CRIMINALITATEA CIBERNETICĂ ÎN PERIOADA DIGITALIZĂRII ECONOMIEI ȘI ÎN VREME DE RĂZBOI

ALBU LEGAL
DREPT PENAL AL AFACERILOR

CRIMINALITATEA CIBERNETICĂ – PREVENȚIE DE TIPUL DIY (DO IT YOURSELF)

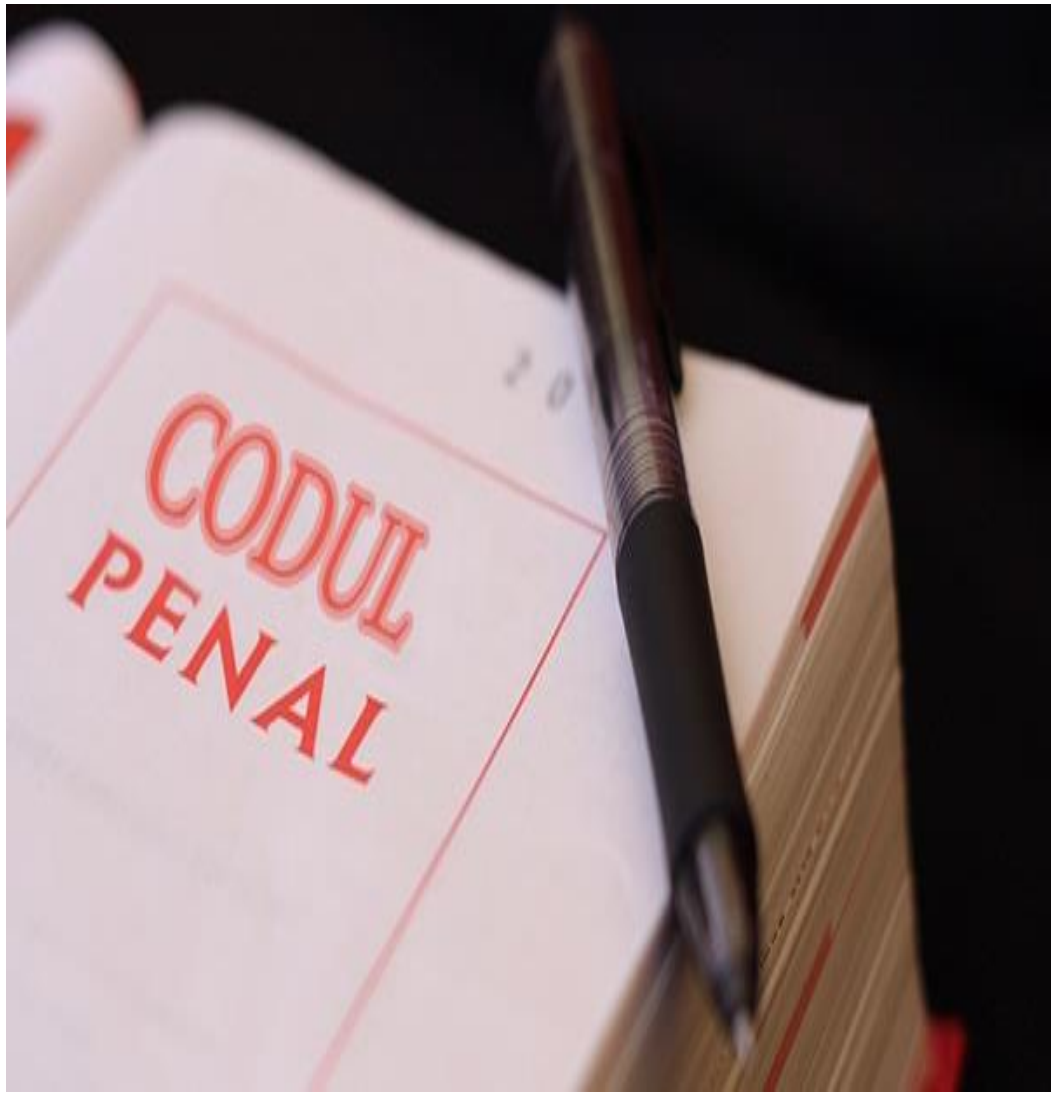
1 Istoria sancționării criminalității cibernetice în legislația din România

- În ciuda intensificării criminalității cibernetice în România odată cu dezvoltarea internetului, dispozițiile legale sancționatoare nu aveau un cadru legislativ de sine stătător, ci erau prevăzute în Legea 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.*
- Astfel, în opinia legiuitorului de la momentul respectiv, faptele de natură penală care s-ar fi putut încadra sau, cel puțin, ar fi avut legătură cu fenomenul criminalității informatice, constituiau un domeniu conex celui al infracțiunilor de corupție.
- În mod evident, singurul numitor comun era caracterul infracțional al ambelor categorii de fapte cu iz penal, însă pentru ca delimitarea să fie efectuată, a fost necesară trecerea unei perioade de 11 ani, finalizată prin constituirea unui capitol distinct în Codul Penal pentru aceaste infracțiuni.

2 Criminalitatea cibernetică în lumina dispozițiilor Codului Penal

- În capitolul VI din Codul Penal, denumit generic *„Infracțiuni contra siguranței și integrității sistemelor și datelor informatice”* sunt prezentate încadrările juridice (infracțiunile) ce pot fi date faptelor săvârșite pe *„teritoriul”* cibernetic, respectiv:

1. **Accesul ilegal la un sistem informatic (art. 360 Cod Penal)**
2. **Interceptarea ilegală a unei transmisii de date informatice (art. 361 Cod Penal)**
3. **Alterarea integrității datelor informatice (art. 362 Cod Penal)**
4. **Perturbarea funcționării sistemelor informatice (art. 363 Cod Penal)**
5. **Transferul neautorizat de date informatice (art. 364 Cod Penal)**
6. **Operațiuni ilegale cu dispozitive sau programe informatice (art. 365 Cod Penal)**



3 Frauda informatică

- Frauda informatică este considerată a fi o infracțiune contra patrimoniului, motiv pentru care a fost sancționată separat, prin introducerea unui capitol distinct în Codul Penal denumit generic *„Fraude comise prin sisteme informatice și mijloace de plată electronice”;*
- În cadrul acestui capitol, legiuitorul a inclus următoarele infracțiuni:

1. **Frauda informatică (art. 249 Cod Penal)**
2. **Efectuarea de operațiuni financiare în mod fraudulos (art. 250 Cod Penal)**
3. **Operațiuni ilegale cu instrumente de plată fără numerar (art. 250 ind. 1 Cod Penal)**
4. **Acceptarea operațiunilor financiare efectuate în mod fraudulos (art. 251 Cod Penal)**

4 Cele mai întâlnite tipuri de fraude informatice

- **Frauda *„Mesaj de la Șef”* (CEO fraud)** – vizează angajații autorizați să efectueze plăți, autorul trimite un e-mail folosind o adresă **aproape** identică cu cea a unei persoane decidente din companie și îi solicită achitarea cu celeritate a unei facturi false;
- **Frauda cu facturi (Invoice fraud)** – presupune transmiterea către companii de e-mailuri identice cu cele recepționate din partea furnizorilor de diverse utilități ce au atașate facturi în care este modificat doar contul bancar în care se solicită a se efectua plata;
- **Phishing/ Smishing/ Vishing** – autorii apelează telefonic, trimit un mesaj text (SMS/ Whatsapp) ori un e-mail, prin care se urmărește inducerea în eroare cu scopul divulgării datelor personale, financiare ori de securitate;
- **Website-uri bancare contrafăcute (Spoofed bank website fraud)** – autorii folosesc mesaje de tip *„phishing”* cu link-uri către site-uri bancare false. Site-ul contrafăcut arată precum cel pe care il imită, cu foarte mici diferențe, deseori greu sesizabile. Odată accesat link-ul, datele personale și/ sau bancare sunt colectate ilegal;

4 Cele mai întâlnite tipuri de fraude informatice

- **Fraude cu investiții (Investment scam)** – autorii, profitând de notorietatea unor platforme de investiții, prezintă diverse oferte despre care menționează că există un timp limitat în care se poate profita de respectiva oportunitate. În esență, este tot o formă de *phishing* prin care se urmărește colectarea datelor personale și bancare;
- **Fraude în cadrul cumpărăturilor online (Shopping scams)** – cu același scop, respectiv al colectării datelor, autorii prezintă *„oferte”* de nerefuzat în legătură cu anumite produse;
- **Fraude în cadrul vânzărilor online pe site-urile de profil** – una dintre cele mai noi și inovative tipuri de fraudă care presupune ca, după ce este plasat un anunț pe platforma de comerț online, vânzătorul este contactat prin intermediul aplicației *Whatsapp* de către o persoană care se arată foarte interesată de achiziționarea acelui produs.

5 Metode de prevenție

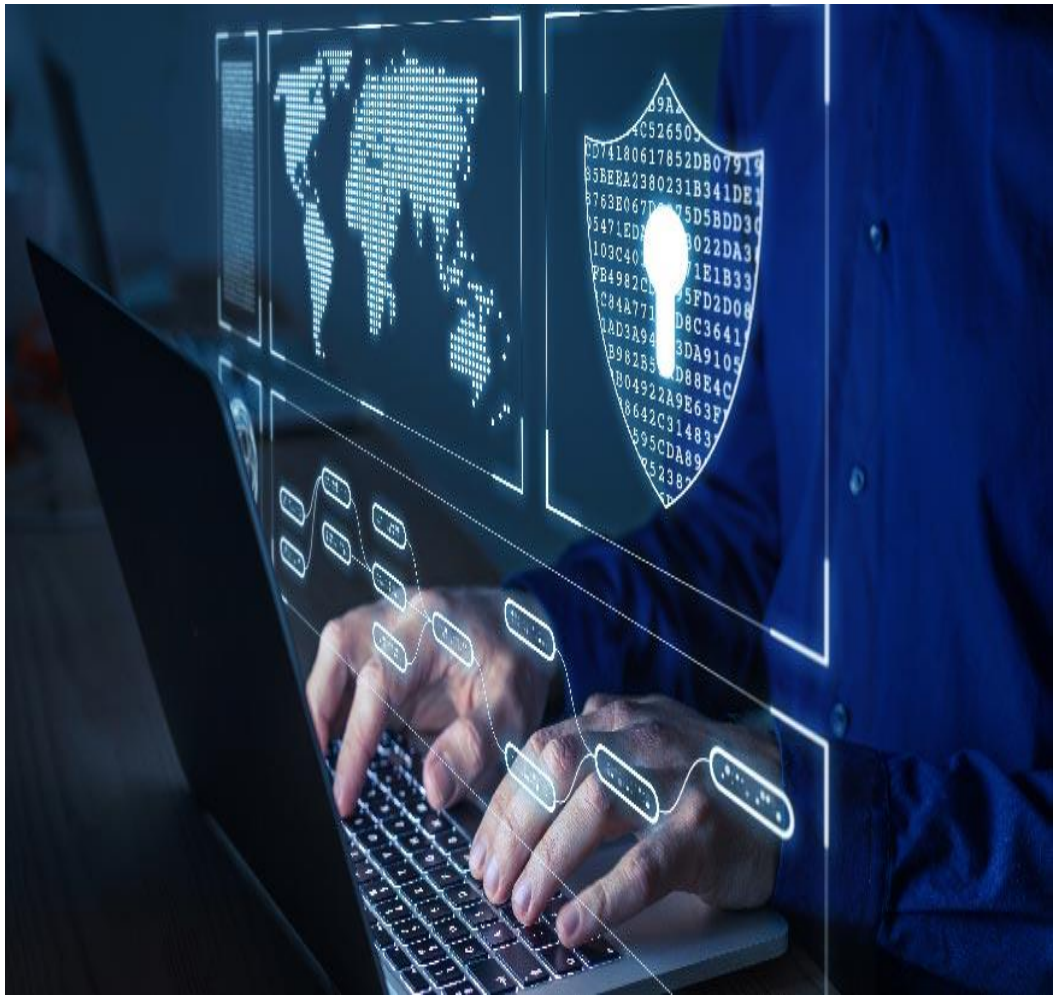
- Obținerea unei confirmări prealabile anterior efectuării plății ori introducerii datelor bancare și/ sau personale prin folosirea datelor de contact din corespondența anterioară;
- Neutilizare funcției *„reply”* pentru a răspunde în corespondența de serviciu – folosirea funcției *„forward”* urmată de introducerea manuală a adresei de e-mail aparținând persoanei cu care corespondați;
- Verificarea recenziilor în legătură cu site-ul/ produsul respectiv;
- Neaccesarea link-urilor din e-mailuri ori SMS-uri pentru care nu există un demers anterior de generare;
- Prezența greșelilor de scriere în conținutul e-mailului/ paginii web reprezintă un indiciu temeinic;
- Pentru verificarea identității, se poate apela organizația pentru care respectiva persoană pretinde că lucrează;
- Deținerea unui card bancar utilizat exclusiv pentru mediul online ce corespunde unui cont în care niciodată nu se regăsesc sume mari de bani.

6 Importanța prevenției de tipul DIY

- Organele de urmărire penală nu dețin tehnologia necesară pentru identificarea și tragerea la răspundere a infractorilor cibernetici;
- Chiar și în ipoteza identificării autorilor fraudei, recuperarea banilor este dificilă din cauza faptului că în majoritatea covârșitoare a cazurilor sumele nu se mai regăsesc în contul respectiv;
- Prejudiciul suferit în urma fraudei se acoperă de către bancă numai în ipoteza îndeplinirii cumulative a unui număr considerabil de condiții;
- Datele de card odată puse la dispoziție unei alte persoane vor fi utilizate pentru golirea contului bancar prin metode care fac imposibilă stabilirea trasabilității banilor.

6 Concluzii

- Clasicul proverb *„paza bună trece primejdia rea”* are aplicabilitate și în mediul online;
- Verificările suplimentare pentru plățile ce urmează a fi efectuate din fondurile companiei unde persoana lucrează ar trebui apreciate și, nicidecum, contestate întrucât conduc la întârzieri;
- *Dacă sună prea bine pentru a fi adevărat, cel mai probabil, nu este;*
- În ciuda gradului de dezvoltare a comerțului în mediul online, șansele sunt minime ca pentru produsul pus la vânzare să se găsească, în decurs de câteva minute, un cumpărător.



7 Întrebări?

ALBU LEGAL
DREPT PENAL AL AFACERILOR

Mihai Lemnaru

Senior Lawyer **Albu Legal**

mihai.lemnaru@albu-legal.ro

M: +40 744 676 347

VĂ MULȚUMIM!

Str. Roma nr. 23, Sector 1, București, România, 011773
(intrarea și expedierile poștale în Str. Washington nr. 27, București, 011793)
office@albu-legal.ro www.albu-legal.ro