**CZU: 343.37:343.53:004** **DOI: 10.5281/zenodo.7366583**

# APLICAREA TEHNOLOGIEI CONTRAR LEGII PENALE – FRAUDE BANCARE

**SÎRBU Uliana,**

lector universitar, Institutul de Ştiinţe Penale şi Criminologie Aplicată
ORCID: 0000-0003-4159-3714

*Tehnology used outside the law is a threat to the modern word. Bank fraud intersects with other types of crime: digital, financial, economic, etc. The law must not allow any evasion of punishment, but necessary ensure the personal and financial safety, security of persons. In these circumstances is needed europeanian community cooperation to ensure information, financial, banking and economical security.*

***Keywords:*** tehnology, credit card, bank fraud, digital crime, financial crimes, safety, security.

Fenomenul fraudelor bancare şi a celor legate de aplicarea ilegală a tehnologiei, apărut în vizorul subiecţilor cercetării, a vloggerilor, internauţilor din lume de zeci de ani în urmă.

Aceste ilegalităţi pot fi observate şi cunoscute epistemologic prin următoarele fapte şi acţiuni:

1. Furtul banilor din conturile bancare, sustragerea datelor personale;
2. Dobândirea banilor prin scheme de escrocherie de la deţinătorii conturilor bancare;
3. Estorcarea datelor bancare, a banilor prin înşelăciune sau ameninţări, cu forţa;
4. Folosirea ilegală a datelor personale biometrice;
5. Sustragerea datelor bancare, a cardului bancar;
6. Furtul datelor de pe banda magnetică a cardului sau a codului PIN;
7. Furtul banilor din conturile bancare a persoanelor fizice sau juridice;
8. Falsificarea cardurilor bancare;
9. Jaful băncii, a bancomatelor;
10. Acordarea creditelor neperformante, dobândite prin înşelăciune;
11. Efectuarea operaţiunilor bancare, care permit spălarea de bani sau finanţarea terorismului;
12. Prin unele operaţiuni bancare se produce gestionarea iraţională a resurselor materiale sau a celor financiare cu scopul de a fi ulterior sustrase;
13. Utilizarea banilor neconformă de către instituţiile financiare: bănci, organizaţiile de microfinanţare;
14. Scheme criminale, frauduloase, care se realizează prin intermediul băncii;

15. Transferuri sau achitări băneşti, ce mimează şi ascunde activitate antreprenorială, prin care se poate face spălarea de bani sau evaziune fiscală;
16. Extragerea portofoliului activelor băncii pe timp de asediu, război, stare excepţională stabilită.

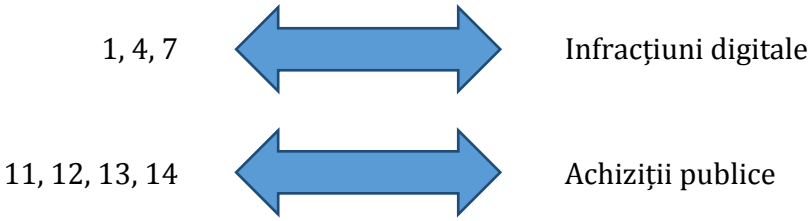
În mare parte aceste ilegalităţi se realizează cu ajutorul tehnologiei, adica a telefoniei IP, internetului. În unele cazuri, fiind iniţiate şi dirijate de criminalii dintr-o ţară, faptic înfăptuite pe teritoriul altei ţări.

La multe din ele detectăm caracterul cumulativ, corelativ sau competitiv. De aici putem deduce şi delimita tipurile acestor fără de legi.

Primele, din acele încălcări enumerate se atribuie infracţinilor digitale.

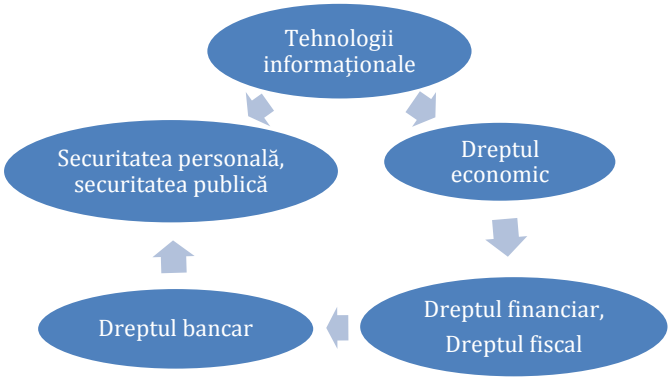
Cele din şirul de ordine cu numărele unsprezece, doisprezece, treisprezece, paisprezece, fac parte din achiziţii publice, adica domeniul dreptului financiar.

**Figura 1.** Corelare segmentară interpătrunzătoare




Dar nu putem trece cu vederea faptul că, acestă corelare vizează mai multe domenii, în special cel informaţional, economic, financiar, bancar. Putem analiza acest circuit reprezentat grafic în figura următoare.

**Figura 2.** Circuitul sectorial



Actualmente comunicaţiile radio cu o cheie cifrată sunt folosite în diverse sisteme, precum şi pentru a proteja banii de pe cardurile bancare. Cardul bancar instrument multifunctional care nu deţine bani în sine, cheia de acces pentru banii din bancă, dând permisiunea de a diminua aceste fonduri din cont. Banii electronici sunt mai greu de furat. Dar totuşi, e posibil, de exemplu, atunci când se fac cumpărături într-un magazin online, de unde se pot fura datele personale, iar apoi pot fi folosite pentru a sustrage banii. Sau alt exemplu, când victima însuşi îi dă date bancare, personale, criminalului care s-a prezentat drept angajat al băncii sau al reţelei de comerţ, de telecomunicaţii. Cea mai frecventă modalitate, cea de citire a datelor de pe banda magnetică. Introdus într-un bancomat, cu ajutorul unui glisor, care se instalează de infractori, acesta citeşte datele. Astfel, o copiere a cardului se face chiar şi în momentul în care acesta a fost introdus sau expus la finalizarea operaţiunii de către bancomat.

Altă modalitate criminală, poate fi realizată cu ajutorul camerei video, plasata de-a supra tastei care fotografiază codul PIN introdus de utilizator. Protecţia acestui sistem se află în continuă îmbunătăţire şi, în consecinţă, şi gradul de siguranţă. Cipul disponibil de pe card bancar, obiect foarte mic care conţine toate datele necesare şi cel care este responsabil de asigurarea securităţii personale şi financiare. Această tehnologie permite protejarea mai bună a datelor personale a deţinătorului cardului. Robotul de producţie pregăteşte carduri şi microcipuri, care sunt plasate deasupra orificiului tăiat în card. Datele strict secretizate sunt aplicate cipului într-o maşină automatizat închisă, folosind computerul. Informaţii secrete, sunt criptate cu algoritm complex. Codificarea cipului cea mai dificilă etapă de producţie, dar şi cea mai fiabilă din punct de vedere al securităţii, adică disponibilitatea cheilor electronice ale băncii, cheile ale cardului şi sistemele de plată. Cardurile protejează direct împotriva pirateriei, de furtul datelor. Dar permite şi face posibil în cazul furnizării personale acestor date sau prin atacul conturilor pe cale electronică, ca înşelătorii sau hoţii să-şi îndeplinească intenţiile şi faptele criminale. Datele acestor carduri, tip, culoare, intră în producţie separat, fiind necunoscute pe foi laminate şi apoi suprapuse pe foi de plastic alb, iar abia apoi robotul le decupează în cartonaşe de plastic separate. Cunoscând tehnologia de producţie, infractorii pot falsifica sau introduce în ele cititor de date, care, după extragea cardului real dintr-un bancomat, acest dispozitiv colectează instantaneu date şi goleşte contul proprietarului. Secretul principal al portmoneului electronic reprezintă tehnologia comunicaţiilor radio la distanţă scurtă.

Cardul din plastic rezistă la temperaturi ridicate, la soluții chimice, anumitor lovituri puternice sau presiunii, dar e neputincios în faţa lăcomiei, vicleniei şi ticăloşiei umane. Tehnologia bancară modernă deține nivel ridicat de securitate şi se îmbunătăţeşte odată cu cerinţele crescânde a schimbărilor lumii moderne.

*Securitatea în mediul online* în permanenţă supusă pericolului, uneori nu mai poate fi asigurată. Aceste încălcări de lege ne fiind bine contracarate, periclitează nu doar securitatea informaţională, dar şi cea statală, econimică, securitatea şi siguranţa financiară a persoanelor.

În dependenţă de elementul prejudiciabil, gravitatea faptei săvârşite putem rezuma nu doar tipul acestor ilegalităţi, dar şi de a face divizarea acestora ramurală şi calificarea, în cele contravenţionale sau penale. Evident, şi pentru stabilirea formei de *răspundere juridică* în urma acestor încălcări de lege comise. Însă mai multe întrebări apar la răspunderea penală şi cea din dreptul international penal şi pentru faptul că, convenţiile, tratatele, alte acte internaţionale, la care ţara noastră face parte, au o mai mare importanţă şi aplicabilitate asupra oricărui act normativ moldav.

Cadrul normativ moldav are necorespunderi, lipsa în mare parte a încălcărilor de lege prezentate în respectiva cercetare, dar şi unele neconformităţi, erori, precum şi absenţa răspunderii juridice în acest sens. Susţin părerea lui Bujor Valeriu, rector al Institutului de Ştiinţe Penale şi Criminologie Aplicată, profesor universintar, în ceea ce priveşte necesitatea stringentă de modificare, actualizare a Codului penal, care trebuie modificat din mai multe considerente. Însă modificarea se cere şi la Codul contravenţional, alte acte normative adiacente.

Astfel, deficienţele Codului penal al Republicii Moldova le vedem în Capitolul X Infracţiuni economice şi în Capitolul XI Infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor. Infracţiunile economice, financiare, bancare, fiscale se regăsesc într-un capitol, dar nu şi celea existente, specificate mai sus. Este extrem de important de a face modificările necesare, actualizare, de a face divizarea, dispersarea infracţiunilor financiare, fiscale, de cele bancare şi economice, chiar şi de cele comerciale, vamale. Deoarece natura juridică a acestora fiind total diferită, dar şi din considerentul apariţiei unor noi tipuri de infracţiuni, şi care necesită să-şi găsească locul în compartimentul potrivit, ca de exemplu a celor informaţionale/digitale.

Potrivit art. 8, alin. (1) din Legea nr.75/2020, Serviciul Prevenirea şi Combaterea Spălării Banilor ”notifică entitatea raportoare despre intenţia sa de

a efectua controlul planificat cu cel puţin 10 zile înainte de începerea controlului”, art. 15, alin. (1) prevede că, înaintea efectuării controlului, inspectorii Serviciului sunt obligaţi să informeze reprezentantul entităţii raportoare despre înfăptuirea controlului care va acea loc, în alin. (2) al acestui articol ”accesul în spaţiile şi în sediile entităţii raportoare supuse controlului se execute cu permisiunea persoanei cu funcţie de răspundere sau a unui alt reprezentant al entităţii”[3]. Ceea ce vădit denotă faptul că, în urma anunţării entităţii despre controlul care urmează a fi efectuat, cele mai valoroase dovezi şi probe pot fi nimicite, de exemplu acte cu înscrisuri, hard discul, diferite date electronice, etc. Iar lipsa accesului poate duce la tergeversarea depistării, documentării, examinării cauzei, sancţionării.

Aceste interpretări de lege nu trebuie să permită delapidări, tăinuire, adica nici o formă de încălcare sau de ocolire, scăpare de răspundere.

În concluzie subliniez faptul că, tehnologiile se îmbunătăţesc considerabil, la fel ca atacatorii, care au modalităţi de piratare a sistemelor de securitate bancară, noi modalităţi de sustragere sau de înşelare a deţinătorilor conturilor de bani. Prin urmare, tehnologiile ştiinţifice caută nu doar să asigure protecţie, securitatee, ci şi să înainteze asupra sferei de activitate criminală.

Știința dă răspuns fundamental şi principal la aceasta, deoarece lupta împotriva fraudei e felul de confruntare între tehnologii. În lume, furtul, jaful, atacul electronic şi escrocheria sunt cele mai comune şi răspândite crime acestui secol. Iar știința dreptului evoluiază în felul său, corespunzător.

**Propuneri:**

1. Modificdarea Codului penal, Codului contravenţional, altor acte normative subordonate din motivul invocat mai sus;
2. Realizarea educaţiei financiare, digitale în instituţiile de învăţământ, precum şi publicului larg;
3. Elaborarea de softuri, care să permită depistarea, aplicarea metodei cantitative de cercetare şi efectuare a analizei criminologice, criminalistice, geolocal şi a măsurilor operativ-investigative la moment;
4. Consolidare europeană la securitatea informaţională, economică şi financiară;
5. Crearea sistemului informaţional naţional de evidenţă a infracţiunilor digitale, economice, financiare;
6. Conlucrarea intenaţională la combaterea, evidența electronică a acestor tipuri de infracţiuni.

**Referinţe:**

1. Codul penal al Republicii Moldova, nr. 985 din 18.04.2002. În: Monitorul Oficial al Republicii Moldova, 2009, nr. 72 – 74;
2. Codul contravenţional al Republicii Moldova, nr. 218 din 24.10.2008. În: Monitorul Oficial al Republicii Moldova, 2017, nr. 78 – 84;
3. Legea nr. 75 din 21.05.2020 privind procedura de constatare a încălcărilor în domeniul prevenirii spălării banilor şi finanţării terorismului şi modul de aplicare a sancţiunilor. În: Monitorul Oficial al Republicii Moldova, 2020, nr. 142 – 146;
4. Here`s How Hackers Are Trying To Seal Your Credit Card At The Gas Pump. [Accesat 20.03.2022] Disponibil: https://youtu.be/hKPpxF8SBJk