Eliza ENE CORBEANU (avocat)

# Criminalitatea informatică

*Coordonator: Gheorghe CORNESCU (procuror PICCJ)*

**Universul Juridic**
Bucureşti
-2025-

**Curriculum vitae**

Sunt absolventă a Facultăţii de Drept şi a Facultăţii de Istorie din cadrul Universităţii Bucureşti, dar şi a studiilor universitare de masterat, Disciplina Geopolitică şi Relaţii Economice Internaţionale, Facultatea de Relaţii Economice Internaţionale, Academia de Studii Economice din Bucureşti.

Sunt avocat în Baroul Bucureşti din anul 2006, autor al rubricii Viaţa la Curte şi publicist la Ziarul Evenimentul Zilei, dar şi colaborator al revistei Evenimentul Istoric.

**Lucrări de specialitate publicate:**

Cărţi publicate:

- *Evaziunea fiscală*, Ed. Hamangiu, Bucureşti, 2020.

Articole:

- *„Necesitatea introducerii procedurii renunţării la urmărire penală printre soluţiile prevăzute de art. 482 C. proc. pen. referitor la conţinutul acordului de recunoaştere”,* Curierul Judiciar nr. 2/2019.
- *„Reflecting the Right to Privacy in the Decisions of the Constitutional Coúrt of Romania”,* Lex ET Scientia International Journal nr. 1/2019.

**Alte lucrări:**

Cărţi publicate:

- *Printre gratii şi cătuşe*, Ed. RAO, Bucureşti, 2018.
- *Suflete rătăcite. Jurnalul unor criminali*, Ed. RAO, Bucureşti, 2019.
- *Le Journal de crimes*, Edilivre, Paris, 2021.
- *Cătuşele Anei*, Ed. RAO, Bucureşti, 2022.

În curs de publicare:

- *Dramaturgie. Între lumi. Parfum de femeie. Pacienta tăcută* (2025).

# Cuprins

consistenţa juridică, volumul de faţă oferă nu doar o fundamentare teoretică solidă, ci şi un sprijin practic, actual şi eficient în faţa uneia dintre cele mai provocatoare forme de criminalitate ale prezentului.

**Alex Florin Florenţa**
Procuror General al Parchetului de pe lângă
Înalta Curte de Casaţie şi Justiţie

# Capitolul I
# Reglementarea criminalităţii informatice: Evoluţie istorică, norme internaţionale şi cadrul juridic naţional

## 1. Reglementările internaţionale: SUA, Consiliul Europei, OCDE

A doua jumătate a secolului XX a fost marcată de o accelerare a utilizării sistemelor informatice în domenii cheie, precum cel bancar, comercial, administrativ sau guvernamental, însă această evoluţie a condus la apariţia unor noi tipuri de infracţiuni, care nu îşi găseau reglementarea în legislaţiile existente; vidul legislativ a obligat sistemul judiciar să apeleze la artificii juridice pentru a incrimina infracţiuni cu care societatea nu se mai confruntase până atunci, calificările raportându-se la dispoziţiile generale referitoare la înşelăciune, furt, fals în înscrisuri sau acces ilegal la proprietate, însă au existat şi fapte care au rămas nepedepsite, din cauza caracterului lor inedit.

Nevoia reglementării infracţiunilor informatice a devenit acută în anii '80-'90, odată cu creşterea numărului de atacuri informatice, recunoaşterea necesităţii unor dispoziţii legale specifice fiind un fapt care nu mai putea fi ignorat, în special de către Statele Unite ale Americii şi Europa Occidentală.

În anul 1986, Congresul american a promulgat Computer Fraud and Abuse Act (CFAA)[1], unul dintre cele mai de impact acte normative în domeniul securităţii informatice, care a servit drept model pentru legislaţiile altor state; justificarea adoptării s-a bazat pe creşterea alarmantă a atacurilor cibernetice asupra instituţiilor federale şi a marilor corporaţii.

CFAA, reglementat în Titlul 18 din Codul Statelor Unite ale Americii (U.S. Code, § 1030), sancţiona mai multe categorii de infracţiuni, printre care: accesul neautorizat la sisteme informatice protejate, inclusiv cele guvernamentale şi financiare [§ 1030(a)(2)][2], frauda informatică prin acces ilegal la date cu scopul obţinerii unui avantaj economic [§ 1030(a)(4)], modificarea, deteriorarea sau ştergerea neautorizată a datelor informatice [§ 1030(a)(5)],

[1] Computer Fraud and Abuse Act (CFAA) of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012).

[2] U.S. Code, Title 18, § 1030 – Fraud and related activity in connection with computers. Disponibil la: https://www.law.cornell.edu/uscode/text/18/1030.

utilizarea frauduloasă a unor programe informatice pentru compromiterea securităţii cibernetice [§ 1030(a)(6)][3].

Totuşi, unii autori americani, cum ar fi Ric Simmons[4], profesor la Facultatea de Drept Moritz, Universitatea de Stat din Ohio, consideră că Legea privind Frauda şi Abuzul în Domeniul Informatizării (CFAA) reprezintă un exemplu de eşec legislativ în materie de criminalitate informatică, întrucât majorează artificial sfera de incidenţă penală prin suprapunerea cu infracţiuni tradiţionale deja reglementate, fără a aduce o valoare adăugată normativă.

Simmons subliniază că termenii-cheie ai legii precum „acces neautorizat", „autorizare" sau „pierdere" nu beneficiază de o definire juridică riguroasă, ceea ce conduce la aplicări contradictorii şi la încălcarea principiului legalităţii, afectând astfel previzibilitatea şi coerenţa dreptului penal.

În opinia sa, încercările legislative de a actualiza CFAA nu au reuşit să ţină pasul cu dinamica tehnologică, iar complexitatea infracţionalităţii digitale reclamă o schimbare de paradigmă normativă.

În Europa, procesul de reglementare a criminalităţii informatice a avut un parcurs diferit, fiind influenţat în mare măsură de recomandările unor organizaţii internaţionale, precum Consiliul Europei şi Organizaţia pentru Cooperare şi Dezvoltare Economică (OCDE).

Aceste instituţii au emis primele norme de orientare, care au stat la baza adoptării unor acte normative naţionale şi a unor instrumente internaţionale precum Convenţia de la Budapesta (2001)[5].

Consiliul Europei a fost prima organizaţie europeană care a recunoscut necesitatea unei reglementări unitare în domeniul criminalităţii informatice, astfel că, în 1989, a emis Recomandarea R(89)9 privind criminalitatea informatică, prin care statele membre erau îndemnate să îşi adapteze legislaţiile penale pentru a putea sancţiona infracţiuni precum accesul neautorizat la sisteme informatice, falsificarea datelor electronice şi frauda informatică[6].

În anul 1995, a fost adoptată Recomandarea R(95)13 privind procedurile penale aplicabile criminalităţii informatice, punându-se bazele standardelor de

[3] *United States of America: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act)*. Disponibil la: https://www.refworld.org/search?sm_document_source_name%5B%=National+Legislative+Bodies+%2F+National+Authorities&sort=score&order=desc.

[4] The George Washington Law Review, nr. 6, vol. 84, decembrie 2016, p. 1706.

[5] Council of Europe, Recommendation No. R(89)9 on Computer-Related Crime. Disponibil la: https://rm.coe.int/16807096c6.

[6] Council of Europe, Recommendation No. R(95)13 on Criminal Procedural Law and Information Technology. Disponibil la: https://rm.coe.int/16804f3f76.



colectare a probelor digitale şi ale procedurilor specifice investigării acestui tip de infracţiuni[7].

În anul 1992, Organizaţia pentru Cooperare şi Dezvoltare Economică (OCDE) a publicat Ghidul privind securitatea sistemelor informatice şi a reţelelor, în care se evidenţia necesitatea unor măsuri legislative pentru prevenirea şi sancţionarea fraudelor informatice[8]; impactul acestui document asupra politicilor de securitate cibernetică adoptate de statele membre OCDE a fost semnificativ, contribuind la dezvoltarea unor norme internaţionale în domeniu.

Ca urmare a recomandărilor cuprinse în Ghidul privind securitatea sistemelor informatice şi a reţelelor al OCDE, multe ţări europene au început să adopte legislaţii privind criminalitatea informatică.

Marea Britanie a adoptat Computer Misuse Act (1990), care sancţiona accesul neautorizat la sisteme informatice şi modificarea ilegală a datelor digitale[9], Franţa a introdus în Codul Penal (1992), frauda informatică şi manipularea frauduloasă a datelor digitale[10], iar Germania a modificat Codul Penal (1997), sancţionând fraudele informatice şi utilizarea abuzivă a sistemelor informatice[11].

Aşadar, spre sfârşitul secolului XX, criminalitatea informatică, prin natura sa transnaţională, risca să devină o ameninţare serioasă la adresa securităţii economice, juridice şi politice a statelor, necesitând o reglementare unitară şi măsuri de cooperare internaţională, deoarece, în lipsa unor norme comune, dificultăţile în investigarea şi sancţionarea infracţiunilor comise prin mijloace electronice reprezentau o adevărată provocare.

## 2. Convenţia de la Budapesta şi influenţa asupra legislaţiilor europene

În acest sens, Consiliul Europei a iniţiat elaborarea unui instrument juridic internaţional care să ofere un cadru legislativ coerent pentru prevenirea şi

[7] OECD, Guidelines for the Security of Information Systems and Networks (1992). Disponibil la: https://www.oecd.org/digital/ieconomy/15582260.pdf.

[8] *Ibidem*.

[9] Computer Misuse Act 1990, Regatul Unit. Disponibil la: https://www.legislation.gov.uk/ukpga/1990/18/contents.

[10] French Penal Code, Law No. 92-1336 of 16 December 1992, Franţa. Disponibil la: https://www.legifrance.gouv.fr/.

[11] German Penal Code, Amendments of 1997 on Cybercrime, Germania. Disponibil la: https://www.gesetze-im-internet.de/englisch_stgb/.

combaterea criminalităţii informatice[12], materializat, la 23 noiembrie 2001, prin adoptarea Convenţiei de la Budapesta privind criminalitatea informatică, considerat primul tratat internaţional dedicat reglementării infracţiunilor comise prin mijloace informatice; trebuie amintită şi participarea unor state non-europene, precum Statele Unite ale Americii, Canada şi Japonia, ceea ce i-a conferit un caracter global[13].

Structurată în patru capitole, Convenţia de la Budapesta urmărea armonizarea legislaţiilor naţionale privind criminalitatea informatică şi stabilea un set de infracţiuni informatice care trebuiau sancţionate de statele semnatare.

Însă, cel mai important aspect constă în faptul că tratatul instituia, într-un cadru normativ coerent şi supranaţional, dispoziţii de natură procedurală esenţiale pentru investigarea infracţiunilor informatice, consacrând obligaţii precise în sarcina statelor părţi privind adoptarea de măsuri eficiente de identificare, conservare, obţinere şi valorificare a probelor digitale.

Totodată, prevedea mecanisme avansate de cooperare judiciară internaţională în materie penală, facilitând schimbul operativ de informaţii, asistenţa reciprocă între autorităţi competente, extrădarea suspecţilor, precum şi constituirea unor canale directe de comunicare între state, toate acestea în scopul combaterii eficace a criminalităţii informatice transfrontaliere şi al armonizării reacţiei penale la nivel global[14].

Infracţiunile care urmau să fie armonizate în dreptul penal al statelor semnatare au fost prevăzute în articolele 2-10 ale Convenţiei, acestea fiind grupate tematic pentru a reflecta principalele forme de manifestare ale criminalităţii informatice.

Prima categorie vizează infracţiunile comise împotriva confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice, având ca obiect protecţia securităţii şi funcţionalităţii mediului digital.

A doua categorie cuprinde infracţiuni de natură economică, precum frauda informatică şi falsificarea datelor, care afectează patrimoniul şi încrederea în tranzacţiile electronice.

Cea de-a treia categorie se referă la faptele privind conţinutul ilegal al informaţiei electronice, în special distribuirea de materiale interzise prin lege,

[12] S.W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, Praeger, 2010, p. 45.

[13] Budapest Convention on Cybercrime, 2001, Council of Europe. Disponibil aici: https://rm.coe.int/1680081561.

[14] Art. 2-10, 16-18, 23-35 din Convenția de la Budapesta, Legea nr. 64/2004 privind ratificarea Convenției și Codul penal român (art. 249, 325, 360).



cu scopul de a preveni folosirea abuzivă a reţelelor informatice în dauna ordinii publice şi a valorilor fundamentale.

Totodată, Convenţia obliga statele semnatare să sancţioneze următoarele fapte:

- accesul ilegal la un sistem informatic (art. 2) – orice acces neautorizat la un sistem informatic este incriminat, indiferent dacă este realizat prin spargerea parolelor, exploatarea vulnerabilităţilor sau utilizarea altor metode frauduloase[15].

- interceptarea ilegală a datelor informatice (art. 3) – prevede sancţiuni pentru captarea neautorizată a datelor electronice, inclusiv a comunicaţiilor private[16].

- interferenţa cu datele informatice (art. 4) – incriminează modificarea, ştergerea sau deteriorarea neautorizată a datelor informatice[17].

- interferenţa cu sistemele informatice (art. 5) – sancţionează orice acţiune care afectează funcţionarea sistemelor informatice, inclusiv atacurile[18] de tip *denial-of-service* (DoS)[19].

În cadrul articolelor 7 şi 8, Convenţia de la Budapesta consacră incriminări cu un pronunţat caracter patrimonial, adaptate specificului mediului digital, care vizează protejarea siguranţei circuitului juridic electronic şi a încrederii în funcţionarea sistemelor informatice utilizate în scopuri economice.

Astfel, art. 7 reglementează infracţiunea de fals informatic, calificată prin acţiuni deliberate de introducere, alterare sau utilizare a unor date informatice inexacte ori fabricate, în vederea producerii unui efect juridic prin inducerea în eroare a unui subiect de drept şi obţinerii unui folos material injust.

Această formă modernă de fals extinde logica incriminării clasice din dreptul penal la sfera imaterială a datelor electronice, reflectând nevoia de a proteja veridicitatea şi autenticitatea informaţiei digitale cu valoare juridică sau economică.

[15] *Ibidem.*

[16] *Ibidem.*

[17] *Ibidem.*

[18] Atacurile de tip denial-of-service (DoS) reprezintă acțiuni intenționate prin care un atacator suprasolicită un sistem informatic, o rețea sau un server cu un volum excesiv de cereri sau trafic, cu scopul de a-l face inaccesibil pentru utilizatorii legitimi. Aceste atacuri nu vizează distrugerea datelor, ci afectarea disponibilității serviciilor informatice, blocând funcționarea normală a sistemului. Din perspectivă juridico-penală, ele pot constitui o formă de perturbare gravă a funcționării sistemelor informatice și pot fi încadrate ca infracțiuni împotriva securității cibernetice.

[19] Art. 2-10, 16-18, 23-35 din Convenția de la Budapesta, Legea nr. 64/2004 privind ratificarea Convenției și Codul penal român (art. 249, 325, 360).

În completare, art. 8 defineşte frauda informatică drept folosirea abuzivă a unui sistem informatic prin introducerea, modificarea, ştergerea de date sau afectarea funcţionării sistemului, cu scopul de a cauza un prejudiciu patrimonial unei părţi şi, concomitent, de a obţine un avantaj economic necuvenit, conturând astfel o formă de înşelăciune mediată tehnologic.

Pe de altă parte, art. 9 al Convenţiei reglementează infracţiuni legate de conţinutul ilicit al informaţiei electronice, cu accent asupra protecţiei minorilor împotriva exploatării sexuale în mediul digital.

În acest sens, statele semnatare au obligaţia de a introduce în legislaţia naţională incriminări explicite privind pornografia infantilă în format electronic, vizând toate formele de implicare în procesul de creare, oferire, punere la dispoziţie, distribuire, procurare sau simplă deţinere de materiale care prezintă minori în contexte sexuale explicite sau degradante.

Aceste norme exprimă o preocupare constantă pentru combaterea fenomenului transfrontalier al abuzului digital asupra minorilor, consacrând standarde internaţionale clare de protecţie penală în raport cu gravitatea şi amploarea ameninţărilor informatice asupra demnităţii umane.

Aminteam despre importanţa introducerii procedurilor esenţiale pentru investigarea şi combaterea criminalităţii informatice şi cooperarea internaţională, Convenţia de la Budapesta obligând statele semnatare să adopte măsuri pentru reţinerea şi furnizarea rapidă a datelor informatice pentru autorităţile judiciare (art. 16-18)[20], să coopereze în investigarea infracţiunilor informatice şi să înlesnească schimbul de informaţii şi asistenţa judiciară reciprocă (art. 23-35)[21].

## 3. Transpunerea Convenţiei de la Budapesta în România

România a fost unul dintre primele state care au ratificat Convenţia de la Budapesta, prin Legea nr. 64/2004[22].

Codul penal român a suferit modificări esenţiale în scopul alinierii legislaţiei naţionale la standardele internaţionale prevăzute de Convenţie, prin includerea unor infracţiuni specifice domeniului criminalităţii informatice.

Astfel, au fost incriminate fapte precum frauda informatică, reglementată la art. 249, care sancţionează obţinerea nejustificată de beneficii patrimoniale prin introducerea, modificarea sau ştergerea de date informatice ori prin restricţionarea accesului la aceste date, în scopul producerii unui prejudiciu.

[20] *Ibidem.*

[21] *Ibidem.*

[22] Legea nr. 64/2004 privind ratificarea Convenției de la Budapesta, publicată în M. Of. nr. 343 din 20 aprilie 2004.



De asemenea, art. 360 reglementează accesul ilegal la un sistem informatic, vizând pătrunderea fără drept într-un sistem informatic, cu sau fără încălcarea măsurilor de securitate, indiferent dacă s-a produs sau nu o daună.

În acelaşi sens, art. 325 prevede infracţiunea de fals informatic, constând în introducerea, modificarea sau ştergerea, fără drept, de date informatice cu scopul de a produce un act juridic sau de a genera consecinţe juridice, extinzând astfel noţiunea tradiţională de fals în contextul digital.

Convenţia de la Budapesta reprezintă un reper fundamental în reglementarea criminalităţii informatice la nivel global, oferind un cadru juridic unitar pentru prevenirea, investigarea şi sancţionarea acestor infracţiuni. Impactul său asupra legislaţiilor naţionale, inclusiv în România, a fost semnificativ, contribuind la consolidarea mecanismelor de combatere a infracţiunilor informatice şi la îmbunătăţirea cooperării judiciare internaţionale.

Necesitatea armonizării legislaţiei naţionale a fost determinată de creşterea exponenţială a infracţiunilor comise prin intermediul tehnologiei informatice, precum frauda informatică, accesul ilegal la sisteme informatice şi atacurile cibernetice.

Lipsa unor norme clare şi coerente în acest domeniu a creat dificultăţi în investigarea şi sancţionarea faptelor comise, motiv pentru care România a procedat la o integrare treptată şi sistematică a dispoziţiilor prevăzute în Convenţia de la Budapesta, precum şi în alte instrumente juridice internaţionale cu relevanţă în materia criminalităţii informatice, prin adaptarea cadrului legislativ naţional la exigenţele cooperării judiciare internaţionale şi ale protecţiei eficiente a valorilor sociale în mediul digital.

Acest proces de armonizare s-a materializat prin modificări succesive ale Codului penal şi ale legislaţiei speciale, în vederea consacrării unor incriminări corespunzătoare noilor forme de pericol generate de utilizarea abuzivă a tehnologiei informaţiei.

Transpunerea standardelor convenţionale a urmărit atât definirea riguroasă a unor infracţiuni informatice esenţiale precum accesul ilegal, frauda informatică, falsul informatic sau perturbarea funcţionării sistemelor, cât şi instituirea unor mecanisme procedurale menite să faciliteze investigarea transfrontalieră a acestora.

Prin Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, România a introdus în legislaţia penală prima reglementare cuprinzătoare privind criminalitatea informatică[23]; aceste dispoziţii au fost ulterior incluse în Codul penal din 2009, în cadrul

[23] Legea nr. 161/2003 privind măsuri pentru asigurarea transparenței în exercitarea demnităților publice, publicată în M. Of. nr. 279 din 21 aprilie 2003.

Titlului VII – Infracțiuni contra siguranței și integrității sistemelor și datelor informatice.

Prin aceste incriminări, România a transpus în legislația sa obligațiile prevăzute în Capitolul II al Convenției de la Budapesta, care impunea statelor semnatare să sancționeze accesul ilegal la sisteme informatice, frauda informatică, falsul informatic și atacurile asupra datelor și sistemelor electronice[24].

Implementarea Convenției de la Budapesta a determinat și modificări în Codul de procedură penală, pentru a permite investigarea eficientă a infracțiunilor informatice.

Printre măsurile introduse se numără: obligația furnizorilor de servicii IT de a furniza date autorităților judiciare în cadrul investigațiilor penale (art. 138 C. pr. pen.)[25], măsura reținerii și conservării rapide a datelor informatice necesare unei anchete penale (art. 170 C. pr. pen.)[26], percheziția informatică (art. 168 C. pr. pen.) – reglementează accesul autorităților la sisteme informatice pentru obținerea de probe în cadrul procesului penal[27].

Aceste măsuri sunt conforme cu Capitolul III al Convenției de la Budapesta, care impune statelor semnatare adoptarea unor proceduri judiciare clare pentru investigarea și sancționarea criminalității informatice[28].

Un alt aspect important al transpunerii Convenției de la Budapesta în legislația română a fost implementarea mecanismelor de cooperare internațională în domeniul criminalității informatice. România și-a asumat angajamente în cadrul Convenției ONU împotriva criminalității organizate transnaționale și a Regulamentelor Uniunii Europene privind securitatea cibernetică, consolidând astfel, cadrul legislativ intern pentru combaterea infracțiunilor informatice transfrontaliere[29].

Printre măsurile implementate se numără: asistența judiciară reciprocă între state în investigarea și urmărirea penală a infracțiunilor informatice (art. 14 din Legea nr. 302/2004 privind cooperarea judiciară internațională în materie penală)[30], extrădarea infractorilor informatici între statele semnatare

[24] Legea nr. 302/2004 privind cooperarea judiciară internațională în materie penală, publicată în M. Of. nr. 594 din 1 iulie 2004.

[25] Codul de procedură penală al României, cu modificările ulterioare.

[26] *Ibidem.*

[27] *Ibidem.*

[28] Convenția de la Budapesta privind criminalitatea informatică, 2001, Consiliul Europei.

[29] Legea nr. 302/2004 privind cooperarea judiciară internațională în materie penală, publicată în M. Of. nr. 594 din 1 iulie 2004.

[30] *Ibidem.*



ale Convenției de la Budapesta (art. 20 din Legea nr. 302/2004)[31], schimbul de informații între autoritățile judiciare și organismele de aplicare a legii, precum INTERPOL și Europol, în cadrul investigațiilor privind criminalitatea informatică[32].

## 4. Norme europene: GDPR, Directiva 2013/40/UE, Directiva NIS

Adoptarea Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice, a Regulamentului (UE) 2016/679 privind protecția datelor cu caracter personal (GDPR) și a Directivei (UE) 2016/1148 privind securitatea rețelelor și a sistemelor informatice (Directiva NIS) au fost pași esențiali în direcția consolidării cadrului juridic european pentru combaterea criminalității informatice și protejarea securității cibernetice[33].

*Directiva 2013/40/UE,* adoptată de Parlamentul European și Consiliul UE la 12 august 2013, a înlocuit Decizia-cadru 2005/222/JAI privind atacurile împotriva sistemelor informatice și a introdus sancțiuni mai severe pentru infracțiunile informatice[34]; această directivă obligă statele membre să adopte măsuri pentru combaterea accesului ilegal la sisteme informatice, a interferenței ilegale cu datele și a utilizării abuzive a unor instrumente informatice.

Totodată, directiva impune statelor membre obligația de a sancționa următoarele infracțiuni informatice: accesul ilegal la sisteme informatice (art. 3), definit că pătrunderea neautorizată într-un sistem informatic protejat, indiferent de mijloacele utilizate[35]; interferența ilegală cu datele (art. 4) constând în modificarea, ștergerea, deteriorarea sau restricționarea accesului la date informatice fără autorizație[36]; interferența ilegală cu sistemele informatice (art. 5) reprezentată de atacuri informatice de tip *denial-of-service* (DoS) sau alte acțiuni menite să împiedice funcționarea normală a unui sistem

[31] *Ibidem.*

[32] *Ibidem.*

[33] Regulamentul (UE) 2016/679 (GDPR) privind protecția datelor cu caracter personal, publicat în JOUE L119/1 din 2016. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679.

[34] Directiva NIS (UE) 2016/1148 privind securitatea rețelelor și sistemelor informatice, JOUE L 194/1 din 19 iulie 2016. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L1148.

[35] Directiva (UE) 2019/713 privind combaterea fraudelor și contrafacerii mijloacelor de plată fără numerar, JOUE L 123/18 din 10 mai 2019. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019L0713.

[36] Directiva (UE) 2022/2555 – Directiva NIS 2.0 privind măsuri pentru un nivel ridicat de securitate cibernetică în UE, JOUE L 333/80 din 14 decembrie 2022. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32022L2555.

informatic[37]; utilizarea ilegală a unor instrumente informatice (art. 7) – definită ca producerea, distribuirea sau utilizarea unor programe informatice destinate să faciliteze comiterea de infracţiuni informatice[38].

Adoptat la 27 aprilie 2016, *Regulamentul General privind Protecţia Datelor* (Regulamentul UE 2016/679 privind protecţia datelor – GDPR) a intrat în vigoare la 25 mai 2018, stabilind un cadru unic şi obligatoriu pentru protecţia datelor personale în Uniunea Europeană[39]; spre deosebire de directive, regulamentele UE au aplicabilitate directă în toate statele membre, ceea ce înseamnă că normele GDPR nu necesită transpunere în legislaţia naţională, ci sunt direct aplicabile.

Regulamentul[40] a introdus o serie de obligaţii pentru operatorii de date şi persoanele împuternicite, vizând protecţia drepturilor fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal: principiul legalităţii prelucrării datelor (art. 6), potrivit căruia prelucrarea datelor personale trebuie să aibă un temei juridic, precum consimţământul persoanei vizate sau obligaţiile legale ale operatorului[41]; dreptul la ştergerea datelor („dreptul de a fi uitat") (art. 17) în virtutea căruia persoanele fizice pot solicita ştergerea datelor personale în anumite condiţii legale[42]; notificarea încălcărilor securităţii datelor (art. 33) în conformitate cu care operatorii de date au obligaţia de a informa autorităţile competente şi persoanele afectate în cazul unor breşe de securitate[43].

[37] Regulamentul (UE) 2021/1232 privind prevenirea utilizării frauduloase a identităților digitale, JOUE L 273/1 din 12 iulie 2021. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32021R1232.

[38] Regulamentul (UE) 2022/2065 privind serviciile digitale (Digital Services Act – DSA), JOUE L 277/1 din 27 octombrie 2022. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32022R2065.

[39] Regulamentul (UE) 2023/2414 privind inteligența artificială (AI Act), JOUE L 305/1 din 20 noiembrie 2023. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32023R2414.

[40] România a implementat măsurile necesare pentru aplicarea GDPR prin Legea nr. 190/2018, care stabilește reguli specifice privind prelucrarea datelor personale în context național; Directiva (UE) 2018/1972 privind instituirea Codului European al Comunicațiilor Electronice, JOUE L 321/36 din 17 decembrie 2018. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32018L1972.

[41] Regulamentul (UE) 2022/1925 privind piețele digitale (Digital Markets Act – DMA), JOUE L 265/1 din 14 octombrie 2022. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32022R1925.

[42] Directiva (UE) 2021/2167 privind combaterea spălării banilor și a finanțării terorismului, JOUE L 430/1 din 10 decembrie 2021. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32021L2167.

[43] Directiva (UE) 2023/1423 privind protecția datelor și securitatea rețelelor în instituțiile Uniunii Europene, JOUE L 201/10 din 28 iulie 2023. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32023L1423.



Directiva (UE) 2016/1148 privind securitatea reţelelor şi a sistemelor informatice, cunoscută sub denumirea de Directiva NIS (Network and Information Systems Directive), adoptată în anul 2016, reprezintă primul instrument juridic la nivelul Uniunii Europene care stabileşte un cadru unitar de măsuri pentru consolidarea securităţii cibernetice în toate statele membre.

Actul normativ consacră obligaţii legale cu caracter imperativ în sarcina unor categorii precise de entităţi, şi anume operatorii de servicii esenţiale, activi în domenii strategice precum transporturile, energia, sănătatea şi infrastructurile digitale, precum şi furnizorii de servicii digitale, între care se numără motoarele de căutare, platformele de tip cloud şi pieţele electronice.

Directiva urmăreşte creşterea rezilienţei operaţionale a acestora, prin impunerea unor standarde minime de securitate, obligaţia notificării incidentelor de securitate cibernetică şi colaborarea cu autorităţile competente.

Adoptarea sa a marcat un pas decisiv în direcţia armonizării legislaţiilor naţionale în domeniul securităţii informatice şi a creat premisele unei reacţii coordonate şi eficiente la nivel european în faţa ameninţărilor digitale[44].

România a transpus Directiva NIS prin Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, care impune obligaţii stricte pentru instituţiile publice şi companiile private ce gestionează infrastructuri critice IT[45].

Printre obligaţiile esenţiale instituite prin Directiva (UE) 2016/1148 (Directiva NIS) şi transpunerea sa în dreptul intern prin Legea nr. 362/2018 se regăsesc o serie de măsuri cu caracter preventiv, coercitiv şi operaţional, menite să consolideze securitatea reţelelor şi sistemelor informatice ce susţin servicii esenţiale sau digitale.

Astfel, în conformitate cu art. 14 din Directivă, entităţile vizate au obligaţia legală de a notifica, în mod prompt, incidentele de securitate cibernetică către autorităţile naţionale competente, în special către Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), pentru a asigura o reacţie coordonată şi limitarea impactului.

Conform art. 16, aceste entităţi trebuie să adopte şi să implementeze măsuri tehnice şi organizatorice adecvate, proporţionale cu riscurile identificate, în scopul prevenirii şi reducerii vulnerabilităţilor informatice care pot afecta disponibilitatea, autenticitatea, integritatea sau confidenţialitatea datelor şi serviciilor informatice.

[44] Regulamentul (UE) 2021/241 privind Mecanismul de Redresare și Reziliență, JOUE L 57/17 din 18 februarie 2021. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32021R0241.

[45] Regulamentul (UE) 2018/1807 privind cadrul pentru libera circulație a datelor non-personale în Uniunea Europeană, JOUE L 303/59 din 28 noiembrie 2018. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32018R1807.

Totodată, art. 21 consacră un regim sancţionator sever, ce include aplicarea unor amenzi substanţiale în cazul nerespectării obligaţiilor prevăzute, accentuând caracterul imperativ al normelor şi importanţa protejării infrastructurilor informatice critice într-un context digital marcat de ameninţări persistente şi sofisticate[46].

Adoptarea Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice, a Regulamentului general privind protecţia datelor (GDPR) şi a Directivei (UE) 2016/1148 privind securitatea reţelelor şi a sistemelor informatice (NIS) au reprezentat momente definitorii în consolidarea arhitecturii juridice a Uniunii Europene în domeniul criminalităţii informatice şi al protecţiei infrastructurii digitale.

Aceste instrumente normative au instituit un cadru coerent şi interdependent de norme penale, obligaţii administrative şi cerinţe tehnice, menite să asigure un nivel ridicat de securitate cibernetică şi protecţie a datelor în faţa ameninţărilor tot mai sofisticate din spaţiul digital.

România a implementat aceste acte printr-un ansamblu de modificări legislative, inclusiv în Codul penal şi în legi speciale, precum şi prin adoptarea unor măsuri administrative instituţionale, consolidând rolul autorităţilor naţionale competente în prevenirea şi gestionarea incidentelor de securitate.

Prin aceste demersuri, statul român a contribuit activ la creşterea rezilienţei infrastructurilor informatice critice şi la întărirea cooperării judiciare şi operaţionale între statele membre ale Uniunii în domeniul securităţii cibernetice.

## 5. Primele reglementări privind infracţiunile informatice în România înainte de anul 2003

Până la începutul anilor 2000, cadrul legislativ românesc nu conţinea reglementări distincte privind criminalitatea informatică, întrucât fenomenul nu fusese încă recunoscut ca o formă autonomă de pericol social în ordinea juridico-penală.

Faptele comise prin utilizarea mijloacelor electronice sau a sistemelor informatice erau subsumate normelor generale ale Codului Penal din 1968, fiind încadrate, în funcţie de circumstanţele concrete, în infracţiuni precum înşelăciunea (art. 215), falsul în înscrisuri sub semnătură privată (art. 290) sau delapidarea (art. 295).

[46] Decizia-cadru 2001/413/JAI privind combaterea fraudei şi falsificării plăţilor electronice, JOUE L 149/1 din 2 iunie 2001. Disponibil online la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32001F0413.



Această abordare legislativă reflecta o percepţie formalistă asupra ilicitului penal, fără a distinge particularităţile mediului digital, cum ar fi intangibilitatea suportului informatic sau automatizarea acţiunilor frauduloase.

Lipsa unei reglementări adaptate realităţilor tehnologice a generat dificultăţi în investigarea şi sancţionarea faptelor informatice, impunând, ulterior, necesitatea alinierii legislaţiei naţionale la standardele europene şi internaţionale în materie de criminalitate cibernetică[47].

Întrucât aceste infracţiuni nu reflectau pe deplin specificitatea criminalităţii informatice, iar numărul cazurilor de fraude prin mijloace electronice era în creştere, s-a impus necesitatea unei reglementări distincte.

Primele încercări de reglementare au fost influenţate de evoluţiile internaţionale în domeniul dreptului penal al tehnologiei informaţiei, în special de Convenţia de la Budapesta privind criminalitatea informatică (2001), precum şi de recomandările Organizaţiei pentru Cooperare şi Dezvoltare Economică (OCDE) privind securitatea sistemelor informatice.

Aşa cum s-a evidenţiat anterior, în lipsa unor norme penale dedicate, fraudele comise prin intermediul mijloacelor electronice erau încadrate, în mod forţat, în textele generale ale Codului Penal din 1968, în special în materia înşelăciunii şi a falsului.

Totuşi, aceste dispoziţii s-au dovedit insuficiente şi inadecvate, întrucât fraudele informatice presupun mijloace de comitere specifice mediului digital, precum utilizarea unor interfeţe electronice, exploatarea vulnerabilităţilor tehnice sau manipularea fluxurilor automate de date, care nu se regăsesc în tiparul juridic al infracţiunilor clasice.

Mai mult, vechiul cod nu reglementa infracţiuni esenţiale pentru protecţia integrităţii sistemelor informatice, precum accesul neautorizat, interceptarea ilegală a comunicaţiilor electronice ori alterarea conţinutului digital.

Aceste omisiuni legislative au generat un vid de incriminare în faţa noilor forme de criminalitate, determinând, în mod inevitabil, necesitatea unei reforme legislative care să răspundă specificului tehnologic al faptelor şi să asigure o protecţie penală adecvată în era digitală.

Deşi Codul Penal din 1968 nu conţinea dispoziţii exprese referitoare la criminalitatea informatică, unele intervenţii normative cu caracter administrativ au încercat, într-o formă incipientă, să răspundă riscurilor generate de utilizarea tehnologiei digitale, în special în domeniile sensibile din punct de vedere economic şi operaţional, precum sectorul bancar şi al telecomunicaţiilor.

Un exemplu semnificativ în acest sens îl constituie *Regulamentul nr. 6/1994 al Băncii Naţionale a României privind sistemele electronice de*

[47] Codul Penal din 1968, republicat în M. Of. nr. 65 din 16 aprilie 1997.

*plată*, care a reprezentat una dintre primele încercări de reglementare formală a riscurilor asociate tranzacţiilor electronice.

Acesta a introdus cerinţe minime privind securitatea şi fiabilitatea sistemelor de plată electronică, stabilind obligaţii pentru instituţiile financiare în vederea prevenirii accesului neautorizat şi a manipulării frauduloase a datelor.

Regulamentul reflecta conştientizarea timpurie a vulnerabilităţilor informatice în infrastructurile critice şi anticipa, într-o manieră limitată, necesitatea unei reglementări specializate în materia criminalităţii informatice[48].

*Regulamentul* stabilea, pentru prima dată în România, cadrul juridic necesar implementării unor standarde de securitate pentru tranzacţiile electronice, obligând instituţiile financiare să adopte măsuri pentru protejarea confidenţialităţii, integrităţii şi disponibilităţii tranzacţiilor efectuate prin intermediul sistemelor electronice.

Confidenţialitatea datelor viza protejarea informaţiilor cu caracter sensibil împotriva accesului neautorizat, integritatea tranzacţiilor avea ca scop prevenirea alterării acestora în timpul procesării sau transmiterii, iar disponibilitatea sistemului urmărea asigurarea funcţionării continue a serviciilor financiare, evitând întreruperile sau disfuncţionalităţile accidentale sau intenţionate[49].

Deşi nu oferea detalii tehnice specifice, regulamentul stabilea un cadru general pentru adoptarea unor măsuri de securitate adecvate în funcţie de riscurile asociate tranzacţiilor electronice: criptarea datelor transmise (instituţiile financiare aveau obligaţia de a utiliza tehnologii de criptare a informaţiilor transmise pentru a preveni interceptarea datelor de către terţi neautorizaţi[50]), existenţa unor mecanisme de autentificare (pentru a preveni accesul neautorizat la sistemele electronice de plată, regulamentul impunea implementarea unor proceduri de autentificare, inclusiv utilizarea parolelor, a codurilor PIN sau a altor mijloace de verificare a identităţii[51]), controlul accesului şi monitorizarea activităţilor (instituţiile financiare erau obligate să implementeze proceduri stricte de control al accesului la sistemele informatice, astfel încât numai personalul autorizat să aibă permisiunea de a efectua operaţiuni critice).

Banca Naţională a României deţinea un rol central în cadrul normativ instituit prin Regulamentul nr. 6/1994, fiind autoritatea competentă pentru supravegherea, controlul şi evaluarea modului de implementare a măsurilor de securitate aferente sistemelor electronice de plată.

[48] Publicat în M. Of. nr. 106 din 26 aprilie 1994.
[49] Art. 4 din Regulament.
[50] Art. 7 din Regulament.
[51] Art. 10 din Regulament.



În temeiul atribuţiilor conferite, BNR avea competenţa de a verifica conformitatea instituţiilor financiare cu cerinţele impuse prin regulament, inclusiv în ceea ce priveşte protejarea integrităţii datelor, prevenirea accesului neautorizat şi funcţionarea corespunzătoare a infrastructurilor informatice utilizate în procesul de plată. În cazul constatării unor abateri sau încălcări ale obligaţiilor stabilite, Banca Naţională putea dispune măsuri corective şi aplica sancţiuni administrative, rolul său fiind esenţial în asigurarea disciplinei operaţionale şi a unui climat de încredere în funcţionarea mecanismelor electronice din sectorul financiar-bancar.

Sancţiunile prevăzute de Regulamentul nr. 6/1994 pentru nerespectarea obligaţiilor instituite constau în măsuri restrictive cu caracter administrativ, precum limitarea temporară sau suspendarea totală a dreptului instituţiilor financiare de a desfăşura operaţiuni prin sisteme electronice de plată.

Aceste măsuri aveau un rol preventiv şi corectiv, vizând protejarea stabilităţii sistemului financiar şi a intereselor utilizatorilor.

În plus, regulamentul consacra răspunderea instituţiilor bancare pentru prejudiciile cauzate utilizatorilor ca urmare a deficienţelor de securitate ale sistemelor informatice utilizate, stabilind un standard ridicat de diligenţă în gestionarea infrastructurii electronice şi transferând asupra băncilor riscul aferent unei protecţii necorespunzătoare a tranzacţiilor.

*O.U.G. nr. 18/1999 privind organizarea şi funcţionarea serviciilor de plată electronică*[52] a fost emisă într-un context de modernizare a sistemului financiar şi adaptare la noile tehnologii emergente din domeniul plăţilor electronice, oferind cadrul necesar pentru efectuarea tranzacţiilor electronice în condiţii de siguranţă şi transparenţă prin introducerea unor reguli clare privind protecţia datelor personale şi securitatea tranzacţiilor.

Printre măsurile riguroase de securitate s-au numărat: obligativitatea autentificării utilizatorilor pentru accesul la serviciile de plată electronică, folosind mijloace sigure, precum parolele sau semnăturile electronice, obligaţia furnizorilor de servicii de a proteja datele personale şi bancare ale utilizatorilor prin criptare şi alte metode de securizare a datelor, obligaţia instituţiilor financiare de a implementa sisteme de detecţie şi prevenire a fraudelor, inclusiv raportarea tranzacţiilor suspecte către autorităţile competente, sau răspunderea directă a furnizorilor de servicii pentru asigurarea infrastructurii tehnice care să minimizeze riscurile de fraudă sau acces neautorizat.

O.U.G. nr. 18/1999 a suferit mai multe modificări, în special în urma armonizării legislaţiei româneşti cu directivele Uniunii Europene privind

[52] Publicată în M. Of. nr. 81 din 26 februarie 1999.

serviciile de plată şi securitatea cibernetică, câteva dintre cele mai importante modificări fiind aduse de Legea nr. 365/2002 privind comerţul electronic[53], care a extins cadrul legal pentru plăţile electronice şi a clarificat responsabilităţile furnizorilor, de Legea nr. 209/2019 privind serviciile de plată şi pentru modificarea unor acte normative (transpunerea Directivei PSD2 în legislaţia românească).

*Legea nr. 365/2002* a fost adoptată pentru a reglementa aspectele juridice ale comerţului electronic în România, în conformitate cu directivele europene privind comerţul electronic (Directiva 2000/31/CE), printre modificările relevante aduse O.U.G. nr. 18/1999 numărându-se introducerea conceptului de semnătură electronică avansată şi extinsă, clarificarea normelor privind încheierea contractelor la distanţă şi confirmarea comenzilor online şi protecţia consumatorilor în comerţul electronic.

*Legea nr. 209/2019 privind serviciile de plată şi instituţiile de plată*[54] a transpus în legislaţia românească Directiva (UE) 2015/2366 privind serviciile de plată (PSD2[55]), scopul principal fiind acela de a creşte securitatea plăţilor electronice şi de a stimula concurenţa în industria serviciilor financiare.

Printre modificările şi completări importante aduse O.U.G. nr. 18/1999 se numără securitatea tranzacţiilor electronice (a introdus măsuri de autentificare strictă a utilizatorului – Strong Customer Authentication[56] – SCA), accesul terţilor la conturi bancare (instituţiile financiare au fost obligate să permită accesul controlat la conturi pentru furnizori terţi autorizaţi), supraveghere sporită din partea Băncii Naţionale a României care a primit noi atribuţii de supraveghere şi control asupra instituţiilor de plată.

*Legea nr. 8/1996 privind drepturile de autor şi drepturile conexe*[57] includea unele dispoziţii referitoare la utilizarea ilegală a software-ului, dar fără a incrimina explicit fraudele informatice, însă această lege a marcat un moment decisiv în cadrul juridic autohton, aliniindu-se cerinţelor internaţionale privind protecţia proprietăţii intelectuale, în special în contextul aderării la

[53] Publicată în M. Of. nr. 483 din 5 iulie 2002.

[54] Publicată în M. Of. nr. 868 din 13 noiembrie 2019.

[55] European Central Bank, Payment Services Directive 2 (PSD2) – Official Journal of the European Union, 2015.

[56] Autentificarea Strictă a Clientului (Strong Customer Authentication – SCA) este un mecanism de securitate impus de legislația europeană (PSD2) care presupune utilizarea a cel puțin două elemente independente din trei categorii: ceva ce clientul cunoaște (ex. parolă), ceva ce deține (ex. telefon mobil) și ceva ce este parte din el (ex. amprentă digitală). Scopul acestei măsuri este de a reduce riscul de fraudă în tranzacțiile electronice și de a proteja integritatea procesului de autentificare în mediul online.

[57] Publicată în M. Of. nr. 60 din 26 martie 1996.



Uniunea Europeană şi respectării convenţiilor internaţionale relevante, precum Convenţia de la Berna[58] şi Acordul TRIPS[59].

Totuşi, chiar dacă Legea nr. 8/1996 nu incrimina explicit fraudele informatice, oferea un cadru esenţial pentru protejarea drepturilor de autor asupra programelor informatice, prevenind utilizarea neautorizată a acestora şi stabilind sancţiuni pentru încălcările normelor în cauză.

Astfel, potrivit art. 139 din lege, reproducerea sau distribuirea programelor informatice fără permisiunea expresă a titularului dreptului de autor este considerată o încălcare a legii şi poate atrage sancţiuni administrative sau penale.

De asemenea, legea interzice în mod expres modificarea sau decompilarea software-ului, cu excepţia cazurilor în care acestea sunt efectuate pentru interoperabilitate sau pentru realizarea unor copii de siguranţă, conform art. 75 alin. (1).

Un element semnificativ al Legii nr. 8/1996 îl reprezintă reglementarea clară a excepţiilor privind utilizarea programelor informatice; potrivit art. 75 alin. (2), utilizatorii sunt autorizaţi să efectueze o copie de siguranţă a unui program de calculator, cu condiţia ca această copie să fie destinată exclusiv protejării în cazul deteriorării sau pierderii versiunii originale, această prevedere asigurând un echilibru între protecţia titularilor de drepturi şi dreptul utilizatorilor de a-şi proteja investiţiile în software-ul legal deţinut.

Deşi Legea nr. 8/1996 oferă un cadru legislativ clar pentru protejarea programelor informatice în calitate de opere protejate prin drept de autor,

[58] Convenția de la Berna pentru protecția operelor literare și artistice, adoptată în anul 1886 și administrată de Organizația Mondială a Proprietății Intelectuale (OMPI), este principalul instrument internațional în materia dreptului de autor, având ca scop garantarea unei protecții uniforme și echitabile a creațiilor intelectuale în toate statele membre. Convenția consacră principii fundamentale, precum tratamentul național (autoritățile unui stat parte acordă autorilor străini aceeași protecție ca autorilor naționali), protecția automată (drepturile există fără nicio formalitate) și independența protecției (dreptul este recunoscut indiferent de existența protecției în țara de origine). De asemenea, stabilește drepturi morale și patrimoniale pentru autori și impune standarde minime de protecție pentru operele literare, muzicale, dramatice, cinematografice, fotografice și plastice.

[59] Acordul TRIPS (Agreement on Trade-Related Aspects of Intellectual Property Rights) este un tratat internațional semnat sub egida Organizației Mondiale a Comerțului (OMC), care stabilește standarde minime de protecție juridică pentru toate formele principale de drepturi de proprietate intelectuală, inclusiv drepturi de autor, mărci, brevete, desene industriale, indicații geografice și secrete comerciale. Adoptat în 1994, în cadrul Rundei Uruguay, Acordul TRIPS impune statelor membre ale OMC obligația de a armoniza legislațiile naționale în domeniul proprietății intelectuale și de a institui mecanisme eficiente de aplicare, asigurând un echilibru între protecția titularilor de drepturi și interesul public în accesul la cunoaștere, inovație și tehnologie.

aplicarea sa în domeniul criminalității informatice este adesea limitată de insuficiența resurselor instituționale și a mijloacelor tehnice de investigare.

Utilizarea neautorizată a software-ului, una dintre formele recurente ale criminalității informatice, continuă să se manifeste la scară largă, fiind favorizată de lipsa accesului la alternative legale accesibile și de o cultură digitală deficitară.

În aceste condiții, fenomenul pirateriei software nu doar că subminează protecția juridică a titularilor de drepturi, dar alimentează și alte forme de infracționalitate informatică, precum distribuirea de conținut ilegal sau compromiterea securității cibernetice prin utilizarea de programe modificate.

## 6. Legea nr. 161/2003 – prima reglementare a infracțiunilor informatice în România

Adoptarea Legii nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției[60] a marcat una dintre primele inițiative legislative consistente în domeniul combaterii criminalității informatice.

Într-un context european dominat de presiunea armonizării normelor interne cu legislația comunitară – în special cu Convenția Consiliului Europei privind criminalitatea informatică (adoptată la Budapesta în 2001) – Legea nr. 161/2003 a devenit un instrument esențial în prevenirea și combaterea infracțiunilor ce implică utilizarea tehnologiilor informaționale[61].

În acest sens, o sursă principală de inspirație a fost Directiva 2001/29/CE privind armonizarea anumitor aspecte ale dreptului de autor în societatea informațională, precum și Decizia-cadru 2005/222/JAI privind atacurile împotriva sistemelor informatice[62].

Art. 49 din Titlul III al Legii nr. 161/2003 definește frauda informatică drept o *„introducere, modificare, ștergere sau deteriorare de date informatice, restricționarea accesului la aceste date ori perturbarea funcționării unui sistem informatic în scopul obținerii unui folos material injust pentru sine sau pentru altul"*; această definiție acoperă o gamă largă de acțiuni, de la manipularea intenționată a datelor informatice până la atacurile asupra sistemelor

[60] Publicată în M. Of. nr. 279 din 21 aprilie 2003.

[61] Convenția Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta, 23 noiembrie 2001.

[62] Directiva 2001/29/CE a Parlamentului European și a Consiliului din 22 mai 2001, privind armonizarea anumitor aspecte ale dreptului de autor și ale drepturilor conexe în societatea informațională.



informatice, constituind un precedent legislativ solid pentru reglementările ulterioare în materia infracțiunilor informatice.

Legea nr. 161/2003 a reprezentat un moment esențial în conturarea unui cadru juridic specializat în materia criminalității informatice, oferind primele instrumente legale destinate sancționării accesului neautorizat la sisteme informatice, interferenței cu datele și comiterii de fraude prin mijloace electronice.

Cu toate acestea, reglementarea a rămas, în timp, parțial insuficientă în raport cu evoluția rapidă a fenomenului, neacoperind în mod adecvat formele complexe și sofisticate de fraudă informatică, precum ingineria socială, care exploatează vulnerabilitățile umane, sau atacurile automatizate bazate pe inteligență artificială.

În contextul acestor riscuri reale, legea nu asigura un nivel corespunzător de protecție pentru infrastructurile critice informatice, ale căror compromiteri pot produce consecințe grave asupra securității naționale și funcționării serviciilor esențiale.

Astfel, s-a impus necesitatea adoptării unor măsuri legislative și tehnico-operative suplimentare, menite să răspundă complexității noilor forme de criminalitate cibernetică și să consolideze reziliența sistemelor informatice strategice.

## 7. Legea nr. 64/2004 și integrarea normelor internaționale

Într-adevăr, dinamica accelerată a tehnologiilor digitale impune o revizuire continuă a instrumentelor juridice existente, întrucât formele de manifestare ale criminalității informatice devin tot mai sofisticate și dificil de anticipat.

Actualizările legislative ulterioare, precum cele aduse prin Legea nr. 64/2004, care a transpus în legislația națională prevederile Convenției de la Budapesta, și Legea nr. 365/2002 privind comerțul electronic, au contribuit la consolidarea și extinderea cadrului normativ în domeniul infracțiunilor informatice și al reglementării activităților digitale cu relevanță juridică.

Cu toate acestea, complexitatea amenințărilor cibernetice moderne, inclusiv atacurile automatizate, utilizarea inteligenței artificiale sau exploatarea platformelor digitale în scop infracțional, evidențiază limitele actuale ale reglementărilor în vigoare.

În acest context, nevoia de intervenții legislative suplimentare și de actualizări normative constante constituie o provocare majoră și permanentă pentru legiuitorul român, aflat în necesitatea de a menține un echilibru între