Criminalitatea informatică

Eliza ENE CORBEANU (avocat)

Criminalitatea informatică

Coordonator: Gheorghe CORNESCU (procuror PICCJ)

Universul Juridic
Bucureşti
-2025-

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.