CZU: 343.9:004 **DOI: https://doi.org/10.5281/zenodo.12166307**

PARTICULARITĂŢI ŞI CARACTERISTICI ALE CRIMINALITĂŢII ORGANIZATE DIGITALE

Sîrbu Uliana

lectoră universitară, Institutul de Științe Penale și Criminologie Aplicată
ORCID: 0000-0003-4159-3714

Digital crime is widely investigated worldwide. It also has an international normative basis for combating it. International law enforcement is weak. Less research is done on digital organised crime. It is practised in countries with a high level of crime, with a low economy, but also where a state of emergency has been established: disaster, epidemic, war. Criminal groups commit various particularly or exceptionally serious crimes digitally. Causing social danger and great, in some cases extremely great, damage.

Keywords: *digital crime, digital organised crime, danger, damage, security, preventing, counteraction.*

Introducere. **Criminalitatea organizată digitală** se consideră transfrontalieră. Se realizează cu aplicarea tehnologiilor, resurselor informaţionale. Se consideră consumată şi prin acţiunea de sustragere sau a diverselor atentate la datele electronice. Această formă de infracţionalitate fiind răspândită în toată lumea. Se realizează preponderent în ţările cu nivelul de criminalitate înalt, economie slab funcţională, precum şi în ţările unde este situată oricare din formele stării excepţionale.

Potrivit Codului Penal al Republicii Moldova această crima includentă, cu toate derivatele sau variaţiile sale infracţionale se poate incorpora în tipul celor grave, deosebit de grave, excepţional de grave, având toate circumstanţele agravante. Datorită faptului că, pericolul social fiind extrem de mare, alarmantă fiind: securitatea personală a persoanelor, securitatea publică, securitatea interstatală, la nivel internaţional. Dar şi prejudiciul cauzat produs individual, statului va fi apreciat ca unul mare sau chiar colosal de mare, calculat procedural, estimat, apreciat de responsabilii justiţiei.

Această formă de criminalitate este extrem de profitabilă, dar şi latentă pentru că activitatea lor se desfăşoară la distanţă, online. Prin care se mai desfăşoară şi economia tenebră. Criminalii comunică la distanţă prin reţeaua de Internet, înfăptuiesc acţiunile infracţionale prin diverse aplicaţii ca exemplu Vaiber, Telegram, WatsApp, Facebook, Twitter, Dragnet, WebMoney, QIWI pentru plăţile electonice, şi altele. Fiind o activitate de profit înalt, cu riscuri şi

costuri minore. Mai are un specific, membrii realizează faptic aceste acţiuni, fapte criminale într-o ţară, dar sunt conduşi de liderul său, aflat în altă ţară sau în altă locaţie. Ceea ce şi determină primordial colaborare internaţională, de combatere şi predarea justiţiei pentru răspundere.

În determinarea cauzalităţii, se observă legătura obiectivă, între cauză şi efect. În doctrina criminologică este efectuată separarea cauzelor sociale şi a proceselor care determină criminalitatea. Care şi permite de a separa această formă de infracţiune de altele.

Determinantele cauzalităţii, a condiţiilor apariţiei statorniciei, extrapolării, se datorează creşterii economiei industrializării cibernetice, care a favorizat apariţia, persistenţa acestor crime prin utilizarea celor mai performante şi progresiste instrumente cu scop de îmbogăţire sigură, fabuloasă, fără cheltuieli mari, pierderi şi riscuri.

Astfel, **infracţiunile comise digital, de un grup criminal organizat sunt:**

1. *economice* (cu scopul de surmenare şi sau a distrugerii economiei unei ţări, pentru deţinerea sau uzurparea puterii, altele: blocarea investiţiilor, deposedare de proprietate privată a persoanelor fizice sau juridice, contrafacerea sau falsificarea produselor cu transportare ilicită şi vânzare, etc.);
2. *financiare şi fiscale* (piramidele financiare, jocuri de pariu, fabricarea banilor falşi şi vânzarea, sustragerea banilor virtuali: cripto monedă, bit coin; furtul banilor publici, spălarea de bani şi legalizare, investiţii tenebre, evaziune fiscală, etc.);
3. *bancare* (de sustragere a banilor, a cardurilor, a datelor prin înşelăciune, de citire a datelor de pe card, etc.);
4. *excrocherii* prin diverse forme şi modalităţi;
5. *de încălcare a drepturilor proprietăţii intelectuale* (în special la încălcarea dreptului de autor, a mărcii comerciale);
6. *vânzarea de droguri, a substanţelor psihotrope, persecutorilor, anabolizantelor şi altor substanţe nocive*, interzise de lege;
7. *asasinare, omor la comandă;*
8. *atacuri cibernetice* (de tip haking)*;*
9. *vânzarea de arme şi a muniţiilor, a obiectelor explozive, de piraterie;*
10. *porno industria* în toată diversitatea sa, cu vânzarea;
11. *trafic de fiinţe umane, cu exploatarea prin muncă, exploatarea sexuală;*
12. *corupţia;*
13. *terorism şi extremism* (aparentă în ultimii ani).

De fapt, la modul general, crima organizată digitală, faţă de cea obişnuită are

aceleaşi trăsături specifice stabilite şi prezentate de cercetătorii occidentali, europeni, ruşi, naţionali. Investigaţii ştiinţifice înfăptuite mai mult de trei, chiar de cinci decenii. Însă actualmente s-a mai diversificat, datorită digitalizării şi a unor infracţiuni noi aparente în acest sens. Cele mai active organisme internaţionale, din anul 1990 au fost: Organizaţia Naţiunilor Unite, Interpol, Europol, Comisia Europeană. Care au prezentat oficial date alarmante, au elaborat acte normative, ghiduri, instrucţiuni pentru prevenirea şi combaterea crimelor electronice şi a crimei organizare digitale. Diverse acte normative, standarde ca de exemplu ISO 13482-cerinţe privind măsuri de securitate tehnică în utilizarea roboţilor, obiectelor robotizate, şi Directive Europene cu un conţinut precis şi concis, focusate pe combaterea infracţiunilor cibernetice, asigurarea securităţii publice, a celei cibernetice, dar şi cu conţinut de colaborare internaţională.

Una din aceste deconspirări, descoperire a fost efectuată în luna noiembrie a anului 2023. Potrivit ştirilor, colaboratorii de poliţie au identificat grupul criminal organizat, alcătuit din membrii cetăţeni ai diferitori ţări. Faptă penală multiplă, de 4.000.000 lei. Cercetată penal ca ”escrocherie cu cripto valută”. Făptaşii criminali au creat o aplicaţie de gestionare a bani electronici, identică cu cea originală. Banii parveniţi în cont, în urma sustragerii de către infractori, au fost cheltuiţi pentru procurarea bunurilor materiale: apartamente, automobile în oraşele Chişinău şi Bucureşti. În cadrul percheziţiilor la domiciliul infractorilor, atât în ţară, cât şi peste hotare a fost aplicat sechestrul asupra bunurilor în sumă de peste 1.500.000 lei, pentru despăgubirea ulterioară [3].

În desprinsa cercetare problemele stabilite ţin nu doar de securitate. Sunt şi altele: inexistenţa normelor juridice cu privire la crima dată şi mecanismului juridic real de combatere, precum şi a celui legat de asigurarea securităţii; necesitatea elaborării unor politici penale sistemice; securizarea slabă a informaţiilor de acces limitat, în special a acelor de acces liber, lipsa restricţionării accesului; lipsa supravegherii şi controlului; lipsa conlucrării între structurile statale de drept; starea tehnică, materială este foarte precară; insuficienţa de cadre, şi a celor pricepuţi în domeniu; conlucrarea insuficienţă la nivel regional, global.

Colaborarea internaţională joacă un rol important atât în prevenţie, cât şi în combatere. Deoarece problema priveşte, afectează mai multe ţări. Neasigurarea cărei, va duce inevitabil la creşterea criminalităţii internaţionale. Este nevoie de lucru comun: de acces, schimb de date, informaţii, crearea şi utilizarea comună a resurselor, instrumentelor tehnologice, etc. Cercetătorul Luca Iamandi prezintă o abordare aparte, despre prevenirea ”mai eficientă a criminalităţii transfrontaliere”, prin elaborarea unui complex de măsuri administrative, promovarea şi acceptarea cooperării propriu zise, în prevenirea criminalităţii la nivel european, despre

protecţie contra infracţiunilor grave şi a criminalităţii organizare. ”Întrucât criminalitatea organizată continuă să dezvolte o dimensiune globală sporită, este din ce în ce mai important ca legea să poată fi pusă în aplicare în mod eficace dincolo de frontiere şi jurisdicţii”. Autorul face şi propunere de asigurare a protecţiei internaţionale asupra ”grupurilor în situaţii vulnerabile”, prioritar minorilor [2].

În activitatea lucrătorilor structurilor de drept este recomandabil:

1. Folosirea metodei de observare, în special cu ajutorul tehnologiilor (depistare geo local, de informare, sesizare, detectare, urmărire, inclusiv pentru identificarea victimelor).
2. Întrebuinţarea sistematică a metodei de analiză şi monitorizare criminologică. Complementar cu ajutorul metodei aplicării tehnologiilor informaţionale: IP (adresa, utilizatorul), GPS, şi altele pentru prevenire, depistare, urmărire, detectare, supraveghere, combatere.
3. Folosirea metodei de prevenire şi combatere, inclusiv prin utilizarea tehnologiilor informaţionale.
4. În cercetarea penală a acestei crime, este important de determinat scopul, intenţia, motivele făptaşilor pentru a face o calificare corectă, ţinând cont de particularităţile şi caracteristicile penale a grupului, fiecărui membru în parte, a liderului grupului criminal organizat digital. Inclusiv de caracteristica victimologică a victimei.
5. Efectuarea prognosticului criminologic: geografic, determinarea motivelor şi condiţiile de declanşare a crimelor digitale, stabilirea şi evaluarea nivelului criminalităţii digitale în diverse perioade, calcule matematice, rezultate realizate şi prezentare.

Acţiunile prognozei criminologice pot fi:

- ✓ Operative, înfăptuite zilnic de către colaboratorii organelor de drept;
- ✓ Tactice şi strategice. De coordonare, şi stabilire a traseului cercetării;
- ✓ Factoriale, când sunt investigate mai multe fenomene, cauze;
- ✓ Sistemice. Inter relaţionarea obiectelor supuse prognozării, a parametrilor socio-psihologici.
- ✓ Stabilirea riscurilor, pericolelor prognozei. Rezultatele cercetării trebuie puse la baza planificării activităţii organelor de drept.

6. Participare activă şi implicare în colaborare internă, externă.
7. Reducerea acestor infracţiuni este posibilă prin aplicarea unui sistem de acţiuni preventive: socială, de prevenire generală, de prevenire individuală.

Pentru efectuarea profilaxiei victimologice sunt recomandate anumite acţiuni:

1. Sporirea nivelului de eficientizare a securităţii cibernetice;
2. Modernizarea mijloacelor şi instrumentelor tehnologice;
3. Îmbunătăţirea instrumentelor software şi hardware pentru a proteja informaţiile electronice;
4. Informarea şi reamintirea electronică continuă despre existenţa acestor infracţiuni în internet.

Încheiere. Creşterea eficacităţii prevenirii depinde în mod direct de interacţiunea dintre subiecţii prevenţiei, deoarece desfăşurând o activitate planificată, pe baza unor programe, legi, care trebuie să fie intersectoriale, interdepartamentale, interregionale şi, bineînţeles, internaţionale, se va produce rezultatul dorit.

În cadrul cercetării au fost identificate numeroase probleme, respectiv, au fost elaborate soluţii de depăşire, de soluţionare. Prin rezumarea celor expuse mai sus şi prin identificarea celor mai principale probleme, prezentate în cadrul cercetării în cauză:

Principalele probleme		*Soluţii*
✓ Codul Penal al RM nu conţine astfel de norme.		Ajustarea întregului cadru legislativ penal.
✓ Lipsa cadrelor, a specialiştilor bine pregătiţi din punct de vedere criminologic, în aplicarea tehnologiilor informaţionale.		Instruirea specialiştilor, şi utilizare a metodei aplicării tehnologiilor informaţionale (prevenire, depistare, urmărire, contracarare).
✓ Insuficienţa tehnico-materială şi digitală. Dotarea slabă.		Dezvoltare, modernizare, introducerea inovaţiilor tehnologice, digitalizare.
✓ Colaborare slabă inter structural, la nivel naţional şi internaţional.		Fortificarea, eficientizarea colaborării în plan intern, regional, internaţional.

Referinţe:

1. Codul Penal al Republicii Moldova, nr. 985 din 18.04.2002. În: Monitorul Oficial al Republicii Moldova, 2009, nr. 72 – 74.
2. LUCA, IAMANDI. Cooperare internaţională în domeniul criminalităţii. Bucureşti: Editura. AIT Laboratories s.rl, 2011, p. 15-17.
3. Ştiri, [Accesat:24.11.2023]. Disponibil: https://www.youtube.com/live/M4NTaDdaxsc?si=QwLEAndhyfv2y86B
4. Echipadegardă. [Accesat:21.12.2023]. Disponibil: https://youtu.be/63a2rBxM4vI?si=OX_oQu1lBYQKbY_-