crime, identity theft, illegal access, information system.*

INTRODUCERE

Prin Legea nr. 6 din 02.02.2009 [1] Parlamentul Republicii Moldova a ratificat Convenția Consiliului Europei privind criminalitatea informatică adoptată la Budapesta la 23 noiembrie 2001 [2].

Astfel, în versiunea de până la adoptarea Legii nr. 136 din 6 iunie 2024 [3], încălcarea regulilor de securitate a sistemului informatic, era necesar să producă, printre altele cu provocarea de urmări grave, fapt la care a renunțat, ulterior legislatorul autohton.

Dispoziția articolului 261 CP RM, în versiunea actuală, adică de după adoptarea Legii nr. 136 din 6 iunie 2024, stabilește răspunderea pentru *încălcarea regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informației ori a regulilor de protecție a sistemului informatic, prevăzute în conformitate cu statutul informației sau gradul ei de protecție, dacă această acțiune a contribuit la însușirea (a se citi – sustragerea), denaturarea sau distrugerea informației.*

La momentul actual, vulnerabilitatea rețelilor se manifestă prin diferite variații. Un aspect primordial al rețelilor de calculatoare, în special al comunicațiilor prin intermediul internetului, îl constituie securitatea sistemului informatic.

Utilizatorii aflați la mari distanțe unul de celălalt urmează a fi bine identificați în mod tipic prin parole. Din păcate, sistemele prin parole au devenit vulnerabile, atât dat fiind faptul că hackerii și-au perfecționat metodele, cât și din cauza alegerii de către utilizatori a parolelor nesigure.

Necesitatea siguranței și autenticității apare la toate nivelurile arhitecturale ale rețelilor. Astfel, utilizatorii vor siguranță că poșta electronică, de exemplu, sosește chiar de la persoana care pretinde a fi expeditorul. Alteori utilizatorii, mai ales când acționează în numele unor agenții, urmăresc să-și asigure caracterul confidențial al mesajelor transmise.

Mai ales în contextul tranzacțiilor financiare, alături de autenticitate și confidențialitate, un rol de mare importanță îl joacă și integritatea mesajelor, ceea ce presupune că mesajul recepționat nu a fost alterat în timpul transmiterii prin rețea.

În afaceri este foarte important ca, odată ce a fost recepționată o comandă, aceasta să fie nu doar autentică, cu conținut nemodificat, dar și să nu existe posibilitatea ca expeditorul să nu o mai recunoască, adică să se respecte proprietatea de nerepudiare. La nivel scăzut, gateway-urile și routerele trebuie să discearnă între calculatoarele autorizate să comunice și cele intruse. De asemenea, este necesar ca, de exemplu, informația medicală transmisă prin rețele să fie confidențială și să ajungă nealterată (voit sau nu) la nodurile care rețin marile baze de date ale sistemelor de asigurări medicale [4].

În aceeași ordine de idei, se prezintă ca oportună apărarea penală a ordinii de drept împotriva infracțiunii de încălcare a regulilor de securitate a sistemului informatic.

MATERIALE ȘI METODE

Obiectul juridic special al infracțiunii consemnate la art. 261 din Codul Penal al Republicii Moldova îl formează relațiile sociale cu privire la securitatea sistemului informatic.

Obiectul material/imaterial al infracțiunii analizate îl constituie informația computerizată sau alte entități.

Prin „informație computerizată” trebuie de înțeles informația prelucrată cu ajutorul computerului (calculatorului), care este stocată în computer (calculator), pe suporturile materiale de informație sau este traficată în sistemul informatic sau în rețeaua informatică [5].

Prin „entități” (altele decât informația computerizată), inerente pe fundalul provocării unor urmări grave, se pot reține: calculatorul; modemul; scannerul; imprimanta matriceală, cu jet, termică, cu laser etc.

Victimă a infracțiunii prevăzute la art. 261 CP RM poate fi: 1) proprietarul sau alt deținător al resurselor sau sistemelor informaționale, al tehnologiilor și mijloacelor de asigurare a acestora; 2) proprietarul sau alt deținător al informației computerizate.

Latura obiectivă a acestei infracțiuni se exprimă prin următoarea structură: 1) fapta prejudiciabilă care se manifestă în acțiunea/inacțiunea de încălcare a regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informației ori a regulilor de protecție a sistemului informatic, prevăzute în conformitate cu statutul informației sau cu gradul ei

de protecție; 2) urmările prejudiciabile sub formă de: a) însușire (sustragere), denaturare sau distrugere a informației; 3) legătura cauzală dintre fapta prejudiciabilă și urmările prejudiciabile.

Regulile de colectare, prelucrare, păstrare, difuzare, repartizare a informației ori de protecție a sistemului informatic sunt prevăzute în: certificatele de calitate ale calculatoarelor; descrierile tehnice și instrucțiunile de exploatare a calculatoarelor; instrucțiunile de utilizare a programelor pentru calculatoare.

REZULTATE ȘI DISCUȚII

Este necesar ca în cadrul calificării faptei să se stabilească în mod exact ce regulă tehnică de exploatare a fost încălcată și dacă era obligat făptuitorul să respecte regula respectivă.

Sub incidența art. 261 CP RM nu intră încălcarea regulilor de realizare a dreptului de acces la informație, de culegere sau răspândire a acesteia, reguli care nu au nicio legătură cu exploatarea tehnică a calculatoarelor; cele comise întrunesc, după caz, semnele unei infracțiuni prevăzute la art. 177, 180, 338 sau altele din Codul penal.

Încălcarea unor reguli de colectare, prelucrare, păstrare, difuzare, repartizare a informației ori de protecție a sistemului informatic se poate exprima în mod fizic (cuplarea incorectă a calculatorului; încălcarea regimului termic și de umiditate în încăpere; încălcarea termenelor deservirii tehnice; utilizarea unor produse program necertificate etc.) sau în mod intelectual (încălcarea regulilor de dialogare cu programul pentru calculator; introducerea informației a cărei prelucrare este imposibilă, ținându-se cont de parametrii tehnici disponibili etc.).

Infracțiunea prevăzută la art. 261 CP RM este o infracțiune materială. Se consideră consumată din momentul producerii urmărilor prejudiciabile sub forma însușirii (sustragerii), denaturării sau distrugerii informației.

Latura subiectivă a infracțiunii de încălcare a regulilor de securitate a sistemului informatic se exprimă în vinovăție sub forma intenției sau imprudenței în raport cu fapta prejudiciabilă și doar prin imprudență în raport de urmările prejudiciabile.

Motivul infracțiunii se exprimă, de cele mai dese ori, în superficialitatea manifestată în raport cu respectarea regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informației ori a regulilor de protecție a sistemului informatic, prevăzute în conformitate cu statutul informației sau cu gradul ei de protecție.

Subiectul infracțiunii consemnate la art.261 CP RM poate fi: 1) persoana fizică responsabilă care la momentul săvârșirii infracțiunii a atins vârsta de 16 ani; 2) persoana juridică (cu excepția autorității publice).

Totodată, atât persoana fizică, cât și cea juridică trebuie să aibă calitatea unui subiect special, deoarece poate fi numai persoana în ale cărei obligații intră respectarea regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informației ori a regulilor de protecție a sistemului informatic. În absența acestei calități, art.261 CP RM nu poate fi reținut.

CONCLUZII

În contextul celor invocate mai sus, vom reitera conținutul art. 24-28 ale Legii cu privire la informatică, potrivit căruia autoritățile administrației publice, care au colectat informația, sunt obligate să o furnizeze, la solicitare, celorlalte autorități ale administrației publice, în conformitate cu legislația.

Bazele de date se organizează conform criteriului calității și securității datelor ce le conțin, indiferent de faptul că ele sunt ținute pentru păstrare și consultare internă sau că din acestea se furnizează produse informatice transmise unor terți, inclusiv pe cale neinformatică. Întru aplicarea acestor prevederi legale în raport cu bazele de date din domeniul public, se desemnează responsabili pentru prelucrarea datelor.

Titularii de date care nu aparțin domeniului public, dar care stochează, prelucrează, difuzează sau utilizează date ce pot intra în categoria celor cu caracter personal sau a datelor nominative trebuie să desemneze responsabili pentru prelucrarea datelor [6].

Titularul bazelor de date protejează, prin măsuri adecvate, datele colectate, echipamentele și produsele de program utilizate pentru administrarea acestora, asigurând securitatea datelor împotriva riscurilor de pierdere, distrugere, precum și împotriva folosirii neautorizate sau divulgării. Persoanele care activează în cadrul sistemelor și rețelelor informatice sunt obligate să asigure protecția și confidențialitatea datelor, cu excepția celor care sunt determinate drept date publice [7].

Totodată, vom apela și la conținutul art. 7 al Legii privind prevenirea și combaterea criminalității informatice, potrivit căruia furnizorii de servicii sunt obligați:

- a) să țină evidența utilizatorilor de servicii;
- b) să comunice autorităților competente datele despre traficul informatic, inclusiv datele despre accesul ilegal la informația din sistemul informatic, despre tentativele de introducere a unor programe ilegale, despre încălcarea de către persoane responsabile a regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informației ori a regulilor de protecție a sistemului informatic prevăzute în conformitate cu statutul informației sau cu gradul ei de protecție, dacă acestea au contribuit la însușirea, la denaturarea sau la distrugerea informației ori au provocat alte urmări grave, perturbarea funcționării sistemelor informatice, alte delikte informatice;
- c) să execute, în condiții de confidențialitate, solicitarea autorității competente privind conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, față de care există pericolul distrugerii ori alterării, pe un termen de până la 120 de zile calendaristice, în condițiile legislației naționale;
- d) să prezinte autorităților competente, în temeiul unei solicitări efectuate în condițiile legii, date referitoare la utilizatori, inclusiv la tipul de comunicație și la serviciul de care a beneficiat utilizatorul, la modalitatea de plată a serviciului, precum și orice alte date care pot conduce la identificarea utilizatorului;
- e) să întreprindă măsuri de securitate prin utilizarea unor proceduri, dispozitive

sau programe informatice specializate cu al căror ajutor accesul la un sistem informatic să fie restricționat sau interzis utilizatorilor neautorizați;

f) să asigure monitorizarea, supravegherea și păstrarea datelor referitoare la trafic, pe o perioadă de cel puțin 180 de zile calendaristice, pentru identificarea furnizorilor de servicii, utilizatorilor de servicii și a canalului prin al cărui intermediu comunicația a fost transmisă;

g) să asigure descifrarea datelor informatice care se conțin în pachetele protocoalelor de rețea cu conservarea acestor date pe o perioadă de cel puțin 90 de zile calendaristice.

Acestea sunt regulile care urmează a fi respectate și care cad sub incidența dispoziției art. 261 CP RM.

REFERINȚE:

1. Legea nr. 6 din 02.02.2009 pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică. În: Monitorul Oficial al Republicii Moldova, 2009, nr. 37-40.
2. Convenția Consiliului Europei privind criminalitatea informatică. <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Romanian.pdf>.
3. Monitorul Oficial al Republicii Moldova nr. 245/246 din 07.06.2024. p. 5-30.
4. Brînza S., Stati V. Tratat de drept penal. Partea specială. Vol. I. Chișinău: Tipografia Centrală, 2015. 1328 p. ISBN 978-9975-53-469-7, p. 381.
5. Brînza S., Stati V. Tratat de drept penal. Partea specială. Vol. I. Chișinău: Tipografia Centrală, 2015. 1328 p. ISBN 978-9975-53-469-7, p. 347.
6. Ștefănoaia, Mihai. Drept penal. Parte generală, vol II, Editura Universul Juridic, 2020, ISBN, 978-606-27-0977-8, https://www.ujmag.ro/drept/drept-penal/drept-penal-parte-general-a-2020-stefanoia/?ref=pagina_https://www.ujmag.ro/autori/mihai-stefanoia
7. Mihai Ștefănoaia, Mihaela RUS. The impact of respecting human rights and civil rights on the development of a democratic and inclusive society, Madrid Proceedings of 9th International Conference on Modern Approaches in Humanities and Social sciences, ISBN: 978-609-485-674-7, <https://www.dpublication.com/proceeding/9th-icmhs/#Table-of-Contents>